CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridad Industrial

Catálogo de buenas prácticas y controles de seguridad para entornos ICS/OT

Junio 2026

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

Edita: Xunta de Galicia

Agencia para la Modernización Tecnológica de Galicia (AMTEGA)

Lugar: Santiago de Compostela

Año: 2026

Índice

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
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.

--

El presente trabajo se integra en la línea de generación de conocimiento especializado orientado a **apoyar la mejora de la protección de las organizaciones industriales, de las infraestructuras críticas y de las administraciones públicas con entornos operativos y tecnológicos de carácter híbrido** (la gran mayoría), en los que conviven activos y procesos de **tecnología de la información (IT) y** de **tecnología de operación (OT)**.

La progresiva digitalización de la industria, la automatización de los procesos productivos, la creciente conectividad de los sistemas de control y supervisión y la incorporación de tecnologías como el **IoT industrial**, la analítica avanzada o la monitorización remota están transformando profundamente la realidad operativa de múltiples sectores. Esta evolución está aportando **ganancias de eficiencia, trazabilidad, flexibilidad y capacidad de gestión**, pero también amplía de manera significativa la **superficie de exposición frente a incidentes de ciberseguridad**. La **convergencia entre IT y OT**, lejos de ser una hipótesis de futuro, constituye ya una **realidad consolidada** en entornos como la energía, el agua, la automoción, la alimentación, la logística, el ámbito farmacéutico o los servicios públicos esenciales.

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

En este contexto, la protección de los entornos industriales exige un enfoque específico, **más allá de la simple traslación de controles tradicionales de seguridad de la información al ámbito operativo**. Los sistemas OT presentan **particularidades propias** que condicionan la selección y la implantación de medidas de seguridad: **largos ciclos de vida de los activos**, presencia de sistemas legados, restricciones de parada y mantenimiento, dependencia de fabricantes e integradores, requisitos estrictos de disponibilidad y continuidad, así como la necesidad de preservar en todo momento **la seguridad de las personas**, la **integridad del proceso y estabilidad de la operación**. Por este motivo, cualquier aproximación eficaz a la ciberseguridad industrial debe combinar criterios técnicos, organizativos y operativos, y hacerlo desde una perspectiva de **defensa en profundidad**, gestión del riesgo y compatibilidad con la realidad del negocio.

El objetivo de este informe es ofrecer un **catálogo estructurado de buenas prácticas y controles de seguridad lógica** que sirva como guía para su selección, priorización, implantación y mejora progresiva en entornos industriales. El documento recoge **controles de naturaleza organizativa, técnica y procedimental**, con un enfoque deliberadamente práctico y por motivos de espacio, sintetizado. No se limita a describir tecnologías aisladas, sino que trata de presentar las diferentes capacidades de protección como parte de un **conjunto coherente de medidas complementarias**, aplicables en función del **nivel de madurez**, del **perfil de riesgo**, del sector de actividad y de las características de la arquitectura tecnológica de cada organización.

La vocación del catálogo es, además, **integradora**. La realidad de la mayor parte de las empresas industriales no responde a una separación estanca entre el mundo corporativo y el operativo, sino a una convivencia continua entre sistemas de oficina, infraestructuras de comunicación, plataformas cloud, aplicaciones de gestión, sistemas MES, estaciones de ingeniería, HMI, redes industriales, activos de control y servicios remotos de mantenimiento. Por ello, este documento adopta una **visión combinada IT/OT**, en la que tienen cabida tanto controles claramente asociados a la protección de la red y de la operación industrial como otras capacidades que, siendo más habituales en el ámbito IT, resultan igualmente relevantes para **la seguridad global de la organización**.

De la misma manera, el informe concede una atención especial a las medidas **compensatorias**, especialmente necesarias en entornos en los que la remediación inmediata no siempre es viable. En numerosos escenarios industriales, la aplicación de un parche, la sustitución de un activo o la modificación de una configuración pueden no

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

ser posibles a corto plazo por razones operativas, contractuales, técnicas o de seguridad funcional. En estos casos, resulta imprescindible disponer **de un marco que permita reducir el riesgo** mediante segmentación, restricción de accesos, bastionado, monitorización reforzada, control de soportes externos, visibilidad de red o mecanismos de detección temprana, entre otras opciones.

En definitiva, este catálogo pretende constituir una **herramienta de apoyo a la revisión y a la implantación progresiva de capacidades de ciberseguridad industrial**, útil tanto para organizaciones que están iniciando su proceso de madurez como para aquellas que desean revisar, ampliar o reorganizar sus controles existentes. Su finalidad última es contribuir a una **protección más robusta, proporcionada y sostenible** de los entornos industriales gallegos, reforzando su **resiliencia frente a las amenazas actuales y futuras** y favoreciendo una **evolución segura de su transformación digital**.

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

2 Resumen ejecutivo

El presente documento constituye un **catálogo estructurado de buenas prácticas y controles de seguridad lógica** orientado a apoyar la **selección, priorización y posterior implantación de medidas de ciberseguridad** en entornos industriales reales en los que generalmente conviven sistemas y procesos de **tecnología de la información (IT)** y de **tecnología de operación (OT)**. Su finalidad es proporcionar una referencia práctica y ordenada que facilite la toma de decisiones, la definición de hojas de ruta de mejora y la adopción de un enfoque de protección más coherente, progresivo y adaptado a la realidad operativa de las organizaciones.

El catálogo está dirigido a un **abanico amplio de perfiles profesionales y organizativos**: empresas industriales, operadores de servicios esenciales, infraestructuras críticas, administraciones públicas con instalaciones técnicas o industriales, responsables de ciberseguridad, equipos de operación y mantenimiento, personal de ingeniería, responsables de continuidad y resiliencia, así como proveedores e integradores que participen en el diseño, operación o protección de estos entornos. Su valor principal reside en ofrecer una visión integrada que **no separa artificialmente los ámbitos IT y OT**, sino que los aborda como partes interdependientes de una misma realidad tecnológica y operativa.

El documento recoge controles distribuidos en **grandes bloques funcionales**, que abarcan desde la **consultoría, gobernanza y análisis**, **las auditorías técnicas** y **la identificación de debilidades**, hasta la **defensa perimetral y la segmentación**, **la detección de amenazas y protección activa**, **la monitorización, visibilidad y operación de seguridad**, la **protección del puesto, de los activos y de los soportes de operación**, **la identidad y el acceso seguro**, **la gestión de vulnerabilidades, la respuesta y recuperación**, así como capacidades ligadas al **DevSecOps** (operación y desarrollo seguro del software), al **software conectado** y a las **tendencias emergentes**. Esta estructura permite combinar controles organizativos, procedimentales y técnicos en un marco común de aplicación práctica.

Entre los mensajes principales que se desprenden del catálogo, destacaríamos las siguientes.

- **No existe un control único suficiente** para proteger de forma efectiva un entorno industrial. La seguridad se real construye a partir de la **combinación de medidas complementarias**, desplegadas de manera coherente y sostenidas

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

en el tiempo. En este sentido, la **defensa en profundidad** constituye un principio esencial: segmentar, limitar accesos, reforzar la visibilidad, detectar anomalías, bastionar sistemas, disponer de capacidad de respuesta y asegurar la recuperación son acciones que se refuerzan mutuamente y que deben entenderse como partes de un mismo sistema de protección.

- **La priorización de los controles debe basarse en el riesgo y en la viabilidad operativa**, y no únicamente en la disponibilidad de tecnología o en la severidad teórica de una amenaza. En entornos industriales, la criticidad del proceso, la dependencia de la continuidad de servicio, las restricciones de mantenimiento, la presencia de activos legados y la interacción entre seguridad lógica y seguridad funcional obligan a adoptar una visión pragmática, contextualizada y gradual. Por ello, el catálogo no debe interpretarse como un listado cerrado de obligaciones, sino como una herramienta para **ordenar prioridades y orientar decisiones de implantación realistas**.

- **Subrayar el papel central de las medidas compensatorias**, especialmente en el ámbito OT. En muchos entornos industriales, la aplicación inmediata de un parche, la sustitución de un equipo o la modificación de un sistema pueden no ser viables a corto plazo. En esos casos, resulta necesario reducir la exposición mediante otras medidas, como la **segmentación**, **la restricción de accesos**, **el hardening** o **bastionado**, la **monitorización reforzada**, la **visibilidad de red**, **el control de dispositivos externos** o **la detección temprana de anomalías**. La capacidad de articular este tipo de respuestas proporcionadas forma parte esencial de una estrategia madura de ciberseguridad industrial.

Finalmente, el documento destaca que la protección de los entornos industriales requiere incorporar también **capacidades tradicionalmente asociadas al ámbito IT**, siempre que resulten relevantes para la seguridad global de la organización. Elementos como la gestión de identidades, la protección del correo electrónico, la seguridad de aplicaciones, los servicios cloud, el desarrollo seguro o la gestión centralizada de eventos pueden desempeñar un papel decisivo en la reducción del riesgo cuando existen interdependencias reales entre entornos corporativos y operativos. El catálogo adopta así una visión **integradora, práctica y orientada a la resiliencia**, pensada para servir de apoyo tanto a organizaciones que comienzan a estructurar sus capacidades como a aquellas que buscan reforzar o reordenar los controles ya existentes.

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 presente catálogo fue elaborado a partir **de un enfoque de síntesis, estructuración y contextualización funcional de capacidades de ciberseguridad**, apoyado en el **conocimiento experto del mercado, de las buenas prácticas y de las soluciones disponibles** por parte de los consultores de seguridad de la información que participan en la elaboración de los contenidos técnicos del Observatorio, y complementado con fuentes especializadas de referencia en el ámbito de la ciberseguridad industrial.

Su propósito no es ofrecer una recopilación exhaustiva de soluciones disponibles en el mercado ni un inventario comercial de productos, sino construir una **guía técnico-funcional**, que permita identificar, contextualizar y relacionar las principales familias de controles y buenas prácticas relevantes para la protección de entornos industriales con componentes **IT** y **OT**.

Una de las decisiones metodológicas más importantes fue la de **organizar el catálogo por tipologías funcionales y no por fabricantes, marcas o soluciones comerciales concretas**. Aunque se ha tenido en cuenta un conjunto de capacidades existentes en el mercado para contrastar la pertinencia de algunos controles, el documento adopta deliberadamente una formulación neutral, centrada en categorías como firewall, NDR, EDR, SIEM, PAM, acceso remoto seguro, escáner de vulnerabilidades, honeypots, monitorización ciberfísica o copias de seguridad y restauración. Esta decisión refuerza el carácter técnico del informe, evita una lectura promocional o prescriptiva de tecnologías concretas y facilita que el catálogo pueda ser utilizado por organizaciones con distintos niveles de madurez, recursos y preferencias tecnológicas.

La metodología empleada ha incorporado también, de forma explícita, **el enfoque de medidas compensatorias**, especialmente relevante en entornos industriales en los que la remediación inmediata no siempre es viable. La selección y descripción de controles tuvo en cuenta que, en muchos escenarios, la reducción del riesgo no depende exclusivamente de la eliminación directa de una vulnerabilidad o de la sustitución de un activo, sino de la combinación de medidas complementarias como la segmentación, la restricción de accesos, el bastionado, la monitorización reforzada, la visibilidad de red, la detección temprana o el control de soportes externos.

En este sentido, el catálogo contempla y consolida un enfoque ya presente, de manera parcial o implícita, en otras publicaciones técnicas de la serie del Observatorio, especialmente en los informes de ciberalertas [1] [2] y de inteligencia de amenazas [3]

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

[4], en los que muchas de estas capacidades aparecen ya como recomendaciones, mecanismos de mitigación o ámbitos de mejora recurrentes.

Como base documental y técnica complementaria, se han empleado **estándares, marcos de buenas prácticas, guías técnicas y bibliografía especializada** en el ámbito de la seguridad de la información, de la ciberseguridad industrial y de la resiliencia ciberfísica. Con todo, este informe presenta deliberadamente un **peso relativamente mayor del conocimiento experto aplicado** y un uso más contenido de la bibliografía explícita que otros entregables de la serie, precisamente por su naturaleza de **catálogo técnico-funcional orientado a la práctica**.

Con el fin de ofrecer al lector una visión más amplia, el documento remite indirectamente a otras publicaciones de la serie del Observatorio que desarrollan con mayor profundidad cuestiones relacionadas con el catálogo de controles. Como decíamos, resulta especialmente recomendable la consulta de los informes ya publicados sobre **ciberalertas**, **inteligencia de amenazas, pero también tendencias y regulación** [5], que aportan contexto, ejemplos y desarrollo adicional para algunas de las tendencias emergentes recogidas.

Desde el punto de vista metodológico, es interesante señalar también algunas **limitaciones inherentes** al tipo de ejercicio realizado. En primer lugar, el tejido industrial presenta una notable **heterogeneidad sectorial**, lo que implica que no todos los controles tendrán la misma relevancia ni viabilidad en sectores como la energía, el agua, la alimentación, la automoción, la salud, la logística o la administración pública. En segundo lugar, existen **diferencias significativas de madurez organizativa y técnica** entre entidades, tanto en lo referente a su capacidad interna de seguridad como a la arquitectura y gobernanza de sus activos. En tercer lugar, la propia **diversidad de arquitecturas, tecnologías, protocolos, modelos de operación y relaciones con terceros** hace que la aplicabilidad concreta de cada control deba ser interpretada siempre en función del contexto.

Por lo tanto, **este catálogo no debe entenderse como una prescripción uniforme**, sino como una base estructurada para orientar análisis, decisiones y hojas de ruta adaptadas a la realidad de cada organización.

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

4 Marco conceptual y guía de uso del catálogo

4.1 Particularidades de la ciberseguridad en entornos industriales IT/OT

La ciberseguridad en entornos industriales requiere una aproximación diferenciada respecto de la que habitualmente se aplica en entornos corporativos convencionales. Aunque ambos ámbitos comparten principios generales de la seguridad de la información, como la necesidad de preservar **la confidencialidad**, la **integridad y la disponibilidad**, la realidad operativa de las organizaciones industriales introduce condicionantes específicos que afectan de manera directa a la selección, al diseño y a la implantación de los controles de seguridad. En consecuencia, la protección de estos entornos no puede basarse en una simple traslación de medidas propias del ámbito IT, sino en una adaptación consciente a las particularidades técnicas, operativas y organizativas de los sistemas industriales [6].

- Un primer elemento diferencial reside en la propia **finalidad de los sistemas implicados**. Mientras que en IT los activos adoptan estar orientados principalmente al tratamiento, almacenamiento e intercambio de información, en OT los sistemas tecnológicos interactúan de manera directa con el **proceso físico**, con la **operación industrial** y, en muchos casos, **con la seguridad de las personas y de las instalaciones**. Ello significa que un incidente de ciberseguridad no sólo puede traducirse en pérdida de información, indisponibilidad de servicios o impacto reputacional, sino también en alteraciones del proceso productivo, daños materiales, pérdida de calidad, afectación a la continuidad de la actividad o, en los casos más graves, consecuencias sobre la seguridad física.

- Derivado de lo anterior, **los criterios de prioridad también suelen diferir**. En los entornos industriales, **la disponibilidad**, **la continuidad de la operación y la estabilidad del proceso** tienden a tener un peso especialmente elevado. En determinados escenarios, la aplicación de una medida que en IT se consideraría habitual —como un parcheo inmediato, un reinicio programado, una actualización forzosa o la instalación de un agente de protección— puede resultar inviable o incluso contraproducente si compromete el funcionamiento normal de una línea, de un sistema de control o de un servicio esencial. Este

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

hecho obliga a valorar la seguridad en un equilibrio permanente entre la reducción del riesgo y la preservación de la operación.

- Otro factor distintivo es la presencia frecuente de **activos legados**, sistemas propietarios, protocolos industriales específicos y componentes con un ciclo de vida muy superior al habitual en el mundo IT. Muchos equipos industriales permanecen en servicio durante largos periodos, a las veces durante décadas, y pueden depender de versiones antiguas de software, firmware o sistemas operativos sin soporte actualizado. A ello se añade, en numerosas ocasiones, una fuerte dependencia de fabricantes, integradores o proveedores de mantenimiento, lo que condiciona tanto la capacidad de intervención técnica como los tiempos y márgenes de actuación ante una vulnerabilidad o incidente.
- A todo ello se suma la creciente **convergencia entre IT y OT**, que constituye una de las características más relevantes del panorama industrial actual. La incorporación de sistemas de supervisión remota, plataformas de analítica, soluciones MES, acceso remoto para soporte, integración con servicios cloud, intercambio de datos en tiempo real o conexión con sistemas corporativos de gestión hace que los límites tradicionales entre la red corporativa y la red operativa sean cada vez más porosos. Esta interdependencia genera oportunidades evidentes en términos de eficiencia y capacidad de control, pero también amplía la superficie de exposición y multiplica los puntos de contacto a través de los cuales puede producirse una intrusión, una propagación lateral o una afectación indirecta al proceso industrial.
- A diferencia de otros ámbitos, además **los entornos industriales exigen una coordinación más estrecha entre perfiles que tradicionalmente operaron con lógicas distintas**: responsables de sistemas, especialistas en ciberseguridad, personal de operación, equipos de mantenimiento, ingeniería de procesos, fabricantes, integradores y responsables de continuidad o de seguridad física. La madurez de la protección depende, en buena medida, de la capacidad de alinear a estos perfiles en torno a criterios comunes, procedimientos compatibles y prioridades compartidas. La ciberseguridad industrial no es, por tanto, un problema exclusivamente tecnológico, sino también **organizativo, procedimental y de coordinación interfuncional**.
- Por otro lado, hay que tener presente que **la implantación de controles en entornos industriales habitualmente está sujeta a restricciones prácticas significativas**: ventanas de mantenimiento limitadas, necesidad de

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

convalidación previa, riesgo de impacto no deseado sobre el proceso, requisitos de seguridad funcional, dependencia de terceros y limitaciones de capacidad interna. Estas restricciones explican por qué, en muchas ocasiones, la gestión del riesgo descansa en combinaciones graduales de medidas, y no en una remediación inmediata y completa. De esta forma, cobran especial relevancia mecanismos como la segmentación, el control de accesos, la visibilidad de red, el bastionado, la monitorización reforzada, la restricción de dispositivos externos o el uso de medidas compensatorias.

Particularidades de la ciberseguridad en entornos ICS/OT. Fuente: elaboración propia (2026)

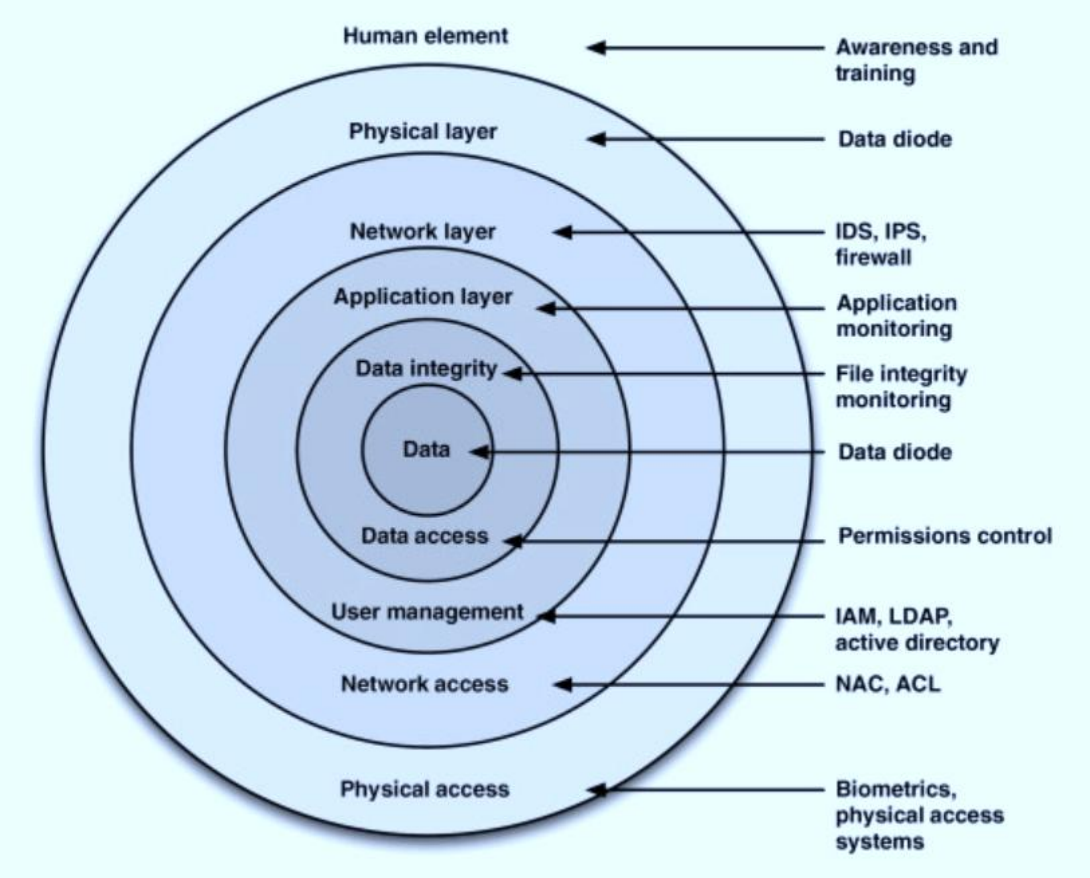
4.2 Principios generales de protección y defensa en profundidad

La protección eficaz de los entornos industriales IT/OT no puede descansar en un único mecanismo ni en una capa aislada de seguridad. La experiencia acumulada en el ámbito de la ciberseguridad industrial, tanto desde la perspectiva normativa como desde el

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

análisis de incidentes reales, muestra que la reducción del riesgo requiere combinar **controles organizativos, técnicos y operativos** de manera coordinada, graduada y sostenida en el tiempo. Esta aproximación se conoce habitualmente como **defensa en profundidad**, y constituye uno de los principios más asentados para la protección de sistemas industriales e infraestructuras críticas [7].

La defensa en profundidad parte de una idea sencilla: asumir que ninguna medida de seguridad es perfecta ni suficiente por sí misma. Un cortafuegos mal configurado, una credencial comprometida, una vulnerabilidad no parcheada, un equipo legado o un acceso remoto deficiente pueden abrir la puerta a una intrusión incluso en organizaciones que disponen de controles maduros en otros ámbitos. Por ello, la protección debe articularse en **capas complementarias**, de forma que la debilidad o la quiebra de una de ellas no implique automáticamente el compromiso del conjunto [8].



Defensa en profundidad. Fuente: Science Direct (n.d.)

Esta lógica es especialmente importante en entornos industriales, donde las consecuencias de un incidente pueden trascender el plano estrictamente digital y afectar a la **continuidad de la operación**, la **calidad del proceso**, a los **equipos físicos** o a la **seguridad de las personas**.

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

Aplicada al ámbito IT/OT, la defensa en profundidad se traduce en la combinación de medidas que actúan en distintos niveles: **el gobierno y la gestión del riesgo**, **la segmentación de la arquitectura**, **el control de identidades y accesos**, **la protección perimetral**, la **detección de amenazas**, la **visibilidad sobre los activos y las comunicaciones**, **el bastionado de sistemas**, la **gestión de vulnerabilidades**, **la respuesta ante incidentes y la capacidad de recuperación y continuidad**. El valor de esta aproximación no reside únicamente en sumar tecnologías, sino en **establecer relaciones lógicas entre capacidades**, de manera que cada control refuerce o complemente los demás.

Un primer principio general es la necesidad de **conocimiento suficiente del entorno a proteger**. No es posible defender adecuadamente aquello que no se conoce: activos no inventariados, comunicaciones no documentadas, accesos de terceros poco gobernados o dependencias tecnológicas mal comprendidas introducen puntos ciegos que debilitan cualquier estrategia defensiva. La visibilidad, por tanto, no es sólo una capacidad operativa, sino una condición previa para la gestión del riesgo, la segmentación, detección y la respuesta.

El segundo principio es el de **mínimo privilegio y control de acceso proporcional al riesgo**. En un entorno industrial, esto implica limitar los permisos al estrictamente necesario, separar funciones cuando proceda, controlar los accesos privilegiados, reforzar la autenticación y establecer mecanismos seguros para el acceso remoto y la intervención de terceros. La exposición innecesaria de cuentas, sesiones o canales de administración continúa siendo uno de los vectores más habituales de compromiso, especialmente en entornos interconectados y con dependencia de mantenimiento remoto.

El tercer principio **es la segmentación y segregación de las comunicaciones**. La separación entre dominios con diferentes necesidades de seguridad —por ejemplo, entre la red corporativa y la red OT, o entre diferentes zonas funcionales dentro del entorno operativo— constituye una medida esencial para limitar la propagación lateral, contener incidentes y reducir la exposición de los activos más sensibles. La segmentación, además, no debe entenderse sólo como una decisión de diseño de red, sino como una medida transversal que condiciona el acceso remoto, la monitorización, la gestión de vulnerabilidades y la respuesta ante incidentes.

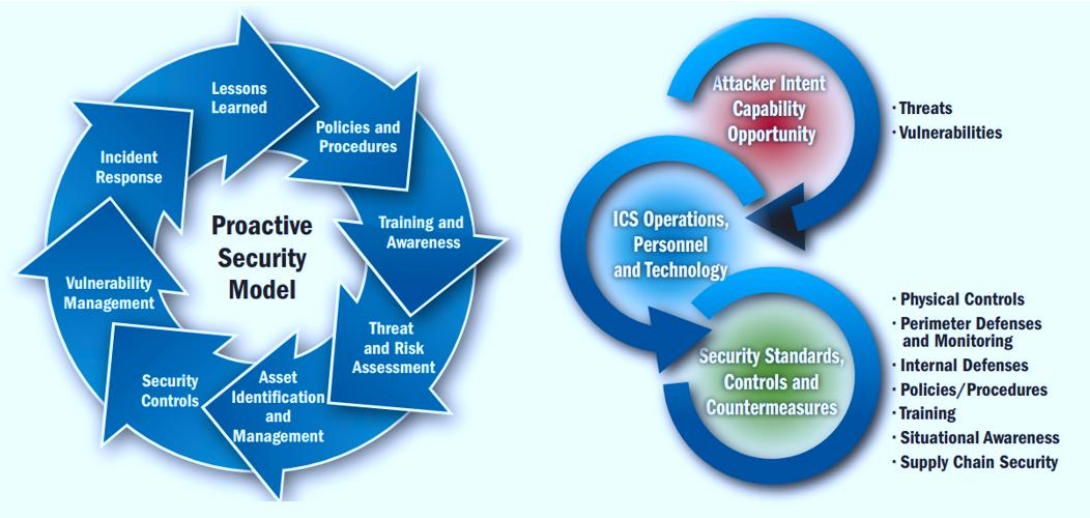
El cuarto principio es el de **seguridad adaptada a la operación**. Los controles deben ser compatibles con la realidad del proceso industrial y con las restricciones de mantenimiento, validación y continuidad. Ello significa que la implantación de medidas

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

debe priorizar soluciones proporcionadas, técnicamente viables y operativamente sostenibles. En muchos casos, la seguridad efectiva no depende de una remediación inmediata, sino de la combinación gradual de mecanismos como el bastionado, la monitorización reforzada, la restricción de servicios, la limitación de accesos o el despliegue de medidas compensatorias.

El quinto principio es la necesidad de incorporar **capacidades de detección y respuesta**, asumiendo que la prevención absoluta no existe. La protección moderna de entornos industriales requiere no sólo impedir accesos indebidos, sino también detectar comportamientos anómalos, correlacionar eventos, analizar desviaciones y actuar con rapidez para contener o mitigar un incidente. Esto refuerza el papel de capacidades como el SIEM, el SOC, el NDR, la monitorización ciberfísica, la visibilidad de activos y la respuesta planificada.

El sexto principio es **la resiliencia**, entendida no sólo como recuperación tras un incidente, sino como capacidad de la organización para anticipar, resistir, absorber, responder y restaurar la operación en condiciones aceptables. En un entorno industrial, esta visión es particularmente relevante, ya que la protección no se termina en la prevención ni en la detección, sino que debe incluir copias de seguridad, restauración probada, continuidad operativa, procedimientos de crisis y coordinación entre áreas técnicas y funcionales. La resiliencia constituye, así, la expresión más completa de la defensa en profundidad aplicada a sistemas con impacto físico y operativo.



Modelo de seguridad proactiva y diseño de defensa en profundidad. Fuente: CISA (2016)

Estos fundamentos permiten comprender que la seguridad industrial no debe formularse como una acumulación desordenada de productos o medidas aisladas, sino como una **arquitectura coherente de controles**, alineada con el riesgo, con el nivel de

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

exposición, con la criticidad del proceso y con la madurez de la organización. Este enfoque es el que da sentido al catálogo que se desarrolla en este informe: no como un simple listado de soluciones posibles, sino como una estructura ordenada para apoyar decisiones informadas, graduales y sostenibles en el tiempo.

4.3 Medidas compensatorias en entornos industriales

Uno de los trazos más característicos de la ciberseguridad en entornos industriales es la necesidad frecuente de recurrir a **medidas compensatorias** como parte de la gestión del riesgo. La diferencia de lo que sucede en muchos entornos corporativos, en los que la remediación técnica suele asociarse a actualizaciones rápidas, sustitución de componentes o cambios de configuración relativamente asumibles, en el ámbito IT/OT existen múltiples situaciones en las que la eliminación inmediata de una vulnerabilidad o la implantación del control ideal no es viable en el corto plazo. Esta realidad no implica aceptar pasivamente la exposición, sino adoptar un enfoque pragmático en el que la reducción del riesgo se apoya en combinaciones alternativas de controles, procedimientos y restricciones operativas.

Las medidas compensatorias pueden definirse como **controles alternativos o complementarios** que permiten disminuir la probabilidad de explotación o reducir el impacto de un incidente cuando la medida correctiva directa no puede aplicarse de forma inmediata o completa. En el contexto industrial, esto puede responder a motivos muy diversos: dependencia de fabricantes, ausencia de parches estables, riesgo de impacto sobre el proceso, ventanas de mantenimiento muy limitadas, requisitos de seguridad funcional, validación previa obligatoria, incompatibilidades con sistemas legados o limitaciones de capacidad técnica y organizativa. En todos estos casos, la lógica de protección debe orientarse a **compensar la exposición existente** en tanto no sea posible abordar una remediación definitiva.

La relevancia de estas medidas se incrementa en entornos en los que **la disponibilidad**, **continuidad operativa y la estabilidad del proceso** constituyen prioridades irrenunciables. En una planta industrial, en una infraestructura crítica o en un servicio esencial, la aplicación de un parche sin validación, la sustitución de un activo sensible o la modificación de un sistema de control pueden introducir riesgos superiores a los que se pretenden mitigar. Por ello, la gestión prudente de la ciberseguridad industrial requiere aceptar que, en determinados momentos, la opción más razonable no es actuar de manera inmediata sobre el componente vulnerable, sino reforzar su entorno, limitar su exposición y aumentar la capacidad de detección y respuesta.

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

Entre las medidas en ocasiones consideradas compensatorias más habituales empleadas en entornos industriales pueden incluirse, de manera aislada o combinada, la **segmentación de red**, la creación de una **DMZ industrial o de un borde IT/OT controlado**, el **parcheo virtual** o el uso de mecanismos de filtrado en capa de aplicación, la **monitorización pasiva y detección de anomalías**, el **logging inmutable** o registro inviolable, el **control de acceso robusto y la separación de funciones**, **el acceso remoto seguro para mantenimiento**, las estrategias compensatorias de gestión de parches**, las copias de seguridad y recuperación** orientadas a OT**,** el **bastionado de HMI y sistemas de ingeniería, la gestión de la cadena de suministro y del firmware**, el refuerzo de la **resiliencia y de la seguridad funcional**, así como los **procedimientos operativos y de formación del personal** [9] [10]. Su eficacia, con todo, no depende de cada medida por separado, sino de la capacidad de combinarlas según la criticidad del activo, la naturaleza del riesgo, la arquitectura existente y el nivel de madurez de la organización.

Es importante subrayar que **las medidas compensatorias no deben entenderse como soluciones improvisadas ni como sustitutos permanentes por defecto** de las medidas correctivas estructurales. Su valor reside en formar parte de un proceso ordenado de gestión del riesgo, en el que la exposición se identifica, se evalúa, se prioriza y se trata mediante mecanismos proporcionados al contexto. Ello requiere documentar las decisiones adoptadas, definir responsabilidades, establecer plazos de revisión y mantener una visión clara del **riesgo residual** que continúa asumiendo la organización.

Otro aspecto clave es que **las medidas compensatorias** adoptan tener un fuerte componente **arquitectónico y operativo**, además de tecnológico. Su eficacia depende tanto de la existencia de ciertos controles como de la forma en que se implantan y gobiernan. Por ejemplo, la segmentación sólo cumple adecuadamente su función se va acompañada de reglas coherentes, control de accesos, supervisión de tráfico y revisión periódica. Del mismo modo, la limitación del acceso remoto requiere autenticación reforzada, control de sesiones, trazabilidad y gobernanza de terceros. Y la monitorización intensificada sólo aporta valor si existen capacidades reales de análisis, correlación y respuesta. Esto refuerza la idea de que compensar no es simplemente añadir un producto, sino **reorganizar la protección alrededor de un riesgo concreto**.

Desde una perspectiva metodológica, la implantación de medidas compensatorias debería responder, al menos, a cuatro preguntas básicas: **qué riesgo se pretende mitigar**, **por qué la remediación directa no es viable en ese momento**, **qué combinación de medidas permite reducir razonablemente la exposición y cuándo**

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

se revisará la necesidad de mantener o sustituir esa compensación cuando el control es temporal o mejorable. Esta formulación es especialmente útil en entornos industriales con gran dependencia de terceros y con activos heterogéneos, ya que obliga a hacer explícita la racionalidad técnica y operativa de la decisión.

La práctica muestra, además, que muchas organizaciones industriales mejoran sustancialmente su postura de seguridad no tanto por aplicar de forma inmediata grandes transformaciones, sino por introducir **mejoras compensatorias bien priorizadas y sostenibles**: separar redes, endurecer configuraciones, limitar canales remotos, controlar soportes externos, reforzar la detección o mejorar la trazabilidad. Estas medidas, aunque a veces percibidas como menos ambiciosas que otras iniciativas, son con frecuencia las que permiten reducir más rápidamente la superficie de exposición real y crear condiciones más seguras para futuras actuaciones de mayor alcance.

En este sentido, **las medidas compensatorias guardan una relación directa con la madurez de la organización**. No sólo constituyen una respuesta a limitaciones inmediatas, sino también un mecanismo para transitar desde escenarios de baja visibilidad o alta exposición hacia estados de control progresivamente más robustos. Un programa de seguridad industrial maduro no elimina la necesidad de compensar; al contrario, la integran como parte de un modelo racional de decisión, priorización y resiliencia.

4.4 Cómo utilizar este catálogo

El presente catálogo ha sido concebido como una **herramienta práctica de referencia**, y no como una relación cerrada, lineal o uniforme de medidas de obligada implantación. Su utilidad reside precisamente en permitir que cada organización pueda interpretar los controles desde su realidad específica, teniendo en cuenta la criticidad de sus procesos, el grado de exposición, la arquitectura tecnológica existente, las restricciones operativas, el nivel de madurez alcanzado y la disponibilidad real de recursos técnicos, humanos y económicos.

En este sentido, el catálogo debe emplearse con una lógica de **selección contextualizada e implantación progresiva**. No todos los controles serán igualmente necesarios, viables o prioritarios en todos los entornos. Una planta industrial con alto nivel de automatización, múltiples accesos remotos de terceros y dependencia intensiva de sistemas OT tendrá necesidades distintas a las de una organización con menor complejidad operativa o con un mayor peso del entorno corporativo. Del mismo modo,

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

una entidad que ya disponga de visibilidad de red, procedimientos maduros y capacidades internas de respuesta podrá orientar el catálogo hacia capas más avanzadas, mientras que otras organizaciones deberán comenzar por medidas más básicas, pero de alto impacto en la reducción del riesgo.

Un primer modo de utilizar el catálogo consiste en emplearlo como **guía de diagnóstico o autoevaluación**. En este caso, los diferentes bloques y sub-bloques permiten revisar de forma estructurada qué capacidades están presentes, cuáles existen sólo parcialmente y cuáles no están todavía desarrolladas. Esta lectura resulta especialmente útil para organizaciones que necesitan identificar carencias, ordenar capacidades o establecer una secuencia de mejora. El catálogo puede servir así como referencia para análisis GAP, revisiones internas, ejercicios de madurez, propuestas técnicas o esquemas de priorización.

Un segundo uso posible es como **instrumento de planificación y estructuración de medidas**. Los controles recogidos no deben interpretarse de forma aislada, sino como componentes de un sistema de protección más amplio. Por ello, durante su utilización conviene analizar no solo si una capacidad existe o no, sino también cómo se relaciona con el resto. Por ejemplo, la segmentación de red gana eficacia cuando va acompañada de control de accesos, visibilidad de comunicaciones y procedimientos de mantenimiento seguro; la monitorización reforzada pierde parte de su valor si no existen capacidades reales de análisis y respuesta; y la gestión de vulnerabilidades resulta insuficiente si no se integra con criterios de criticidad operativa, convalidación previa y medidas compensatorias. El catálogo, por tanto, debe leerse también como una **estructura de relaciones entre controles**, no sólo como un listado temático.

Un tercer enfoque de uso es el de la **lectura basada en riesgo**. El catálogo permite identificar que medidas ofrecen una mayor reducción de la exposición en función de los escenarios más probables o más gravosos para la organización. En entornos industriales, esta lectura es especialmente relevante, ya que la presión por implantar medidas de seguridad debe convivir con la necesidad de mantener la operación, respetar restricciones de mantenimiento y evitar impactos no deseados sobre el proceso. Por ello, la aplicación del catálogo debería estar siempre vinculada al análisis de riesgos, a la criticidad de los activos y evaluación del impacto potencial sobre la continuidad, la seguridad física, la calidad o el servicio.

También puede emplearse como **marco común entre perfiles distintos**, algo especialmente relevante en entornos industriales. Uno de los problemas habituales en la implantación de controles es que los diferentes equipos —ciberseguridad, sistemas,

operación, mantenimiento, ingeniería, dirección o proveedores— no siempre comparten el mismo lenguaje ni la misma percepción de las prioridades. La estructura del catálogo puede facilitar una visión común, permitiendo analizar medidas no desde una perspectiva puramente tecnológica, sino en términos de finalidad, dependencia, impacto y viabilidad. En ese sentido, el documento puede cumplir también una función de apoyo a la gobernanza y a la coordinación interfuncional.

Además, el catálogo puede utilizarse como **soporte para la elaboración de hojas de ruta graduales**, algo particularmente útil en organizaciones con un punto de partida heterogéneo. La madurez en ciberseguridad industrial no suele construirse mediante transformaciones abruptas, sino a través de iteraciones sucesivas en las que se consolidan capacidades, se revisan decisiones previas y se introducen mejoras de mayor profundidad una vez fortalecida la base. La lectura del catálogo desde esta óptica permite distinguir entre medidas iniciales, mejoras intermedias y capacidades más avanzadas, sin perder de vista que la prioridad no debe ser la sofisticación del control, sino su contribución real a la protección del entorno.

Es importante insistir en que este documento **no sustituye un análisis de riesgo específico**, ni resuelve por sí mismo la adecuación concreta de cada control a una arquitectura determinada. El catálogo proporciona una base ordenada de referencia, pero su aplicabilidad debe interpretarse siempre a la luz del contexto de la organización, del sector, de las obligaciones reguladoras que resulten de aplicación, de la arquitectura disponible, de las dependencias de terceros y del nivel de exposición asumido. Su valor está en **ordenar y contextualizar los controles**, no en sustituir el análisis específico.

Finalmente, se recomienda que **la utilización del catálogo siga una secuencia lógica**. En primer lugar, resulta conveniente comprender **las particularidades de los entornos industriales IT/OT** y los **principios generales de protección y defensa en profundidad** expuestos en los apartados anteriores. En segundo lugar, debe revisarse el papel de las **medidas compensatorias**, ya que éstas condicionan una parte importante de la implantación real en entornos industriales. Solo después resulta plenamente útil abordar el bloque central del catálogo, en el que cada familia de controles puede interpretarse de manera más precisa. De esta forma, el documento funciona no sólo como repositorio de capacidades, sino como una guía estructurada para apoyar análisis más informados, coherentes y sostenibles en el tiempo.

En definitiva, este catálogo debe ser leído como un **instrumento de referencia flexible y acumulativo**, útil para diagnosticar, priorizar, estructurar, coordinar y mejorar la postura de seguridad de las organizaciones industriales. Su eficacia dependerá, en

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

último término, de la capacidad de cada entidad para emplearlo con criterio, adaptándolo a su contexto e integrándolo en una visión más amplia de riesgo, operación y resiliencia.

4.5 Criterios de clasificación de los controles

La utilidad de un catálogo como el presente depende, en buena medida, de su capacidad para **ordenar los controles de manera comprensible, coherente y funcional**. En un documento que reúne más de setenta medidas diferentes de naturaleza diversa —organizativas, técnicas, operativas y procedimentales— la clasificación no cumple un papel meramente formal, sino que condiciona la forma en que el lector interpreta el contenido, identifica relaciones entre capacidades y localiza más fácilmente los elementos relevantes para su contexto. Por este motivo, el catálogo se estructura siguiendo criterios de clasificación que combinan una lógica funcional con las particularidades propias de los entornos industriales IT/OT.

El primer criterio empleado es el de la **familia funcional del control**. Esto significa que los controles no se agrupan según tecnologías aisladas, fabricantes concretos o marcos normativos específicos, sino según la función principal que desempeñan dentro de la protección global de la organización. Así, el catálogo distingue entre bloques ligados a la gobernanza y al análisis, a las auditorías técnicas e identificación de debilidades, a la ingeniería social, a la defensa perimetral y segmentación, la detección de amenazas, la monitorización y operación de seguridad, la protección de puestos y activos, a la identidad y acceso seguro, la gestión de vulnerabilidades, a la respuesta y recuperación, al desarrollo seguro y a las tendencias emergentes. Esta estructura permite leer el documento como un **mapa de capacidades**, en el que cada bloque representa un ámbito de protección con una finalidad específica.

El segundo criterio es el de la **naturaleza del control**, ya que no todos los mecanismos de seguridad tienen la misma expresión ni el mismo modo de implantación. Algunos controles son eminentemente **organizativos**, como el análisis de riesgos, la definición de procedimientos o la continuidad de negocio; otros son principalmente **técnicos**, como el firewall, el NDR, el PAM o el SIEM; y otros presentan una naturaleza **mixta**, al combinar tecnología, procedimiento y operación, como ocurre con la gestión de accesos de terceros, la monitorización, la gestión de parches o la respuesta ante incidentes. Esta distinción resulta útil para evitar una visión reducionista de la ciberseguridad industrial, entendida sólo como adquisición de herramientas, y para poner en valor el peso que

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

tienen la gobernanza, los procedimientos y la coordinación en la eficacia real de los controles.

El tercer criterio de clasificación es el de la **función defensiva predominante**. Desde esta perspectiva, los controles pueden cumplir un papel principalmente:

- **preventivo**, cuando buscan reducir la probabilidad de compromiso;
- **detectivo**, cuando permiten identificar anomalías, eventos o incidentes;
- **correctivo o de recuperación**, cuando facilitan contener, restaurar o retornar a condiciones aceptables de operación;
- **compensatorio**, cuando se emplean para mitigar un riesgo ante la imposibilidad de implantar de forma inmediata la medida correctiva ideal.

En la práctica, muchos controles pueden participar en más de una de estas funciones. Por ejemplo, la segmentación es claramente preventiva, pero también contribuye a la contención de un incidente; la monitorización reforzada es detectiva, pero puede cumplir un papel compensatorio; y el bastionado es preventivo, aunque también puede utilizarse para reducir exposición en contextos con vulnerabilidades no remediadas. El criterio adoptado en el catálogo no pretende encuadrar de forma rígida cada control en una única categoría, sino destacar su **función principal dentro del conjunto**.

El cuarto criterio es el de **la función del control dentro del NIST Cybersecurity Framework (NIST CSF)**, uno de los marcos más utilizados internacionalmente para estructurar programas de ciberseguridad de forma comprensible y transversal [11] [12]. Esta norma organiza la protección alrededor de **seis funciones principales**, que permiten describir que papel cumple cada capacidad dentro de un sistema más amplio.

- La función **Govern** se relaciona con la gestión de la ciberseguridad, incluyendo políticas, roles, supervisión, gestión de riesgo y cadena de suministro.
- La función **Identify** se traslada en el conocimiento del entorno, de los activos, de las dependencias y de los riesgos existentes.
- La función **Protect** abarca las medidas destinadas a limitar o reducir la probabilidad de impacto, como el control de acceso, la formación, el bastionado o la protección de datos.
- La función **Detect** recoge las capacidades orientadas a identificar eventos, anomalías o señales de compromiso.
- La función **Respond** incluye la gestión del incidente una vez detectado, desde el análisis hasta la contención y la comunicación.

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

- Finalmente, la función **Recover** alude a la restauración de servicios y capacidades, a la continuidad y al aprendizaje posterior al incidente.

Function	Category
Govern (GV)	Organizational Context
	Risk Management Strategy
	Roles, Responsibilities, and Authorities
	Policy
	Oversight
	Cybersecurity Supply Chain Risk Management
Identify (ID)	Asset Management
	Risk Assessment
	Improvement
Protect (PR)	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience
Detect (DE)	Continuous Monitoring
	Adverse Event Analysis
Respond (RS)	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	Incident Mitigation
Recover (RC)	Incident Recovery Plan Execution
	Incident Recovery Communication

Funciones NIST CSF y relación con categorías. Fuente: NIST (2024)

Emplear este criterio complementa los anteriores, porque permite **situar cada control dentro de una lógica de ciclo completo de la ciberseguridad,** y no sólo dentro de una categoría técnica u organizativa.

Es destacable también que los criterios de clasificación adoptados **no son excluyentes entre sí**. Un mismo control puede localizarse en un bloque determinado por su familia funcional, tener una naturaleza técnica o mixta, cumplir una función defensiva predominantemente preventiva o detectiva, y encajar además en una o varias de las funciones del NIST CSF. Esta superficie no debe entenderse como un defecto del modelo, sino como una expresión de la propia complejidad de la ciberseguridad industrial. De hecho, una de las finalidades del catálogo es precisamente hacer visible que los controles no existen de forma aislada ni pueden comprenderse adecuadamente desde una única dimensión.

En consecuencia, la clasificación contemplada en este informe responde a un equilibrio entre **claridad expositiva** y **fidelidad a la realidad operativa**. No se busca construir una taxonomía académica exhaustiva, ni replicar literalmente la estructura de un estándar concreto, sino ofrecer un marco de lectura suficientemente robusto para organizar el catálogo y, al tiempo, suficientemente flexible como para ser útil a organizaciones con perfiles, sectores y arquitecturas muy diferentes.

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

5 Catálogo de buenas prácticas y controles

5.1 Consultoría, gobernanza y análisis

Este primer bloque reúne **capacidades de carácter organizativo, estratégico y técnico-funcional que permiten establecer las bases de una ciberseguridad industrial madura**. Incluye actividades orientadas a comprender el riesgo, definir prioridades, alinear decisiones con el negocio y estructurar programas de protección adaptados a la realidad operativa de los entornos ICS/OT, sirviendo así como punto de partida para una implantación coherente del resto de controles.

5.1.1 Análisis de riesgos tecnológicos

Categoría: Consultoría, gobernanza y análisis

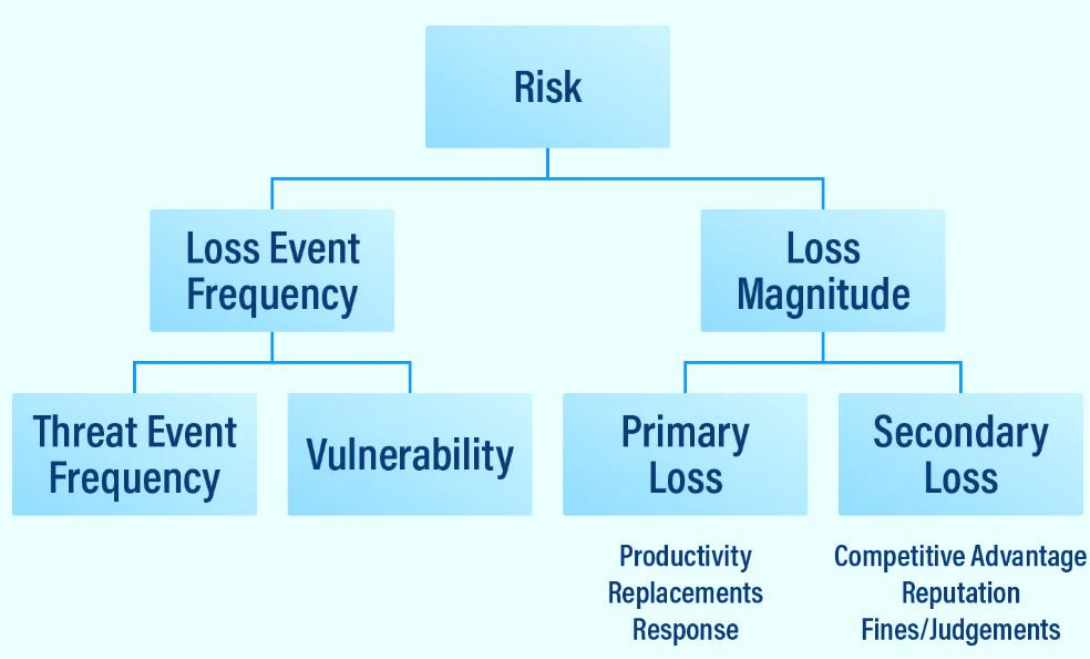
Tipología: Organizativa / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Govern, Identify

Descripción: El análisis de riesgos tecnológicos es el proceso sistemático mediante el cual una organización identifica, evalua y trata los riesgos derivados de las amenazas que pueden afectar a sus activos, procesos, servicios y dependencias tecnológicas. En el contexto industrial, este análisis debe considerar tanto los componentes propios de la infraestructura corporativa como los elementos operativos y de control que intervienen en la producción, supervisión, mantenimiento y continuidad del proceso. Su valor reside en proporcionar una visión estructurada de la exposición real de la organización, permitiendo relacionar activos, amenazas, vulnerabilidades, impactos y medidas de tratamiento en un marco coherente [13] [14].

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



Análisis de riesgos cuantitativo. Fuente: FAIR Institute (n.d.)

Objetivo: Establecer una base formal para comprender qué riesgos afectan a la organización, que activos son más críticos, que escenarios de amenaza resultan más relevantes y qué medidas de protección, mitigación o compensación deben implantarse. El análisis de riesgos no persigue sólo cuantificar exposición, sino también facilitar una visión priorizada y contextualizada de la seguridad, alineada con la operativa del negocio y con la criticidad de los procesos industriales.

Cómo funciona / cómo se implanta: Su implantación suele comenzar con la definición del alcance, la identificación de los activos y procesos incluidos, la caracterización de las amenazas y vulnerabilidades relevantes y la estimación del impacto y de la probabilidad de materialización de los distintos escenarios. A partir de esa base, se estaban criterios de aceptación del riesgo, se priorizan tratamientos (evitar, mitigar, transferir o aceptar los riesgos) y se documentan las medidas previstas. En entornos industriales, este ejercicio debe incorporar no sólo activos digitales clásicos, sino también sistemas de control, redes OT, componentes de campo, dependencias de terceros, accesos remotos, seguridad funcional, continuidad operativa y posibles efectos físicos, productivos o reputacionales. El proceso puede apoyarse en marcos como ISO 27005, NIST SP 800-30, MAGERIT, IEC 62443 o metodologías adaptadas al sector.

Ventajas:

- Permite priorizar los esfuerzos de seguridad en función de la criticidad real de los activos y procesos.

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

- Facilita la selección proporcionada de controles técnicos, organizativos y procedimentales.
- Ayuda a justificar inversiones, excepciones y medidas compensatorias.
- Mejora la trazabilidad entre amenazas, exposición, impacto y tratamiento previsto.
- Sirve de base para auditorías, planes directores, continuidad y gobernanza de la seguridad.

Limitaciones y consideraciones:

- Su utilidad depende de la calidad del inventario de activos y del conocimiento real de la arquitectura.
- Puede perder valor si se formula como ejercicio puramente documental y no como proceso vivo.
- En entornos industriales, una evaluación insuficientemente adaptada puede infravalorar impactos operativos, físicos o de seguridad funcional.
- Requiere participación de perfiles diversos: sistemas, ciberseguridad, operación, mantenimiento, ingeniería y responsables de proceso.
- Debe revisarse periódicamente, especialmente tras cambios de arquitectura, incorporación de terceros, nuevas interconexiones o aparición de amenazas relevantes.

Relación con otros controles: Se relaciona de forma directa con la recomendación de controles de seguridad, la implantación de marcos normativos, la segmentación de red, la gestión de vulnerabilidades, el acceso remoto seguro, el patch management, las medidas compensatorias, la respuesta ante incidentes y los planes de continuidad. Constituye, en términos prácticos, un control vertebrador del resto del catálogo, ya que permite contextualizar y priorizar su implantación.

Casos habituales de uso: Se emplea para elaborar planes directores de seguridad, definir hojas de ruta de mejora, preparar auditorías o certificaciones, justificar excepciones en entornos OT, priorizar activos críticos, revisar dependencias de terceros, orientar medidas compensatorias o evaluar el impacto de cambios tecnológicos y normativos.

Observaciones / medidas compensatorias asociadas: En un entorno industrial, el análisis de riesgos tecnológicos resulta especialmente relevante para fundamentar la

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

aplicación de medidas compensatorias cuando un control no puede implantarse de forma inmediata. También es el mecanismo más adecuado para justificar por qué determinados activos legados, accesos remotos, sistemas sin soporte o arquitecturas heredadas deben tratarse con un enfoque gradual y proporcional, en lugar de mediante remediaciones inmediatas potencialmente incompatibles con la operación.

5.1.2 Recomendación de controles de seguridad

Categoría: Consultoría, gobernanza y análisis

Tipología: Organizativa / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Govern, Protect

Descripción: La recomendación de controles de seguridad consiste en la definición estructurada de las medidas técnicas, organizativas y procedimentales que resultan más adecuadas para reducir los riesgos identificados en una organización. No se trata de una simple enumeración de soluciones posibles, sino de un ejercicio de contextualización en el que los controles se seleccionan en función de la arquitectura existente, de la criticidad de los activos, de las amenazas relevantes, de las obligaciones normativas aplicables y de las limitaciones operativas del entorno. En el ámbito industrial, esta actividad requiere traducir los aportes procedentes del análisis de riesgos, de las auditorías o de las revisiones técnicas a un conjunto coherente de actuaciones priorizadas y compatibles con la realidad IT/OT. Podría realizarse el ejercicio inspirado en este catálogo, o en las propuestas de CISA Cybersecurity Performance Goals [15] o ISO 27002 (más generalistas en este caso [16]).

Objetivo: Determinar qué controles deben implantarse, reforzarse, combinarse o revisarse para mejorar la postura de seguridad de la organización de forma proporcionada, realista y sostenible. Su propósito es conectar el análisis con la acción, evitando tanto la implantación indiscriminada de medidas como la dependencia de recomendaciones genéricas poco adaptadas al contexto industrial.

Cómo funciona / cómo se implanta: Habitualmente, la recomendación de controles parte de un conjunto previo de entradas: análisis de riesgos, resultados de auditoría, evaluaciones técnicas, revisión de arquitectura, requisitos regulatorios o incidentes observados. A partir de esa base, se establece una propuesta de medidas que puede incluir controles preventivos, detectivos, correctivos y compensatorios, ordenados según criterios de criticidad, viabilidad y relación con el resto de la arquitectura de

seguridad. En entornos industriales, esta recomendación debe considerar aspectos como la segmentación IT/OT, el acceso remoto de terceros, la presencia de activos legados, la necesidad de validaciones previas, el impacto potencial sobre la operación, la seguridad funcional y la dependencia de fabricantes o integradores. El resultado suele materializarse en informes técnicos, planes de acción, hojas de ruta o propuestas de mejora.

Ventajas:

- Traducir inputs técnicos o de riesgo a actuaciones concretas y ordenadas.
- Evitar enfoques genéricos o poco adaptados al contexto real de la organización.
- Facilitar la priorización de medidas según impacto y viabilidad.
- Mejorar la coherencia entre controles, arquitectura, procedimientos y operación.
- Servir de base para planes directores, auditorías, inversiones y revisiones de seguridad.

Limitaciones y consideraciones:

- Pierde valor si se formula como listado estándar de medidas sin contexto ni priorización.
- Requiere conocimiento suficiente del entorno, de las dependencias operativas y de las restricciones de implantación.
- En entornos industriales, una recomendación técnicamente correcta puede resultar inviable si no se considera el impacto sobre la disponibilidad y el proceso.
- Debe evitar una visión excesivamente centrada en herramientas, incorporando también medidas organizativas, procedimentales y compensatorias.
- Conviene revisar las recomendaciones cuando cambian la arquitectura, el marco normativo, la exposición o el modelo de operación.

Relación con otros controles: Se relaciona directamente con el análisis de riesgos tecnológicos, la implantación y auditoría de marcos y normas de seguridad, las auditorías técnicas, la gestión de vulnerabilidades, la segmentación, el acceso remoto seguro, el hardening, la monitorización, la respuesta ante incidentes y los planes de continuidad. Funciona como puente entre el diagnóstico y la estructuración del resto de controles del catálogo.

Casos habituales de uso: Se utiliza para elaborar planes de mejora, propuestas técnicas, hojas de ruta de implantación, adecuaciones a marcos como ENS, ISO 27001, IEC 62443 o NIST CSF, revisiones de arquitectura, procesos de compra o contratación, y para definir medidas compensatorias cuando un control no puede implantarse de forma inmediata.

Observaciones / medidas compensatorias asociadas: En un entorno industrial, la recomendación de controles resulta especialmente útil cuando debe equilibrarse la reducción del riesgo con la preservación de la operación. Por ello, no debería formularse únicamente en términos de control ideal, sino también contemplando secuencias graduales de implantación, dependencias entre medidas y alternativas compensatorias cuando existan restricciones técnicas, operativas o de seguridad funcional.

5.1.3 Implantación y auditoría de marcos y normas de seguridad

Categoría: Consultoría, gobernanza y análisis

Tipología: Organizativa / mixta

Función defensiva predominante: Preventiva

Función en el NIST CSF: Govern

Descripción: La implantación y auditoría de marcos y normas de seguridad consiste en la adopción estructurada de referencias reconocidas para organizar, evaluar y mejorar la ciberseguridad de una organización. Estos marcos pueden tener naturaleza general, como ISO 27001, ENS o NIST CSF [11], o una orientación más específica a entornos industriales, como IEC 62443 o NIST SP 800-82. Su utilidad reside en proporcionar un lenguaje común, un conjunto de requisitos o buenas prácticas y una metodología de revisión que permita pasar de una gestión ad hoc de la seguridad a un modelo más ordenado, trazable y verificable.

Objetivo: Dotar a la organización de un marco de referencia coherente para estructurar sus controles, revisar su grado de adecuación, identificar desviaciones, establecer prioridades de mejora y demostrar un determinado nivel de madurez, cumplimiento o capacidad de gestión de la seguridad. En el ámbito industrial, esto resulta especialmente útil para alinear a la ciberseguridad con el riesgo operativo, con la gobernanza interna y con las exigencias regulatorias y sectoriales aplicables.

Cómo funciona / cómo se implanta: La implantación suele comenzar con la selección del marco o combinación de marcos más adecuados al contexto de la organización, en función del sector, de la arquitectura, el alcance y de las obligaciones de cumplimiento.

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

A partir de ese punto, se partir de un ejercicio de análisis GAP o de evaluación inicial, en el que se compara la situación real con los requisitos o principios del marco escogido. Sobre esa base, se establecen medidas de adecuación, documentos de gobernanza, procedimientos, evidencias y controles técnicos u organizativos. La auditoría, por su parte, verifica el grado de cumplimiento o adecuación mediante revisión documental, entrevistas, análisis técnico y comprobación de evidencias. En entornos industriales, la implantación no debería limitarse a trasladar requisitos IT de forma mecánica, sino a adaptarlos a la realidad OT, la seguridad funcional, la disponibilidad, los sistemas legados, la segmentación, el acceso remoto y a las necesidades de coordinación entre operación y seguridad.

Ventajas:

- Proporciona una estructura ordenada y reconocible para la gestión de la seguridad.
- Facilita la identificación de carencias y la planificación de mejoras.
- Ayuda a alinear la organización con requisitos normativos, contractuales o sectoriales.
- Mejora la trazabilidad documental y la capacidad de auditoría.
- Permite integrar gobernanza, riesgo, operación y control técnico en un mismo marco de referencia.

Limitaciones y consideraciones:

- Su implantación pierde valor si se orienta sólo al cumplimiento formal y no a la eficacia real de los controles.
- No todos los marcos tienen el mismo nivel de adecuación a entornos industriales, por lo que su selección debe ser contextualizada.
- En OT, una interpretación demasiado literal de ciertos requisitos puede resultar poco viable o incluso contraproducente si no se adapta al proceso.
- Requiere participación de múltiples áreas: seguridad, sistemas, operación, ingeniería, continuidad, cumplimiento y dirección.
- La auditoría debe valorar no sólo la existencia documental de un control, sino también su aplicación efectiva y sostenibilidad.

Relación con otros controles: Se relaciona directamente con el análisis de riesgos tecnológicos, la recomendación de controles de seguridad, las auditorías técnicas, la

gestión de vulnerabilidades, la segmentación, la respuesta ante incidentes, los planes de continuidad y las medidas compensatorias. Funciona como marco vertebrador para ordenar y dar consistencia al resto de los controles del catálogo.

Casos habituales de uso: Se utiliza para procesos de adecuación al ENS, implantación de SGSI basados en ISO 27001, revisiones frente a NIST CSF, programas sectoriales de seguridad, marcos OT como IEC 62443, procesos de certificación, auditorías internas o externas, licitaciones, requerimientos de clientes e iniciativas de mejora continua con alcance corporativo e industrial.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la implantación de marcos y normas de seguridad resulta especialmente valiosa cuando se emplea con un criterio de aplicabilidad y adaptación al riesgo, y no como ejercicio de cumplimiento abstracto. En este sentido, marcos como el ENS, IEC 62443 o NIST CSF pueden servir también para fundamentar excepciones justificadas y la utilización de medidas compensatorias, siempre que exista trazabilidad, evaluación del riesgo residual, validación y revisión periódica.

5.1.4 Plan de continuidad de negocio y resiliencia operativa

Categoría: Consultoría, gobernanza y análisis

Tipología: Organizativa / mixta

Función defensiva predominante: Correctiva / de recuperación

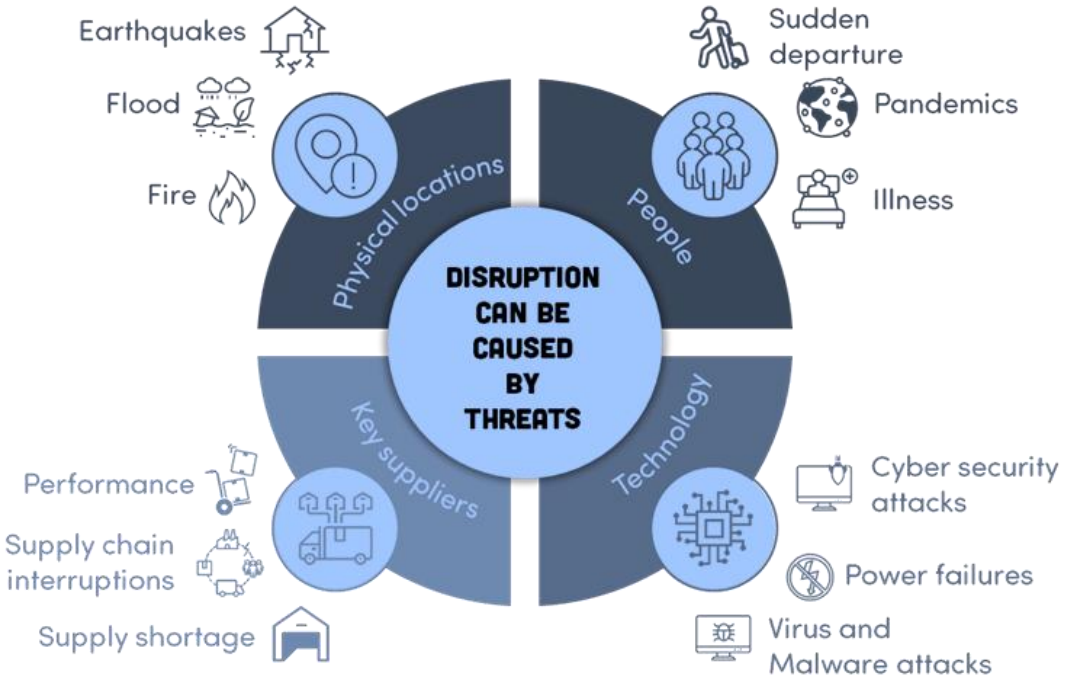
Función en el NIST CSF: Govern, Recover

Descripción: El plan de continuidad de negocio y resiliencia operativa es el conjunto estructurado de políticas, procedimientos, roles y medidas técnicas y organizativas destinadas a garantizar que la organización pueda mantener, restablecer o adaptar sus funciones críticas ante incidentes disruptivos que afecten a su actividad [17] [18]. En el contexto industrial, este control abarca no sólo la continuidad de los servicios corporativos, sino también la preservación de la operación, la recuperación de los procesos productivos, la restauración de sistemas OT y la coordinación entre áreas técnicas, operativas y directivas. Su finalidad va más allá de la mera recuperación tras un fallo, integrando también la capacidad de absorción, adaptación y respuesta frente a interrupciones con impacto operativo (ya sean de naturaleza humana, por causas naturales o técnicas).

Objetivo:

Minimizar el impacto de incidentes, fallos, ataques o interrupciones sobre los procesos

esenciales de la organización, asegurando que existan criterios previos para priorizar servicios, restaurar capacidades, coordinar actuaciones y mantener la continuidad en condiciones aceptables. En entornos industriales, el objetivo incluye también reducir el riesgo de paradas prolongadas, preservar la seguridad de las personas y del proceso, y asegurar que la recuperación no comprometa la integridad de los sistemas ni introduzca nuevos riesgos operativos.



Ejemplo de causas de disrupción en industria. Fuente: DigitalTransformation.org (n.d.)

Cómo funciona / cómo se implanta: Su implantación parte de la identificación de las funciones críticas de negocio y de los procesos operativos esenciales, así como de las dependencias que los soportan: sistemas, redes, personal clave, proveedores, instalaciones, energía, comunicaciones, servicios externos y componentes OT. Sobre esa base se establecen escenarios de interrupción, tiempos objetivo de recuperación, prioridades, puntos de restauración de datos y servicios y procedimientos específicos para distintos tipos de incidente. En un entorno industrial, el plan debe contemplar la recuperación de sistemas de supervisión y control, HMI, estaciones de ingeniería, comunicaciones industriales, recetas, configuraciones, copias de seguridad, acceso remoto, relación con terceros e interacción con la seguridad funcional. Su eficacia depende también de la realización de pruebas, simulacros, revisiones periódicas y actualizaciones tras cambios significativos en la arquitectura o en la operación.

Ventajas:

- Reduce el tiempo y el impacto de las interrupciones sobre la actividad.

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

- Mejora la preparación de la organización ante incidentes operativos y ciberincidentes.
- Facilita la coordinación entre áreas técnicas, operación, mantenimiento, dirección y terceros.
- Ayuda a priorizar la recuperación en función de la criticidad real de los procesos y servicios.
- Refuerza la resiliencia organizativa y la capacidad de recuperación sostenible en el tiempo.

Limitaciones y consideraciones:

- Pierde valor si se formula como documento estático sin pruebas, actualización ni integración con la realidad operativa.
- Su eficacia depende de la calidad del inventario de activos críticos y de la identificación de dependencias.
- En entornos industriales, una visión excesivamente centrada en TI puede dejar fuera componentes esenciales de la recuperación en OT.
- Requiere coordinación real con operación, mantenimiento, ingeniería, proveedores y, cuando proceda, responsables de seguridad funcional.
- Debe mantener coherencia con los planes de respuesta ante incidentes, con las copias y restauración y con los procedimientos de crisis.

Relación con otros controles: Se relaciona directamente con el análisis de riesgos tecnológicos, la recomendación de controles de seguridad, la implantación de marcos y normas, la respuesta ante incidentes, los servicios forenses, las copias de seguridad y restauración, la gestión de vulnerabilidades, la segmentación y las medidas compensatorias. Constituye una capa esencial para dar continuidad práctica al resto de los controles cuando la prevención no resulta suficiente.

Casos habituales de uso: Se emplea para preparar escenarios de recuperación frente a ransomware, fallo de sistemas críticos por múltiples causas, pérdida de comunicaciones industriales, indisponibilidad de personal clave, problemas en cadena de suministro, interrupciones prolongadas de servicios tecnológicos, ataques con impacto físico o degradación de procesos productivos y servicios esenciales.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la continuidad y la resiliencia operativa no deben limitarse a la restauración técnica de un

sistema, sino contemplar la vuelta segura a la operación, la verificación del estado del proceso, la disponibilidad de configuraciones válidas, la coordinación con los responsables de operación y la revisión de las condiciones de seguridad antes de la reanudación completa. También resulta especialmente relevante para justificar medidas compensatorias temporales cuando la recuperación definitiva de un activo o proceso no puede ejecutarse de inmediato.

5.1.5 Evaluaciones técnicas y revisión de arquitectura

Categoría: Consultoría, gobernanza y análisis

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Identify

Descripción: Las evaluaciones técnicas y la revisión de arquitectura consisten en el análisis estructurado de los componentes tecnológicos, de las comunicaciones, de las interdependencias y del diseño general de un entorno para identificar debilidades, exposiciones innecesarias, errores de segmentación, puntos únicos de fallo y carencias de protección. En el ámbito industrial, este control abarca tanto la arquitectura corporativa relacionada con los servicios de apoyo a la operación como la infraestructura OT propiamente dicha, incluyendo redes, accesos remotos, sistemas de supervisión, estaciones de ingeniería, HMI, integraciones con terceros, activos legados e interconexiones entre dominios IT y OT.

Objetivo: Comprobar si la arquitectura tecnológica existente responde a criterios adecuados de seguridad, resiliencia y compatibilidad operativa, detectando diseños inseguros, exposiciones evitables y relaciones de dependencia que puedan incrementar el riesgo. Su finalidad es proporcionar una visión técnica y estructural del entorno, permitiendo corregir debilidades de diseño antes de que se deriven en incidentes, auditorías desfavorables, degradación de la operación o dificultades de recuperación.

Cómo funciona / cómo se implanta: Su ejecución suele partir de la recopilación de información sobre la arquitectura existente: diagramas de red, inventarios de activos, flujos de comunicación, políticas de acceso, integraciones con terceros, procedimientos operativos y configuraciones relevantes. Sobre esa base, se revisan aspectos como la separación entre dominios, la existencia y coherencia de la segmentación, los accesos administrativos y remotos, la exposición de servicios, los mecanismos de autenticación, la protección de activos críticos, la resiliencia de comunicaciones, la dependencia de

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

sistemas sin soporte y la trazabilidad de las comunicaciones. En entornos industriales, este ejercicio debe tener en cuenta también la seguridad funcional, la disponibilidad, la latencia, la compatibilidad con los protocolos industriales, los requisitos de mantenimiento y el impacto potencial sobre el proceso. El resultado se materializa en informes de situación, propuestas de mejora arquitectónica, planes de adecuación o recomendaciones específicas de refuerzo.

Ventajas:

- Permite detectar debilidades estructurales antes de que se materialicen en incidentes.
- Mejora la coherencia entre seguridad, arquitectura y operación.
- Facilita la revisión de segmentación, accesos, exposiciones y dependencias críticas.
- Ayuda a justificar cambios de diseño, refuerzos de protección y medidas compensatorias.
- Sirve de base para auditorías, adecuación normativa y hojas de ruta de mejora.

Limitaciones y consideraciones:

- Su calidad depende de la disponibilidad y fiabilidad de la documentación técnica existente.
- Puede ofrecer una visión incompleta si no se incorpora conocimiento operativo y de proceso.
- En entornos industriales, una revisión exclusivamente orientada a IT puede ignorar restricciones críticas de OT.
- Requiere participación coordinada de sistemas, ciberseguridad, operación, mantenimiento e ingeniería.
- Debe actualizarse cuando se producen cambios relevantes de arquitectura, nuevas interconexiones, incorporación de terceros o evolución de procesos.

Relación con otros controles: Se relaciona de manera directa con el análisis de riesgos tecnológicos, la recomendación de controles de seguridad, la segmentación de red y separación IT/OT, la DMZ industrial, el acceso remoto seguro, la visibilidad de activos y comunicaciones OT, la gestión de vulnerabilidades, el bastionado y las medidas compensatorias. Actúa como soporte técnico para muchos de los controles posteriores del catálogo.

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

Casos habituales de uso: Se emplea en proyectos de revisión de arquitectura IT/OT, procesos de adecuación a IEC 62443 o ENS, implantación de segmentación, incorporación de acceso remoto de terceros, migraciones tecnológicas, revisión de redes industriales, análisis previos a auditorías, integración de nuevos sistemas o evaluación de exposición de activos críticos y legados.

Observaciones / medidas compensatorias asociadas: En un entorno industrial, la revisión de arquitectura es especialmente útil para identificar medidas compensatorias de carácter estructural, como la reorganización de zonas y conductos (IEC 62443), la limitación de flujos innecesarios, el refuerzo de controles de acceso, el despliegue de DMZ industriales, la mejora de la visibilidad o la reducción de la exposición de activos que no pueden ser actualizados o sustituidos a corto plazo.

5.1.6 Análisis de vulnerabilidades hardware

Categoría: Consultoría, gobernanza y análisis

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Identify

Descripción: El análisis de vulnerabilidades hardware consiste en la identificación, evaluación y contextualización de debilidades que afectan a componentes físicos, dispositivos embebidos, firmware, electrónica de control, interfaces de comunicación y otros elementos materiales que forman parte de la infraestructura tecnológica de una organización. En el ámbito industrial, este control resulta especialmente relevante porque buena parte de la exposición no se concentra sólo en software convencional, sino también en PLC, RTU, sensores, gateways, equipos de red industrial, HMI, dispositivos IIoT, controladores y componentes propietarios cuya superficie de riesgo puede estar vinculada al diseño físico, al firmware, a la configuración de bajo nivel o a la cadena de suministro.

Objetivo: Detectar debilidades de seguridad en componentes hardware o firmware que puedan comprometer la integridad, la disponibilidad o la fiabilidad de un sistema, y establecer medidas de mitigación, compensación o control que reduzcan la exposición real de la organización. Su propósito es ampliar el análisis clásico de vulnerabilidades software hacia elementos físicos y embebidos que, en entornos industriales, pueden tener un impacto directo sobre la operación y el proceso.

Cómo funciona / cómo se implanta:

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

Su implantación parte habitualmente de la identificación de los activos físicos más relevantes y de la recopilación de información técnica sobre modelos, versiones, firmware, interfaces disponibles, funciones críticas y relaciones de dependencia. A partir de esa base, pueden revisarse advisories de fabricantes, boletines de seguridad (véase [1] [2]), bases de datos de vulnerabilidades, documentación técnica, configuraciones de bajo nivel y, cuando resulta viable, realizar pruebas específicas de análisis o validación sobre laboratorio, banco de pruebas o entornos controlados. En entornos industriales, este ejercicio debe ejecutarse con especial prudencia, ya que determinados métodos de análisis intensivo pueden no ser compatibles con la operación en producción. Por ello, acostumbra a combinar revisión documental, correlación con inteligencia de vulnerabilidades, contraste con fabricantes o integradores y, cuando procede, ensayos controlados sobre componentes equivalentes o entornos aislados.

Ventajas:

- Permite identificar riesgos que no serían visibles en un análisis centrado solo en software.
- Ayuda a comprender mejor la exposición real de dispositivos embebidos y componentes propietarios.
- Facilita la priorización de medidas compensatorias en activos que no pueden ser parcheados fácilmente.
- Refuerza la visión sobre firmware, interfaces físicos y cadena de suministro.
- Resulta especialmente útil en entornos con elevada dependencia de activos industriales legados o específicos.

Limitaciones y consideraciones:

- La disponibilidad de información técnica o de advisories detallados puede ser limitada en ciertos dispositivos industriales.
- Muchos equipos propietarios dificultan el análisis directo o la validación independiente.
- En entornos de producción, algunas pruebas pueden resultar inviables por el riesgo de impacto en la operación.
- Requiere conocimiento especializado sobre firmware, electrónica, protocolos industriales y arquitectura de dispositivo.

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

- Su eficacia mejora cuando se integra con gestión de activos, inteligencia de amenazas, revisión de arquitectura y gestión de vulnerabilidades.

Relación con otros controles: Se relaciona con el análisis de riesgos tecnológicos, con la gestión de vulnerabilidades en software clásico (ver sección siguiente), el hardening de HMI y sistemas de ingeniería, la gestión de la cadena de suministro y del firmware, la segmentación, la monitorización de activos OT, las medidas compensatorias y las estrategias de parcheo o sustitución gradual.

Casos habituales de uso: Se emplea en la revisión de PLC, RTU, equipos IIoT, sensores, Gateways industriales, dispositivos de comunicación, HMI, firmware de equipos de planta, componentes de fabricantes específicos, sistemas con ciclos de vida largos o entornos en los que se detectan advisories recurrentes asociados a dispositivos físicos críticos.

Observaciones / medidas compensatorias asociadas: En entornos industriales, es frecuente que las vulnerabilidades hardware o firmware no puedan ser tratadas mediante actualización inmediata. Por ello, este control suele desembocar en la adopción de medidas compensatorias como segmentación reforzada, aislamiento de activos, limitación de servicios expuestos, control estricto de accesos, monitorización específica, gestión de la cadena de suministro o sustitución planificada a medio plazo. Su utilidad es especialmente alta cuando se emplea para fundamentar decisiones de contención y priorización sobre activos críticos con soporte limitado.

5.1.7 CyberRange y entornos de prueba

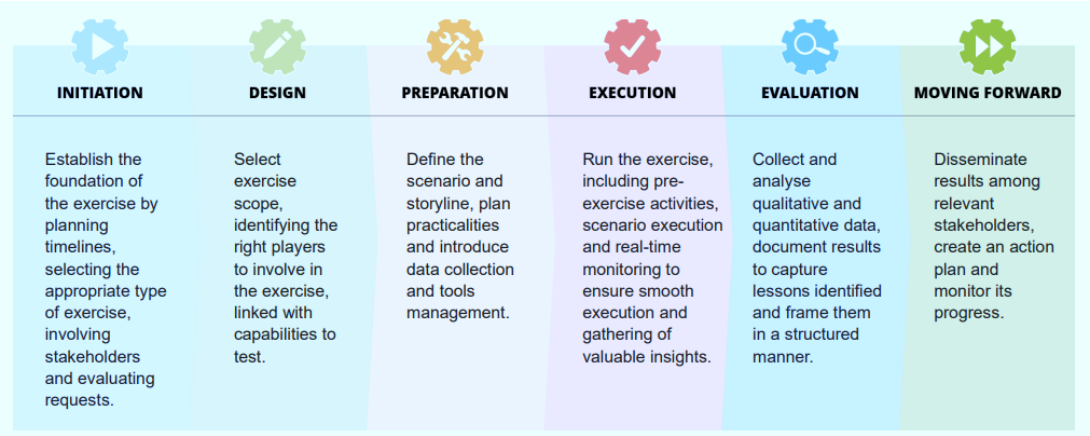
Categoría: Consultoría, gobernanza y análisis

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: Los CyberRange y entornos de prueba son infraestructuras controladas diseñadas para reproducir, con mayor o menor fidelidad, componentes tecnológicos, procesos, comunicaciones y escenarios de seguridad con el fin de convalidar controles, ensayar procedimientos, formar personal y analizar el comportamiento de sistemas y amenazas sin afectar a la operación real, utilizando escenarios de propuestas como la de ENISA [19].



Metodología propuesta para la ejecución de ciberejercicios. Fuente: ENISA (2026)

En el ámbito industrial, estos entornos pueden incluir simulación de redes IT/OT, representación de activos industriales, estaciones de ingeniería, HMI, PLC, protocolos específicos, accesos remotos, flujos de datos y casos de uso de respuesta ante incidentes. Su valor principal reside en proporcionar un espacio seguro para probar, aprender y mejorar sin introducir riesgo directo sobre producción o servicios esenciales.

Objetivo: Disponer de un entorno controlado en el que sea posible verificar medidas de seguridad, comprobar cambios técnicos, ensayar escenarios de incidente, adiestrar equipos y reducir la incertidumbre asociada a la implantación de controles o a la respuesta frente a eventos reales. En entornos industriales, el objetivo incluye también mejorar la preparación operativa, validar la compatibilidad de medidas con el proceso y reducir el riesgo de impacto sobre sistemas en producción.

Cómo funciona / cómo se implanta: Su implantación puede adoptar diferentes formatos, desde laboratorios sencillos con activos representativos hasta plataformas avanzadas de simulación y adiestramiento que recrean arquitecturas industriales completas o parciales. El diseño del entorno de prueba debe partir de los objetivos perseguidos: validación de configuraciones, ensayo de segmentación, pruebas de acceso remoto, formación técnica, simulación de incidentes, adiestramiento de respuesta, revisión de actualizaciones o comprobación de medidas compensatorias. En entornos industriales, resulta especialmente útil reproducir activos críticos, flujos de comunicación, dependencias entre sistemas e interacciones con el proceso, aun cuando esa representación no sea idéntica al entorno real. Algunas plataformas permiten hibridar elementos virtuales y físicos. Su eficacia aumenta cuando se integra con procedimientos de prueba, criterios de aceptación, registro de resultados y lecciones aprendidas.

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

Ventajas:

- Permite validar cambios y controles sin afectar directamente a la operación.
- Reduce el riesgo asociado a la implantación de medidas en producción.
- Mejora la formación práctica de perfiles técnicos, operativos y de seguridad.
- Facilita ejercicios de simulación, respuesta y coordinación entre equipos.
- Resulta útil para probar medidas compensatorias, actualizaciones, configuraciones y escenarios de incidente.

Limitaciones y consideraciones:

- Su representatividad depende del grado de semejanza con el entorno real.
- Puede requerir inversión relevante en diseño, mantenimiento y actualización de componentes.
- No siempre es viable replicar con exactitud sistemas propietarios, activos legados o condiciones reales de proceso.
- Debe evitarse asumir que una prueba satisfactoria en laboratorio elimina por completo el riesgo en producción.
- Su valor disminuye si no se integra con procedimientos, objetivos claros y revisión de los resultados obtenidos.

Relación con otros controles: Se relación con el análisis de riesgos tecnológicos, la recomendación de controles de seguridad, la revisión de arquitectura, el patch management, el bastionado, el acceso remoto seguro, la monitorización, la respuesta ante incidentes, las copias y restauración y las medidas compensatorias. Funciona como soporte transversal para validar o simular buena parte de los controles do catálogo.

Casos habituales de uso: Se emplea para validar segmentación y flujos de red, probar actualizaciones o cambios de configuración, ensayar accesos remotos, adiestrar equipos SOC/CSIRT, simular escenarios de ransomware o indisponibilidad, comprobar procedimientos de recuperación, evaluar herramientas de detección y formar personal de operación, mantenimiento y ciberseguridad en contextos industriales realistas.

Observaciones / medidas compensatorias asociadas: En entornos industriales, los CyberRange y entornos de prueba son especialmente valiosos cuando la implantación directa de un cambio en producción implica incertidumbre elevada. En ese sentido, permiten validar previamente medidas compensatorias, secuencias de recuperación, procedimientos de respuesta o controles nuevos antes de su despliegue real. También

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

resultan útiles para mejorar la coordinación interfuncional y para reducir la dependencia de decisiones tomadas exclusivamente sobre supuestos teóricos, además de fines formativos.

5.2 Auditorías técnicas e identificación de debilidades

La mejora de la seguridad requiere conocer con suficiente precisión que debilidades existen realmente en el entorno y cómo pueden ser explotadas. Esta subsección contempla **servicios y capacidades orientados a evaluar técnicamente la exposición, validar hipótesis de riesgo e identificar vulnerabilidades, errores de configuración, superficies de ataque y carencias de protección** en infraestructuras, redes, dispositivos y componentes industriales.

5.2.1 Análisis de vulnerabilidades

Categoría: Auditorías técnicas e identificación de debilidades

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Identify

Descripción: El análisis de vulnerabilidades consiste en el proceso sistemático de identificación, clasificación y contextualización de debilidades técnicas presentes en sistemas, aplicaciones, servicios, dispositivos y componentes de red que puedan ser explotados por un atacante o derivar en fallos de seguridad [20]. Su propósito no se limita a detectar vulnerabilidades conocidas, sino también a comprender su relevancia dentro del entorno real de la organización, teniendo en cuenta la exposición del activo, su criticidad, las dependencias operativas y la posibilidad efectiva de explotación. En entornos industriales, este control abarca tanto activos IT como OT, aunque su ejecución requiere cautelas específicas cuando afecta a sistemas de control, supervisión u operación.

Proceso de gestión de vulnerabilidades. Fuente: DataCypher (2025)

Objetivo: Identificar debilidades técnicas que puedan comprometer la confidencialidad, integridad, disponibilidad o resiliencia de un entorno, proporcionando una base ordenada para priorizar medidas de mitigación, bastionado, segmentación, parcheo o compensación. En el ámbito industrial, su objetivo incluye también reducir la exposición de activos críticos sin introducir riesgos innecesarios para la continuidad de la operación ni para la seguridad funcional.

Cómo funciona / cómo se implanta: Su implantación suele partir de la identificación del alcance, del inventario de activos y de la selección de la metodología de análisis más adecuado según la naturaleza del entorno. El proceso puede combinar revisión de configuraciones, contraste con bases de datos de vulnerabilidades, correlación con advisories de fabricantes, identificación de software y firmware instalados y, cuando resulta viable, uso de herramientas de análisis automatizado. En entornos IT, estas revisiones pueden ser más intrusivas y frecuentes; en entornos OT, por el contrario, deben adaptarse al riesgo operativo, priorizando técnicas pasivas, revisión documental, coordinación con fabricantes o ensayos en entornos controlados cuando el análisis activo pueda afectar a la estabilidad del sistema. El resultado suele expresarse mediante informes que relacionan cada vulnerabilidad con el activo afectado, su nivel de exposición, el impacto potencial y las posibles vías de tratamiento.

Ventajas:

- Permite detectar debilidades técnicas antes de que se materialicen en incidentes.

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

- Facilita la priorización de actuaciones sobre la base de la exposición real de los activos.
- Ayuda a orientar medidas de mitigación, parcheo, hardening o compensación.
- Mejora la visibilidad técnica sobre sistemas, versiones, configuraciones y componentes afectados.
- Sirve de apoyo a auditorías, revisiones de arquitectura y programas de gestión de vulnerabilidades.

Limitaciones y consideraciones:

- La simple detección de una vulnerabilidad no determina por sí sola la prioridad real de tratamiento.
- En entornos industriales, un análisis agresivo o mal planificado puede generar impacto en la operación.
- Los resultados pueden ser incompletos si no existe un inventario de activos adecuado o si hay poca visibilidad sobre componentes legados.
- Se requiere interpretación contextual: no todas las vulnerabilidades tienen la misma relevancia ni la misma explotabilidad en el entorno real.
- Debe combinarse con criterios de criticidad, exposición, arquitectura y continuidad, y no leerse como un listado aislado de CVES.

Relación con otros controles: Se relaciona con el análisis de riesgos tecnológicos, la revisión de arquitectura, la propia gestión de vulnerabilidades, el patch management, el hardening, la segmentación, la monitorización, las medidas compensatorias y la inteligencia de amenazas. Constituye un control técnico de entrada para buena parte de las actuaciones posteriores de mitigación y refuerzo.

Casos habituales de uso: Se emplea en auditorías técnicas, revisiones periódicas de exposición, adecuación a marcos normativos, análisis previos a cambios de arquitectura, revisión de activos críticos, entornos con accesos remotos, sistemas expuestos a advisories de fabricante o escenarios en los que se necesita priorizar la mitigación de debilidades conocidas.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el análisis de vulnerabilidades no debe entenderse automáticamente como paso previo a un parcheo inmediato. En muchos casos, su utilidad principal reside en permitir la contextualización del riesgo y la adopción de medidas de priorización o compensatorias

como segmentación, limitación de accesos, monitorización reforzada, hardening o reducción de la exposición, especialmente cuando existen activos legados, sistemas propietarios o restricciones de mantenimiento (más detalle de este contexto en [2]).

5.2.2 Pentesting y pruebas de seguridad controladas

Categoría: Auditorías técnicas e identificación de debilidades

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Identify

Descripción: El test de intrusión y las pruebas de seguridad controladas consisten en la simulación planificada de acciones de ataque sobre sistemas, aplicaciones, redes o servicios con el fin de comprobar si determinadas debilidades pueden ser explotadas y con qué consecuencias. A diferencia del análisis de vulnerabilidades, que se centra principalmente en la identificación de fallos conocidos o configuraciones débiles, estas pruebas buscan verificar la explotabilidad real, el encadenamiento de debilidades, la eficacia de los controles existentes y el impacto potencial de un compromiso. En entornos industriales, este tipo de ejercicios requiere un nivel de prudencia y planificación superior al habitual, dado que determinadas interacciones pueden afectar a la estabilidad de la operación, a la comunicación entre sistemas o, en algunos casos, a la seguridad funcional. Pueden emplearse diversas metodologías, como OSSTMM adaptadas [21].

Objetivo: Comprobar de forma controlada si un sistema o entorno puede ser efectivamente comprometido a partir de debilidades existentes, obteniendo evidencias prácticas sobre exposición, movimiento lateral, escalada de privilegios, eficacia de los controles e impacto potencial. En el ámbito industrial, su propósito es aportar visibilidad realista sobre la superficie de ataque sin comprometer la disponibilidad ni introducir riesgos desproporcionados para el proceso.

Cómo funciona / cómo se implanta: Su implantación requiere definir con precisión el alcance, los activos afectados, las limitaciones operativas, las reglas del ejercicio, los horarios, los mecanismos de parada segura y los criterios de éxito. En entornos convencionales, las pruebas pueden incluir explotación de vulnerabilidades, movimiento lateral, comprobación de credenciales, análisis de servicios expuestos o revisión de aplicaciones. En entornos industriales, por el contrario, suele ser necesario limitar técnicas intrusivas en producción, priorizar ensayos sobre laboratorios,

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

entornos replicados, sistemas representativos o activos no críticos, y contar con la validación previa de operación, mantenimiento y responsables técnicos. En algunos casos, el valor de la prueba reside más en la simulación controlada de escenarios y en el contraste de hipótesis de explotación que en una acción agresiva directa sobre sistemas de planta.

Ventajas:

- Aporta evidencias prácticas sobre la explotabilidad real de determinadas debilidades.
- Permite validar la eficacia de controles preventivos, detectivos y de contención.
- Ayuda a identificar cadenas de ataque que no son visibles en una revisión puramente documental.
- Mejora la comprensión de la exposición real del entorno y de las posibles vías de compromiso.
- Puede apoyar la revisión de arquitectura, segmentación, acceso remoto y respuesta ante incidentes.

Limitaciones y consideraciones:

- En entornos industriales, una prueba mal diseñada puede afectar a la disponibilidad, a la estabilidad del proceso o a la seguridad funcional.
- No todas las técnicas habituales de pentesting son aceptables sobre activos OT en producción.
- Requiere conocimiento técnico especializado y coordinación estrecha con operación, mantenimiento e ingeniería.
- Los resultados son dependientes del alcance definido: una prueba limitada no representa necesariamente toda la exposición real.
- Debe ejecutarse con autorización formal, reglas claras y procedimientos de contención o reversión cuando proceda.

Relación con otros controles: Se relaciona con el análisis de vulnerabilidades, la revisión de arquitectura, la segmentación de red, el acceso remoto seguro, la monitorización y detección, la respuesta ante incidentes, el hardening y con los entornos de prueba o CyberRange. Funciona como mecanismo de validación práctica de otros controles e hipótesis de riesgo.

Casos habituales de uso: Se emplea en la revisión de perímetros expuestos, validación de segmentación, comprobación de accesos remotos, ensayo de escenarios de movimiento lateral, revisión de aplicaciones o servicios concretos, auditorías previas la puesta en producción, evaluación de entornos replicados y ejercicios controlados de verificación técnica en arquitectura IT/OT.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el test de intrusión debe formularse siempre desde un criterio de proporcionalidad, alcance limitado y control estricto del riesgo. En muchos casos, el ejercicio más recomendable no será una explotación plena en producción, sino pruebas parciales, simulaciones, validación en laboratorio o revisión técnica reforzada. También puede ser útil para comprobar la robustez de medidas compensatorias ya implantadas, como segmentación, restricción de accesos, limitación de servicios o mecanismos de detección.

5.2.3 Auditorías de infraestructura

Categoría: Auditorías técnicas e identificación de debilidades

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Identify

Descripción: Las auditorías de infraestructura consisten en la revisión técnica y estructurada de los componentes que soportan la operación tecnológica de una organización, incluyendo redes, servidores, sistemas, servicios, dispositivos de comunicación, activos de seguridad y elementos de interconexión entre dominios. Su propósito es evaluar si la infraestructura presenta una configuración adecuada, si responde a criterios mínimos de seguridad y resiliencia y si existen debilidades de diseño, exposiciones innecesarias o dependencias críticas insuficientemente controladas. En entornos industriales, este tipo de auditoría abarca tanto la infraestructura corporativa vinculada a la operación como los componentes de red y comunicación que dan soporte a los sistemas OT, a las estaciones de ingeniería, a los HMI, a las comunicaciones remotas y a las integraciones con terceros. Pueden emplearse diferentes metodologías como OSSTMM [21].

Objetivo: Verificar el estado real de la infraestructura tecnológica desde el punto de vista de la seguridad, identificando configuraciones incorrectas, exposiciones evitables, carencias de protección, problemas de segmentación, dependencias no documentadas o

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

puntos únicos de fallo que puedan incrementar el riesgo de la organización. En el ámbito industrial, el objetivo incluye también comprobar que la infraestructura que soporta la operación es compatible con un nivel adecuado de disponibilidad, control y trazabilidad.

Cómo funciona / cómo se implanta: Su implantación combina revisión documental, análisis de configuraciones, inspección técnica, entrevistas con responsables de sistemas y operación y, cuando procede, verificación sobre los componentes en alcance. El ejercicio puede abarcar elementos como topología de red, segmentación, firewalls, switches, routers, servidores, sistemas de virtualización, mecanismos de autenticación, servicios expuestos, infraestructura de acceso remoto, políticas de administración y dependencias entre sistemas. En entornos industriales, la auditoría debe extenderse también a componentes como redes de supervisión, comunicaciones industriales, servidores OT, HMI, servidores de salto, enlaces con integradores, mecanismos de recogida de logs y soportes de continuidad. El análisis debe adaptarse a la realidad del entorno, evitando acciones que puedan comprometer la operación y combinando, cuando sea necesario, observación pasiva y contraste con documentación y configuraciones exportadas.

Ventajas:

- Permite obtener una visión estructurada del estado real de la infraestructura.
- Ayuda a detectar configuraciones inseguras, exposiciones innecesarias y dependencias críticas.
- Facilita la revisión de segmentación, accesos, servicios expuestos y controles de base.
- Mejora la capacidad de priorizar refuerzos de arquitectura y medidas de protección.
- Sirve de apoyo a auditorías normativas, análisis de riesgo y revisiones de continuidad.

Limitaciones y consideraciones:

- Su profundidad depende de la disponibilidad de documentación fiable y acceso a los componentes auditados.
- Puede ofrecer una visión parcial si no se integra con el conocimiento operativo y con los flujos reales de la organización.
- En entornos industriales, una revisión diseñada sólo con criterios IT puede pasar por alto condicionantes críticos de OT.

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

- Debe ejecutarse con coordinación suficiente para evitar interferencias con el proceso y con los sistemas productivos.
- Su valor disminuye si los hallazgos no se traducen después en medidas concretas de corrección, refuerzo o compensación.

Relación con otros controles: Se relaciona con la revisión de arquitectura, el análisis de riesgos tecnológicos, el análisis de vulnerabilidades, la segmentación de red, la DMZ industrial, el acceso remoto seguro, la visibilidad de activos y comunicaciones OT, el bastionado, la monitorización y continuidad de negocio. Funciona como base técnica para comprender el estado general del entorno y ordenar mejoras posteriores.

Casos habituales de uso: Se emplea en revisiones previas a auditorías de cumplimiento, programas de refuerzo de la arquitectura, proyectos de segmentación IT/OT, evaluación de infraestructuras de acceso remoto, revisión de redes industriales y corporativas, incorporación de nuevos servicios o terceros, análisis tras incidentes o ejercicios periódicos de verificación de la postura técnica del entorno.

Observaciones / medidas compensatorias asociadas: En entornos industriales, las auditorías de infraestructura son especialmente útiles para identificar medidas compensatorias de base arquitectónica, como refuerzo de la segmentación, limitación de servicios expuestos, mejora del control de accesos, introducción de servidores de salto, aislamiento de componentes legados, mejora de la visibilidad o revisión de dependencias críticas que no puedan ser eliminadas a corto plazo.

5.2.4 Auditorías de redes inalámbricas

Categoría: Auditorías técnicas e identificación de debilidades

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Identify

Descripción: Las auditorías de redes inalámbricas consisten en la revisión técnica y funcional de las tecnologías sin hilos empleadas por una organización, con el objetivo de identificar configuraciones inseguras, exposiciones no controladas, deficiencias de segmentación, mecanismos de autenticación débiles, canales no autorizados o riesgos asociados al uso de comunicaciones radio. En el ámbito industrial, este control abarca no solo redes Wi-Fi de las connvencionales, sino también otros medios inalámbricos presentes en planta o en infraestructuras operativas, como enlaces de radio, dispositivos móviles, sensores conectados, componentes IIoT, redes de apoyo logístico

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

o soluciones de mantenimiento y supervisión remota que emplean comunicación inalámbrica. Ejemplo de una metodología propuesta, aquí [22].

Objetivo: Verificar que las comunicaciones inalámbricas presentes en el entorno no introducen una superficie de exposición desproporcionada y que existen medidas adecuadas para limitar accesos no autorizados, interferencias, movimiento lateral, fuga de información o incorporación no controlada de dispositivos. En entornos industriales, el objetivo incluye también comprobar que el uso de tecnologías no cableadas es compatible con la seguridad, continuidad y la estabilidad de la operación.

Cómo funciona / cómo se implanta: Su implantación suele partir de la identificación de las tecnologías inalámbricas existentes, de su propósito operativo y de su integración con la arquitectura general. A partir de esa base, se revisan aspectos como cobertura, cifrado, autenticación, segregación, inventario de dispositivos, exposición a SSID no autorizados, mecanismos de gestión, políticas de acceso, presencia de puntos de acceso no controlados, uso de credenciales por defecto e interacción con el resto de la infraestructura. En entornos industriales, la auditoría debe considerar además el papel que estas redes juegan en la operación, mantenimiento, movilidad de personal, sensorización o la conectividad de equipos auxiliares, prestando especial atención a dependencias ocultas, uso informal de redes inalámbricas y posibles impactos sobre la disponibilidad o la integridad del proceso. El ejercicio puede combinar revisión documental, inspección técnica, captura pasiva de tráfico, análisis de cobertura y comprobación de configuraciones y políticas.

Ventajas:

- Permite identificar exposiciones que suelen pasar inadvertidas en revisiones centradas sólo en red cableada.
- Mejora el control sobre accesos, dispositivos y comunicaciones inalámbricas.
- Ayuda a detectar configuraciones débiles, redes no autorizadas o segmentación insuficiente.
- Refuerza la protección frente a movimiento lateral, acceso oportunista o uso informal de conectividad inalámbrica.
- Aporta visibilidad sobre componentes IIoT, movilidad y canales radio presentes en el entorno.

Limitaciones y consideraciones:

- Puede ofrecer una visión incompleta si la organización no dispone de un inventario claro de las tecnologías inalámbricas en uso.
- En entornos industriales, la conectividad sin hilos puede estar dispersa entre múltiples áreas y proveedores, dificultando su gobernanza.
- No todas las debilidades se derivan de la tecnología; muchas proceden de usos informales, configuraciones heredadas o falta de segmentación.
- El análisis debe tener en cuenta no sólo la seguridad, sino también cobertura, interferencias, estabilidad y compatibilidad con la operación.
- Debe integrarse con el control de accesos, la gestión de dispositivos, la segmentación y la monitorización del entorno.

Relación con otros controles: Se relaciona con la auditoría de infraestructura, la segmentación de red, el NAC, la protección de endpoints industriales, la conexión segura de dispositivos externos, la monitorización de activos y comunicaciones OT, la gestión de identidades y accesos y las medidas compensatorias orientadas a limitar exposición de canales sin hilos.

Casos habituales de uso: Se emplea en la revisión de redes Wi-Fi corporativas y operativas, puntos de acceso en planta, dispositivos móviles de mantenimiento, sensores inalámbricos, entornos IIoT, soluciones de supervisión remota, redes temporales de soporte, radioenlaces o escenarios en los que se sospecha de la existencia de conectividad sin hilos no inventariada o insuficientemente controlada.

Observaciones / medidas compensatorias asociadas: En entornos industriales, las auditorías de redes inalámbricas son especialmente útiles para detectar canales de exposición poco visibles y para fundamentar medidas compensatorias como segregación específica, refuerzo de autenticación, limitación de dispositivos autorizados, aislamiento de SSID, desactivación de servicios innecesarios, control reforzado de acceso o monitorización específica de comunicaciones radio.

5.2.5 Auditorías de dispositivos móviles y endpoints

Categoría: Auditorías técnicas e identificación de debilidades

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Identify

Descripción: Las auditorías de dispositivos móviles y endpoints consisten en la revisión técnica y funcional de los equipos de usuario, dispositivos portátiles y terminales que interactúan con la infraestructura tecnológica de la organización, a fin de comprobar su nivel real de protección, configuración, control y exposición. Este control abarca, entre otros, ordenadores corporativos, portátiles de mantenimiento, estaciones de trabajo, tablets, smartphones, equipos de soporte técnico y otros dispositivos que puedan conectarse a la red, acceder a servicios corporativos o intervenir, directa o indirectamente, en la operación. Pueden emplearse para este fin buenas prácticas del NIST [23]. En el ámbito industrial, esta revisión adquiere especial relevancia porque muchos de estos dispositivos constituyen un puente entre el entorno corporativo, los servicios remotos, el personal de mantenimiento y los sistemas OT.

Objetivo: Comprobar si los dispositivos finales y móviles de la organización presentan un nivel adecuado de seguridad, control y trazabilidad, identificando configuraciones inseguras, carencias de protección, software no autorizado, gestión insuficiente de accesos, exposición innecesaria o riesgos de propagación hacia otros dominios. En entornos industriales, el objetivo incluye también reducir el riesgo de que un portátil de mantenimiento, un equipo de terceros o un dispositivo móvil se convierta en vector de acceso, movimiento lateral o alteración de sistemas operativos y productivos.

Cómo funciona / cómo se implanta: Su implantación suele partir del inventario de los dispositivos en alcance, de su función dentro de la organización y del grado de interacción que mantienen con los distintos entornos tecnológicos. A partir de esa base, se revisan aspectos como sistema operativo, nivel de actualización, configuración de seguridad, cifrado, gestión de credenciales, mecanismos de autenticación, registro y monitorización, software instalado, políticas de uso, privilegios disponibles, protección antimalware, control de dispositivos externos e integración con soluciones de administración centralizada. En entornos industriales, la auditoría debe prestar especial atención a los portátiles de ingeniería y mantenimiento, a los equipos utilizados por integradores y proveedores, a los dispositivos con acceso remoto, a las estaciones de trabajo que interactúan con HMI o sistemas de supervisión, y a los terminales que operan en entornos mixtos IT/OT. El ejercicio puede combinar revisión documental, análisis de configuración, verificación técnica y contraste con las políticas corporativas y operativas.

Ventajas:

- Permite detectar configuraciones inseguras y debilidades de protección en equipos finales.

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

- Mejora el control sobre dispositivos que pueden actuar como vector de acceso o propagación.
- Ayuda a reforzar la trazabilidad, el control de software y la gestión de privilegios.
- Aportación de visibilidad sobre portátiles de mantenimiento, equipos de terceros y dispositivos móviles con acceso relevante.
- Sirve de apoyo para reforzar políticas de acceso, hardening y administración centralizada.

Limitaciones y consideraciones:

- Su eficacia depende de la existencia de un inventario fiable y de una gobernanza suficiente sobre los dispositivos.
- Puede verse limitada por la presencia de equipos no gestionados, legados o pertenecientes a terceros.
- En entornos industriales, algunos portátiles o estaciones pueden tener restricciones de actualización o compatibilidad con software específico de fabricante.
- No debe analizarse sólo desde la óptica corporativa, ya que algunos endpoints tienen impacto directo o indirecto sobre la operación.
- Debe combinarse con control de accesos, gestión de software, restricción de dispositivos externos y monitorización de actividad.

Relación con otros controles: Se relaciona con la protección del puesto de trabajo, la protección de endpoints industriales, el MDM, la seguridad en el correo, la conexión segura de dispositivos externos, la gestión de identidades y accesos, el acceso remoto seguro, la monitorización, el hardening y las medidas compensatorias orientadas a limitar exposición de equipos con capacidad de interacción con entornos OT.

Casos habituales de uso: Se emplea en la revisión de portátiles de mantenimiento e ingeniería, equipos de terceros con acceso a planta, dispositivos móviles corporativos, estaciones de trabajo con acceso a sistemas críticos, terminales con acceso remoto, revisión de privilegios locales, control de software instalado y escenarios en los que se necesita evaluar el riesgo de propagación desde endpoints hacia redes industriales o sistemas sensibles.

Observaciones / medidas compensatorias asociadas: En entornos industriales, estas auditorías resultan especialmente útiles para fundamentar medidas compensatorias

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

como limitación de privilegios, endurecimiento específico, control reforzado de software, uso de servidores de salto, segmentación de accesos, restricción de portátiles autorizados, control de dispositivos USB, monitorización intensificada o segregación de equipos utilizados por proveedores y personal de mantenimiento.

5.2.6 Revisión de perímetro físico-lógico

Categoría: Auditorías técnicas e identificación de debilidades

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Identify

Descripción: La revisión de perímetro físico-lógico consiste en el análisis conjunto de los elementos de acceso, separación, conexión y control que delimitan la exposición de un entorno tecnológico tanto desde el punto de vista físico como desde el punto de vista lógico. Su propósito es identificar de qué manera los espacios, armarios, salas técnicas, puertos, interfaces, conexiones de red, dispositivos de acceso, medios extraíbles y puntos de interconexión pueden actuar como superficie de entrada, manipulación o propagación de un incidente. En entornos industriales, este control resulta especialmente relevante porque la seguridad no depende sólo de la red o del software, sino también de la forma en que los activos están físicamente desplegados, protegidos y conectados a la infraestructura operativa.

Objetivo: Verificar que los límites físicos y lógicos del entorno están suficientemente definidos y protegidos, reduciendo la posibilidad de accesos no autorizados, manipulación local de equipos, conexión de dispositivos indebidos, exposición de interfaces de administración o interconexiones inseguras entre dominios. En el ámbito industrial, el objetivo incluye también reducir el riesgo derivado de accesos a sala, armarios de control, puestos de mantenimiento, puertos de comunicación, equipos de campo y otros puntos en los que una interacción física puede traducirse en un compromiso lógico con impacto operativo.

Cómo funciona / cómo se implanta: Su ejecución suele combinar revisión in situ, contraste con documentación de arquitectura, análisis de los puntos de acceso físico y lógico y verificación de la protección existente sobre componentes clave. Esto incluye, entre otros aspectos, control de acceso a salas y armarios, protección de puestos de operación y mantenimiento, exposición de puertos físicos, presencia de interfaces no utilizadas, conectividad de dispositivos externos, separación entre redes, acceso a

consolas locales, uso de servidores de salto, protección de cuartos de comunicaciones, trazabilidad de intervenciones físicas y relación entre acceso local y privilegios lógicos. En entornos industriales, esta revisión debe extenderse la PLC, HMI, estaciones de ingeniería, switches industriales, gateways, armarios de planta, componentes de campo y cualquier otro elemento en el que una interacción física pueda alterar el proceso, introducir malware, modificar configuraciones o abrir una vía de acceso hacia la red operativa.

Ventajas:

- Permite detectar exposiciones que no serían visibles en una revisión puramente lógica o documental.
- Mejora la comprensión de las relaciones entre acceso físico y compromiso tecnológico.
- Ayuda a identificar puntos de entrada local, interfaces innecesarias y conexiones mal gobernadas.
- Refuerza la protección de activos críticos, puestos de mantenimiento y componentes de comunicación.
- Resulta útil para limitar accesos oportunistas, manipulaciones locales y propagación a partir de dispositivos conectados físicamente.

Limitaciones y consideraciones:

- Puede quedar incompleta si no se realiza con conocimiento del proceso y de la realidad operativa del entorno.
- En entornos industriales, muchos puntos de acceso físico responden a necesidades de mantenimiento u operación que no pueden eliminarse sin más.
- La existencia de protección física no garantiza por sí sola un control lógico adecuado, y viceversa.
- Se requiere coordinación con operación, mantenimiento, infraestructuras, seguridad física y responsables técnicos.
- Debe integrarse con políticas de acceso, trazabilidad, gestión de dispositivos externos y segmentación de la red.

Relación con otros controles: Se relaciona con la auditoría de infraestructura, con la segmentación de red, con el acceso remoto seguro, con la conexión segura de dispositivos externos, con la protección del puesto de trabajo, con la gestión de

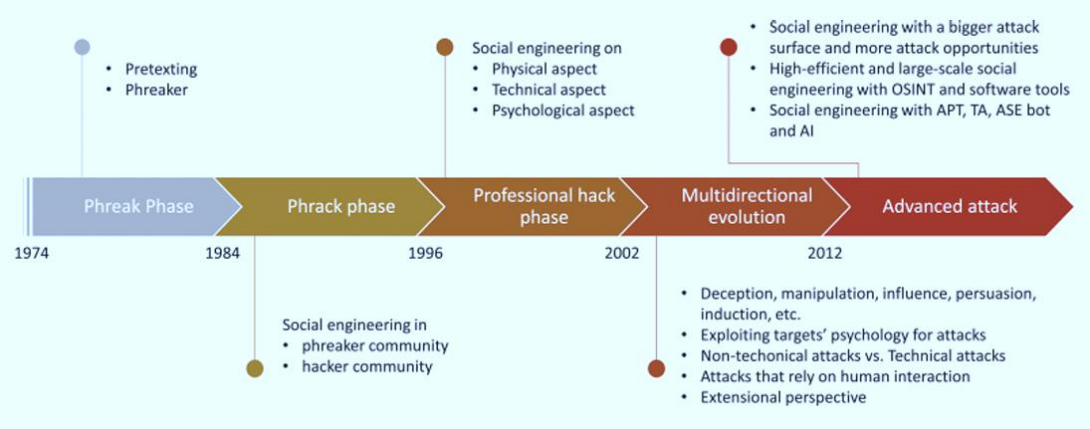
identidades y accesos, con el hardening, con la monitorización y con las medidas compensatorias destinadas a reducir la exposición de activos e interfaces críticas.

Casos habituales de uso: Se emplea en la revisión de salas técnicas y armarios de control, puestos de operación e ingeniería, equipos de mantenimiento, puertos físicos en HMI y PLC, cuartos de comunicaciones, interconexión entre redes corporativas y operativas, gestión de USB y portátiles autorizados, y escenarios en los que se precisa evaluar la relación entre acceso local y capacidad de alteración del entorno tecnológico.

Observaciones / medidas compensatorias asociadas: En entornos industriales, esta revisión resulta especialmente útil para fundamentar medidas compensatorias como sellado o desactivación de puertos no necesarios, refuerzo de control de acceso a armarios y salas, uso de servidores de salto, restricción de conexión de dispositivos externos, monitorización de intervenciones locales, refuerzo de trazabilidad o segregación física y lógica adicional en componentes con alta criticidad.

5.3 Contra ingeniería social y seguridad del factor humano

La protección de los entornos industriales no depende sólo de la robustez de la arquitectura técnica, sino también del comportamiento de las personas que interactúan con los sistemas, información y los procesos. Este bloque aborda las medidas **destinadas a reducir el riesgo derivado de la manipulación humana** (ingeniería social [24]**), de la suplantación y del error, combinando capacidades de prevención, concienciación, simulación y respuesta** frente a técnicas cada vez más sofisticadas.



Evolución conceptual de la historia de la ingeniería social. Fuente: Wang, Sun & Zhu (2010)

5.3.1 Phishing, vishing, smishing y técnicas afines

Categoría: Contra ingeniería social y seguridad del factor humano

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

Tipología: Organizativa / técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: El phishing, el vishing, el smishing y otras técnicas afines forman parte del conjunto de tácticas de ingeniería social orientadas a manipular a las personas para obtener información, credenciales, acceso inicial o ejecución de acciones que favorezcan un compromiso posterior. Su diferencia principal reside en el canal empleado: correo electrónico en el caso del phishing, llamadas telefónicas en el vishing, mensajería móvil en el smishing, aunque todas comparten la misma lógica de explotación de la confianza, de la urgencia, de la autoridad aparente o del desconocimiento.

En entornos industriales, estas técnicas no afectan sólo al personal corporativo, sino también a perfiles de operación, mantenimiento, ingeniería, proveedores y terceros con acceso a sistemas o procesos críticos.

Objetivo: Reducir la probabilidad de que la manipulación del factor humano se convierta en un vector de acceso, fraude, fuga de información o alteración de la operación, reforzando la capacidad de la organización para identificar, bloquear, informar y responder frente a interacciones maliciosas dirigidas a personas con acceso o influencia sobre el entorno tecnológico.

Cómo funciona / cómo se implanta: Su abordaje no se limita a la detección de mensajes fraudulentos, sino que requiere combinar concienciación, procedimientos, protección técnica y canales de reporte. Ello incluye formación adaptada a distintos perfiles, mecanismos de doble validación para acciones sensibles, protección del correo y de las identidades, procedimientos de verificación de solicitudes críticas, revisión de canales de comunicación, simulaciones controladas cuando proceda e integración con los procesos de respuesta. En entornos industriales, resulta especialmente importante adaptar el enfoque a los escenarios reales del entorno: mensajes dirigidos a personal de planta, llamadas fraudulentas a servicios de mantenimiento, suplantación de proveedores, peticiones urgentes de acceso remoto, cambios de credenciales, envío de ficheros o instrucciones aparentando proceder de responsables internos o fabricantes.

Ventajas:

- Reduce uno de los vectores de acceso inicial más frecuentes en incidentes reales.
- Mejora la capacidad del personal para identificar interacciones sospechosas.
- Refuerza la protección de identidades, credenciales y canales de comunicación.

- Ayuda a limitar fraudes, acceso indebido y ejecución de acciones no autorizadas.
- Favorece una cultura de reporte y verificación frente a solicitudes anómalas.

Limitaciones y consideraciones:

- La concienciación por sí sola no elimina el riesgo ni sustituye a los controles técnicos.
- Los atacantes adaptan rápidamente mensajes, canales y elementos de suplantación al contexto de la organización.
- En entornos industriales, ciertos perfiles pueden no estar expuestos con frecuencia a la formación convencional de seguridad y seguir siendo un objetivo relevante.
- Debe evitarse un enfoque excesivamente genérico o centrado sólo en el correo electrónico, dejando fuera teléfono, mensajería instantánea o interacciones con terceros.
- Su eficacia depende de que existan procedimientos claros para validar peticiones e informar sobre incidentes sospechosos.

Relación con otros controles: Se relaciona con la seguridad en el email, la gestión de identidades y accesos, el acceso remoto seguro, la conexión segura de dispositivos externos, la monitorización, la respuesta ante incidentes y las campañas de concienciación y simulación. Constituye una capa esencial para reducir riesgo humano y reforzar la protección de los accesos al entorno IT/OT.

Casos habituales de uso: Se emplea en la prevención de robo de credenciales, suplantación de proveedores, fraude en peticiones urgentes, acceso remoto no autorizado, envío de ficheros maliciosos, manipulación de personal de mantenimiento o ingeniería, campañas dirigidas a usuarios con privilegios y escenarios de compromiso inicial por interacción humana.

Observaciones / medidas compensatorias asociadas: En entornos industriales, este control gana eficacia cuando se combina con procedimientos reforzados de convalidación, limitación de privilegios, MFA, monitorización de accesos y segregación de funciones. También resulta útil establecer canales específicos para confirmar solicitudes de mantenimiento, cambios de configuración, intervenciones remotas o actuaciones que puedan tener impacto sobre la operación.

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

5.3.2 Campañas de concienciación y simulación

Categoría: Contra ingeniería social y seguridad del factor humano

Tipología: Organizativa / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: Las campañas de concienciación y simulación consisten en el conjunto de acciones planificadas destinadas a mejorar la percepción del riesgo, la capacidad de identificación de amenazas y la respuesta del personal frente a situaciones que puedan comprometer la seguridad de la organización. Incluyen tanto actividades formativas y divulgativas como ejercicios prácticos, simulaciones controladas y mecanismos de refuerzo orientados a comprobar el comportamiento real de las personas ante intentos de manipulación, fraude, acceso indebido o ejecución de acciones no autorizadas. En entornos industriales, este control resulta especialmente relevante porque el factor humano interviene no sólo en la gestión de la información, sino también en el mantenimiento de la continuidad operativa, en el acceso a sistemas OT, en la gestión de incidencias y en la relación con proveedores y terceros.

Objetivo: Incrementar la capacidad del personal para reconocer, evitar y reportar situaciones de riesgo relacionadas con la ingeniería social, con el uso indebido de canales de comunicación, con la suplantación de identidad o con comportamientos inseguros que puedan afectar a los entornos tecnológicos y operativos. Su propósito es reducir la exposición derivada del factor humano y reforzar la cultura de seguridad de la organización de manera sostenida y contextualizada.

Cómo funciona / cómo se implanta: Su implantación suele partir de la identificación de los perfiles de usuario, de sus funciones y del nivel de exposición de cada colectivo. Sobre esa base, se diseñan acciones de concienciación adaptadas al contexto real de la organización, combinando contenidos generales de seguridad con escenarios específicos del entorno. Estas campañas pueden incluir materiales formativos, sesiones presenciales o en línea, recordatorios periódicos, guías prácticas, cápsulas temáticas, simulaciones de phishing u otras técnicas de ingeniería social, así como medición de resultados y refuerzo sobre los comportamientos detectados. En entornos industriales, es importante adaptar el enfoque a los distintos perfiles implicados —personal de operación, mantenimiento, ingeniería, administración, sistemas, proveedores— e incorporar ejemplos relacionados con acceso remoto, uso de portátiles de

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

mantenimiento, suplantación de fabricantes, validación de cambios, procedimientos críticos o interacción con sistemas de control.

Ventajas:

- Mejora la capacidad del personal para identificar y evitar interacciones maliciosas.
- Refuerza la cultura organizativa de seguridad y el hábito de reporte.
- Permite adaptar mensajes y ejercicios a colectivos con exposición y funciones distintas.
- Ayuda a detectar debilidades de comportamiento antes de que se materialicen en incidentes reales.
- Complementa los controles técnicos reforzando la primera capa de defensa humana.

Limitaciones y consideraciones:

- Su eficacia disminuye si se formula como acción puntual y no como proceso continuado.
- No sustituye los controles técnicos ni elimina por sí sola el riesgo de error humano o manipulación.
- Las simulaciones deben diseñarse con criterio proporcional, evitando efectos contraproducentes o rechazo por parte del personal.
- En entornos industriales, algunos perfiles pueden tener poca exposición a la formación corporativa tradicional y requerir enfoques específicos.
- Conviene medir resultados no sólo en tasas de error, sino también en mejora del reporte, comprensión del riesgo y adecuación de los procedimientos.

Relación con otros controles: Se relaciona con el phishing, vishing, smishing y técnicas afines, el email security, la gestión de identidades y accesos, el acceso remoto seguro, la conexión segura de dispositivos externos, los procedimientos operativos y la respuesta ante incidentes. Funciona como capa complementaria para reducir la probabilidad de que el factor humano actúe como vector de entrada o de propagación.

Casos habituales de uso: Se emplea en programas anuales de concienciación, campañas periódicas de simulación de phishing, formación específica para personal de mantenimiento e ingeniería, refuerzo de buenas prácticas en accesos remotos, sensibilización frente a la suplantación de terceros, revisión de procedimientos de

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

validación y ejercicios orientados a colectivos con acceso privilegiado o con impacto operativo relevante.

Observaciones / medidas compensatorias asociadas: En entornos industriales, estas campañas son especialmente útiles cuando se combinan con procedimientos formales de validación, segregación de funciones, MFA, restricción de privilegios y canales claros de reporte. También pueden actuar como medida compensatoria parcial en escenarios en los que no es posible reforzar de inmediato todos los controles técnicos, siempre que se integren en un programa más amplio y sostenido de protección del factor humano.

5.3.3 Otras técnicas anti-ingeniería social

Categoría: Contra ingeniería social y seguridad del factor humano

Tipología: Organizativa / mixta

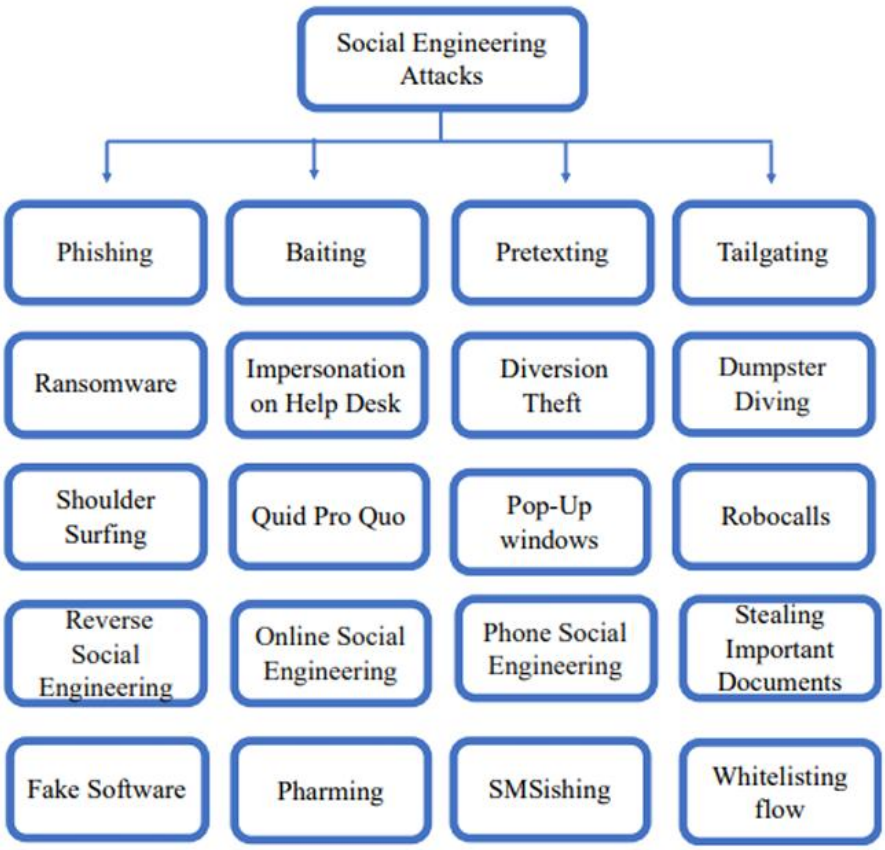
Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: Las otras técnicas anti-ingeniería social comprenden el conjunto de medidas organizativas, procedimentales y de validación destinadas a reducir el riesgo de manipulación humana más allá de las campañas específicas de phishing, vishing o smishing. Incluyen prácticas como la doble verificación de solicitudes sensibles, la verificación de identidad por canales independientes, los procedimientos formales de autorización, la segregación de funciones, la restricción de acciones críticas a roles determinados, los protocolos frente a cambios urgentes o no planificados y el uso de canales seguros para interacciones con terceros. En entornos industriales, estas medidas son especialmente relevantes porque muchas acciones de alto impacto no se ejecutan a través de un simple mensaje malicioso, sino mediante peticiones aparentemente legítimas de acceso, modificación, mantenimiento, cambio de configuración o intervención operativa.

Objetivo: Reducir la probabilidad de que una interacción humana manipulada o una suplantación de identidad pueda derivar en acceso indebido, ejecución de cambios no autorizados, entrega de información sensible, alteración del proceso o activación de cadenas de riesgo con impacto operativo. Su propósito es reforzar la seguridad a través de controles procedimentales que introduzcan verificación, trazabilidad y separación de responsabilidades en las acciones más sensibles.

A continuación, ejemplos de ataques de ingeniería social, más allá de los descritos antes.



Ataques de ingeniería social. Fuente: Salahdine & Kaabouch (2019)

Cómo funciona / cómo se implanta: Su implantación parte de la identificación de las operaciones e interacciones más expuestas a manipulación, como peticiones urgentes de acceso remoto, cambios de credenciales, modificaciones de configuración, envío de ficheros, actuaciones de mantenimiento, intervenciones de terceros o solicitudes que impliquen impacto sobre la operación. Sobre esa base, se establecen procedimientos formales de convalidación, mecanismos de confirmación por segunda vía, requisitos de autorización, registro de actuaciones, segregación de roles y controles de supervisión. En entornos industriales, resulta especialmente importante aplicar estas medidas a actividades como acceso de proveedores, modificación de lógicas o parámetros, actualizaciones, intervenciones en planta, uso de portátiles de mantenimiento, conexión de dispositivos externos y actuaciones sobre HMI, estaciones de ingeniería o activos críticos. El valor de estas técnicas depende de que sean conocidas, practicables y realmente integradas en el funcionamiento diario de la organización.

Ventajas:

- Introducen barreras procedimentales frente a la manipulación humana y a la suplantación de identidad.

- Reducen la probabilidad de ejecución de acciones críticas basadas en peticiones fraudulentas o no validadas.
- Mejoran la trazabilidad y la separación de responsabilidades.
- Resultan aplicables a múltiples escenarios, aun cuando no existe un mensaje malicioso evidente.
- Complementan los controles técnicos reforzando la seguridad de las interacciones sensibles.

Limitaciones y consideraciones:

- Pierden eficacia si no se interiorizan como práctica habitual y quedan reducidas a políticas formales.
- Pueden generar fricción operativa si se diseñan sin criterio de proporcionalidad o sin adaptación al contexto.
- En entornos industriales, los procesos urgentes de mantenimiento o continuidad pueden llevar a relajar estos controles si no están bien integrados.
- Requieren apoyo de la Dirección, conocimiento de los equipos y revisión periódica para evitar bypass informales.
- Deben acompañarse de formación, concienciación y mecanismos claros de reporte y escalado.

Relación con otros controles: Se relaciona con el phishing, vishing, smishing y técnicas afines, con las campañas de concienciación y simulación, con la gestión de identidades y accesos, con el acceso remoto seguro, con la segregación de funciones, con la conexión segura de dispositivos externos, con los procedimientos operativos y con la respuesta ante incidentes. Constituye una capacidad procedimental de protección muy relevante en escenarios de interacción con terceros y operación sensible.

Casos habituales de uso: Se emplean para validar peticiones de acceso remoto, cambios de configuración, actualizaciones, uso de credenciales privilegiadas, actuaciones de proveedores, conexión de portátiles o dispositivos externos, modificaciones en sistemas de control, autorizaciones de mantenimiento urgente y cualquier otra acción que pueda tener impacto sobre la operación o la seguridad del entorno.

Observaciones / medidas compensatorias asociadas: En entornos industriales, estas técnicas anti-ingeniería social resultan especialmente valiosas cuando se combinan con

MFA, registro de sesiones, segregación de funciones, control de privilegios y validación por segunda canal. También pueden actuar como medida compensatoria parcial cuando no es posible reforzar de inmediato determinados controles técnicos, siempre que existan procedimientos claros, trazables y asumidos por los equipos implicados.

5.4 Defensa perimetral y segmentación

La separación adecuada de redes, funciones y zonas de confianza sigue siendo uno de los principios más eficaces para reducir exposición y limitar la propagación lateral de un incidente. Esta subsección agrupa **controles destinados a reforzar el perímetro, ordenar los flujos de comunicación y establecer barreras lógicas entre dominios IT y OT, favoreciendo una arquitectura más resistente**, controlable y compatible con la operación industrial.

5.4.1 Firewall

Categoría: Defensa perimetral y segmentación

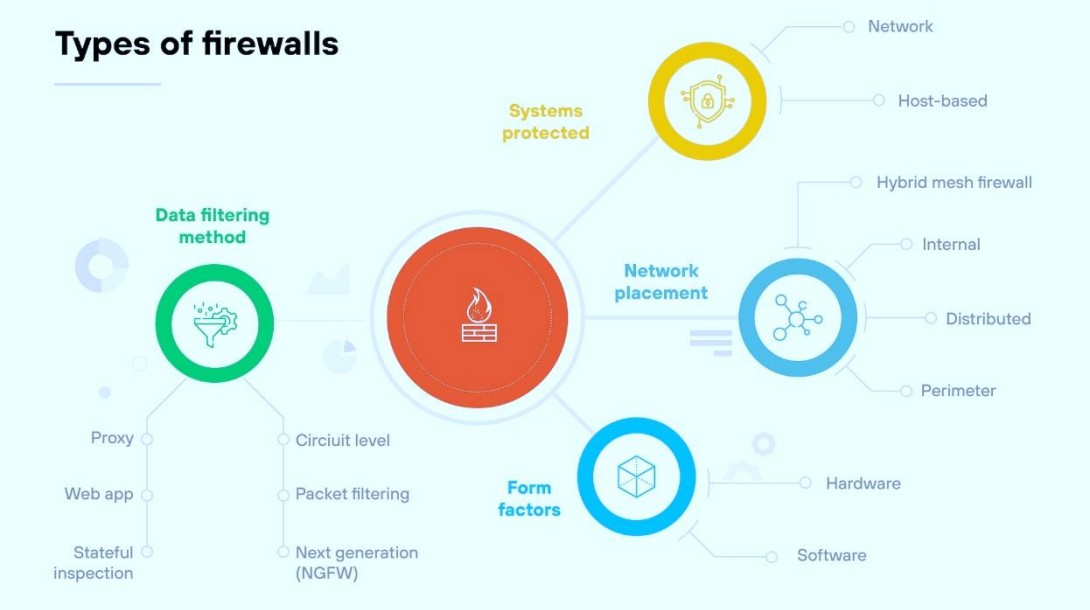
Tipología: Técnica

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: El firewall es un control de seguridad destinado a regular, filtrar y supervisar las comunicaciones entre redes, zonas, sistemas o activos, de acuerdo con un conjunto definido de reglas. Su función principal consiste en permitir únicamente el tráfico necesario y bloquear o restringir aquellas conexiones no autorizadas, innecesarias o potencialmente peligrosas, aunque existen diversas tipologías con funciones diferentes.

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



Tipos de firewalls. Fuente: Palo Alto Networks (n.d.)

En entornos industriales, su papel va más allá de la protección perimetral tradicional, ya que constituye una pieza fundamental para la separación entre dominios IT y OT, para la segmentación interna de la red operativa y para el control de los flujos entre activos con distintos niveles de criticidad.

Objetivo: Reducir la superficie de exposición del entorno, limitar las comunicaciones a lo estrictamente necesario y dificultar el acceso no autorizado, el movimiento lateral y la propagación de incidentes entre zonas o sistemas. En el ámbito industrial, el firewall contribuye también a reforzar la compartimentación de la arquitectura y a proteger activos sensibles frente a comunicaciones improcedentes o no controladas.

Cómo funciona / cómo se implanta: Su implantación se basa en la definición de reglas de filtrado que determinan qué tráfico puede circular entre dos redes, equipos o segmentos, y bajo qué condiciones. Estas reglas pueden basarse en direcciones IP, puertos, protocolos, aplicaciones, estados de conexión u otros criterios según la tecnología empleada. En entornos industriales, su configuración debe partir de un conocimiento detallado de los flujos necesarios para la operación, la criticidad de los activos, de los protocolos utilizados, de las necesidades de mantenimiento y de los puntos de interconexión con la infraestructura corporativa o con terceros. Su eficacia aumenta cuando se integra en un diseño de zonas y conductos, con revisión periódica de reglas, trazabilidad, monitorización y coordinación con los cambios en la arquitectura.

Ventajas:

- Limita las comunicaciones no autorizadas entre redes, sistemas y zonas.
- Reduce la superficie de exposición y dificulta el movimiento lateral.
- Aporta control y trazabilidad sobre los flujos permitidos y bloqueados.
- Constituye una base fundamental para la segmentación IT/OT y la compartimentación interna.
- Puede actuar como medida compensatoria frente a activos vulnerables o con soporte limitado.

Limitaciones y consideraciones:

- Su eficacia depende de la calidad del diseño de las reglas y del conocimiento real de los flujos necesarios.
- Una configuración incorrecta puede interrumpir comunicaciones legítimas o, por contra, ser excesivamente permisiva.
- En entornos industriales, no todos los protocolos o patrones de tráfico responden bien a enfoques de filtrado tradicionales.
- No sustituye otros controles como segmentación lógica completa, gestión de accesos, monitorización o bastionado.
- Requiere mantenimiento continuo, revisión de excepciones y adaptación a cambios de arquitectura, operación o terceros.

Relación con otros controles: Se relaciona con la segmentación de red y separación IT/OT, la DMZ industrial, el NGFW/UTM, el NAC, el acceso remoto seguro, la monitorización y detección, la revisión de arquitectura, la gestión de vulnerabilidades y las medidas compensatorias. Constituye uno de los controles estructurales más relevantes dentro de la defensa perimetral y de la compartimentación del entorno.

Casos habituales de uso: Se emplea para separar la red corporativa de la red OT, proteger celdas o zonas industriales, controlar accesos desde terceros, limitar tráfico entre servidores y activos de supervisión, reforzar enlaces con sedes remotas, aislar sistemas legados y establecer barreras de control entre distintos niveles de la arquitectura.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el firewall es una de las medidas compensatorias más utilizadas cuando no resulta viable parchear de inmediato ciertos activos o sustituir componentes vulnerables. En esos casos, puede emplearse para restringir protocolos, limitar orígenes y destinos

autorizados, reducir la exposición de servicios e introducir una capa adicional de control en tanto no se acomete una remediación definitiva.

5.4.2 NGFW / UTM

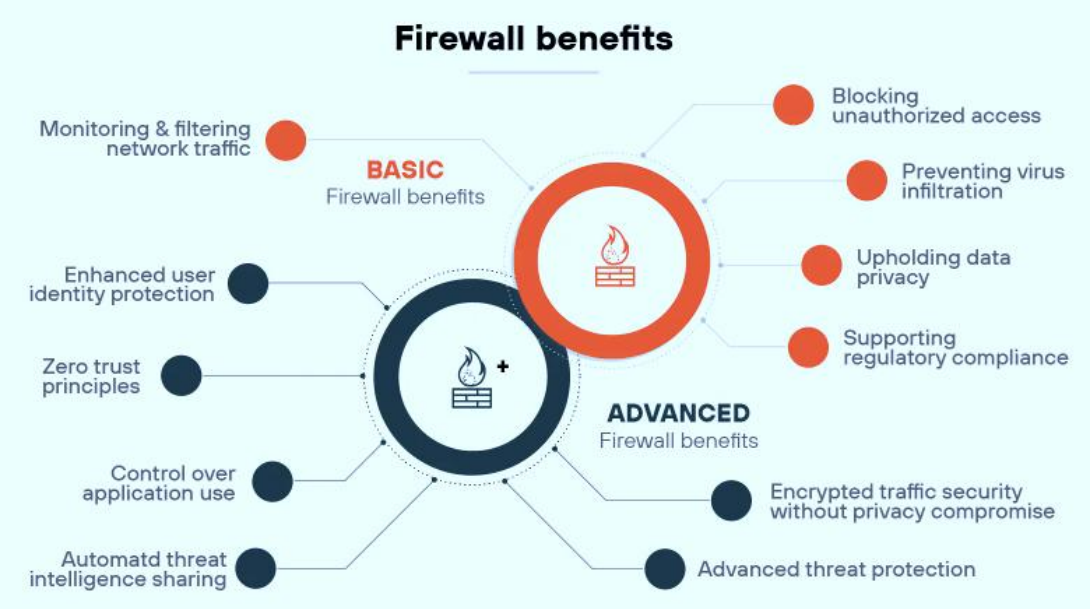
Categoría: Defensa perimetral y segmentación

Tipología: Técnica

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: Los NGFW (*Next-Generation Firewall*) y las soluciones UTM (*Unified Threat Management*) son plataformas de seguridad que amplían las capacidades del firewall tradicional incorporando funciones adicionales de inspección, control y detección. Además del filtrado básico de tráfico, pueden incluir identificación de aplicaciones, inspección profunda de paquetes, prevención de intrusiones, control de contenido, filtrado web, descifrado de tráfico cifrado, integración con inteligencia de amenazas y capacidades de registro y análisis más avanzadas. En entornos industriales, estas soluciones pueden desempeñar un papel relevante cuando existe interconexión con entornos corporativos, servicios externos, acceso remoto o necesidades de control reforzado sobre flujos complejos, siempre que su implantación sea compatible con los requisitos de estabilidad y continuidad del entorno operativo.



Beneficios de un firewall tradicional frente a un NGFW/UTM. Fuente: Palo Alto Networks (n.d.)

Objetivo: Incrementar el control sobre el tráfico y los servicios que atraviesan los límites entre redes, zonas o dominios, combinando filtrado, visibilidad y capacidad de

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

detección frente a comunicaciones no autorizadas, aplicaciones no previstas o patrones de tráfico potencialmente maliciosos. En el ámbito industrial, su objetivo es reforzar la protección perimetral e interzonal cuando el nivel de exposición o interdependencia requiere algo más que un filtrado clásico basado sólo en IP, puertos y protocolos.

Cómo funciona / cómo se implanta: Su implantación se basa en la colocación de estos dispositivos en puntos estratégicos de la arquitectura, como enlaces entre la red corporativa y la DMZ, entre la DMZ y la red OT, en salidas a Internet o en accesos de terceros. A partir de esa posición, las políticas de seguridad pueden construirse no sólo sobre reglas de tráfico básicas, sino también sobre identificación de aplicaciones, categorías de servicio, perfiles de usuario, mecanismos de detección y correlación con amenazas conocidas. En entornos industriales, su configuración debe realizarse con especial cautela, ya que determinadas funciones —como la inspección profunda, el descifrado o ciertas formas de prevención activa— pueden no ser compatibles con protocolos industriales, con el rendimiento de la red o con el comportamiento esperado de sistemas sensibles. Por ello, su implantación requiere conocer bien los flujos autorizados, los protocolos presentes, la criticidad de las comunicaciones y el impacto potencial de las funciones avanzadas sobre la operación.

Ventajas:

- Añaden visibilidad y capacidad de control más allá del filtrado tradicional.
- Permiten identificar aplicaciones, patrones de tráfico y comportamientos no previstos.
- Pueden integrar capacidades de prevención, detección y registro más avanzadas.
- Resultan útiles en entornos con acceso remoto, servicios externos o elevada interconexión.
- Refuerzan la seguridad perimetral y la compartimentación cuando se diseñan y configuran correctamente.

Limitaciones y consideraciones:

- No todas las funciones avanzadas son adecuadas para entornos OT o protocolos industriales.
- Una inspección excesivamente intrusiva puede afectar a la latencia, la disponibilidad o la estabilidad de la comunicación.

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

- Requieren configuración, mantenimiento y revisión más complejos que un firewall básico.
- No sustituyen a la segmentación arquitectónica, la gestión de accesos ni la monitorización específica de activos OT.
- Deben implantarse con criterio de proporcionalidad, evitando activar capacidades que no aportan valor real al entorno protegido.

Relación con otros controles: Se relaciona con el firewall tradicional, la segmentación de red y separación IT/OT, la DMZ industrial, el acceso remoto seguro, el IDS/IPS, el NDR, la monitorización y detección, la revisión de arquitectura y las medidas compensatorias asociadas a la limitación de exposición y control de flujos.

Casos habituales de uso: Se emplean para reforzar la frontera entre red corporativa y OT, proteger DMZ industriales, controlar accesos de terceros, inspeccionar comunicaciones salientes a servicios externos, mejorar el control sobre flujos interzonales y complementar la protección perimetral en organizaciones con elevada conectividad o dependencia de servicios digitales y remotos.

Observaciones / medidas compensatorias asociadas: En entornos industriales, estas soluciones pueden ser útiles como medida compensatoria cuando se precisa añadir una capa adicional de control sobre aplicaciones, servicios o flujos expuestos y no resulta viable acometer cambios estructurales inmediatos en la arquitectura. Con todo, su despliegue debe hacerse siempre tras validar la compatibilidad con el entorno, los protocolos presentes y los requisitos de continuidad y seguridad funcional.

5.4.3 Segmentación de red y separación IT/OT

Categoría: Defensa perimetral y segmentación

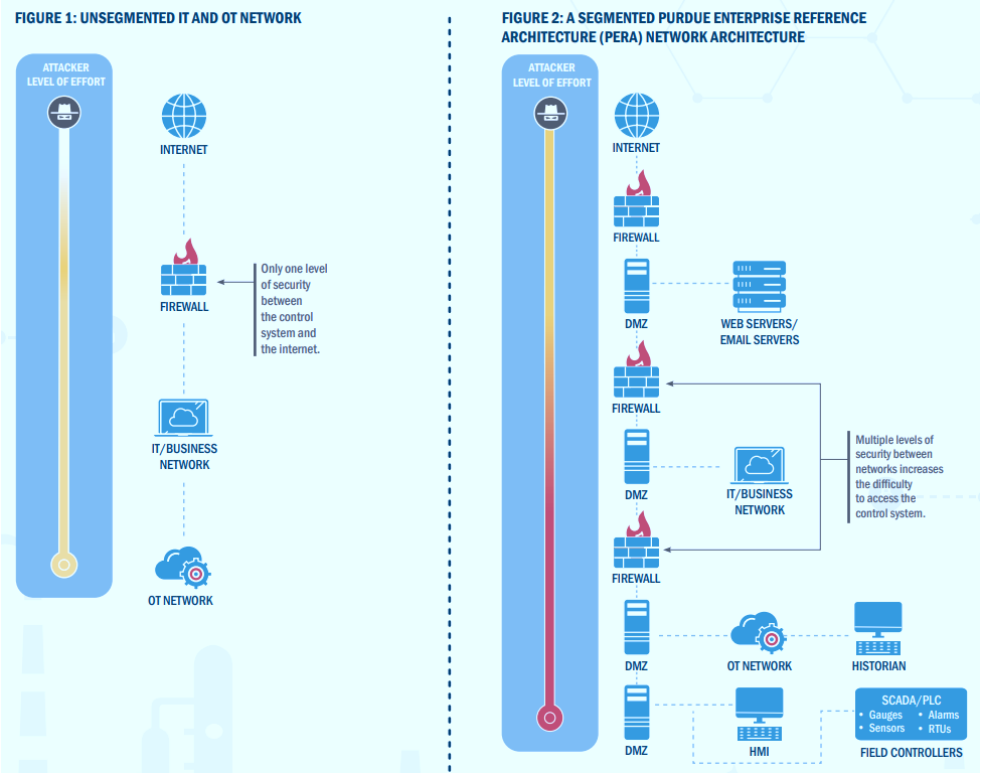
Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: La segmentación de red y la separación IT/OT consisten en la organización de la arquitectura en zonas, dominios o segmentos diferenciados, estableciendo límites claros entre ellos y controlando de forma explícita las comunicaciones permitidas (ver IEC 62443 en [25]). Su propósito es evitar que todos los sistemas compartan el mismo plano de exposición, reduciendo la probabilidad de propagación lateral, acceso indebido e impacto sistémico ante un incidente. En entornos industriales, este control resulta especialmente crítico porque la convergencia entre

redes corporativas y operativas incrementa la eficiencia y la visibilidad, pero también multiplica los puntos de contacto a través de los cuales una incidencia en IT puede llegar a afectar activos OT o procesos físicos.



Redes no segmentadas frente a IT-OT segmentado. Fuente: CISA (2022)

Objetivo: Reducir la superficie de exposición del entorno, limitar las comunicaciones a lo estrictamente necesario y contener de forma más eficaz un posible compromiso, evitando que una incidencia localizada se propague entre dominios con distinta criticidad. En el ámbito industrial, su objetivo incluye también proteger la red OT frente a dependencias innecesarias de la red corporativa y establecer niveles de separación compatibles con la continuidad y con la seguridad del proceso.

Cómo funciona / cómo se implanta: Su implantación se basa en la identificación de los activos, de los flujos de comunicación necesarios y de la criticidad relativa de cada sistema, para después estructurar la arquitectura en zonas y conductos o segmentos con reglas de interconexión bien definidas. Esto puede materializarse mediante VLAN, ACL, firewalls, DMZ industriales, servidores de salto, proxys, conductos controlados u otros mecanismos equivalentes, siempre en función de la arquitectura existente. En entornos industriales, esta segmentación debe considerar no sólo la separación entre red corporativa y red OT, sino también la compartimentación interna entre niveles de supervisión, operación, ingeniería, mantenimiento, activos legados, acceso remoto y comunicación con terceros. Su eficacia depende del conocimiento real de los flujos

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

necesarios, de la revisión periódica de las reglas y de la capacidad de adaptar la arquitectura a los cambios del proceso.

Ventajas:

- Reduce la exposición global y limita el movimiento lateral entre dominios.
- Mejora la capacidad de contención ante un incidente.
- Facilita el control y la trazabilidad de las comunicaciones entre zonas.
- Refuerza la protección de activos críticos y componentes legados.
- Sirve de base para la implantación de otros controles como DMZ, firewalls, NAC o acceso remoto seguro.

Limitaciones y consideraciones:

- Su implantación pierde eficacia si no existe un conocimiento suficiente de los flujos reales del entorno.
- Un diseño incorrecto puede introducir bloqueos, excepciones continuas o dependencia excesiva de reglas ad hoc.
- En entornos industriales, la segmentación debe tener en cuenta latencia, disponibilidad, seguridad funcional y necesidades de mantenimiento.
- No sustituye la gestión de accesos, la monitorización, el bastionado ni la gestión de vulnerabilidades.
- Requiere mantenimiento continuo, revisión de cambios y coordinación entre sistemas, operación, ingeniería y seguridad.

Relación con otros controles: Se relaciona con el firewall, el NGFW/UTM, la DMZ industrial, el NAC, el acceso remoto seguro, la monitorización y detección, la revisión de arquitectura, la gestión de vulnerabilidades y las medidas compensatorias. Constituye uno de los pilares centrales de la defensa en profundidad en entornos industriales.

Casos habituales de uso: Se emplea para separar la red corporativa de la red OT, compartimentar redes de supervisión y control, aislar activos legados, limitar comunicaciones entre líneas o celdas, proteger entornos de ingeniería, controlar accesos de terceros y reducir la exposición de sistemas con alta criticidad operativa.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la segmentación es simultáneamente un control y una de las medidas compensatorias más relevantes cuando no es viable actualizar, sustituir o endurecer de inmediato

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

determinados activos. A través de ella puede restringirse la exposición de componentes vulnerables, limitar canales de comunicación, reducir dependencias innecesarias y reforzar la contención en tanto no se acomete una remediación estructural más profunda.

5.4.4 DMZ industrial

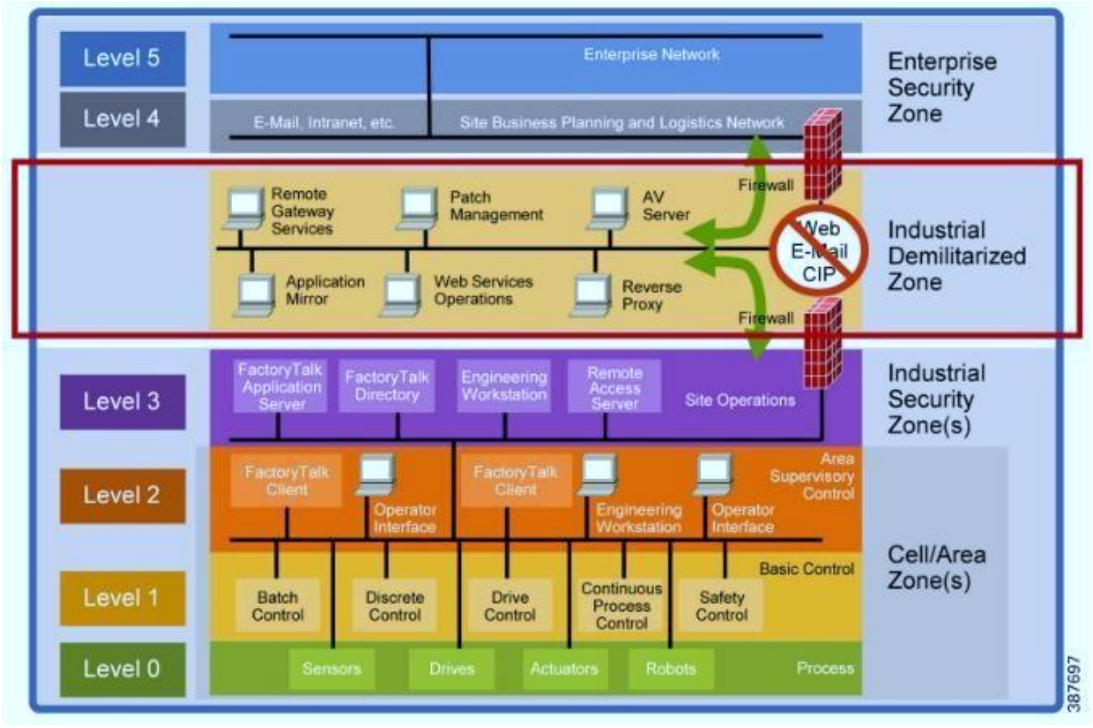
Categoría: Defensa perimetral y segmentación

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: La DMZ industrial es una zona intermedia de comunicación situada entre la red corporativa y la red OT, diseñada para controlar, limitar y supervisar los intercambios de información entre ambos dominios. Su función principal es evitar conexiones directas innecesarias entre entornos con niveles de exposición y criticidad distintos, introduciendo una capa adicional de separación, mediación y control. En entornos industriales, esta arquitectura resulta especialmente útil para canalizar servicios compartidos, acceso remoto, intercambio de ficheros, recogida de registros, integración con sistemas corporativos, actualizaciones o servicios de supervisión sin exponer directamente los activos operativos más sensibles.



Ejemplo de DMZ industrial. Fuente: Dale Peterson (2019)

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

Objetivo: Reducir el riesgo derivado de la interconexión entre la red corporativa y la red operativa, evitando accesos directos, limitando los flujos a los estrictamente necesarios y proporcionando un punto controlado para la inspección, registro y mediación de las comunicaciones. En el ámbito industrial, su objetivo incluye también proteger la red OT frente a compromisos procedentes de IT y reforzar la separación entre servicios de apoyo y sistemas de control.

Cómo funciona / cómo se implanta: Su implantación se basa en la creación de un segmento específico de la arquitectura en el que se ubican servicios que precisan comunicarse con ambos lados, pero que no deben residir ni en el núcleo de la red corporativa ni en el núcleo de la red OT. En esa zona pueden situarse, por ejemplo, servidores de intercambio, proxies, servidores de salto, soluciones de acceso remoto, colectores de logs, réplicas de datos, servidores historiadores o mecanismos de transferencia controlada. Las comunicaciones desde y hacia la DMZ deben regularse mediante firewalls, reglas explícitas, mecanismos de autenticación y supervisión continua. En entornos industriales, su diseño debe partir de un conocimiento preciso de los flujos necesarios, de los protocolos utilizados, de la criticidad de los servicios alojados y de las dependencias operativas, evitando que la DMZ se convierta en un simple espacio de tránsito sin gobernanza ni control real.

Ventajas:

- Introduce una capa adicional de separación entre IT y OT.
- Limita las conexiones directas y reduce la superficie de exposición de la red operativa.
- Facilita el control, registro y supervisión de los intercambios entre dominios.
- Permite albergar servicios compartidos en una zona con políticas específicas de seguridad.
- Resulta especialmente útil para acceso remoto, intercambio de datos, registro centralizado e integración con terceros.

Limitaciones y consideraciones:

- Su eficacia depende del diseño correcto de los flujos y de las reglas de interconexión.
- Puede perder valor si se convierte en un espacio demasiado amplio, mal segmentado o con servicios no justificados.

- En entornos industriales, la presencia de una DMZ no elimina la necesidad de segmentación interna ni de otros controles de acceso y monitorización.
- Requiere mantenimiento continuo, revisión de excepciones y gobernanza clara sobre los servicios alojados.
- Debe evitarse que la DMZ actúe como puente implícito o zona de confianza excesiva entre IT y OT.

Relación con otros controles: Se relaciona con el firewall, con el NGFW/UTM, con la segmentación de red y separación IT/OT, con el acceso remoto seguro, con los servidores de salto, con la monitorización y detección, con la gestión de identidades y accesos, con la revisión de arquitectura y con las medidas compensatorias orientadas a limitar exposición de activos OT.

Casos habituales de uso: Empleada para canalizar acceso remoto de terceros, intercambio seguro de ficheros, publicación controlada de datos operativos hacia sistemas corporativos, recogida centralizada de registros, alojamiento de historiadores o réplicas de información, servicios de supervisión e integración segura entre redes de distinta criticidad.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la DMZ industrial es una de las medidas compensatorias más relevantes cuando se precisa mantener interconexión con entornos corporativos, servicios externos o terceros sin exponer directamente la red OT. Su utilidad es especialmente alta cuando se combina con segmentación adicional, control de acceso robusto, trazabilidad y monitorización continua de los flujos que la atraviesan.

5.4.5 VPN y comunicaciones seguras

Categoría: Defensa perimetral y segmentación

Tipología: Técnica / mixta

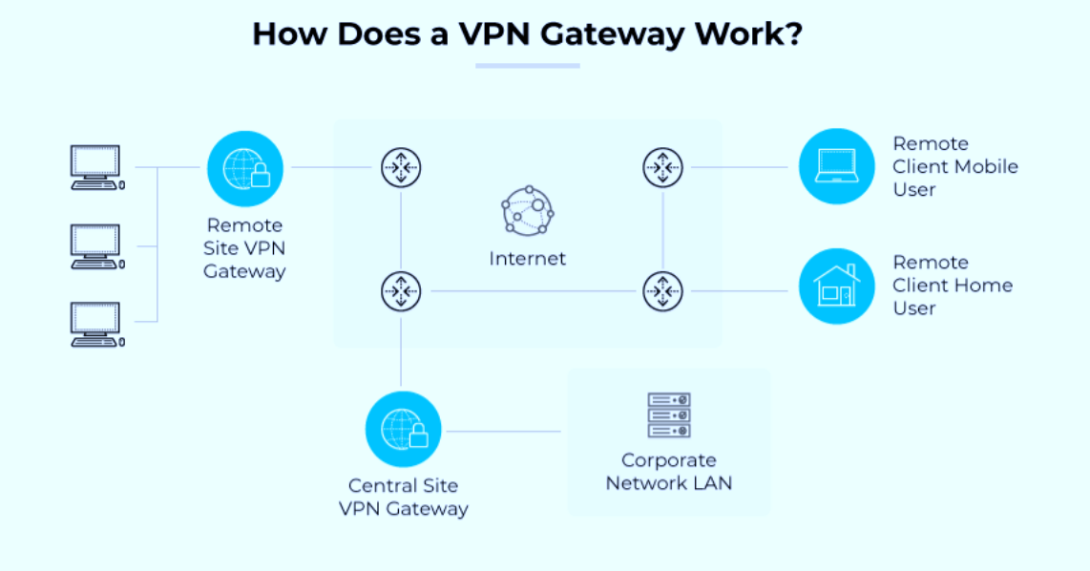
Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: Las VPN y otras comunicaciones seguras son mecanismos destinados a proteger la confidencialidad, integridad y autenticidad de las conexiones entre usuarios, sedes, sistemas o redes que precisan intercambiar información a través de infraestructuras potencialmente expuestas o no confiables. Su función principal es establecer cauces de comunicación cifrados y controlados, reduciendo el riesgo de interceptación, manipulación o acceso indebido durante la transmisión. En entornos

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

industriales, este control resulta especialmente relevante para el acceso remoto de personal interno y de terceros, para la conexión entre instalaciones, para la integración de servicios distribuidos y para el intercambio seguro de información entre dominios con distinta criticidad.



Tipologías de VPN. Fuente: Palo Alto Networks (n.d.)

Objetivo: Garantizar que las comunicaciones entre puntos autorizados se realicen mediante cauces protegidos, reduciendo la exposición a escucha, alteración de tráfico, robo de credenciales o uso indebido de accesos remotos. En el ámbito industrial, su objetivo incluye también habilitar conectividad necesaria para operación, soporte y mantenimiento sin comprometer la separación entre redes ni la seguridad de los sistemas OT.

Cómo funciona / cómo se implanta: Su implantación se basa en la creación de túneles cifrados o canales seguros entre extremos autorizados, combinando mecanismos de autenticación, cifrado, control de sesión, registro de actividad y, cuando procede, restricción por perfil, origen, horario o destino. Esto puede aplicarse tanto a conexiones de usuario remoto como a enlaces entre sedes, servicios o infraestructuras. En entornos industriales, su configuración debe partir de un criterio de mínimo privilegio, limitando el acceso a lo estrictamente necesario, evitando exposición innecesaria de redes completas e integrándose con segmentación, servidores de salto, MFA, trazabilidad y revisión de sesiones. Su eficacia depende no sólo de la fortaleza criptográfica del canal, sino también de la forma en que se gobiernan los accesos, los permisos y los flujos autorizados.

Ventajas:

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

- Protegen las comunicaciones frente a interceptación, manipulación o uso indebido.
- Permiten habilitar acceso remoto e interconexión entre sedes de forma controlada.
- Refuerzan la seguridad de las conexiones de soporte, mantenimiento y operación distribuida.
- Aportan trazabilidad y control cuando se integran con autenticación fuerte y registro de sesiones.
- Resultan útiles para limitar la exposición de servicios que no deben publicarse directamente.

Limitaciones y consideraciones:

- Una VPN segura no garantiza por sí sola un acceso remoto seguro si los permisos son excesivos o la segmentación es insuficiente.
- En entornos industriales, la apertura de túneles amplios o mal gobernados puede convertirse en un vector de acceso de alto riesgo.
- Se requiere control estricto de usuarios, credenciales, horarios, destinos y actividades permitidas.
- No sustituye mecanismos como MFA, servidores de salto, PAM, segmentación ni monitorización de sesiones.
- Debe evitarse que la necesidad operativa de acceso remoto justifique excepciones permanentes sin trazabilidad ni revisión periódica.

Relación con otros controles: Se relaciona con el acceso remoto seguro, el firewall, el NGFW/UTM, la DMZ industrial, la segmentación de red y separación IT/OT, la gestión de identidades y accesos, el PAM, la monitorización y las medidas compensatorias orientadas a limitar exposición y acceso de terceros.

Casos habituales de uso: Se emplea para conexión entre sedes industriales, acceso remoto de personal técnico o corporativo, soporte de proveedores, mantenimiento programado, acceso a sistemas intermedios en DMZ, comunicaciones seguras con centros de supervisión, conexión con servicios corporativos distribuidos o intercambio controlado de información entre instalaciones.

Observaciones / medidas compensatorias asociadas: En entornos industriales, las VPN y comunicaciones seguras deben concebirse como una capa de protección de las

conexiones, no como un permiso amplio de acceso a la red OT. Su utilidad aumenta cuando se combina con segmentación, MFA, servidores de salto, control de sesiones y permisos limitados. También pueden actuar como medida compensatoria cuando es necesario mantener acceso remoto por razones operativas, siempre que la exposición quede acotada y gobernada de forma estricta.

5.4.6 Proxy

Categoría: Defensa perimetral y segmentación

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: El proxy es un mecanismo intermediario que gestiona, filtra, media o encapsula las comunicaciones entre un cliente y un servicio de destino, evitando que ambas partes se conecten de forma directa. Su función puede orientarse a la navegación web, al acceso a determinados servicios, a la publicación controlada de aplicaciones, a la transferencia de contenidos o a la inspección y registro de tráfico. En entornos industriales, su papel suele estar asociado a la canalización segura de determinados flujos entre dominios, al control de acceso a servicios compartidos, a la limitación de exposición de sistemas internos y a la mediación en intercambios que no deben realizarse de manera directa entre la red corporativa, la DMZ y la red OT.

Objetivo: Reducir la exposición directa entre sistemas o redes, introducir un punto intermedio de control sobre las comunicaciones y reforzar la capacidad de filtrado, registro y mediación del tráfico. En el ámbito industrial, su objetivo incluye también canalizar determinados flujos necesarios para la operación o integración sin abrir conexiones directas innecesarias hacia activos sensibles.

Cómo funciona / cómo se implanta: Su implantación consiste en situar un servicio intermediario entre el origen y el destino de una comunicación, de manera que el acceso real al recurso se realice a través del proxy y bajo condiciones definidas. Según el caso, el proyecto puede actuar como mecanismo de salida controlada hacia servicios externos, como intermediario para acceso a aplicaciones internas, como componente de publicación en DMZ o como elemento de control sobre ciertos protocolos y contenidos. En entornos industriales, su configuración debe responder a necesidades concretas y justificadas, por ejemplo para canalizar acceso a servicios compartidos, centralizar salidas controladas, limitar la exposición de aplicaciones o introducir trazabilidad

adicional sobre determinados flujos. Su utilidad depende del diseño arquitectónico en el que se inserta, de las reglas de acceso definidas y de su integración con otros controles perimetrales y de identidad.

Ventajas:

- Evita conexiones directas innecesarias entre sistemas o dominios.
- Introduce un punto adicional de control, filtrado y registro.
- Puede limitar la exposición de aplicaciones y servicios internos.
- Resulta útil para canalizar acceso a recursos compartidos o salidas controladas.
- Refuerza la trazabilidad de ciertas comunicaciones cuando se integra con políticas y autenticación adecuadas.

Limitaciones y consideraciones:

- Su valor depende de que el flujo intermediado esté realmente justificado y bien gobernado.
- No sustituye la segmentación, los firewalls ni la gestión de accesos.
- En entornos industriales, no todos los protocolos o patrones de comunicación son compatibles con un esquema proxy convencional.
- Puede introducir complejidad adicional de operación, mantenimiento y resolución de incidencias.
- Debe evitarse que se convierta en una excepción permanente que acabe ampliando la exposición del entorno en lugar de reducirla.

Relación con otros controles: Se relaciona con la DMZ industrial, con el firewall, con el NGFW/UTM, la segmentación de red y separación IT/OT, el acceso remoto seguro, con la gestión de identidades y accesos, la monitorización y con las medidas compensatorias orientadas a limitar la exposición directa de servicios y aplicaciones.

Casos habituales de uso: Se emplea para canalizar salidas controladas hacia servicios externos, limitar la exposición de aplicaciones internas, mediar en el acceso a servicios compartidos entre dominios, introducir control adicional sobre navegación o transferencia de contenidos, y como parte de una arquitectura más amplia de interconexión segura entre entornos con distinta criticidad.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el proyecto puede resultar útil como medida compensatoria cuando es necesario

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

mantener determinados intercambios entre redes o servicios, pero no es aceptable una conexión directa entre los sistemas implicados. En esos casos, su utilidad aumenta cuando se combina con DMZ, autenticación fuerte, registro detallado y políticas restrictivas de acceso y uso.

5.4.7 WAF

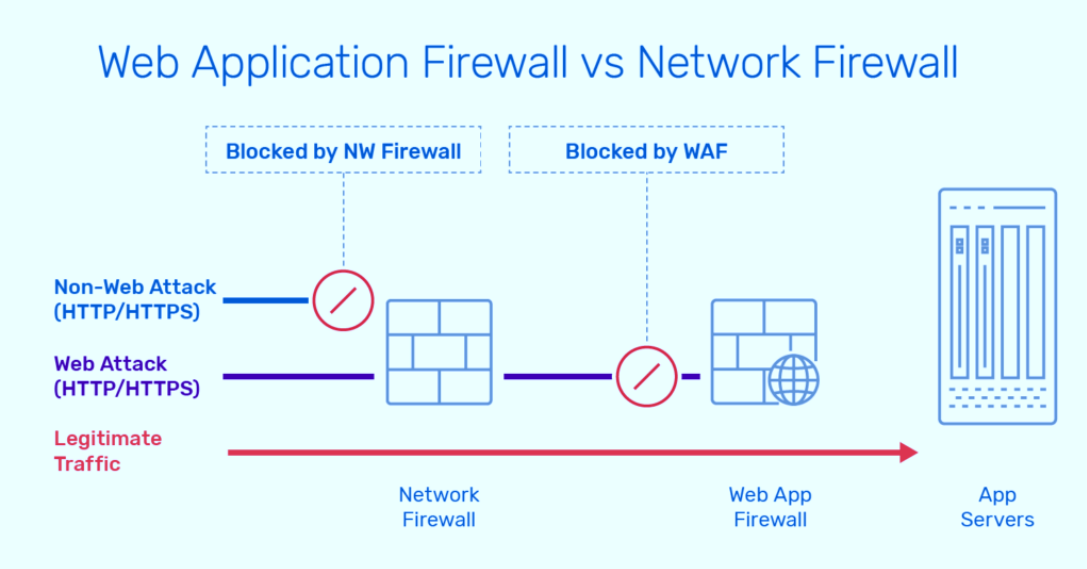
Categoría: Defensa perimetral y segmentación

Tipología: Técnica

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: El WAF (*Web Application Firewall*) es un control de seguridad diseñado para proteger aplicaciones y servicios web frente a peticiones maliciosas, explotación de vulnerabilidades comunes y usos no autorizados de la capa de aplicación. A diferencia del firewall tradicional, que actúa principalmente sobre IP, puertos y protocolos, el WAF analiza el tráfico HTTP/HTTPS y aplica reglas específicas sobre el comportamiento esperado de las aplicaciones, los parámetros intercambiados y los patrones de ataque conocidos. En entornos industriales, su relevancia aparece cuando existen portales web, aplicaciones de gestión, APIs, servicios de acceso remoto vía web, paneles de supervisión publicados o componentes de integración accesibles mediante tecnologías web.



Función del WAF frente al firewall clásico. Fuente: A10 Networks (n.d.)

Objetivo: Reducir el riesgo de explotación de vulnerabilidades en aplicaciones y servicios web, limitando peticiones maliciosas, usos indebidos y patrones de ataque

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

orientados a la capa de aplicación. En el ámbito industrial, su objetivo incluye también proteger servicios web vinculados a la operación, a la supervisión, a la integración de datos o a la interacción con terceros, evitando que una exposición web se convierta en un vector de acceso hacia sistemas más sensibles.

Cómo funciona / cómo se implanta: Su implantación consiste en situar el WAF delante de la aplicación o servicio web que se desea proteger, de manera que todo el tráfico pase por él antes de llegar al destino final. A partir de esa posición, el WAF puede aplicar políticas de filtrado, detección de patrones de ataque, validación de solicitudes, limitación de ciertos comportamientos y registro de eventos. En entornos industriales, su configuración debe partir de un conocimiento claro de los servicios publicados, de los flujos legítimos, de los usuarios autorizados y de las integraciones necesarias, evitando bloqueos indebidos sobre funcionalidades críticas. Su valor es mayor cuando forma parte de una arquitectura segura de publicación de servicios, integrada con segmentación, DMZ, autenticación fuerte, registro y revisión periódica de reglas.

Ventajas:

- Añade una capa específica de protección sobre aplicaciones y servicios web.
- Ayuda a limitar explotaciones comunes de la capa de aplicación.
- Mejora la visibilidad y el registro sobre interacciones con servicios publicados.
- Resulta útil para reducir la exposición de portales, APIs y componentes web con acceso externo o interdominio.
- Puede complementar otros controles perimetrales cuando existen servicios publicados necesarios para la operación o la gestión.

Limitaciones y consideraciones:

- Sólo resulta aplicable cuando existen aplicaciones o servicios basados en tecnologías web.
- No sustituye la seguridad en el desarrollo, la revisión de código ni la corrección de las vulnerabilidades de la aplicación.
- Una configuración insuficiente o demasiado genérica puede reducir su eficacia real.
- En entornos industriales, debe evitarse publicar servicios web sin una revisión previa de su necesidad, criticidad y arquitectura de protección.

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

- Requiere mantenimiento de políticas, análisis de eventos y adaptación a cambios funcionales de la aplicación protegida.

Relación con otros controles: Se relaciona con el firewall, con el NGFW/UTM, la DMZ industrial, la segmentación de red, el acceso remoto seguro, la gestión de identidades y accesos, DevSecOps, el DAST, el RASP, la monitorización y con las medidas compensatorias orientadas a limitar exposición de aplicaciones publicadas.

Casos habituales de uso: Empleado para proteger portales de gestión, aplicaciones corporativas accesibles desde red externa, servicios web publicados en DMZ, APIs de integración, interfaces web de supervisión o mantenimiento y otros componentes expuestos a través de HTTP/HTTPS que, sin ser necesariamente nucleares en la operación, pueden funcionar como punto de entrada hacia dominios más sensibles.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el WAF puede actuar como medida compensatoria útil cuando existe un servicio web que debe permanecer accesible incluso públicamente, pero no es viable corregir de inmediato todas sus debilidades o rediseñar su arquitectura. Su utilidad aumenta cuando se combina con publicación en DMZ, autenticación reforzada, segmentación, registro detallado y revisión continua de la superficie de exposición de la aplicación.

5.4.8 ZTNA

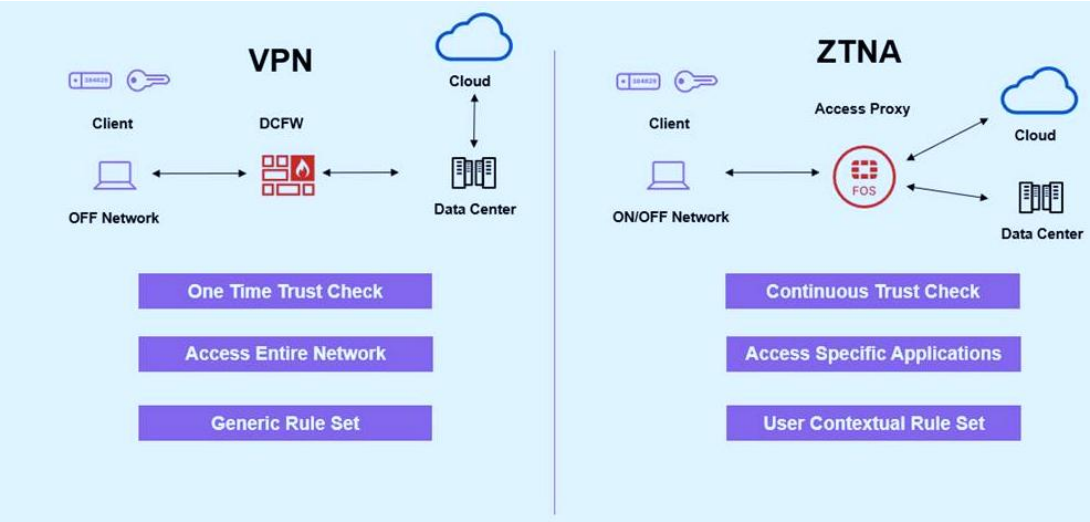
Categoría: Defensa perimetral y segmentación

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: El ZTNA (*Zero Trust Network Access*) es un modelo de acceso que sustituye la confianza implícita en las conexiones por la verificación continua de la identidad, del contexto (aplicación y dispositivo) y de los permisos antes de permitir la interacción con un recurso concreto. Su lógica no se basa en conceder acceso amplio a una red por estar "dentro" de ella o por conectarse a través de un túnel seguro, sino en habilitar un acceso granular, condicionado y limitado al servicio o activo específicamente autorizado. En entornos industriales, este enfoque resulta especialmente relevante cuando existen accesos remotos, interacción con terceros, mantenimiento distribuido, integración de servicios o necesidad de limitar de forma más estricta el alcance de las conexiones hacia sistemas sensibles.



Diferencias de VPN tradicional frente a enfoque ZTNA. Fuente: Fortinet (2022)

Objetivo: Reducir la exposición derivada del acceso remoto o interdominio, evitando permisos excesivos y limitando cada conexión al recurso concreto, al contexto autorizado y al perfil correspondiente. En el ámbito industrial, su objetivo incluye también minimizar el riesgo de que un acceso legítimo se convierta en una vía de movimiento lateral, exploración de red o compromiso de activos OT de alta criticidad.

Cómo funciona / cómo se implanta: Su implantación se basa en convalidar de manera explícita la identidad del usuario o sistema, el dispositivo desde el que se conecta, el contexto de la sesión, los factores adicionales de autenticación y los permisos concretos que le corresponden. A partir de esa validación, el acceso se concede sólo al recurso autorizado, sin exponer la totalidad de la red ni habilitar visibilidad innecesaria sobre otros sistemas. En entornos industriales, el ZTNA suele aplicarse al acceso remoto de personal técnico, integradores, mantenimiento, proveedores o usuarios que necesitan llegar a servicios concretos de forma puntual y controlada. Su eficacia aumenta cuando se integra con MFA, PAM, servidores de salto, segmentación, registro de sesiones, revisión de accesos y políticas de mínimo privilegio. Su despliegue requiere conocer con claridad qué recursos deben ser accesibles, por quiénes, en qué condiciones y durante cuánto tiempo.

Ventajas:

- Reduce la confianza implícita y limita el acceso a lo estrictamente necesario.
- Evita exponer segmentos completos de la red a usuarios o terceros que sólo necesitan un recurso concreto.
- Dificulta el movimiento lateral y la exploración innecesaria del entorno.

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

- Mejora el control contextual del acceso remoto e interdominio.
- Complementa de manera eficaz la segmentación, el PAM y la trazabilidad de sesiones.

Limitaciones y consideraciones:

- Requiere una definición precisa de identidades, recursos, flujos autorizados y políticas de acceso.
- Puede resultar complejo en entornos con arquitectura poco documentada o con muchas excepciones históricas.
- En entornos industriales, su implantación debe respetar la disponibilidad, los requisitos de mantenimiento y compatibilidad con los procedimientos operativos reales.
- No sustituye la segmentación de la red ni la protección de los activos una vez concedido el acceso.
- Su valor disminuye si se configura con permisos excesivos, reglas amplias o excepciones permanentes mal gobernadas.

Relación con otros controles: Se relaciona con el acceso remoto seguro, el firewall, el NGFW/UTM, la segmentación de red y separación IT/OT, la DMZ industrial, la gestión de identidades y accesos, el PAM, los servidores de salto, la monitorización y las medidas compensatorias destinadas a limitar el alcance del acceso de terceros y usuarios con privilegios.

Casos habituales de uso: Empleado para acceso remoto de mantenimiento, intervención de terceros, conexión puntual a servidores o aplicaciones concretas, protección de servicios publicados a usuarios internos o externos, control de acceso a entornos intermedios en DMZ y sustitución progresiva de esquemas tradicionales de acceso remoto basados en VPN amplias o excesivamente permisivas.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el ZTNA puede actuar como medida compensatoria muy útil cuando existe la necesidad de mantener acceso remoto a determinados sistemas, pero no resulta aceptable abrir conectividad amplia hacia la red OT. Su utilidad aumenta cuando se combina con MFA, PAM, segmentación, registro de sesiones y revisión periódica de permisos, reduciendo el alcance efectivo de cada acceso al mínimo imprescindible.

5.4.9 NAC

Categoría: Defensa perimetral y segmentación

Tipología: Técnica / mixta

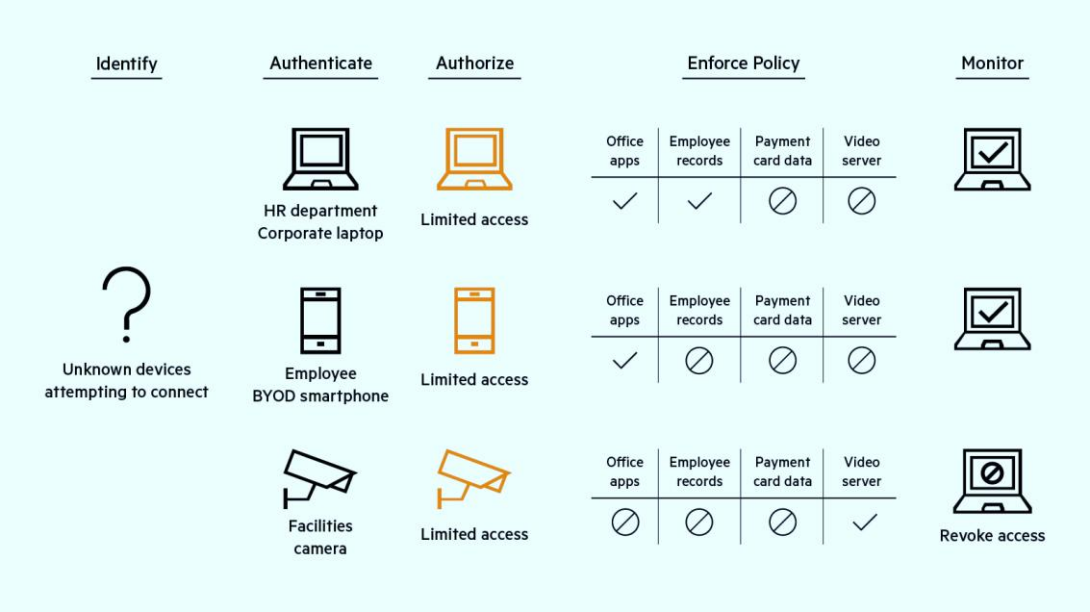
Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: El NAC (*Network Access Control*) es un conjunto de mecanismos destinados a identificar, autenticar, evaluar y controlar los dispositivos que pretenden conectarse a una red, aplicando políticas de acceso en función de su identidad, estado, localización, tipo o nivel de confianza. Su función principal consiste en evitar que equipos no autorizados, mal configurados o insuficientemente gobernados puedan incorporarse libremente al entorno tecnológico. En entornos industriales, este control resulta especialmente relevante porque la incorporación de portátiles de mantenimiento, equipos de terceros, dispositivos móviles, componentes IIoT o activos no inventariados puede convertirse en un vector de acceso o propagación con impacto operativo considerable.

Objetivo: Reducir el riesgo de conexión no autorizada a la red, limitando el acceso de dispositivos a aquellos recursos, segmentos o servicios que les correspondan según su función y nivel de confianza. En el ámbito industrial, su objetivo incluye también impedir que un equipo ajeno, comprometido o no validado pueda acceder a zonas operativas sensibles o establecer conectividad directa con activos OT sin control previo.

Cómo funciona / cómo se implanta: Su implantación se basa en la definición de políticas que condicionan el acceso a la red a la identificación del dispositivo, del usuario asociado, del punto de conexión, del perfil permitido y, cuando procede, del estado de cumplimiento de ciertos requisitos mínimos.



Ejemplos de aplicación de NAC. Fuente: HPE (2025)

Según la arquitectura, el NAC puede actuar en puertos de acceso, redes inalámbricas, segmentos corporativos, entornos mixtos o puntos de conexión de terceros. En entornos industriales, su implantación debe realizarse con especial cautela, ya que no todos los dispositivos OT admiten los mismos métodos de autenticación o comprobación de postura que un endpoint corporativo. Por ello, suele ser más eficaz cuando se orienta a controlar los puntos de entrada de equipos externos, portátiles de mantenimiento, dispositivos no gestionados y zonas de convergencia IT/OT, combinándose con inventario de activos, segmentación, listas de autorización y procedimientos de convalidación previa.

Ventajas:

- Limita la incorporación no controlada de dispositivos a la red.
- Mejora la visibilidad sobre qué equipos se conectan, desde dónde y en qué condiciones.
- Ayuda a reforzar la segmentación y la aplicación de políticas de acceso a la red.
- Resulta especialmente útil para controlar equipos de terceros, portátiles de mantenimiento y dispositivos no gestionados.
- Reduce la probabilidad de que un acceso físico o local se traduzca automáticamente en conectividad lógica amplia.

Limitaciones y consideraciones:

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

- Su implantación puede ser compleja en entornos con activos legados, equipos propietarios o infraestructura poco documentada.
- No todos los dispositivos industriales soportan mecanismos estándar de autenticación o evaluación de postura.
- Debe evitarse que la política de control de acceso interfiera con comunicaciones críticas o con el funcionamiento normal de la operación.
- No sustituye la segmentación, el control de identidades, la monitorización ni la revisión de dispositivos externos.
- Se requiere una gobernanza clara de las excepciones, de los perfiles autorizados y de los procedimientos de conexión temporal o de emergencia.

Relación con otros controles: Se relaciona con la segmentación de red y separación IT/OT, el firewall, el acceso remoto seguro, la gestión de identidades y accesos, la protección de endpoints industriales, la conexión segura de dispositivos externos, con la monitorización de activos y comunicaciones OT y con las medidas compensatorias destinadas a limitar exposición de puntos de acceso físicos o lógicos.

Casos habituales de uso: Se emplea para controlar la conexión de portátiles de mantenimiento, equipos de integradores, dispositivos móviles, puntos de acceso inalámbricos, componentes IIoT, redes de apoyo en planta, zonas de convergencia entre IT y OT y entornos en los que se necesita evitar que la simple conexión física a un puerto o red implique acceso amplio al entorno.

Observaciones / Medidas compensatorias asociadas: En entornos industriales, el NAC resulta especialmente útil como medida compensatoria cuando existe riesgo elevado de conexión de dispositivos externos o no inventariados y no es viable actuar de inmediato sobre toda la arquitectura. Su utilidad aumenta cuando se combina con segmentación, listas de autorización, procedimientos de validación previa, trazabilidad de conexiones y control reforzado sobre equipos de terceros y portátiles de mantenimiento.

5.4.10 CASB / SASE

Categoría: Defensa perimetral y segmentación

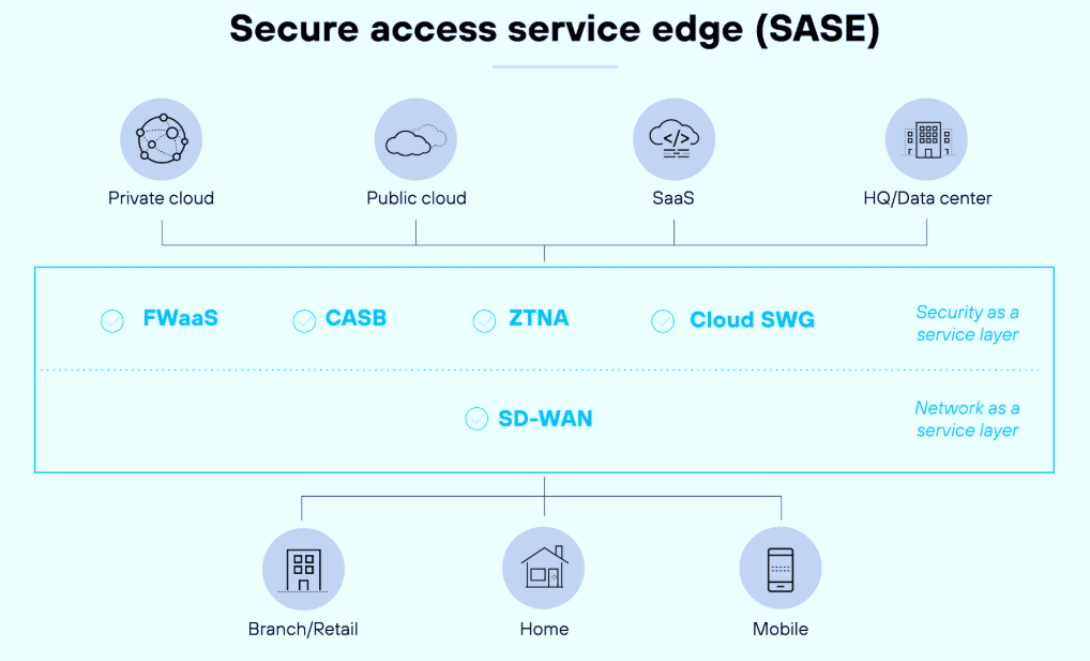
Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

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

Descripción: El CASB (*Cloud Access Security Broker) y* el SASE (*Secure Access Service Edge*) son enfoques y capacidades orientadas a controlar, proteger y supervisar el acceso a servicios, aplicaciones y recursos distribuidos, especialmente cuando éstos se encuentran fuera del perímetro clásico de la organización o combinan componentes locales, cloud y acceso remoto. El CASB se centra principalmente en la visibilidad, control y protección del uso de aplicaciones y servicios cloud, mientras que el SASE integra en un modelo más amplio capacidades de conectividad y seguridad como acceso seguro, filtrado, inspección, políticas contextuales y segmentación de acceso. En entornos industriales, estas capacidades cobran relevancia cuando existen plataformas cloud de gestión, supervisión remota, analítica, colaboración, servicios distribuidos o interacción frecuente entre usuarios, dispositivos y recursos situados en entornos mixtos.



Componentes de la solución SASE. Fuente: Palo Alto Networks (n.d.)

Objetivo: Reducir el riesgo asociado al uso de servicios cloud, accesos distribuidos y modelos de conectividad más descentralizados, garantizando que el acceso a recursos y aplicaciones se realice bajo políticas de seguridad coherentes, con visibilidad suficiente y con control sobre usuarios, dispositivos, datos y sesiones. En el ámbito industrial, su objetivo incluye también evitar que la adopción de servicios externos o modelos híbridos introduzca exposiciones no gobernadas hacia sistemas o información con impacto operativo.

Cómo funciona / cómo se implanta: Su implantación parte de la identificación de los servicios y flujos que se desea controlar: aplicaciones cloud autorizadas, acceso remoto

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

a recursos corporativos u operativos, transferencia de datos, interacción entre usuarios distribuidos, publicación de servicios y conexión entre sedes o dispositivos. A partir de esa base, se definen políticas de acceso, inspección, registro, autenticación, evaluación contextual y protección de datos que se aplican sobre dichas interacciones. En entornos industriales, estas capacidades suelen tener sentido cuando existe integración con plataformas cloud, servicios de soporte remoto, analítica centralizada, gestión distribuida o modelos en los que la simple protección perimetral ya no resulta suficiente. Su utilidad depende de que se implanten sobre flujos reales y justificados, y de que se integren con identidad, segmentación, MFA, trazabilidad y revisión continua del alcance permitido.

Ventajas:

- Mejoran la visibilidad sobre el uso de servicios cloud y accesos distribuidos.
- Permiten aplicar políticas de seguridad más coherentes en entornos híbridos.
- Refuerzan el control contextual de usuarios, dispositivos, sesiones y datos.
- Resultan útiles cuando la organización depende de servicios externos, acceso remoto o conectividad más descentralizada.
- Complementan la evolución desde el perímetro clásico hacia modelos de acceso más segmentados y verificables.

Limitaciones y consideraciones:

- Su utilidad es reducida si la organización no hace uso relevante de servicios cloud o conectividad distribuida.
- En entornos industriales, deben implantarse con cautela para evitar dependencias excesivas de modelos no compatibles con la operación crítica.
- No sustituyen la segmentación OT, la DMZ industrial ni el control directo sobre activos de planta.
- Pueden introducir complejidad adicional de integración, gobernanza y análisis de políticas.
- Deben evitarse despliegues motivados sólo por tendencia tecnológica, sin una necesidad real y bien delimitada en el contexto de la organización.

Relación con otros controles: Se relaciona con el firewall, el NGFW/UTM, el proxy, el ZTNA, el acceso remoto seguro, la gestión de identidades y accesos, el PAM, la

segmentación, la protección de aplicaciones SaaS, la monitorización y las medidas compensatorias orientadas a controlar flujos externos y acceso a servicios distribuidos.

Casos habituales de uso: Se emplean en organizaciones con uso significativo de aplicaciones cloud, servicios de analítica o gestión distribuida, acceso remoto frecuente a recursos corporativos, colaboración con terceros mediante plataformas externas, publicación controlada de servicios y escenarios en los que la seguridad debe acompañar un modelo de conectividad menos centrado en el perímetro clásico.

Observaciones / medidas compensatorias asociadas: En entornos industriales, CASB y SASE deben interpretarse como capacidades complementarias para gobernar mejor entornos híbridos y servicios distribuidos, y no como sustitutos de las medidas básicas de separación y protección de la red OT. Su utilidad aumenta cuando la organización ya tiene una dependencia real de cloud, acceso remoto o servicios externos, y cuando se combinan con identidad fuerte, segmentación, control de sesiones y limitación explícita del acceso a recursos sensibles.

5.5 Detección de amenazas y protección activa

En un contexto en el que la prevención absoluta no existe, las organizaciones necesitan capacidades que les permitan identificar actividad anómala, detectar comportamientos hostiles y actuar antes de que el impacto escale. Este bloque reúne **tecnologías y servicios orientados a la detección temprana, a la respuesta automatizada o asistida y a la protección activa frente a amenazas que afectan tanto a los activos corporativos como a los componentes propios de los entornos industriales**.

5.5.1 IDS / IPS

Categoría: Detección de amenazas y protección activa

Tipología: Técnica / mixta

Función defensiva predominante: Detectiva

Función en NIST CSF: Detect, Respond

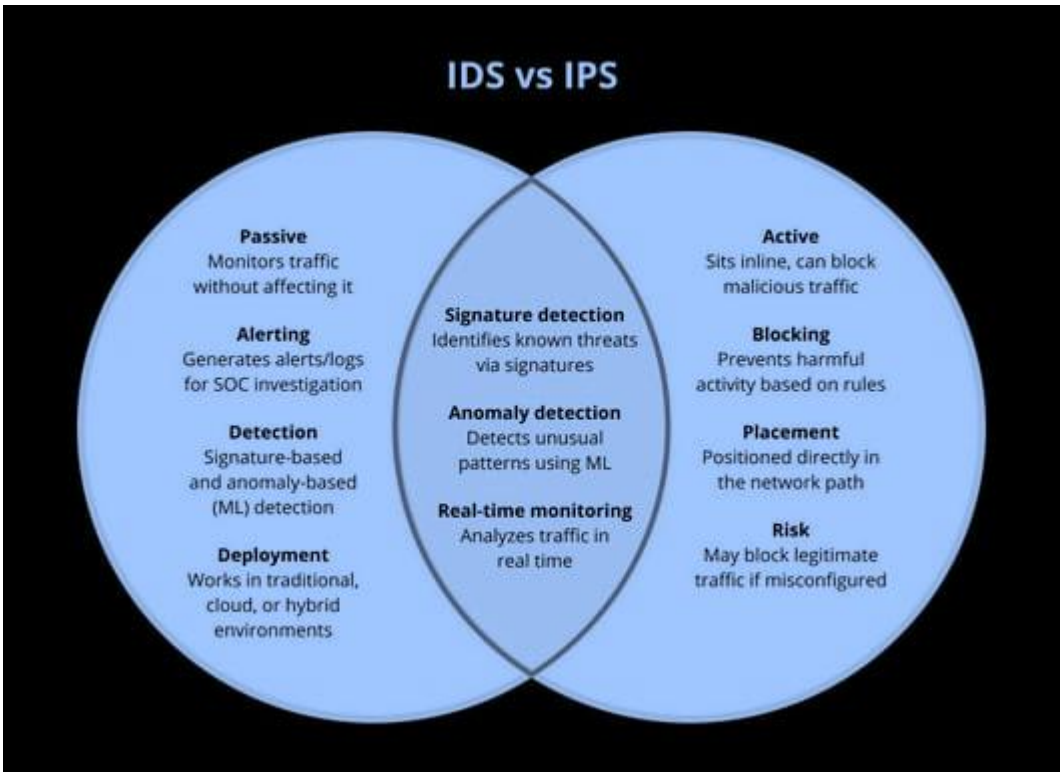
Descripción: Los sistemas IDS (*Intrusion Detection System*) e IPS (*Intrusion Prevention System*) son mecanismos orientados a la identificación —y, en el caso del IPS, también al bloqueo o contención— de tráficos, patrones o comportamientos que pueden indicar intentos de intrusión, explotación de vulnerabilidades, movimiento lateral o uso indebido de la red. Su lógica se basa en el análisis del tráfico y de los eventos que circulan por determinados puntos de la infraestructura, contrastándolos con reglas, firmas,

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

patrones de comportamiento o indicadores conocidos. En entornos industriales, este tipo de control resulta especialmente útil para mejorar la visibilidad sobre la actividad de red y detectar comunicaciones anómalas, accesos no previstos o interacciones improcedentes entre activos con distinta criticidad.

Objetivo: Incrementar la capacidad de la organización para identificar señales de compromiso, actividades maliciosas o comportamientos anómalos en la red, y en determinados casos bloquear o limitar su progresión. En el ámbito industrial, su objetivo incluye también detectar interacciones indebidas sobre protocolos, servicios o activos OT sin introducir un impacto operativo incompatible con la continuidad y estabilidad del proceso.

Cómo funciona / cómo se implanta: Su implantación consiste en situar sensores o componentes de inspección en puntos relevantes de la arquitectura, como perímetros, segmentos internos, enlaces entre zonas, entornos de DMZ o puntos de acceso remoto. Un IDS observa y analiza el tráfico sin intervenir directamente sobre él, mientras que un IPS añade capacidad de respuesta automática, bloqueando o rechazando determinadas comunicaciones según las políticas configuradas. En entornos industriales, la elección entre un enfoque de detección pasiva o un enfoque con capacidad preventiva activa debe hacerse con especial prudencia, ya que un bloqueo inadecuado puede afectar a la operación. Por ello, suele ser recomendable comenzar con configuraciones de detección y alerta (fuera de línea), validar el comportamiento del sistema sobre los protocolos presentes y reservar las medidas de prevención automática para entornos en los que exista seguridad suficiente sobre el impacto de cada regla. Su utilidad depende también de la afinación de las firmas, del conocimiento de los flujos legítimos y de la integración con los procesos de análisis y respuesta.



Capacidades IDS vs IPS. Fuente: Corelight (n.d.)

Ventajas:

- Mejoran la visibilidad sobre la actividad de la red y los patrones de tráfico.
- Permiten identificar señales de intrusión, explotación o comportamiento anómalo.
- Ayudan a detectar interacciones no previstas entre zonas, servicios o activos.
- Pueden complementar la segmentación, el firewall y la monitorización de activos OT.
- En un enfoque bien validado, los IPS pueden contribuir a bloquear ciertos tráficos no autorizados o maliciosos.

Limitaciones y consideraciones:

- Su eficacia depende de la calidad de las reglas, de la afinación y del conocimiento del entorno.
- En entornos industriales, un IPS mal configurado puede introducir riesgo operativo por bloqueo indebido de comunicaciones legítimas.
- No todos los protocolos industriales o patrones de comunicación se interpretan bien con enfoques genéricos basados en firmas.

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

- No sustituyen la segmentación, el control de accesos, la gestión de vulnerabilidades ni la revisión de la arquitectura.
- Pueden generar volumen elevado de alertas si no existen procesos de análisis, contextualización y respuesta suficientes.

Relación con otros controles: Se relaciona con el firewall, el NGFW/UTM, la segmentación de red y separación IT/OT, la DMZ industrial, el NDR, la monitorización y operación de seguridad, con la visibilidad de activos y comunicaciones OT, la respuesta ante incidentes y con las medidas compensatorias orientadas a reforzar la detección en activos con riesgo elevado.

Casos habituales de uso: Se emplean en la supervisión de perímetros, enlaces entre IT y OT, zonas industriales internas, accesos remotos, servicios publicados, entornos con activos legados, redes con elevada criticidad o escenarios en los que se necesita detectar interacciones indebidas, movimiento lateral, escaneos, explotación de vulnerabilidades o uso anómalo de protocolos y servicios.

Observaciones / medidas compensatorias asociadas: En entornos industriales, los IDS resultan especialmente útiles como medida compensatoria cuando no es viable modificar de inmediato la arquitectura, parchear determinados activos o reducir toda la exposición existente. Los IPS, por su parte, pueden aportar valor en segmentos concretos y bien conocidos, siempre que la prevención automática esté validada y no comprometa la continuidad del proceso. En ambos casos, su utilidad aumenta cuando se integran con segmentación, visibilidad OT, correlación de eventos y procedimientos claros de análisis y respuesta.

5.5.2 NDR

Categoría: Detección de amenazas y protección activa

Tipología: Técnica / mixta

Función defensiva predominante: Detectiva

Función en NIST CSF: Detect

Descripción: El NDR (*Network Detection and Response*) es un conjunto de capacidades orientadas a la observación, análisis y contextualización del tráfico de red con el objetivo de identificar comportamientos anómalos, indicios de compromiso, movimiento lateral, uso indebido de protocolos, comunicaciones no previstas o interacciones sospechosas entre activos. A diferencia de otros mecanismos más basados en firmas o reglas estáticas, el NDR suele combinar visibilidad continua, análisis de patrones,

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

contextualización de los flujos y capacidad de investigación para ofrecer una lectura más rica de la actividad real del entorno. En entornos industriales, este control resulta especialmente valioso porque permite mejorar la visibilidad sobre comunicaciones IT/OT, protocolos industriales, activos de alta criticidad y relaciones entre sistemas que no siempre están bien documentadas ni son fácilmente observables por otros mecanismos.

Objetivo: Incrementar la capacidad de la organización para detectar señales de compromiso, desviaciones respecto del comportamiento esperado e interacciones sospechosas dentro de la red, reduciendo el tiempo necesario para identificar incidentes y mejorando la comprensión de su alcance. En el ámbito industrial, su objetivo incluye también detectar alteraciones de comunicación, exploración de activos, movimiento lateral y usos improcedentes de protocolos o servicios que puedan afectar a la operación o a los sistemas OT.

Componentes de un NDR. Fuente: Trend Micro (n.d.)

Cómo funciona / cómo se implanta: Su implantación se basa en la recogida pasiva de tráfico o metadatos en puntos relevantes de la arquitectura, como perímetros, enlaces entre zonas, segmentos internos, entornos de DMZ o zonas de convergencia IT/OT. A partir de esa observación, el NDR analiza patrones de comunicación, relaciones entre activos, frecuencia de flujos, protocolos empleados, comportamientos habituales y desviaciones respecto de la normalidad esperada. En entornos industriales, su eficacia aumenta cuando se adapta a los protocolos y patrones propios de la red OT, cuando se integra con un inventario de activos y cuando permite contextualizar alertas según la

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

criticidad del sistema afectado y la función operativa implicada. Su valor no reside sólo en la generación de alertas, sino también en la posibilidad de apoyar investigaciones, convalidar hipótesis de incidente y aportar evidencia útil para respuesta y contención.

Ventajas:

- Mejora de forma significativa la visibilidad sobre la actividad real de la red.
- Permite detectar anomalías, movimiento lateral e interacciones no previstas entre activos.
- Resulta especialmente útil en entornos con baja visibilidad previa o alta complejidad de flujos.
- Aportación de contexto adicional sobre protocolos, relaciones entre sistemas y comportamiento habitual de la red.
- Complementa muy bien la segmentación, el firewall, los IDS/IPS y la monitorización OT.

Limitaciones y consideraciones:

- Su eficacia depende de la calidad de la captura, de la contextualización de los activos y de la afinación del entorno.
- Puede generar alertas poco accionables si no existe conocimiento suficiente de la arquitectura y de los flujos legítimos.
- En entornos industriales, el valor del análisis disminuye si no se tienen en cuenta protocolos específicos, dependencias operativas y patrones propios del proceso.
- No sustituye la segmentación, la gestión de accesos, la gestión de vulnerabilidades ni la respuesta ante incidentes.
- Requiere integración con procesos de análisis e investigación para convertir la visibilidad en capacidad real de detección y respuesta.

Relación con otros controles: Se relaciona con los IDS/IPS, el firewall, el NGFW/UTM, la segmentación de red y separación IT/OT, la DMZ industrial, la monitorización y operación de seguridad, con la visibilidad de activos y comunicaciones OT, la respuesta ante incidentes y con las medidas compensatorias orientadas a reforzar detección y contextualización del riesgo.

Casos habituales de uso: Se emplea para supervisar enlaces entre IT e OT, detectar movimiento lateral en redes industriales, observar protocolos y flujos entre activos críticos, reforzar la visibilidad en entornos con activos legados, apoyar investigaciones

tras alertas o incidentes y mejorar la detección temprana de comportamientos no habituales en redes complejas o poco documentadas.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el NDR es especialmente útil como medida compensatoria cuando no es viable reducir de inmediato toda la exposición arquitectónica, parchear activos sensibles o modificar la segmentación existente. En esos casos, permite añadir una capacidad de visibilidad y detección que ayuda a identificar comportamientos anómalos, priorizar investigaciones y mejorar la capacidad de respuesta mientras no se acometen medidas estructurales más profundas.

5.5.3 EDR

Categoría: Detección de amenazas y protección activa

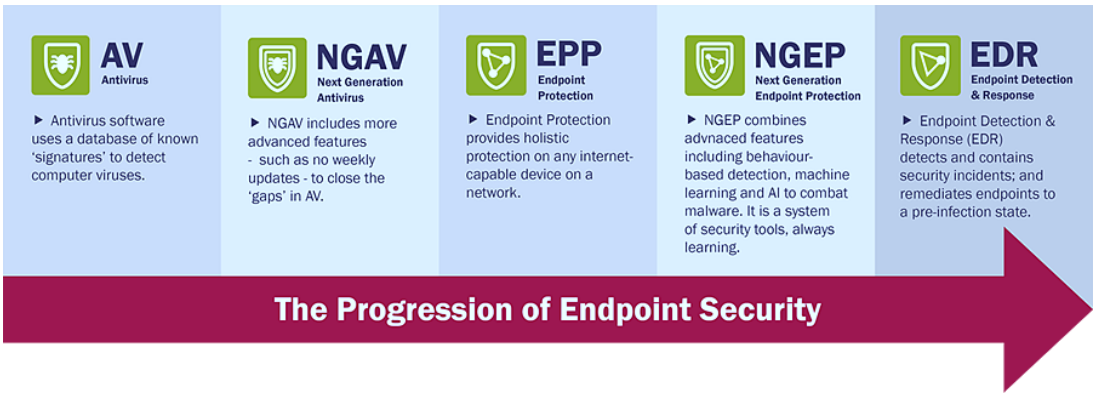
Tipología: Técnica / mixta

Función defensiva predominante: Detectiva

Función en NIST CSF: Detect, Respond

Descripción: El EDR (*Endpoint Detection and Response*) constituye un conjunto de capacidades orientadas a la supervisión continua, detección, investigación y respuesta sobre la actividad de los equipos finales, con el objetivo de identificar indicios de compromiso, comportamientos anómalos, ejecución de código malicioso, movimiento lateral, abuso de credenciales o manipulación de procesos y ficheros. A diferencia de los mecanismos más clásicos de protección de endpoint principalmente basados en firmas, el EDR aporta una capa más avanzada de telemetría, contexto y análisis sobre el comportamiento real de los dispositivos. En entornos industriales, su aplicabilidad depende del tipo de activo: puede resultar muy útil en estaciones de trabajo, portátiles de mantenimiento, servidores de apoyo, HMI o determinados sistemas Windows/Linux compatibles, aunque no siempre será viable o recomendable en controladores, sistemas muy sensibles o activos legados con restricciones estrictas.

Objetivo: Incrementar la capacidad de la organización para detectar e investigar actividad maliciosa o anómala en los equipos finales, mejorando la visibilidad sobre el comportamiento de los endpoints y permitiendo una respuesta más rápida y contextualizada. En el ámbito industrial, su objetivo incluye también reforzar la detección en activos con interacción directa o indirecta con el entorno OT, sin comprometer la disponibilidad ni la estabilidad de los sistemas más sensibles.



Avance histórico de las soluciones de protección de endpoint. Fuente: cyberone.security (n.d.)

Cómo funciona / cómo se implanta: Su implantación se basa normalmente en la instalación de un agente en el endpoint, capaz de recoger telemetría sobre procesos, ejecución, ficheros, conexiones, registro, actividad del usuario y otros eventos relevantes. Esa información se analiza localmente o en una plataforma centralizada para detectar patrones maliciosos, correlacionar eventos y apoyar tareas de investigación y respuesta. En entornos industriales, la implantación debe partir de una evaluación previa de compatibilidad e impacto, diferenciando con claridad entre activos en los que el uso de un agente es viable y beneficioso, y aquéllos en los que puede introducir riesgos de rendimiento, estabilidad, soporte o certificación. Su utilidad aumenta cuando se despliega en portátiles de mantenimiento, estaciones de ingeniería, HMI compatibles, servidores intermedios y otros sistemas con capacidad de ejecución generalista, integrándose con procedimientos de análisis, revisión de alertas y contención.

Ventajas:

- Mejora la visibilidad sobre el comportamiento real de los equipos finales.
- Permite detectar ejecuciones sospechosas, abuso de procesos, persistencia y movimiento lateral.
- Aportación de contexto útil para investigación, respuesta y aprendizaje tras incidentes.
- Resulta especialmente valioso en portátiles, estaciones de trabajo y servidores con mayor exposición.
- Complementa otros controles de red al aportar detección desde el propio endpoint.

Limitaciones y consideraciones:

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

- No todos los activos industriales admiten la instalación de agentes sin riesgo operativo.
- En entornos OT, la compatibilidad con el software de fabricante, el rendimiento y la estabilidad deben validarse previamente.
- Puede generar volumen elevado de telemetría y alertas si no existe capacidad suficiente de análisis.
- No sustituye al bastionado, la segmentación, la gestión de accesos ni la gestión de vulnerabilidades.
- Debe evitarse un despliegue indiscriminado en activos críticos sin revisión previa de impacto y soporte.

Relación con otros controles: Se relaciona con la protección del puesto de trabajo, la protección de endpoints industriales, el IDS/IPS, el NDR, la monitorización y operación de seguridad, la gestión de identidades y accesos, el hardening, la conexión segura de dispositivos externos y la respuesta ante incidentes. Funciona como capa de detección e investigación especialmente útil en activos con sistema operativo generalista y capacidad de ejecución avanzada.

Casos habituales de uso: Se emplea en portátiles de mantenimiento, estaciones de ingeniería, HMI compatibles, servidores de apoyo a la operación, servidores de salto, equipos corporativos con acceso a entornos OT, terminales con acceso remoto y activos en los que se necesita reforzar la detección de comportamiento malicioso sin depender exclusivamente de la red.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el EDR puede actuar como medida compensatoria útil cuando no es viable modificar de inmediato la arquitectura, reducir toda la exposición existente o aplicar ciertas actualizaciones, siempre que el activo sea compatible y el impacto esté validado. Su utilidad es especialmente alta en portátiles y estaciones de ingeniería, donde un compromiso puede servir como puente entre dominios corporativos, terceros y sistemas OT. Con todo, en activos críticos o muy restringidos, pueden ser preferibles enfoques complementarios de segmentación, monitorización pasiva y bastionado antes que un despliegue directo del agente.

5.5.4 CPS PP

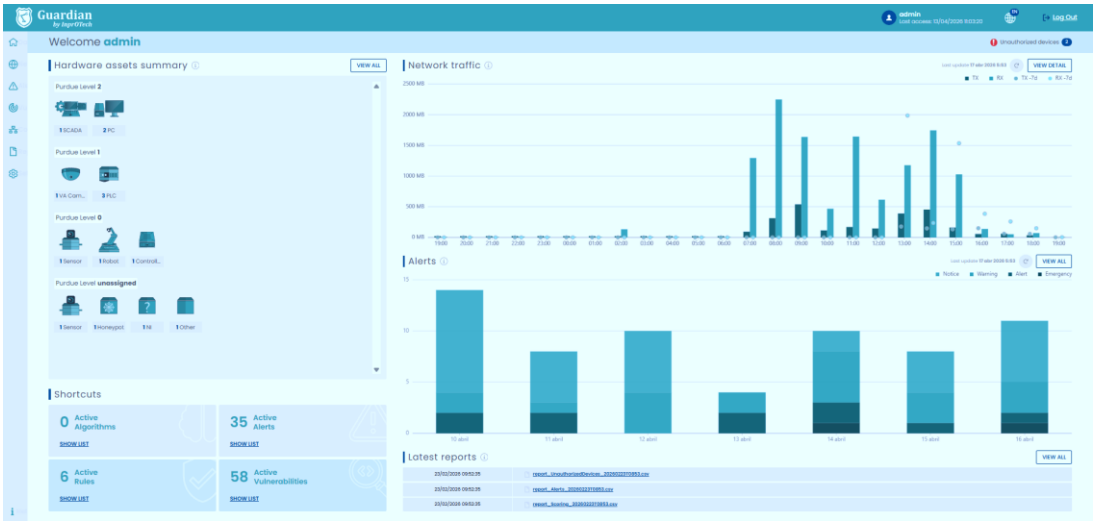
Categoría: Detección de amenazas y protección activa

Tipología: Técnica / mixta

Función defensiva predominante: Detectiva

Función en NIST CSF: Identify, Detect, Protect, Respond

Descripción: Las plataformas de protección de sistemas ciberfísicos (CPS PP, *Cyber-Physical Systems Protection Platform* según el término acuñado por Gartner) son soluciones orientadas a observar, correlacionar y contextualizar información procedente tanto de la capa digital como del comportamiento físico del proceso, a fin de identificar desviaciones, condiciones anómalas o señales de compromiso que podrían no ser visibles desde una monitorización puramente IT o puramente OT. Su lógica consiste en combinar datos de red, activos, protocolos, señales de proceso, estados operativos, telemetría industrial y reglas de comportamiento esperado para ofrecer una visión más amplia del riesgo real sobre sistemas ciberfísicos. En entornos industriales, este control resulta especialmente valioso cuando la detección debe ir más allá de la comunicación de red e incorporar también el contexto funcional del proceso.



Ejemplo de solución CPS PP. Fuente: InprOTech.es (2026)

Objetivo: Incrementar la capacidad de la organización para ganar visibilidad (inventario) detectar alteraciones o amenazas (anomalías o vulnerabilidades) que puedan afectar a la operación física, a la integridad del proceso o a la seguridad de los sistemas ciberfísicos, combinando señales técnicas y operativas en una misma capa de análisis, o incluso aportando capacidades de respuesta. En el ámbito industrial, su objetivo incluye también reducir el riesgo de que una actividad aparentemente legítima desde el punto de vista digital pase inadvertida a pesar de estar produciendo efectos anómalos sobre el proceso, los equipos o las condiciones de operación.

Cómo funciona / cómo se implanta: Su implantación se basa en la recogida y correlación de datos procedentes de múltiples fuentes: tráfico de red, inventario de

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

activos, protocolos industriales, estados de control, variables de proceso, eventos de sistemas, telemetría de sensores, señales de supervisión y, cuando procede, integración con sistemas de operación o gestión. A partir de esa información, la plataforma construye una visión del inventario, mapa de red, comportamiento esperado y detecta desviaciones, inconsistencias, vulnerabilidades, y condiciones anómalas o patrones sospechosos que pueden apuntar a un fallo, a un uso indebido o a un incidente de seguridad. En entornos industriales, su utilidad depende de que se conozca bien el proceso, de que la plataforma esté adaptada a los protocolos y activos presentes, y de que exista capacidad para interpretar correctamente la diferencia entre una anomalía técnica, una variación operativa legítima y un incidente potencialmente malicioso.

Ventajas:

- Mejora la detección integrando contexto digital y comportamiento físico del proceso.
- Permite identificar dispositivos, vulnerabilidades, mapa de red, problemas de segmentación, y desviaciones que pueden no ser visibles con controles basados sólo en red o endpoint.
- Aportación de mayor contexto para investigar incidentes con impacto operativo.
- Resulta especialmente útil en entornos críticos con fuerte dependencia del comportamiento físico del proceso.
- Complementa otras capacidades de detección aportando una visión más cercana al riesgo real sobre la operación, y ocasionalmente ofreciendo mecanismos de engaño (honeypots).
- En algunos casos, permiten respuesta activa automática (bloqueo de tráfico malicioso).

Limitaciones y consideraciones:

- Su eficacia depende de la calidad y cobertura de las fuentes de datos integradas.
- Puede requerir conocimiento avanzado del proceso para interpretar correctamente alertas y desviaciones.
- En entornos industriales, una mala contextualización puede generar falsos positivos o lectura incorrecta de variaciones operativas normales.
- No sustituye la segmentación, la gestión de accesos, ni la protección básica de la arquitectura.

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

- Requiere integración con las áreas de operación, mantenimiento y seguridad para convertir la detección en respuesta útil.

Relación con otros controles: Se relaciona con el IDS/IPS, con el NDR, con la monitorización ciberfísica / MES, con la visibilidad de activos y comunicaciones OT, con la monitorización y operación de seguridad, con la respuesta ante incidentes y con las medidas compensatorias orientadas a reforzar detección y contextualización del riesgo sobre sistemas críticos.

Casos habituales de uso: Se emplea en entornos industriales que requieren controles exigidos por normativa, ganar visibilidad o dotarse de detección de anomalías y correlación de la actividad de red con el comportamiento del proceso, detectar desviaciones en señales o estados operativos, supervisar sistemas ciberfísicos críticos, apoyar investigaciones sobre incidentes con impacto potencial en la operación y reforzar la detección en instalaciones con alta criticidad, automatización avanzada o fuerte dependencia de variables físicas.

Observaciones / medidas compensatorias asociadas: En entornos industriales, las plataformas CPS PP pueden actuar como medida compensatoria especialmente útil cuando no es viable reducir de inmediato toda la exposición de la arquitectura o actualizar determinados activos, ya que aportan una capa adicional de observación centrada en el comportamiento real del sistema ciberfísico. Su utilidad aumenta cuando se combinan con segmentación, visibilidad OT, procedimientos de respuesta y conocimiento operativo suficiente para interpretar correctamente las anomalías detectadas.

5.5.5 Detección de integridad de ficheros

Categoría: Detección de amenazas y protección activa

Tipología: Técnica / mixta

Función defensiva predominante: Detectiva

Función en NIST CSF: Detect, Respond

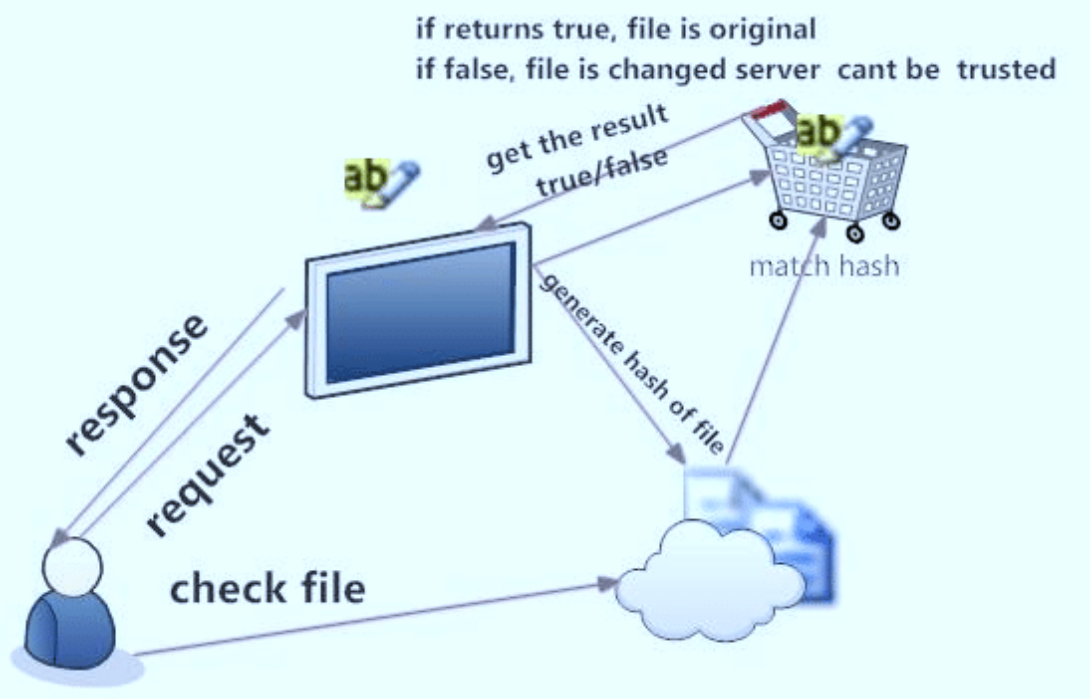
Descripción: La detección de integridad de ficheros es un control orientado a identificar cambios no autorizados, inesperados o anómalos en ficheros, configuraciones, ejecutables, librerías, registros o componentes críticos de un sistema. Su lógica se basa en establecer una referencia conocida del estado esperado de determinados elementos y supervisar posteriormente cualquier modificación que pueda indicar manipulación, persistencia maliciosa, error operativo, instalación no controlada de software o

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

alteración indebida de parámetros. En entornos industriales, este control resulta especialmente útil en sistemas en los que la estabilidad y la previsibilidad son fundamentales, como HMI, estaciones de ingeniería, servidores de apoyo, sistemas de supervisión u otros activos con componentes críticos cuyo cambio debería estar estrictamente controlado.

Objetivo: Detectar modificaciones no autorizadas en componentes clave del entorno tecnológico, mejorando la capacidad de la organización para identificar manipulaciones, compromisos, cambios no aprobados o desviaciones respecto al estado esperado de los sistemas. En el ámbito industrial, su objetivo incluye también proteger configuraciones, proyectos, ficheros de operación y componentes software cuyo cambio puede tener impacto directo sobre la disponibilidad, la integridad del proceso o la fiabilidad de la operación.

Cómo funciona / cómo se implanta: Su implantación suele partir de la identificación de los ficheros, directorios, configuraciones o componentes que deben considerarse sensibles o críticos. Una vez definida esa base, se establece un estado de referencia mediante sumas de verificación, registros de versión, políticas de cambio u otros mecanismos equivalentes. A partir de ese momento, el sistema supervisa modificaciones y genera alertas cuando detecta cambios no previstos o discrepancias respecto del estado autorizado. En entornos industriales, su aplicación debe centrarse especialmente en activos en los que el comportamiento sea relativamente estable y los cambios deban estar documentados, como estaciones de ingeniería, HMI, servidores de supervisión, repositorios de configuración, proyectos de automatización o sistemas de apoyo a la operación. Su utilidad aumenta cuando se integra con procedimientos formales de cambio, bastionado, registro de intervenciones y análisis de alertas.



Mecanismo de verificación de integridad de ficheros. Fuente: Sharma, Rajani & Kumar, Rajender (2014)

Ventajas:

- Permite detectar manipulaciones o cambios no autorizados en componentes críticos.
- Mejora la trazabilidad sobre modificaciones en sistemas estables o sensibles.
- Resulta útil para identificar persistencia maliciosa, alteraciones de configuración o errores de operación.
- Refuerza el control sobre activos en los que los cambios deben ser escasos y bien documentados.
- Complementa la monitorización de red y de endpoint con una visión centrada en el estado interno de los sistemas.

Limitaciones y consideraciones:

- Su eficacia depende de la correcta definición del estado de referencia (y el almacenamiento seguro del mismo) y de los elementos a supervisar.
- Puede generar ruido si se aplica a sistemas con cambios frecuentes o poco gobernados.
- En entornos industriales, debe coordinarse con los procedimientos de mantenimiento y actualización para evitar falsos positivos constantes.
- No sustituye al bastionado, el control de accesos ni la gestión formal de cambios.

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

- Se requiere capacidad de análisis para diferenciar entre modificaciones autorizadas, errores operativos e incidentes reales.

Relación con otros controles: Se relaciona con el EDR, con el bastionado de HMI y sistemas de ingeniería, con la gestión de cambios, con la monitorización y operación de seguridad, con la respuesta ante incidentes, con las copias de seguridad y restauración y con las medidas compensatorias orientadas a reforzar el control sobre activos sensibles o con soporte limitado.

Casos habituales de uso: Se utiliza para supervisar HMI, estaciones de ingeniería, servidores de supervisión, proyectos de automatización, configuraciones críticas, ejecutables de aplicaciones industriales, ficheros de sistema, repositorios de recetas y otros componentes en los que cualquier cambio no autorizado pueda tener impacto relevante sobre la operación o la seguridad.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la detección de integridad de ficheros resulta especialmente útil como medida compensatoria cuando no es viable actualizar de inmediato determinados sistemas o reducir la exposición de ciertos activos, ya que permite añadir una capa adicional de vigilancia sobre componentes críticos. Su utilidad aumenta cuando se combina con procedimientos de cambio estrictos, bastionado, registro de intervenciones, copias de seguridad convalidadas y análisis rápido de las alertas generadas.

5.5.6 DLP

Categoría: Detección de amenazas y protección activa

Tipología: Técnica / mixta

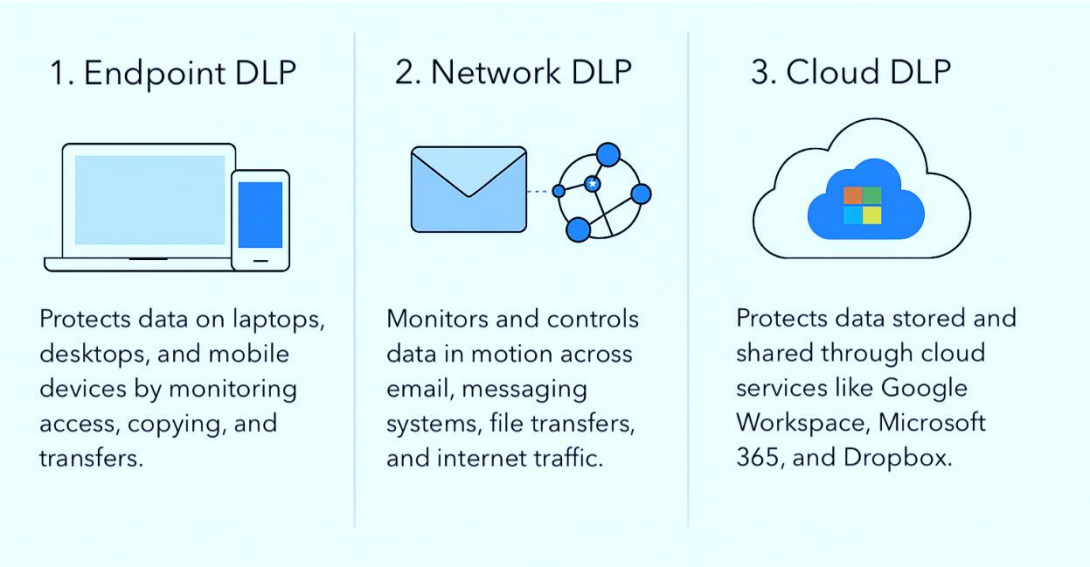
Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: El DLP (*Data Loss Prevention* o prevención de fugas de datos) es un conjunto de capacidades orientadas a identificar, supervisar y limitar la salida, copia, transferencia o uso no autorizado de información sensible. Su finalidad es evitar que datos críticos abandonen la organización por canales no previstos, sin control suficiente o en contextos de riesgo. En entornos industriales, este control no se limita a la protección de información corporativa convencional, sino que puede abarcar también proyectos de automatización, configuraciones de sistemas, recetas, parámetros de proceso, documentación técnica, credenciales, registros operativos y otro conocimiento

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

sensible con impacto sobre la continuidad, la propiedad intelectual o la seguridad de la operación.



Tipos de DLP. Fuente: Lakera (2025)

Objetivo: Reducir el riesgo de exfiltración, copia indebida, transferencia no autorizada o exposición accidental de información sensible, reforzando el control sobre los cauces de salida y los usos permitidos de los datos. En el ámbito industrial, su objetivo incluye también proteger información técnica y operativa que, aun sin ser siempre visible desde una perspectiva puramente corporativa, puede resultar crítica para la continuidad del negocio, la competitividad o la seguridad del proceso.

Cómo funciona / cómo se implanta: Su implantación parte de la identificación de los tipos de información que deben considerarse sensibles, de los canales por los que pueden circular y de los escenarios en los que existe mayor riesgo de pérdida, exfiltración o uso indebido. A partir de esa base, pueden aplicarse políticas de supervisión, clasificación, bloqueo, alerta o restricción sobre correo electrónico, navegación, servicios cloud, impresión, copia a dispositivos externos, movimiento de ficheros, transferencia entre sistemas o acceso desde determinados perfiles. En entornos industriales, el DLP debe configurarse con especial criterio, evitando un enfoque excesivamente genérico y centrando la protección en la información que realmente tiene valor operativo o técnico: proyectos de ingeniería, configuraciones de control, recetas, documentación de fabricante, credenciales, exportación de datos históricos o ficheros empleados en mantenimiento e integración. Su utilidad aumenta cuando se integra con gestión de identidades, clasificación de la información, protección de endpoints y procedimientos operativos claros sobre uso y transferencia de datos.

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

Ventajas:

- Ayuda a limitar la fuga o transferencia no autorizada de información sensible.
- Mejora la visibilidad sobre los canales de salida y los patrones de uso de los datos.
- Resulta útil para proteger propiedad intelectual, documentación técnica e información operativa crítica.
- Complementa otros controles de acceso, monitorización y protección de endpoint.
- Puede reforzar la trazabilidad y el control sobre soportes externos, correo, cloud y movimiento de ficheros.

Limitaciones y consideraciones:

- Su eficacia depende de identificar correctamente que información debe protegerse y por qué canales puede salir.
- Puede generar ruido o fricción operativa si las políticas son demasiado amplias o poco contextualizadas.
- En entornos industriales, una mala definición del alcance puede dejar fuera información técnica crítica o, por el contrario, bloquear flujos necesarios para operación y mantenimiento.
- No sustituye la clasificación de la información, la gestión de accesos ni los procedimientos de uso seguro de los datos.
- Requiere revisión periódica para adaptarse a cambios en procesos, aplicaciones, servicios cloud, terceras partes y necesidades de intercambio de información.

Relación con otros controles: Se relaciona con la seguridad en el mail, la protección del puesto de trabajo, la protección de endpoints industriales, la conexión segura de dispositivos externos, la gestión de identidades y accesos, el CASB / SASE, la monitorización y operación de seguridad y los procedimientos operativos orientados a uso seguro de la información sensible.

Casos habituales de uso: Se emplea para controlar la salida de documentación técnica, proyectos de automatización, recetas, exportación de datos históricos, envío de ficheros por correo, copia a dispositivos USB, uso de servicios cloud, transferencia de información a terceros y escenarios en los que existe riesgo de fuga de conocimiento técnico u operativo con valor crítico para la organización.

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

Observaciones / medidas compensatorias asociadas: En entornos industriales, el DLP resulta especialmente útil cuando la organización maneja información técnica sensible con fuerte impacto sobre operación, propiedad intelectual o seguridad del proceso. También puede actuar como medida compensatoria parcial cuando no es viable restringir de inmediato todos los canales de intercambio con terceros, siempre que se combine con clasificación de la información, control de accesos, revisión de excepciones y procedimientos claros sobre uso y transferencia de datos.

5.5.7 Honeypots

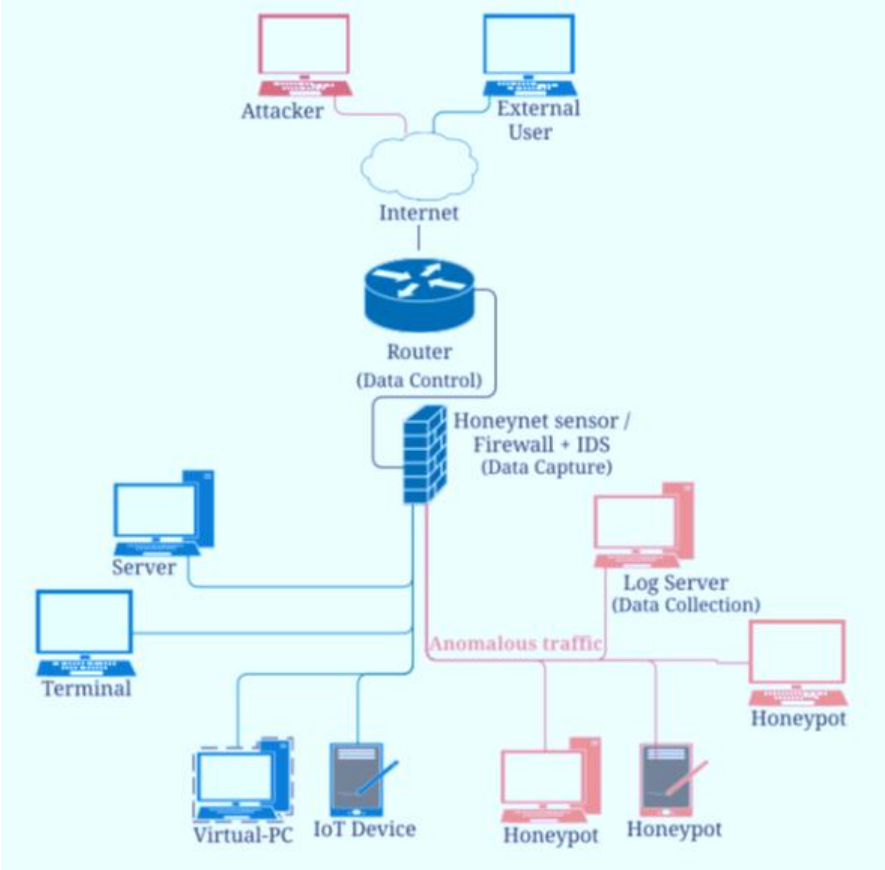
Categoría: Detección de amenazas y protección activa

Tipología: Técnica / mixta

Función defensiva predominante: Detectiva

Función en NIST CSF: Detect

Descripción: Los honeypots son sistemas, servicios o componentes deliberadamente preparados para simular activos atractivos para un atacante, con el objetivo de observar, detectar y analizar interacciones maliciosas o no autorizadas. Su lógica consiste en crear puntos controlados de cebo para cibercriminales que no deberían recibir actividad legítima, por lo que cualquier conexión, intento de autenticación, exploración, ejecución de comandos o manipulación puede interpretarse como indicio de comportamiento sospechoso. En entornos industriales, los honeypots pueden diseñarse para representar activos, protocolos o servicios próximos a la realidad OT, permitiendo identificar exploración de red, actividad automatizada, movimiento lateral, uso indebido de protocolos industriales o tentativas de acceso no previstas.



Ejemplo de ubicación de honeypot en una red OT. Fuente: InprOTech (2025)

Objetivo: Mejorar la capacidad de detección temprana de actividad maliciosa, obteniendo señales de alerta de alta relevancia e información útil para análisis, investigación y mejora de la protección. En el ámbito industrial, su objetivo incluye también captar interacciones anómalas dirigidas a entornos OT o a servicios ciberfísicos, reforzando la visibilidad sobre amenazas que podrían pasar desapercibidas en otras capas de monitorización.

Cómo funciona / cómo se implanta: Su implantación se basa en la colocación de sistemas cebo en puntos seleccionados de la arquitectura, configurados para aparentar ser activos o servicios de interés sin formar parte de la operación real. Estos componentes pueden simular desde servicios sencillos de red hasta protocolos industriales, interfaces de control, dispositivos aparentes o entornos más elaborados según el nivel de realismo buscado. En entornos industriales, su eficacia depende de que estén bien situados, de que resulten creíbles en el contexto de la red y de que su presencia no interfiera con el proceso ni genere confusión operativa. El valor del honeypot aumenta cuando la información recogida se integra con los procesos de análisis, con el SOC, con la inteligencia de amenazas y con los mecanismos de respuesta, permitiendo contextualizar mejor los intentos detectados.

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

Ventajas:

- Aportan señales de alerta de alta calidad, ya que no deberían recibir tráfico legítimo.
- Resultan útiles para detectar exploración, movimiento lateral y actividad automatizada.
- Permiten obtener información valiosa sobre patrones de ataque y comportamiento adversario.
- Complementan la monitorización tradicional con puntos de observación específicos.
- Pueden ser especialmente útiles en entornos OT para captar interacciones indebidas sobre protocolos o servicios aparentes.

Limitaciones y consideraciones:

- Su valor depende del diseño, de la localización y del realismo del cebo.
- No sustituyen la segmentación, la gestión de accesos, la monitorización general ni la respuesta ante incidentes.
- En entornos industriales, deben desplegarse con cuidado para evitar cualquier interferencia con la operación real.
- Un honeypot mal integrado puede generar poco valor o quedar aislado del proceso de análisis y respuesta.
- Requieren mantenimiento, revisión y una interpretación adecuada de los eventos registrados.

Relación con otros controles: Se relaciona con los IDS/IPS, el NDR, el CPS PP, la monitorización y operación de seguridad, la inteligencia de amenazas, la respuesta ante incidentes, la segmentación de red y separación IT/OT y con las medidas compensatorias orientadas a reforzar la detección en entornos con exposición elevada.

Casos habituales de uso: Se emplean para detectar exploración de red en segmentos sensibles, actividad no autorizada en entornos industriales, movimiento lateral en zonas OT, interacciones indebidas con protocolos aparentes, tentativas de acceso a servicios simulados y recogida de información sobre comportamiento adversario en redes con baja visibilidad previa.

Observaciones / medidas compensatorias asociadas: En entornos industriales, los honeypots pueden actuar como medida compensatoria útil cuando no es viable reducir

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

de inmediato toda la exposición de un segmento, actualizar ciertos activos o reforzar estructuralmente la arquitectura, ya que añaden una capa adicional de detección y observación. Su utilidad aumenta cuando se combinan con segmentación, visibilidad OT, monitorización continua y procedimientos claros de análisis y escalado de las alertas generadas.

5.5.8 AntiDDoS

Categoría: Detección de amenazas y protección activa

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

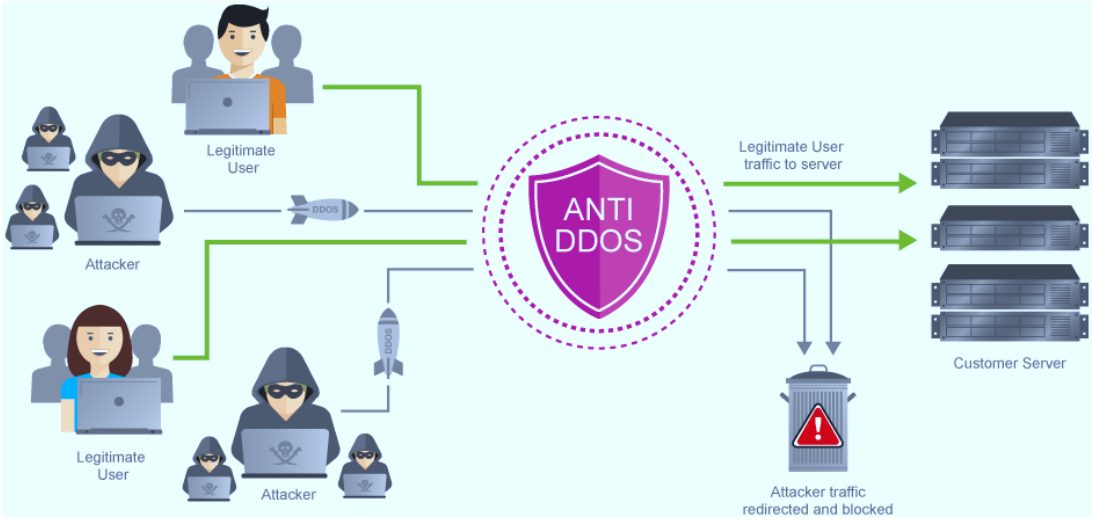
Descripción: Las capacidades AntiDDoS están orientadas a detectar, absorber, filtrar o mitigar ataques de denegación de servicio distribuida (*Distributed Denial of Service*), en los que un volumen elevado de solicitudes o tráfico malicioso intenta degradar, interrumpir o saturar un servicio, una aplicación, una conexión o una infraestructura expuesta. Su propósito es preservar la disponibilidad de los recursos críticos frente a campañas que buscan agotar capacidad de red, procesamiento o atención de sesiones. En entornos industriales, su relevancia tiende a concentrarse en servicios publicados, portales web, accesos remotos, componentes en DMZ, plataformas de gestión expuestas o canales de comunicación esenciales que, sin ser necesariamente activos OT puros, pueden tener impacto indirecto o directo sobre la operación si quedan indisponibles.

Objetivo: Reducir el riesgo de interrupción o degradación de servicios por ataques de denegación de servicio, manteniendo la disponibilidad de recursos críticos y limitando el impacto operativo, reputacional o funcional derivado de la saturación maliciosa de las comunicaciones. En el ámbito industrial, su objetivo incluye también asegurar que los servicios de acceso, supervisión, integración o soporte que dependen de conectividad externa no se conviertan en un apartado único de fallo explotable mediante volumen de tráfico.

Cómo funciona / cómo se implanta: Su implantación puede basarse en distintos mecanismos, según el tipo de servicio protegido y el nivel de exposición: filtrado local, capacidad de absorción en perímetro o en la red del proveedor de comunicaciones, servicios de mitigación en nube, redirección de tráfico, detección de patrones de saturación, limitación de tasa, listas de reputación o combinación de estas medidas. En entornos industriales, su utilidad suele centrarse en la protección de portales,

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

aplicaciones web, servicios de acceso remoto, componentes en DMZ o recursos publicados que dan soporte a la operación o a la relación con terceros. Su eficacia depende de la correcta identificación de los servicios críticos, de la comprensión del tráfico legítimo esperado y de la integración con otros controles perimetrales y de continuidad. En contextos OT, no suele aplicarse tanto a la red de control interna como a los puntos de exposición externa o a las dependencias digitales que pueden afectar a la operación si resultan interrumpidas.



Esquema AntiDDoS en la red. Fuente: Cloud4u.com (n.d.)

Ventajas:

- Ayuda a preservar la disponibilidad de servicios expuestos frente a la saturación maliciosa.
- Reduce el impacto de campañas de interrupción basadas en volumen o consumo de recursos.
- Refuerza la resiliencia de portales, servicios remotos y componentes publicados.
- Complementa otros controles perimetrales y de continuidad.
- Resulta especialmente útil en organizaciones con servicios accesibles desde Internet o con alta dependencia de conectividad externa.

Limitaciones y consideraciones:

- Su utilidad es menor si la organización no dispone de servicios expuestos o dependencias externas relevantes.
- No sustituye la necesidad de segmentación, arquitectura resiliente, balanceo ni continuidad de negocio.

- En entornos industriales, debe evitarse identificar AntiDDoS como control principal de la red OT cuando el riesgo real se concentra en otros vectores.
- Puede requerir coordinación con proveedores de conectividad, publicación o mitigación externa.
- La eficacia depende de conocer bien el patrón normal del servicio y de validar que las medidas de filtrado no afecten a tráfico legítimo crítico.

Relación con otros controles: Se relaciona con el firewall, el NGFW/UTM, la DMZ industrial, el WAF, el proxy, el acceso remoto seguro, la continuidad de negocio y resiliencia operativa, la monitorización y operación de seguridad y con los procedimientos de respuesta ante incidentes e indisponibilidad.

Casos habituales de uso: Se emplea en la protección de portales corporativos o técnicos, servicios web publicados, interfaces de acceso remoto, componentes en DMZ, servicios de integración expuestos, recursos accesibles desde Internet y escenarios en los que la indisponibilidad de un servicio publicado puede afectar a la gestión, la coordinación o al soporte de la operación industrial.

Observaciones / medidas compensatorias asociadas: en entornos industriales, AntiDDoS resulta especialmente útil cuando existen dependencias claras de servicios publicados o conectividad externa necesaria para operación, mantenimiento o integración. También puede actuar como medida compensatoria complementaria cuando no es posible eliminar la exposición de determinados servicios, siempre que se combine con segmentación, DMZ, WAF, continuidad operativa y mecanismos de respuesta ante interrupciones.

5.5.9 Threat hunting

Categoría: Detección de amenazas y protección activa

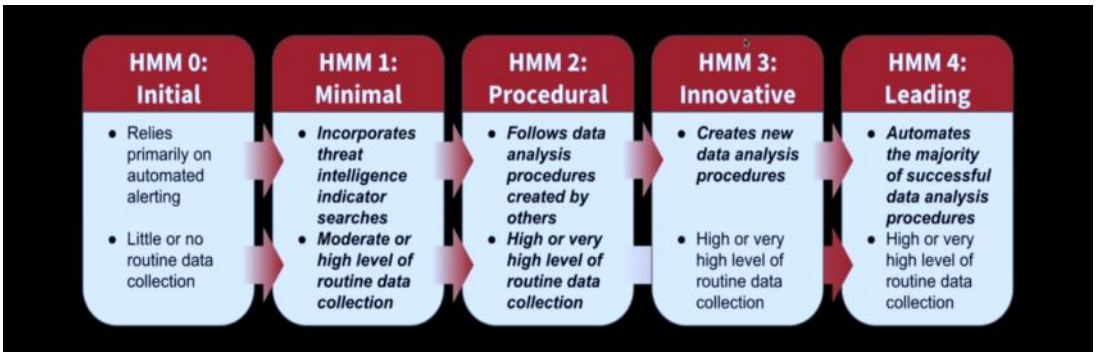
Tipología: Técnica / mixta

Función defensiva predominante: Detectiva

Función en NIST CSF: Detect

Descripción: El *threat hunting* o caza de amenazas es una actividad proactiva de búsqueda, análisis e investigación orientada a identificar indicios de compromiso, comportamientos anómalos o presencia adversaria que no han sido detectados automáticamente por los mecanismos convencionales de seguridad. A diferencia de la monitorización reactiva basada en alertas generadas por reglas, firmas o eventos previamente clasificados, el *threat hunting* parte de hipótesis, señales débiles, patrones

sospechosos o conocimiento sobre tácticas y técnicas adversarias para buscar evidencias de actividad maliciosa oculta o insuficientemente contextualizada. En entornos industriales, esta capacidad resulta especialmente valiosa cuando la organización necesita ir más allá de la detección básica y contrastar si existen movimientos laterales, uso indebido de credenciales, interacciones anómalas entre activos o comportamientos discretos con potencial impacto operativo.



Modelo de madurez de la caza de amenazas. Fuente: SANS Institute (n.d.)

Objetivo:

Incrementar la capacidad de la organización para descubrir amenazas que no han sido identificadas por mecanismos automáticos o que permanecen ocultas entre el ruido operativo del entorno, reduciendo el tiempo de permanencia de un adversario y mejorando la comprensión del alcance real de un posible compromiso. En el ámbito industrial, su objetivo incluye también detectar señales precoces de actividad maliciosa en entornos en los que la disponibilidad y la estabilidad limitan la aplicación de medidas más intrusivas y en los que determinados patrones pueden confundirse con operación legítima si no se contextualizan adecuadamente.

Cómo funciona / cómo se implanta:

Su implantación requiere disponer de fuentes de información suficientes sobre el entorno, como registros, telemetría de red, eventos de seguridad, información de activos, contexto operativo, datos de endpoints compatibles y visibilidad sobre comunicaciones IT/OT. A partir de esa base, los analistas formulan hipótesis de búsqueda —por ejemplo, abuso de credenciales, movimiento lateral, interacciones anómalas con protocolos industriales, uso indebido de acceso remoto o persistencia en sistemas intermedios— y contrastan esas hipótesis mediante consultas, correlación de eventos, revisión de patrones e investigación manual o asistida. En entornos industriales, el valor del *threat hunting* aumenta cuando se integra con conocimiento del proceso, inventario de activos, NDR, IDS/IPS, visibilidad OT y procedimientos de

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

respuesta, ya que muchas de las investigaciones dependen de distinguir entre una variación operativa legítima y una actividad potencialmente maliciosa.

Ventajas:

- Permite descubrir amenazas o comportamientos maliciosos que no generan alertas automáticas claras.
- Reduce la dependencia exclusiva de firmas, reglas estáticas o detección reactiva.
- Mejora la comprensión del comportamiento adversario y del alcance de un posible compromiso.
- Resulta útil para contrastar hipótesis, investigar señales débiles y convalidar sospechas en entornos complejos.
- Complementa la monitorización convencional con un enfoque más contextual y proactivo.

Limitaciones y consideraciones:

- Se requiere visibilidad suficiente, fuentes de datos de calidad y capacidad analítica especializada.
- Su valor es limitado si el entorno carece de registros, contextualización de activos o procesos maduros de investigación.
- En entornos industriales, puede resultar difícil interpretar ciertos patrones sin conocimiento operativo y del proceso.
- No sustituye la monitorización, la segmentación, la gestión de accesos ni los procedimientos de respuesta.
- Debe evitarse formular el *threat hunting* como actividad aislada y puntual, sin integración con los procesos de operación de seguridad y mejora continua.

Relación con otros controles: Se relaciona con el IDS/IPS, con el NDR, con el EDR, con el CPS PP, con la monitorización y operación de seguridad, con la visibilidad de activos y comunicaciones OT, con la inteligencia de amenazas, con la respuesta ante incidentes y con las medidas compensatorias orientadas a reforzar la capacidad de detección en entornos con alta exposición o baja visibilidad histórica.

Casos habituales de uso: Se emplea para investigar señales de acceso remoto sospechoso, movimiento lateral entre dominios IT/OT, uso anómalo de credenciales, exploración discreta de activos industriales, comportamiento extraño en servidores intermedios, persistencia en estaciones de ingeniería o HMI compatibles, y escenarios

en los que la organización sospecha de la existencia de compromiso sin disponer de una alerta concluyente.

Observaciones / medidas compensatorias asociadas: En entornos industriales, *el threat hunting* resulta especialmente útil como medida complementaria cuando no es viable reforzar de inmediato toda la arquitectura, reducir toda la exposición existente o desplegar controles más intrusivos sobre ciertos activos. Su utilidad aumenta cuando se apoya en buena visibilidad de red y activos, conocimiento operativo suficiente y procedimientos claros para escalar, investigar y responder a las evidencias detectadas.

5.6 Monitorización, visibilidad y operación de seguridad

La visibilidad es una condición indispensable para gestionar el riesgo de forma eficaz en entornos industriales complejos e interconectados. Esta subsección contempla **capacidades orientadas a la recogida, correlación y análisis de eventos, a la supervisión continua de la actividad y a la operación diaria de la seguridad**, con el objetivo de mejorar la capacidad de detección, investigación y toma de decisiones tanto en IT como en OT.

5.6.1 SIEM

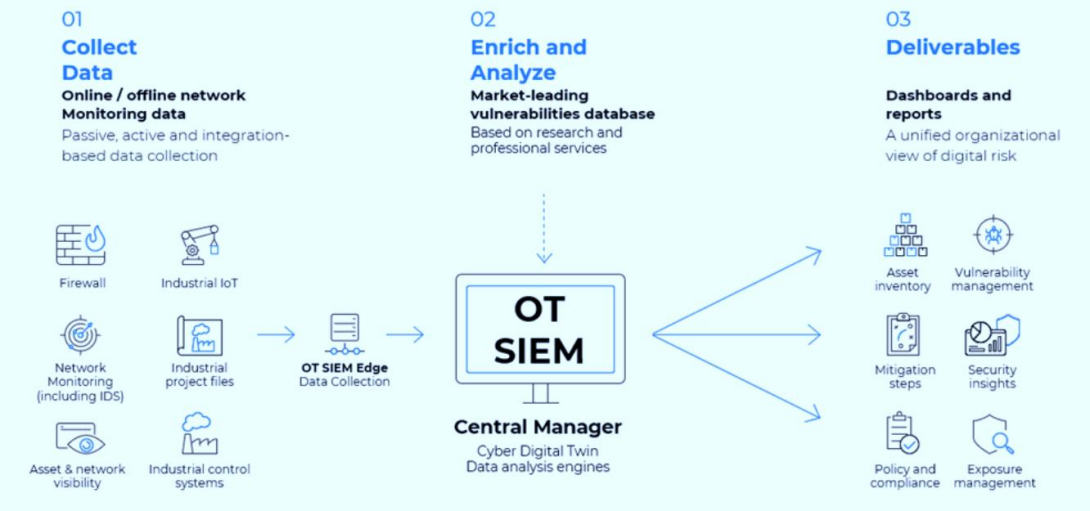
Categoría: Monitorización, visibilidad y operación de seguridad

Tipología: Técnica / mixta

Función defensiva predominante: Detectiva

Función en NIST CSF: Detect

Descripción: El SIEM (*Security Information and Event Management*) es una plataforma orientada a la recogida, normalización, correlación, análisis y conservación de eventos de seguridad procedentes de múltiples fuentes, con el objetivo de mejorar la visibilidad global del entorno y facilitar la detección temprana de incidentes. Su utilidad reside en unificar en un mismo plano de observación registros, alertas y eventos generados por sistemas, redes, aplicaciones, dispositivos de seguridad y, cuando procede, componentes OT, permitiendo analizar relaciones que no serían visibles si cada fuente se hubiera observado de manera aislada. En entornos industriales, el SIEM resulta especialmente valioso cuando la organización necesita correlacionar señales procedentes de dominios IT y OT, contextualizar alertas y apoyar la investigación de incidentes con impacto potencial sobre la operación.



Ejemplo de funcionamiento de SIEM OT. Fuente: Accura.io (n.d.)

Objetivo: Incrementar la capacidad de la organización para detectar, correlacionar e investigar eventos de seguridad a partir de una visión centralizada y estructurada de la telemetría disponible. En el ámbito industrial, su objetivo incluye también integrar señales procedentes de entornos corporativos y operativos para identificar patrones de riesgo, conexiones indebidas, acceso anómalo, propagación entre dominios o comportamientos que puedan afectar a la continuidad y a la seguridad del proceso.

Cómo funciona / cómo se implanta: Su implantación se basa en la conexión progresiva de fuentes de eventos al sistema: firewalls, sistemas de autenticación, servidores, endpoints, aplicaciones, sistemas de correo, mecanismos de acceso remoto, componentes de red, sensores de seguridad y, cuando el contexto lo permite, activos o plataformas de visibilidad OT. Una vez recibidos, los eventos se normalizan, se etiquetan y se analizan mediante reglas de correlación, casos de uso, búsquedas, paneles y alertas. En entornos industriales, su eficacia depende de seleccionar bien las fuentes relevantes, evitar una integración indiscriminada sin contexto y construir casos de uso adaptados al entorno, por ejemplo sobre accesos remotos, movimiento entre IT y OT, cambios no previstos, conexión de terceros, alertas de visibilidad OT o eventos de activos críticos. Su valor real no reside sólo en la acumulación de registros, sino en la capacidad de transformar esa información en detección accionable, contexto operativo y apoyo a la respuesta.

Ventajas:

- Centraliza la visibilidad de eventos procedentes de múltiples fuentes.
- Permite correlacionar señales que, observadas por separado, tendrían poco valor.

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

- Mejora la detección temprana y la investigación de incidentes.
- Refuerza la trazabilidad y la conservación de evidencias.
- Resulta especialmente útil para integrar visión IT/OT en organizaciones con entornos híbridos.

Limitaciones y consideraciones:

- Su valor es limitado si se concibe sólo como repositorio masivo de registros sin casos de uso ni análisis.
- Puede generar volumen elevado de eventos y alertas si no existe una selección adecuada de las fuentes y una correlación bien afinada.
- En entornos industriales, la integración de señales OT debe hacerse con criterio, evitando forzar fuentes poco útiles o mal contextualizadas.
- No sustituye la visibilidad de activos, la detección en red, la segmentación ni los procedimientos de respuesta.
- Se requiere madurez operativa para mantener reglas, revisar alertas, investigar eventos y actualizar casos de uso según la evolución del riesgo.

Relación con otros controles: Se relaciona con el SOC, con el MDR, con el IDS/IPS, con el NDR, con el EDR, con la visibilidad de activos y comunicaciones OT, con la monitorización ciberfísica, con la gestión de identidades y accesos, con el acceso remoto seguro, con la respuesta ante incidentes y con las medidas compensatorias orientadas a reforzar la detección y la trazabilidad.

Casos habituales de uso: Se emplea para correlacionar eventos de autenticación, accesos remotos, tráfico perimetral, alertas de red, actividad de endpoints, interacciones entre IT y OT, cambios no previstos en activos críticos, uso de cuentas privilegiadas, actividad de terceros y escenarios en los que se necesita una visión centralizada de la seguridad del entorno.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el SIEM resulta especialmente útil como capa compensatoria cuando no es viable reforzar de inmediato todos los controles preventivos o reducir toda la exposición existente, ya que permite mejorar la capacidad de detección, correlación e investigación. Su utilidad aumenta cuando se integra con fuentes OT significativas, con procedimientos claros de análisis y respuesta, y con un diseño de casos de uso adaptado a la realidad operativa de la organización.

5.6.2 SOC

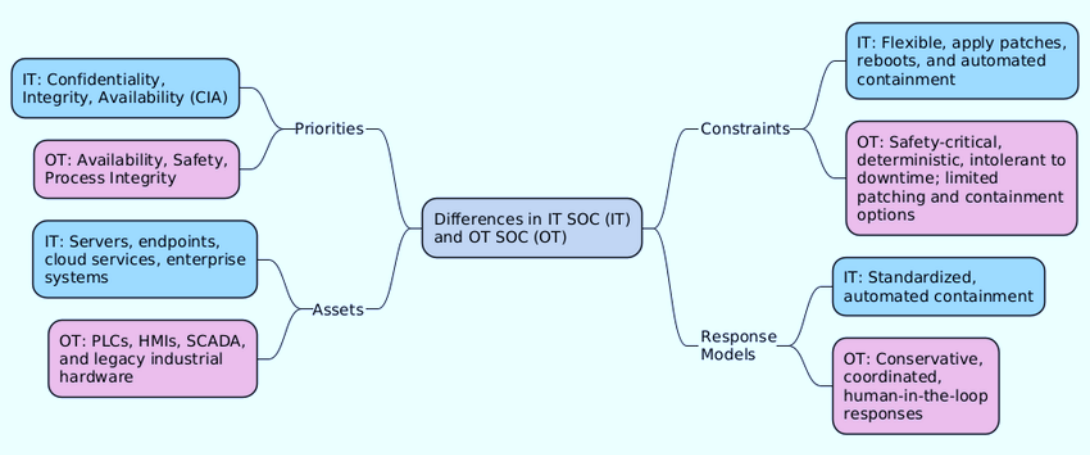
Categoría: Monitorización, visibilidad y operación de seguridad

Tipología: Organizativa / técnica / mixta

Función defensiva predominante: Detectiva

Función en NIST CSF: Detect, Respond

Descripción: El SOC (*Security Operations Center* o Centro de Operaciones de Seguridad) es la capacidad organizativa y operativa encargada de supervisar de manera continuada el entorno tecnológico, analizar alertas y eventos, investigar actividades sospechosas y coordinar la respuesta frente a incidentes de seguridad. No se limita a una plataforma concreta ni a un espacio físico determinado, sino que representa la combinación de personas, procedimientos, herramientas y flujos de trabajo necesarios para transformar la monitorización en capacidad real de detección y respuesta. En entornos industriales, el SOC adquiere especial relevancia cuando la organización precisa integrar señales procedentes de dominios IT y OT, interpretar el contexto operativo de las alertas y coordinar actuaciones sin comprometer la continuidad ni la seguridad del proceso.



Diferencias entre un SOC IT e OT. Fuente: Gnanasekaran, Grønbakk & Einar (2025)

Objetivo: Dotar a la organización de una capacidad estable y estructurada para detectar, analizar, priorizar, escalar y responder frente a incidentes de seguridad, reduciendo el tiempo de identificación, mejorando la calidad del análisis y facilitando la coordinación entre áreas implicadas. En el ámbito industrial, su objetivo incluye también asegurar que las alertas relacionadas con sistemas OT, acceso remoto, terceros, protocolos industriales o activos críticos sean tratadas con conocimiento suficiente de su impacto operativo.

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

Cómo funciona / cómo se implanta: Su implantación requiere definir un modelo operativo claro: fuentes de información, niveles de monitorización, roles y responsabilidades, procedimientos de análisis, escalado, comunicación y respuesta, así como herramientas de apoyo como SIEM, NDR, IDS/IPS, visibilidad OT, gestión de casos o plataformas de inteligencia. El SOC puede ser interno, externo o híbrido, y adaptarse a la dimensión y madurez de la organización. En entornos industriales, su eficacia depende no sólo de las herramientas disponibles, sino de la capacidad para integrar conocimiento de operación, mantenimiento, arquitectura IT/OT, activos críticos, protocolos industriales y dependencia de terceros. Resulta especialmente importante definir casos de uso específicos para el entorno industrial, canales de escalado hacia operación y criterios claros para actuar sobre alertas sin introducir riesgo innecesario sobre el proceso.

Ventajas:

- Centraliza la supervisión y análisis de eventos de seguridad.
- Mejora la capacidad de detección, priorización y respuesta frente a incidentes.
- Facilita la correlación entre señales de múltiples fuentes y dominios.
- Aportación de trazabilidad, continuidad operativa y procedimientos estables de análisis.
- Resulta especialmente útil para integrar visión IT/OT y coordinar actuaciones en entornos híbridos.

Limitaciones y consideraciones:

- Su valor disminuye si se concibe sólo como receptor de alertas sin capacidad suficiente de análisis y respuesta.
- Se requiere madurez organizativa, procedimientos claros e integración real con el resto de la organización.
- En entornos industriales, un SOC centrado solo en TI puede interpretar mal ciertas alertas o escalar acciones incompatibles con la operación.
- No sustituye la necesidad de buenas fuentes de telemetría, segmentación, control de accesos ni gestión de vulnerabilidades.
- Su eficacia depende de la coordinación con operación, mantenimiento, responsables de proceso y, cuando proceda, seguridad funcional y terceros.

Relación con otros controles: Se relaciona con el SIEM, el MDR, los IDS/IPS, el NDR, el EDR, el CPS PP, la visibilidad de activos y comunicaciones OT, la monitorización ciberfísica, la inteligencia de amenazas, la respuesta ante incidentes y los procedimientos de continuidad. Funciona como capacidad operativa que da sentido y coordinación al conjunto de capacidades de monitorización y detección.

Casos habituales de uso: Se emplea para supervisar alertas IT/OT, analizar accesos remotos, actividad de terceros, movimiento entre dominios, cambios no previstos, eventos procedentes de sensores de red o endpoints, investigación de incidentes con impacto operativo y coordinación de la respuesta en organizaciones con exposición significativa o necesidad de vigilancia continuada.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el SOC puede actuar como medida compensatoria muy relevante cuando no es viable reforzar de inmediato todos los controles preventivos, ya que mejora la capacidad de detección temprana, análisis y coordinación frente a incidentes. Su utilidad es especialmente alta cuando integra conocimiento del proceso, casos de uso adaptados a la realidad OT y procedimientos claros para escalar de forma segura decisiones que puedan afectar a la operación.

5.6.3 MDR

Categoría: Monitorización, visibilidad y operación de seguridad

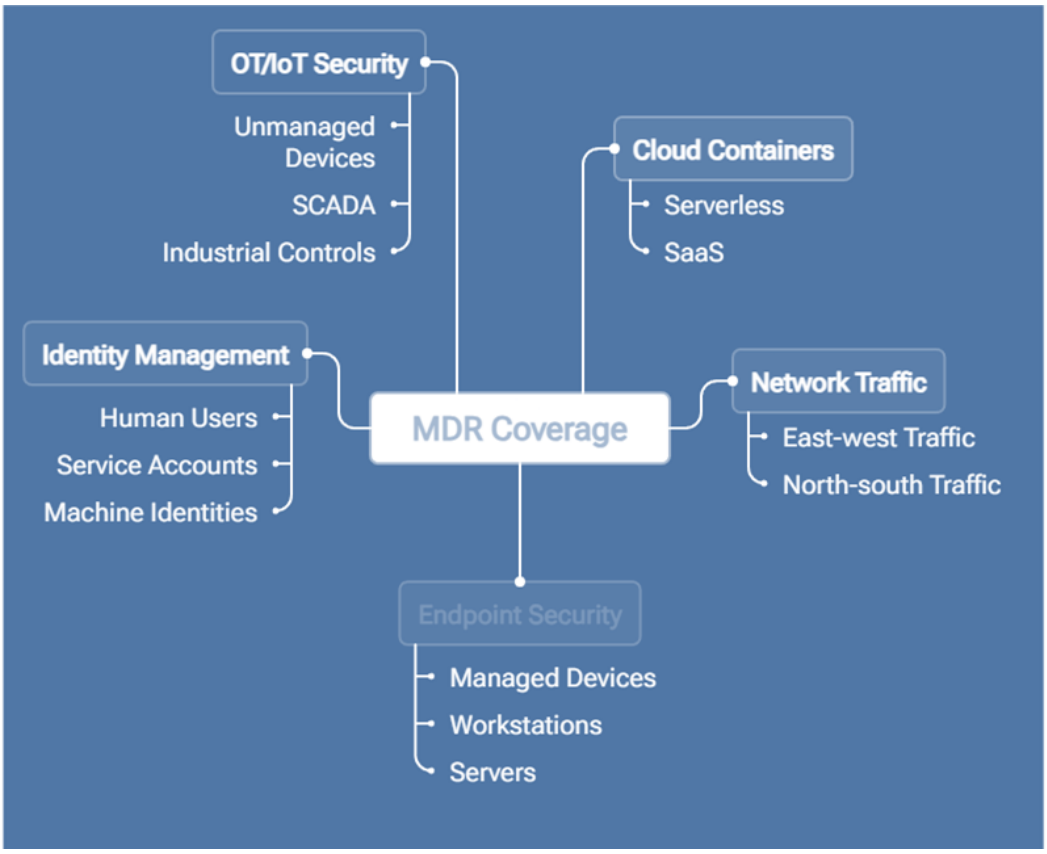
Tipología: Organizativa / técnica / mixta

Función defensiva predominante: Detectiva

Función en NIST CSF: Detect, Respond

Descripción: El MDR (*Managed Detection and Response*) es un modelo de servicio mediante el cual una organización delega, total o parcialmente, capacidades de monitorización, detección, análisis y apoyo a la respuesta ante incidentes en un proveedor especializado. Su finalidad es complementar o sustituir capacidades internas cuando no existe estructura suficiente para operar de manera continuada un modelo propio de supervisión avanzada. A diferencia de un servicio puramente tecnológico o de una simple gestión de alertas, el MDR combina telemetría, análisis, caza de amenazas, investigación y escalado operativo, normalmente apoyándose en herramientas como SIEM, EDR, NDR u otras fuentes de visibilidad. En entornos industriales, esta opción resulta especialmente relevante para organizaciones que necesitan mejorar su

capacidad de detección y respuesta sin disponer de un SOC propio maduro o de recursos internos suficientes para cubrir la vigilancia continuada de entornos híbridos IT/OT.



Áreas de cobertura de un MDR. Fuente: Vectra.ai (n.d.)

Objetivo: Dotar a la organización de una capacidad sostenida de detección, análisis y apoyo a la respuesta ante incidentes, reduciendo el tiempo de identificación y mejorando la calidad del tratamiento de las alertas sin depender exclusivamente de medios internos. En el ámbito industrial, su objetivo incluye también aportar conocimiento especializado y cobertura operativa frente a eventos que afecten a accesos remotos, terceros, activos críticos, interacciones IT/OT o señales de compromiso con impacto potencial sobre la operación.

Cómo funciona / cómo se implanta: Su implantación requiere definir el alcance del servicio, las fuentes de telemetría que serán monitorizadas, los niveles de cobertura, los criterios de escalado, los tiempos de respuesta esperados y la distribución de responsabilidades entre la organización y el proveedor. El MDR puede operar sobre herramientas ya existentes en la organización o incorporar parte de su propia infraestructura de detección y análisis. En entornos industriales, su eficacia depende de que el servicio tenga visibilidad suficiente sobre los activos y flujos relevantes, de que exista una correcta contextualización de la arquitectura IT/OT y de que se definan

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

procedimientos claros para escalar incidentes sin comprometer la continuidad ni la seguridad del proceso. Resulta especialmente importante establecer canales fluidos entre el proveedor, los equipos internos de seguridad, operación, mantenimiento y responsables del proceso, evitando que la gestión externalizada quede desconectada de la realidad operativa de la planta o de la organización.

Ventajas:

- Permite acceder a capacidades avanzadas de detección y análisis sin necesidad de desarrollar internamente toda la estructura.
- Mejora la cobertura temporal y la continuidad de la supervisión.
- Aportación de conocimiento especializado, procedimientos maduros y apoyo en la investigación de incidentes.
- Resulta útil para organizaciones con recursos limitados o sin SOC propio consolidado.
- Puede acelerar la detección y el escalado de incidentes en entornos híbridos IT/OT.

Limitaciones y consideraciones:

- Su valor depende de la calidad del servicio, de la cobertura real y de la integración con el contexto de la organización.
- En entornos industriales, un MDR ajeno a la realidad OT puede interpretar mal alertas o escalar acciones poco compatibles con la operación.
- No sustituye la necesidad de inventario, segmentación, visibilidad suficiente ni procedimientos internos de coordinación.
- Se requiere definir con claridad que decisiones puede tomar el proveedor, que acciones se reservan a la organización y cómo se gestionan incidentes con impacto operativo.
- Debe evitarse tratar el MDR como una externalización completa de la responsabilidad sobre la seguridad.

Relación con otros controles: Se relaciona con el SOC, el SIEM, el EDR, el NDR, los IDS/IPS, la visibilidad de activos y comunicaciones OT, la monitorización ciberfísica, la respuesta ante incidentes, la inteligencia de amenazas y con los procedimientos de continuidad. Funciona como modelo operativo de apoyo o sustitución parcial del centro interno de operaciones de seguridad.

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

Casos habituales de uso: Se emplea en organizaciones que precisan vigilancia continuada sin disponer de SOC propio, en entornos con exposición significativa a acceso remoto o terceros, en infraestructuras con necesidades de monitorización 24/7, en escenarios de refuerzo de la capacidad interna de análisis y respuesta, y en programas de seguridad en los que se busca combinar recursos internos limitados con supervisión especializada externa.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el MDR puede actuar como medida compensatoria muy útil cuando no es viable desarrollar de inmediato una capacidad interna madura de operación de seguridad, siempre que exista visibilidad suficiente y una buena integración con el contexto OT. Su utilidad aumenta cuando se acompaña de procedimientos claros de escalado, conocimiento de los activos críticos, coordinación con operación y limitación explícita de las acciones que pueden afectar al proceso sin convalidación previa.

5.6.4 Monitorización ciberfísica / MES

Categoría: Monitorización, visibilidad y operación de seguridad

Tipología: Técnica / mixta

Función defensiva predominante: Detectiva

Función en NIST CSF: Detect

Descripción: La monitorización ciberfísica / MES comprende el conjunto de capacidades orientadas a la observación continua del comportamiento del proceso industrial, de los sistemas de ejecución y supervisión y de sus interacciones con la capa tecnológica, con el fin de identificar desviaciones, anomalías o condiciones de riesgo con impacto potencial sobre la operación. Este control integra, según el caso, el análisis de variables de proceso, estados operativos, eventos de sistemas, flujos de comunicación, señales de producción e información procedente de plataformas MES (*Manufacturing Ejecution System*) o equivalentes. Su valor reside en aportar una visión más próxima al funcionamiento real de la actividad industrial, permitiendo detectar incidentes o alteraciones que no siempre serían visibles desde una monitorización puramente de red o centrada únicamente en eventos IT.

Objetivo: Incrementar la capacidad de la organización para identificar anomalías con relevancia operativa, correlacionando información procedente del proceso, de la supervisión, de la ejecución y de los sistemas tecnológicos que lo soportan. En el ámbito industrial, su objetivo incluye también detectar cambios de comportamiento que

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

puedan indicar manipulación, fallo, degradación, uso indebido de los sistemas o impacto potencial sobre la producción, la calidad, continuidad o seguridad del proceso.

Cómo funciona / cómo se implanta: Su implantación parte de la identificación de las fuentes de datos más relevantes para comprender el funcionamiento del entorno: variables de proceso, estados de equipos, alarmas, eventos de supervisión, información de sistemas MES, registros de operación, trazas de comunicación, señales de control y otros indicadores asociados a la actividad industrial. A partir de esa base, se establecen mecanismos de recogida, correlación y análisis que permitan distinguir entre condiciones normales de operación, variaciones esperadas y desviaciones que requieran investigación. En entornos industriales, su utilidad aumenta cuando se integra con conocimiento del proceso, inventario de activos, contexto de producción, monitorización de red, visibilidad OT y procedimientos de escalado hacia operación y mantenimiento. No se trata sólo de acumular datos, sino de interpretarlos a la luz del comportamiento esperado de la planta o del servicio industrial.

Ventajas:

- Aporta una visión más cercana al comportamiento real del proceso y de la operación.
- Permite detectar desviaciones que pueden pasar inadvertidas en controles centrados sólo en red o endpoint.
- Mejora la contextualización de alertas y eventos con impacto potencial sobre la producción o la calidad.
- Resulta especialmente útil en entornos con fuerte dependencia de plataformas de ejecución, supervisión o integración operativa.
- Complementa la detección técnica con información directamente relacionada con el estado del proceso.

Limitaciones y consideraciones:

- Su eficacia depende de la calidad, cobertura y contextualización de las fuerzas de datos disponibles.
- Puede requerir conocimiento avanzado del proceso para diferenciar entre variaciones operativas normales y señales de riesgo real.
- En entornos industriales, una mala interpretación de las desviaciones puede generar falsos positivos o escalados innecesarios.

- No sustituye la segmentación, el control de accesos, la gestión de vulnerabilidades ni la monitorización de red.
- Se requiere coordinación estrecha con operación, mantenimiento, ingeniería y responsables de producción para que la información recogida se traduzca en acción útil.

Relación con otros controles: Se relaciona con el SIEM, el SOC, el MDR, el NDR, el CPS PP, la visibilidad de activos y comunicaciones OT, la respuesta ante incidentes, la continuidad de negocio y resiliencia operativa y las medidas compensatorias orientadas a reforzar la detección y la comprensión del riesgo sobre sistemas y procesos críticos.

Casos habituales de uso: Se emplea para detectar desviaciones en parámetros de proceso, cambios no previstos en secuencias de operación, inconsistencias entre eventos de red y comportamiento productivo, anomalías en plataformas MES, degradación de líneas o servicios industriales, impacto operativo derivado de incidentes de seguridad y escenarios en los que se necesita comprender mejor la relación entre actividad tecnológica y estado real del proceso.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la monitorización ciberfísica / MES puede actuar como medida compensatoria especialmente útil cuando no es viable reducir de inmediato toda la exposición arquitectónica o actualizar determinados activos, ya que aporta una capa adicional de detección centrada en el comportamiento real de la operación. Su utilidad aumenta cuando se combina con monitorización de red, visibilidad OT, procedimientos claros de análisis y escalado, y conocimiento suficiente del proceso para interpretar correctamente las anomalías observadas.

5.6.5 Visibilidad de activos y comunicaciones OT

Categoría: Monitorización, visibilidad y operación de seguridad

Tipología: Técnica / mixta

Función defensiva predominante: Detectiva

Función en NIST CSF: Identify, Detect

Descripción: La visibilidad de activos y comunicaciones OT consiste en el conjunto de capacidades orientadas a identificar, inventariar, contextualizar y observar los dispositivos, sistemas, relaciones y flujos que conforman el entorno operativo industrial. Su propósito es aportar una comprensión fiable de qué activos existen, cómo se comunican, qué protocolos utilizan, su rendimiento y qué dependencias mantienen con

la red corporativa, con los sistemas de supervisión, con los proveedores y con el proceso físico. En entornos industriales, este control resulta esencial porque una parte significativa del riesgo deriva precisamente de la falta de conocimiento detallado sobre activos legados, comunicaciones históricas, interconexiones no documentadas, dispositivos de terceros o cambios no suficientemente gobernados. Estas capacidades típicamente se determinan en sistemas CPS PP.

Objetivo: Disponer de una visión actualizada y contextualizada de los activos OT y de sus comunicaciones, reduciendo puntos ciegos y mejorando la capacidad de la organización para detectar exposiciones, anomalías, dependencias críticas y cambios no previstos. En el ámbito industrial, su objetivo incluye también servir de base para la segmentación, la gestión de vulnerabilidades, la respuesta ante incidentes, la revisión de arquitectura y la protección de los sistemas con mayor criticidad operativa.

Cómo funciona / cómo se implanta: Su implantación suele basarse en la observación pasiva del tráfico de red, en la identificación de protocolos industriales, en la correlación con inventarios existentes, en el análisis de configuraciones y en la contextualización funcional de los activos detectados. A partir de esa base, se construye una visión más completa del entorno: qué dispositivos existen, qué versiones o perfiles presentan, con qué sistemas se relacionan, qué patrones de comunicación son habituales y qué desviaciones pueden ser relevantes. En entornos industriales, este control debe aplicarse con criterios compatibles con la continuidad de la operación, priorizando técnicas pasivas y evitando mecanismos intrusivos que puedan afectar a la estabilidad del proceso. Su utilidad aumenta cuando la información recogida se integra con procesos de gestión de activos, revisión de arquitectura, monitorización de seguridad y procedimientos de cambio.

Ventajas:

- Reduce puntos ciegos sobre activos, flujos y dependencias del entorno OT.
- Mejora la base de conocimiento necesaria para segmentación, detección y respuesta.
- Permite identificar activos no documentados, comunicaciones no previstas e interconexiones de riesgo.
- Resulta especialmente útil en entornos con legado tecnológico, terceros o baja gobernanza histórica.
- Facilita la contextualización de otros controles de monitorización y protección.

Limitaciones y consideraciones:

- Su eficacia depende de la cobertura real de la observación y de la capacidad para contextualizar los activos detectados.
- Puede ofrecer una visión incompleta si no se integra con conocimiento operativo y documental de la organización.
- En entornos industriales, la identificación de un activo no siempre implica conocer de inmediato su criticidad o su dependencia funcional.
- No sustituye la segmentación, la gestión de vulnerabilidades, el control de accesos ni la revisión formal de la arquitectura.
- Se requiere mantenimiento continuado para reflejar cambios de configuración, incorporación de terceros, nuevas interconexiones o evolución del proceso.

Relación con otros controles: Se relaciona con el SIEM, el SOC, el MDR, el NDR, la monitorización ciberfísica / MES, la segmentación de red y separación IT/OT, la revisión de arquitectura, la gestión de vulnerabilidades, la respuesta ante incidentes y las medidas compensatorias orientadas a reducir la exposición de activos críticos o poco conocidos.

Casos habituales de uso: Se emplea para construir o mejorar inventarios OT, identificar activos legados o no documentados, analizar flujos entre redes corporativas y operativas, revisar protocolos empleados en planta, detectar comunicaciones anómalas, contextualizar alertas de seguridad, apoyar proyectos de segmentación y reforzar la comprensión del entorno antes de auditorías, cambios o actuaciones correctivas.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la visibilidad de activos y comunicaciones OT suele ser una medida habilitadora y, al mismo tiempo, compensatoria: cuando no es viable acometer de inmediato cambios más profundos, permite al menos conocer mejor el riesgo existente, reducir incertidumbre y priorizar actuaciones sobre los activos y flujos más sensibles. Su utilidad aumenta cuando se combina con segmentación, monitorización, bastionado y procedimientos claros de revisión y cambio.

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

5.7 Monitorización especializada de componentes y eventos críticos

Determinados activos, canales de comunicación y soportes de operación presentan una relevancia especial por su proximidad al proceso, por su sensibilidad o su potencial como vector de compromiso. Este bloque agrupa **medidas de protección y monitorización focalizadas en elementos concretos —puestos de operación, endpoints industriales, correo, dispositivos externos o aplicaciones conectadas— que requieren un tratamiento específico** dentro de la arquitectura global de seguridad.

5.7.1 Protección del puesto, de los activos y de los soportes de operación

Categoría: Protección del puesto, de los activos y de los soportes de operación

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: La protección del puesto de trabajo comprende el conjunto de medidas técnicas, configuraciones, políticas y mecanismos de control destinados a asegurar los equipos de usuario que intervienen en la actividad diaria de la organización, reduciendo su exposición a malware, uso indebido, configuraciones inseguras, instalación de software no autorizado o acceso no controlado. Este control abarca tanto los puestos corporativos convencionales como aquellos equipos que, sin formar parte del núcleo de la red OT, pueden actuar como puente hacia entornos operativos, servicios remotos, plataformas de gestión o sistemas con impacto indirecto sobre la operación. En entornos industriales, el puesto de trabajo no debe entenderse sólo como un elemento de oficina, sino también como un componente que puede influir en la seguridad global del entorno híbrido IT/OT.

Objetivo: Reducir el riesgo de compromiso de los equipos de usuario y limitar su capacidad para actuar como vector de entrada, propagación o apoyo a acciones maliciosas, reforzando el control sobre configuraciones, software, privilegios, acceso a datos e interacción con otros sistemas. En el ámbito industrial, su objetivo incluye también evitar que un puesto aparentemente periférico se convierta en un punto de apoyo para acceder a servicios sensibles, credenciales, recursos compartidos o entornos de operación.

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

Cómo funciona / cómo se implanta: Su implantación se basa en la aplicación de medidas de bastionado, configuración segura, gestión de privilegios, control de software autorizado, protección frente a malware, cifrado, actualización controlada, restricción de dispositivos externos, autenticación reforzada y supervisión de la actividad del endpoint. En entornos industriales, este control debe aplicarse con criterio según el tipo de equipo y su relación con la operación, diferenciando entre puestos corporativos generales, equipos con acceso a servicios de supervisión, portátiles empleados en mantenimiento o puestos con interacción con sistemas de gestión industrial. Su eficacia depende de que exista una política clara de configuración, una administración coherente de los permisos, inventario actualizado de los equipos e integración con otros controles como identidad, monitorización, protección de correo y acceso remoto.

Ventajas:

- Reduce la superficie de exposición de uno de los vectores más habituales de compromiso.
- Mejora el control sobre configuraciones, software y privilegios de los equipos de usuario.
- Dificulta la ejecución de código malicioso, el abuso de credenciales y la propagación desde puestos comprometidos.
- Refuerza la protección de equipos que pueden actuar como puente hacia servicios sensibles o entornos industriales.
- Complementa otros controles de red, identidad y monitorización desde la capa de endpoint.

Limitaciones y consideraciones:

- Su eficacia disminuye si no existe una administración coherente de configuraciones, permisos y excepciones.
- En entornos industriales, algunos puestos pueden depender de software específico con restricciones de actualización o compatibilidad.
- No sustituye la segmentación, la gestión de identidades, la protección de acceso remoto ni la formación del personal.
- Puede generar desviaciones de seguridad si se mantienen excepciones permanentes sin trazabilidad ni revisión.

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

- Se requiere coordinación entre sistemas, seguridad, operación y responsables de las aplicaciones críticas para evitar impactos no deseados.

Relación con otros controles: Se relaciona con la protección de endpoints industriales, el MDM, la seguridad en el email, la conexión segura de dispositivos externos, la gestión de identidades y accesos, el acceso remoto seguro, el EDR, la detección de integridad de ficheros y las medidas compensatorias orientadas a reducir riesgo en equipos con exposición elevada.

Casos habituales de uso: Se emplea para reforzar puestos corporativos con acceso a servicios críticos, equipos de usuario con acceso a información sensible, portátiles empleados por personal técnico, estaciones conectadas a plataformas de gestión industrial, terminales con acceso remoto y entornos en los que el puesto de trabajo puede actuar como punto de entrada hacia recursos de mayor criticidad.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la protección del puesto de trabajo resulta especialmente útil como medida de base para limitar la exposición de los equipos más próximos a la convergencia IT/OT. Su utilidad aumenta cuando se combina con bastionado, control de privilegios, restricción de software, MFA, segmentación, monitorización y procedimientos claros para la gestión de excepciones, especialmente en puestos que interactúan con operación, mantenimiento o terceros.

5.7.2 Protección de endpoints industriales

Categoría: Protección del puesto, de los activos y de los soportes de operación

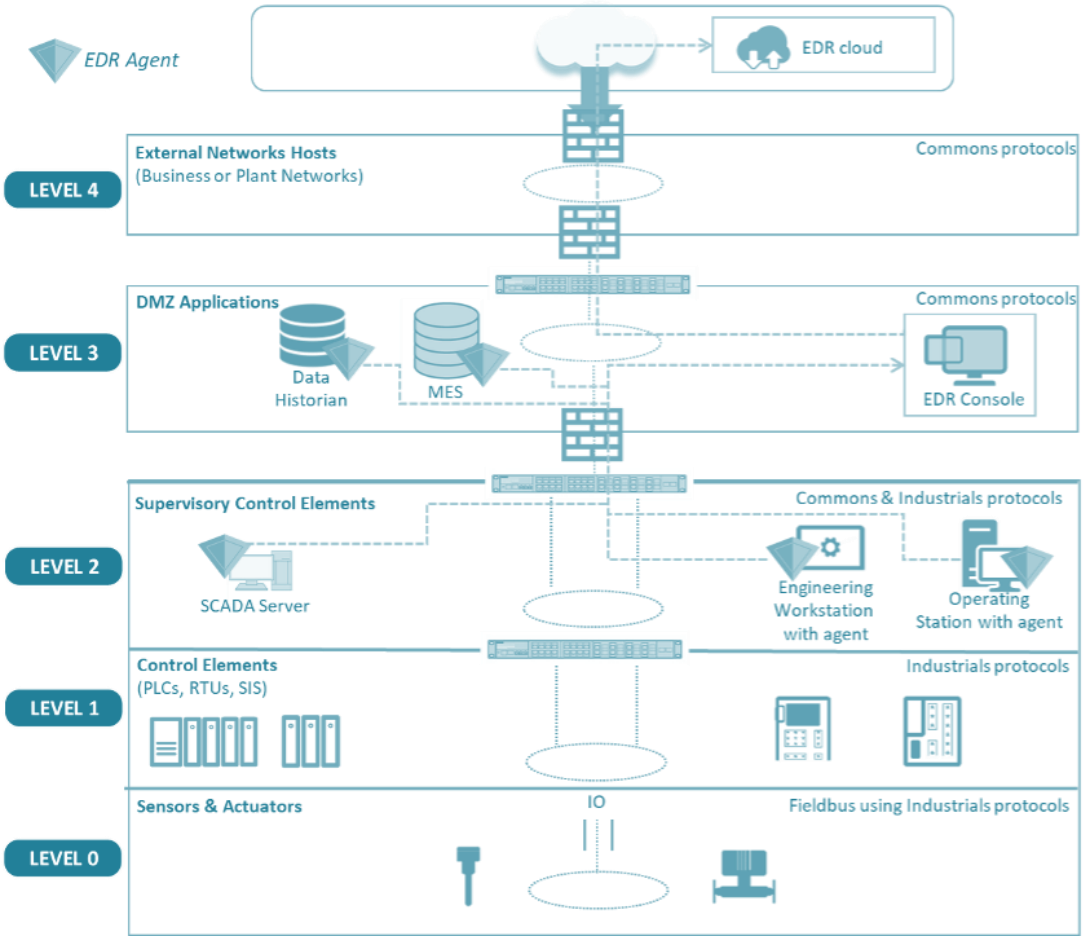
Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: La protección de endpoints industriales comprende el conjunto de medidas técnicas y procedimentales destinadas a reforzar la seguridad de los equipos finales con función operativa o relación directa con los entornos OT, como HMI, estaciones de ingeniería, servidores de supervisión, puestos de mantenimiento, terminales asociados a aplicaciones industriales y otros sistemas con capacidad de interacción con el proceso o la infraestructura de control. A diferencia de la protección genérica del puesto de trabajo, este control debe adaptarse a las restricciones propias del entorno industrial, donde la disponibilidad, la compatibilidad con el software de

fabricante, la estabilidad y la continuidad de la operación condicionan fuertemente las medidas que pueden implantarse.



Ejemplo de despliegue de EDR industrial. Fuente: Orange Cyberdefense (n.d.)

Objetivo: Reducir el riesgo de compromiso, manipulación o uso indebido de los equipos finales industriales, reforzando el control sobre configuraciones, software, privilegios, acceso, ejecución e integridad de los sistemas que pueden afectar de forma directa o indirecta a la operación. En el ámbito industrial, su objetivo incluye también limitar la capacidad de estos equipos para actuar como puente entre terceros, entornos corporativos y sistemas OT sensibles.

Cómo funciona / cómo se implanta: Su implantación se basa en la combinación de medidas como el bastionado específico del sistema, la restricción de software autorizado, el control de privilegios, la limitación de servicios innecesarios, la protección frente a malware cuando sea compatible, la autenticación reforzada, la segregación de accesos, la detección de cambios no autorizados, la revisión de configuraciones y la integración con mecanismos de monitorización. En entornos industriales, estas medidas deben aplicarse tras evaluar la compatibilidad con el software de operación, con las

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

herramientas de fabricante, con los requisitos de rendimiento y con la seguridad funcional. Su eficacia depende de adaptar la protección al papel exacto del endpoint: no es lo mismo un HMI, una estación de ingeniería, un servidor historiador o un portátil técnico empleado en mantenimiento. Por ello, la implantación requiere inventario claro, clasificación funcional y procedimientos de cambio y convalidación bien definidos.

Ventajas:

- Reduce la superficie de exposición de equipos con impacto directo o indirecto sobre la operación.
- Mejora el control sobre configuraciones, software, privilegios y servicios de los sistemas industriales finales.
- Dificulta la ejecución de acciones no autorizadas, la persistencia maliciosa y la propagación desde endpoints sensibles.
- Refuerza la protección de activos como HMI, estaciones de ingeniería y servidores de supervisión.
- Complementa la segmentación, la gestión de accesos y la monitorización del entorno OT.

Limitaciones y consideraciones:

- No todos los endpoints industriales admiten el mismo nivel de protección sin impacto operativo.
- La compatibilidad con aplicaciones de fabricante, software legado y requisitos de rendimiento debe validarse previamente.
- En entornos industriales, una medida técnicamente adecuada puede resultar inviable si compromete la disponibilidad o la estabilidad del proceso.
- No sustituye la segmentación, el control de acceso remoto, la gestión de vulnerabilidades ni los procedimientos operativos.
- Se requiere coordinación entre seguridad, operación, mantenimiento, ingeniería y, cuando proceda, fabricantes o integradores.

Relación con otros controles: Se relaciona con la protección del puesto de trabajo, el EDR, la detección de integridad de ficheros, el bastionado de HMI y sistemas de ingeniería, la conexión segura de dispositivos externos, la gestión de identidades y accesos, el acceso remoto seguro, la segmentación y la monitorización de activos y comunicaciones OT.

Casos habituales de uso: Se utiliza para reforzar HMI, estaciones de ingeniería, servidores de supervisión, historiadores, equipos de mantenimiento con acceso a planta, terminales asociados a aplicaciones industriales y otros activos finales que, sin ser controladores puros, pueden influir en la operación o actuar como vector hacia sistemas de mayor criticidad.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la protección de endpoints industriales resulta especialmente útil como medida compensatoria cuando no es viable actualizar de inmediato ciertos sistemas, sustituir componentes legados o reducir toda la exposición arquitectónica existente. Su utilidad aumenta cuando se combina con bastionado, control de cambios, segmentación, restricción de accesos, monitorización y procedimientos claros de validación antes de introducir modificaciones en equipos con impacto operativo.

5.7.3 MDM

Categoría: Protección del puesto, de los activos y de los soportes de operación

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: El MDM (*Mobile Device Management* o gestión de dispositivos móviles) es el conjunto de capacidades orientadas a la administración, configuración, control y supervisión centralizada de dispositivos móviles y portátiles utilizados en el ámbito de la organización. Su finalidad es garantizar que estos equipos operen bajo políticas de seguridad coherentes, con configuraciones conocidas, mecanismos de autenticación adecuados, capacidad de control remoto y limitación del uso indebido. En entornos industriales, este control adquiere especial relevancia cuando tablets, smartphones, portátiles ligeros u otros dispositivos móviles se emplean para tareas de mantenimiento, supervisión, acceso a información técnica, gestión operativa o interacción con aplicaciones corporativas e industriales.

Funciones de la solución MDM. Fuente: ManageEngine (n.d.)

Objetivo: Reducir el riesgo asociado al uso de dispositivos móviles, reforzando el control sobre su configuración, acceso a la información, las aplicaciones instaladas, los datos almacenados y la conectividad con los distintos servicios de la organización. En el ámbito industrial, su objetivo incluye también evitar que un dispositivo móvil poco gubernado se convierta en un punto de acceso, fuga de información o puente hacia sistemas y entornos con relevancia operativa.

Cómo funciona / cómo se implanta: Su implantación se basa en la inscripción de los dispositivos en una plataforma central que permite aplicar políticas de seguridad, configurar parámetros, gestionar aplicaciones autorizadas, exigir mecanismos de bloqueo y autenticación, cifrar datos, limitar funciones, registrar estado y, cuando proceda, ejecutar acciones remotas como aislamiento, borrado o revocación de acceso. En entornos industriales, el MDM debe desplegarse teniendo en cuenta el papel real de cada dispositivo: acceso a correo y servicios corporativos, consulta de documentación técnica, uso de aplicaciones de supervisión, conexión a plataformas de mantenimiento o interacción con sistemas de gestión operativa. Su eficacia depende de definir políticas proporcionales al riesgo, evitar el uso indiscriminado de dispositivos personales en tareas sensibles e integrar el control móvil con las políticas de identidad, acceso remoto, clasificación de la información y uso de redes no cableadas.

Ventajas:

- Mejora el control centralizado sobre dispositivos móviles y su configuración.

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

- Reduce el riesgo de pérdida de datos, uso indebido o acceso no controlado desde terminales móviles.
- Facilita la aplicación coherente de políticas de seguridad, autenticación y cifrado.
- Resulta útil para gobernar dispositivos con acceso a servicios corporativos, técnicos u operativos.
- Complementa la gestión de identidades, el acceso remoto seguro y la protección de la información sensible.

Limitaciones y consideraciones:

- Su utilidad depende de que los dispositivos estén correctamente inventariados e inscritos en la plataforma de gestión.
- Puede generar fricción si las políticas son excesivamente restrictivas o no se adaptan al uso real de los equipos.
- En entornos industriales, no todos los dispositivos móviles tienen el mismo nivel de exposición ni el mismo impacto potencial sobre la operación.
- No sustituye la segmentación, la gestión de accesos, la protección del puesto de trabajo ni los procedimientos de uso seguro.
- Debe evitarse que la movilidad introduzca excepciones informales o uso de dispositivos personales sin gobernanza suficiente.

Relación con otros controles: Se relaciona con la protección del puesto de trabajo, la seguridad en el correo, la gestión de identidades y accesos, el acceso remoto seguro, las auditorías de dispositivos móviles y endpoints, la conexión segura de dispositivos externos, el NAC, la monitorización y los procedimientos operativos orientados al uso seguro de dispositivos con movilidad.

Casos habituales de uso: Se emplea para gobernar smartphones y tablets corporativas, dispositivos móviles usados por personal técnico, equipos de supervisión o mantenimiento con acceso a documentación o plataformas de gestión, terminales con acceso a correo y servicios cloud y entornos en los que la movilidad forma parte de la operación o del soporte diario.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el MDM resulta especialmente útil cuando existe uso habitual de dispositivos móviles para acceso a servicios corporativos, técnicos o de mantenimiento, y puede actuar como medida compensatoria parcial frente a la imposibilidad de eliminar completamente la

movilidad del entorno. Su utilidad aumenta cuando se combina con MFA, cifrado, control de aplicaciones, segmentación de las redes sin hilos y restricción clara del acceso a recursos sensibles según el perfil y el contexto del dispositivo.

5.7.4 Seguridad en el email

Categoría: Protección del puesto, de los activos y de los soportes de operación

Tipología: Técnica / mixta

Función defensiva predominante: Preventivo

Función en NIST CSF: Protect

Descripción: La seguridad en el email comprende el conjunto de medidas técnicas y organizativas destinadas a proteger el correo electrónico como canal de comunicación, acceso e intercambio de información, reduciendo el riesgo de suplantación, entrega de malware, robo de credenciales, fraude, fuga de datos e interacción con contenidos maliciosos. Su relevancia no se limita al ámbito corporativo general, ya que en muchas organizaciones industriales el correo continúa siendo una vía habitual para la recepción de documentación técnica, coordinación con terceros, gestión de mantenimiento, intercambio de instrucciones operativas, envío de avisos y comunicación entre personal interno y proveedores. Por este motivo, un compromiso a través de este canal puede tener consecuencias que trasciendan el plano informativo y afecten de manera indirecta a la operación.

Amenazas habituales que emplean el email como vector de ataque. Fuente: Norton (2022)

Objetivo: Reducir la exposición de la organización frente a amenazas canalizadas por correo electrónico, limitando la recepción, ejecución o interacción con mensajes

maliciosos, suplantaciones y contenidos no autorizados. En el ámbito industrial, su objetivo incluye también evitar que el correo se convierta en un punto de entrada hacia sistemas, cuentas, documentos técnicos o procesos con impacto operativo.

Cómo funciona / cómo se implanta: Su implantación se basa en la combinación de mecanismos de filtrado, autenticación, análisis de contenidos, protección de enlaces y adjuntos, políticas de entrega, aislamiento de mensajes sospechosos, protección frente a la suplantación de dominio e integración con procedimientos de reporte y respuesta. Ello incluye medidas como verificación de remitentes, control de reputación, análisis antimalware, verificación de autenticidad del dominio, revisión de URLs, sandboxing de ficheros, políticas de marcado o cuarentena e integración con campañas de concienciación. En entornos industriales, estas medidas deben complementarse con un enfoque práctico sobre el uso real del correo: recepción de documentación de fabricante, envío de ficheros de configuración, peticiones de mantenimiento, mensajes urgentes aparentando proceder de terceros, interacción con proveedores y circulación de información técnica u operativa. Su eficacia aumenta cuando se integra con identidad, MFA, formación, DLP y procedimientos claros de convalidación de comunicaciones sensibles.

Ventajas:

- Reduce uno de los vectores más frecuentes de acceso inicial y fraude.
- Mejora la protección frente a la suplantación, malware, enlaces maliciosos y adjuntos peligrosos.
- Refuerza la seguridad de las comunicaciones con terceros y la protección de las identidades.
- Complementa la concienciación del personal con una capa técnica de filtrado y contención.
- Ayuda a limitar la llegada de contenidos que podrían comprometer puestos, credenciales o información sensible.

Limitaciones y consideraciones:

- Su eficacia disminuye si se concibe como control aislado y no se acompaña de formación, MFA y procedimientos de validación.
- Los atacantes adaptan continuamente las técnicas de suplantación e ingeniería social a este canal.

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

- En entornos industriales, ciertos mensajes pueden incluir documentación técnica o anexos legítimos que requieren excepciones bien gobernadas.
- No sustituye el control de accesos, la protección del puesto de trabajo ni la revisión de las interacciones con terceros.
- Se requiere ajuste continuo de las políticas para equilibrar seguridad, usabilidad y necesidades operativas reales.

Relación con otros controles: Se relaciona con el phishing, vishing, smishing y técnicas afines, las campañas de concienciación y simulación, la gestión de identidades y accesos, el DLP, la protección del puesto de trabajo, el MDM, la monitorización y operación de seguridad y los procedimientos de validación frente a solicitudes sensibles o no habituales.

Casos habituales de uso: Se emplea para proteger cuentas corporativas y técnicas, comunicaciones con proveedores e integradores, recepción de documentación o anexos técnicos, peticiones de acceso remoto, mensajes con instrucciones de mantenimiento, notificaciones operativas y escenarios en los que el correo puede actuar como vía de entrada hacia servicios, credenciales o información de valor para la organización.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la seguridad en el email resulta especialmente útil cuando se combina con MFA, procedimientos de verificación por canal alternativo, restricción de privilegios y concienciación específica para personal técnico, operación y mantenimiento. También puede actuar como medida compensatoria parcial cuando la organización mantiene una alta dependencia del correo para la coordinación con terceros y no es viable reducir de inmediato todas las interacciones de riesgo asociadas a este medio.

5.7.5 Conexión segura de dispositivos externos

Categoría: Protección del puesto, de los activos y de los soportes de operación

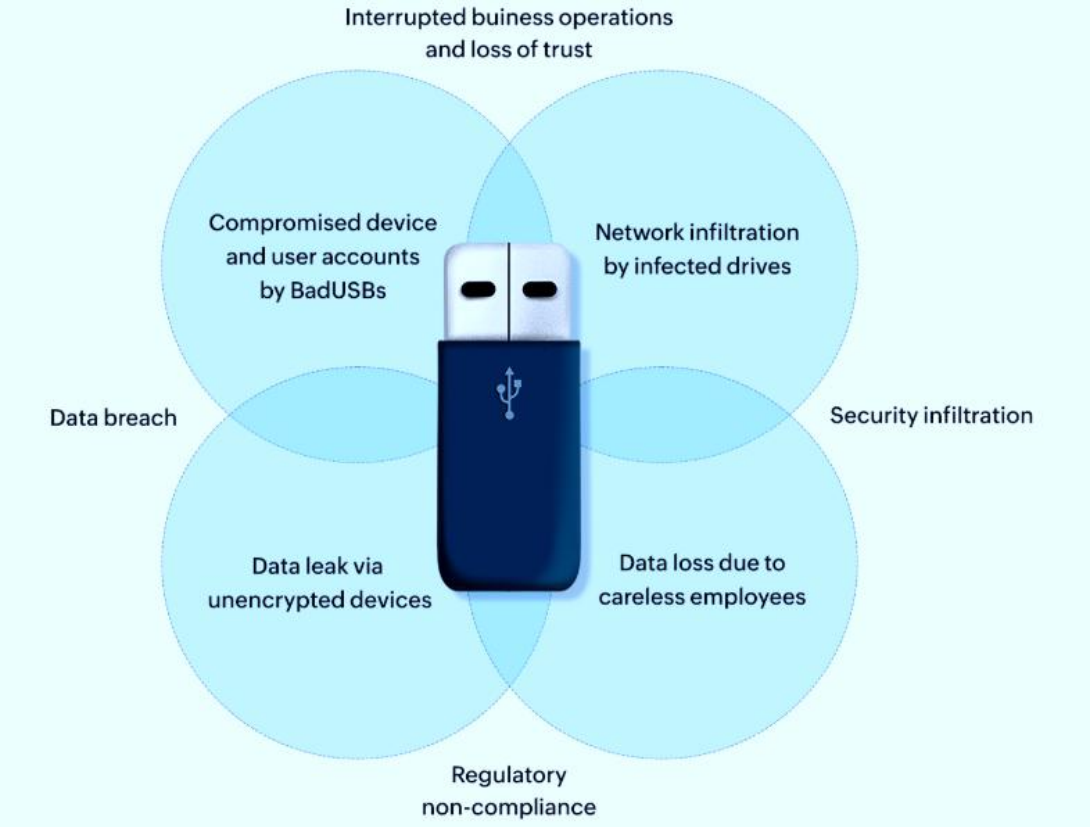
Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: La conexión segura de dispositivos externos comprende el conjunto de medidas destinadas a controlar, restringir, validar y supervisar la incorporación de soportes extraíbles, portátiles de terceros, equipos de mantenimiento, dispositivos USB, herramientas de diagnóstico, medios de transferencia y otros componentes externos que puedan interactuar con los sistemas de la organización. En entornos industriales,

este control tiene una relevancia especial, ya que muchas tareas de mantenimiento, actualización, configuración, soporte o recogida de información continúan dependiendo de la conexión física o lógica de dispositivos ajenos al entorno estable de la planta. Esta realidad convierte los dispositivos externos en un vector recurrente de introducción de malware, alteración no autorizada, fuga de información o acceso indebido a sistemas con impacto operativo.



Riesgos de seguridad del empleo de USBs. Fuente: ManageEngine (n.d.)

Objetivo: Reducir el riesgo derivado de la conexión de dispositivos externos al entorno tecnológico de la organización, limitando la posibilidad de introducir código malicioso, copiar información sensible, ejecutar acciones no autorizadas o establecer vías de acceso no gobernadas hacia activos corporativos o industriales. En el ámbito industrial, su objetivo incluye también asegurar que las tareas legítimas de mantenimiento, soporte y transferencia de información se realicen bajo condiciones controladas, trazables y compatibles con la continuidad de la operación.

Cómo funciona / cómo se implanta: Su implantación se basa en la definición de políticas y mecanismos que determinen qué dispositivos pueden conectarse, en qué condiciones, a qué equipos, por parte de quién y con qué finalidad. Esto puede incluir listas de dispositivos autorizados, control de puertos, validación previa de equipos de terceros, restricción de ejecución automática, análisis previo de soportes, uso de

estaciones intermedias de revisión, trazabilidad de conexiones, segregación de equipos por finalidad, procedimientos de autorización y control físico de los medios empleados. En entornos industriales, su eficacia depende de adaptar estas medidas al uso real en planta: portátiles de mantenimiento, memorias USB para actualizaciones o transferencia de configuraciones, equipos de fabricante, herramientas de diagnóstico, conexiones puntuales a HMI, estaciones de ingeniería o activos de campo. Su utilidad aumenta cuando se integra con segmentación, bastionado, gestión de identidades, registro de intervenciones y procedimientos operativos claros.

Ventajas:

- Reduce un vector frecuente de entrada de malware y acceso no controlado.
- Mejora la trazabilidad sobre qué dispositivos se conectan, cuándo y con qué finalidad.
- Ayuda a proteger activos sensibles frente a intervenciones locales no gobernadas.
- Permite compatibilizar necesidades de mantenimiento y soporte con mayor nivel de control.
- Complementa la protección del puesto, el NAC, la segmentación y la gestión de privilegios.

Limitaciones y consideraciones:

- Su eficacia depende de que las excepciones estén bien definidas y no se conviertan en una práctica informal permanente.
- En entornos industriales, ciertas tareas de mantenimiento o integración pueden depender de soportes y equipos externos difíciles de sustituir.
- Un control excesivamente rígido puede generar bloqueos operativos o fomentar vías alternativas no gobernadas.
- No sustituye al bastionado, la segmentación, la gestión de accesos ni la monitorización del entorno.
- Se requiere coordinación con operación, mantenimiento, proveedores y responsables técnicos para asegurar que el control sea aplicable y sostenible.

Relación con otros controles: Se relaciona con la protección del puesto de trabajo, el MDM, el NAC, la gestión de identidades y accesos, el acceso remoto seguro, el EDR, la

detección de integridad de ficheros, la segmentación, la monitorización de activos y comunicaciones OT y los procedimientos operativos de mantenimiento y cambio.

Casos habituales de uso: Se emplea para controlar memorias USB, discos externos, portátiles de mantenimiento, equipos de integradores, herramientas de diagnóstico, soportes de transferencia de configuraciones, actualizaciones locales, recogida de registros y cualquier otro dispositivo ajeno que precise conectarse a HMI, estaciones de ingeniería, servidores de supervisión, activos OT o equipos corporativos con relevancia operativa.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la conexión segura de dispositivos externos es una de las medidas compensatorias más relevantes cuando no es viable eliminar completamente el uso de medios extraíbles o equipos de terceros. Su utilidad aumenta cuando se combina con procedimientos formales de autorización, análisis previo en estaciones intermedias, control de privilegios, bastionado de los sistemas receptores, segmentación y registro detallado de las intervenciones realizadas.

5.7.6 Protección de aplicaciones SaaS

Categoría: Protección del puesto, de los activos y de los soportes de operación

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: La protección de aplicaciones SaaS comprende el conjunto de medidas orientadas a gobernar, supervisar y asegurar el uso de servicios y aplicaciones consumidos en modalidad *Software as a Service*, reduciendo los riesgos asociados al acceso distribuido, a la exposición de datos, a la configuración insegura, al uso indebido de identidades y a la integración con otros sistemas de la organización. Su relevancia va más allá del ámbito estrictamente corporativo, ya que muchas organizaciones industriales emplean soluciones SaaS para colaboración, gestión documental, ticketing, soporte remoto, monitorización, analítica, mantenimiento, trazabilidad, gestión de terceros o servicios de apoyo a la operación. Por este motivo, una aplicación SaaS mal gobernada puede convertirse en un punto de entrada, de fuga de información o de dependencia insegura con impacto indirecto o directo sobre la actividad.

Objetivo: Reducir el riesgo derivado del uso de aplicaciones SaaS, garantizando que el acceso, la configuración, la compartición de información, las integraciones y los

permisos asociados se gestionen de manera controlada y coherente con las políticas de seguridad de la organización. En el ámbito industrial, su objetivo incluye también evitar que los servicios SaaS introduzcan exposiciones no gobernadas sobre documentación técnica, datos operativos, credenciales, flujos de mantenimiento o dependencias con terceros.

Ejemplo de problemas de seguridad en SaaS. Fuente: Intellisoft (2024)

Cómo funciona / cómo se implanta: Su implantación parte de la identificación de las aplicaciones SaaS autorizadas, del tipo de información que manejan, de los usuarios que acceden a ellas, de las integraciones activas y de los riesgos asociados a su uso. A partir de esa base, se aplican medidas como gestión centralizada de identidades, MFA, políticas de acceso condicional, revisión de permisos, control de compartición, configuración segura de la aplicación, registro de actividad, protección de sesiones, clasificación de la información y supervisión de las integraciones con servicios internos o externos. En entornos industriales, resulta especialmente importante distinguir entre aplicaciones SaaS de uso general y aquellas que tienen relación con documentación técnica, gestión operativa, mantenimiento, monitorización o servicios conectados a la realidad OT, ya que el riesgo asociado no depende sólo de la criticidad de la aplicación, sino también del tipo de información o proceso con el que se vincula. Su eficacia aumenta cuando se integra con identidad, DLP, CASB/SASE, procedimientos de uso seguro y revisión periódica de las configuraciones y permisos.

Ventajas:

- Mejora el control sobre el uso de servicios cloud y aplicaciones distribuidas.
- Reduce el riesgo de exposición indebida de información, permisos excesivos o configuraciones inseguras.

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

- Ayuda a reforzar la protección de identidades y sesiones en aplicaciones de uso frecuente.
- Resulta útil para gobernar integraciones con terceros, compartición documental y servicios de apoyo a la operación.
- Complementa el control de accesos, el DLP y la supervisión de actividades en entornos híbridos.

Limitaciones y consideraciones:

- Su eficacia depende de conocer qué aplicaciones SaaS están realmente en uso y con qué finalidad.
- Puede quedar limitada si existe uso informal o no inventariado de servicios cloud por parte de los usuarios.
- En entornos industriales, el riesgo puede infravalorarse si se considera que una aplicación SaaS no afecta a la operación por no estar dentro de la red OT.
- No sustituye la gestión de identidades, la clasificación de la información ni los procedimientos de uso seguro y compartición.
- Se requiere revisión continuada de configuraciones, permisos, integraciones y cambios introducidos por el proveedor del servicio.

Relación con otros controles: Se relaciona con la seguridad en el email, con el DLP, con el CASB / SASE, con la gestión de identidades y accesos, con el MFA, con el acceso remoto seguro, con el MDM, con la monitorización y operación de seguridad y con los procedimientos organizativos orientados a la clasificación y al uso seguro de la información.

Casos habituales de uso: Se emplea para gobernar aplicaciones cloud de colaboración, gestión documental, soporte técnico, ticketing, analítica, monitorización, mantenimiento, relación con terceros, intercambio de información técnica y otras plataformas SaaS que, sin formar parte de la red OT, pueden influir en la seguridad global de la organización por la información que almacenan, procesan o comparten.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la protección de aplicaciones SaaS resulta especialmente útil cuando la organización depende de plataformas cloud para gestión, soporte o intercambio de información con terceros, y puede actuar como medida compensatoria parcial frente a la imposibilidad de eliminar determinadas dependencias externas. Su utilidad aumenta cuando se combina con MFA, control de permisos, DLP, políticas de acceso condicional, revisión de

integraciones y procedimientos claros sobre el tipo de información que puede almacenarse, compartirse o tratarse en estos servicios.

5.8 Identidad, acceso y administración segura

El control riguroso de las identidades, de los privilegios y de las sesiones de acceso constituye un núcleo fundamental de la ciberseguridad industrial moderna. En esta subsección se regulan **capacidades destinadas a garantizar que el acceso a los sistemas, activos y servicios se realiza de manera autenticada, trazable, proporcionada al riesgo y compatible con las necesidades de operación, mantenimiento e intervención de terceros**.

5.8.1 MFA

Categoría: Identidad, acceso y administración segura

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

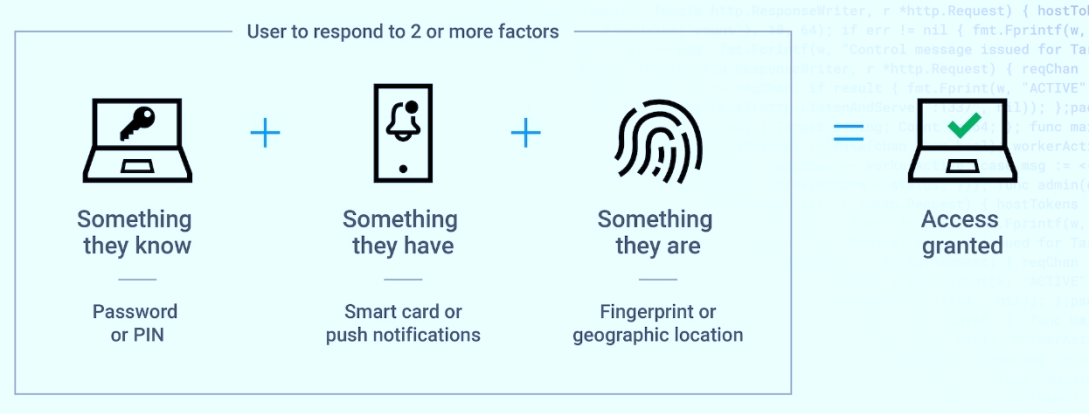
Función en NIST CSF: Protect

Descripción: La autenticación multifactor (MFA, *Multi-Factor Authentication*) es un mecanismo de seguridad que requiere la combinación de dos o más factores de autenticación independientes para verificar la identidad de un usuario antes de conceder acceso a un sistema, servicio o recurso. Estos factores suelen basarse en algo que el usuario sabe, algo que posee o algo que es (biometría). Su propósito es reducir la dependencia exclusiva de las credenciales tradicionales, limitando el riesgo de acceso indebido en caso de robo, filtración, reutilización o compromiso de una contraseña. En entornos industriales, el MFA resulta especialmente relevante para accesos remotos, cuentas privilegiadas, portales de gestión, servicios expuestos y sistemas intermedios desde los que puede conseguirse acceso a la red operativa.

Objetivo: Reducir la probabilidad de acceso no autorizado derivado del compromiso de credenciales, reforzando la verificación de identidad y dificultando el uso indebido de cuentas con acceso a recursos sensibles. En el ámbito industrial, su objetivo incluye también proteger puntos de entrada que pueden servir de puente hacia servicios de supervisión, administración, mantenimiento o interacción con activos OT.

Cómo funciona / cómo se implanta: Su implantación se basa en la incorporación de un segundo factor —o más de uno— al proceso de autenticación habitual. Ello puede materializarse mediante aplicaciones autenticadoras, tokens físicos, certificados,

mensajes de verificación, claves de seguridad u otros mecanismos equivalentes, según el nivel de riesgo y el contexto de uso. En entornos industriales, su aplicación debe priorizar los accesos con mayor impacto potencial: administración remota, acceso de terceros, cuentas privilegiadas, servicios publicados, VPN, servidores de salto, portales de soporte y otros puntos de interconexión entre IT y OT. Su eficacia depende no sólo de la fortaleza del segundo factor, sino también de la correcta integración con la gestión de identidades, con el control de sesiones, con los procedimientos operativos y con la experiencia real de uso, evitando soluciones que induzcan excepciones permanentes o deterioro de la operativa.



Funcionamiento del MFA. Fuente: Akamai (n.d.)

Ventajas:

- Reduce de manera significativa el riesgo asociado al robo o reutilización de contraseñas.
- Refuerza la protección de cuentas privilegiadas, accesos remotos y servicios expuestos.
- Mejora la seguridad de identidades con acceso a entornos sensibles o intermedios.
- Complementa la gestión de identidades y accesos con una capa adicional de verificación.
- Resulta especialmente útil en escenarios con terceros, movilidad y administración distribuida.

Limitaciones y consideraciones:

- Su eficacia disminuye si se mantiene como excepción el acceso sin segundo factor en cuentas críticas.

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

- En entornos industriales, su implantación puede verse condicionada por compatibilidad, disponibilidad o procedimientos legados.
- No sustituye al principio de mínimo privilegio, la segmentación ni el control de sesiones.
- Se requiere una buena gestión del ciclo de vida de los factores, de las altas y bajas de usuarios y de los mecanismos de recuperación.
- Debe evitarse que la dificultad operativa derive en soluciones informales o compartición de credenciales y dispositivos de autenticación.

Relación con otros controles: Se relaciona con la IAM, el PAM, el acceso remoto seguro, la gestión de sesiones y trazabilidad, el control de accesos de terceros y proveedores, la seguridad en el email, el MDM y con las medidas compensatorias orientadas a reducir el riesgo de acceso indebido en entornos con exposición elevada.

Casos habituales de uso: Empleado en accesos VPN, portales de administración, servidores de salto, cuentas privilegiadas, plataformas cloud, servicios de acceso remoto de terceros, consolas de gestión, correo corporativo, aplicaciones críticas y recursos intermedios desde los que puede alcanzarse información sensible o entornos operativos.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el MFA es una de las medidas compensatorias más eficaces cuando no es viable reducir de inmediato toda la exposición de un servicio remoto o eliminar ciertos accesos necesarios para operación y mantenimiento. Su utilidad aumenta cuando se combina con permisos limitados, segmentación, control de sesiones, trazabilidad y revisión periódica de las cuentas con capacidad de acceso a recursos críticos.

5.8.2 IAM

Categoría: Identidad, acceso y administración segura

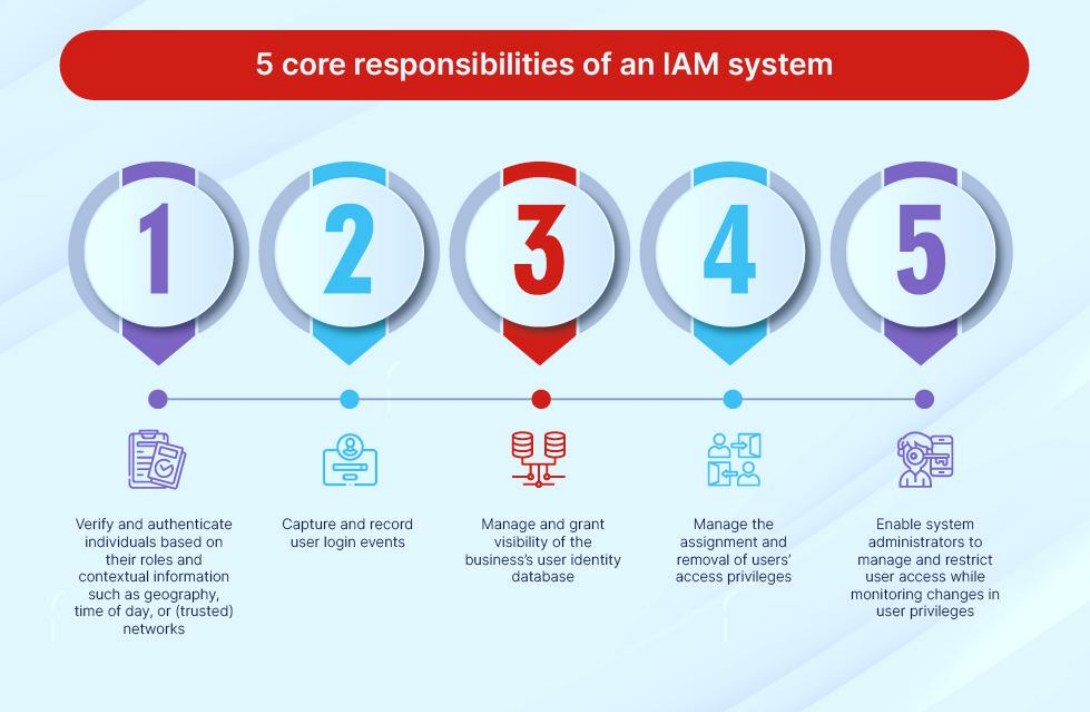
Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect, Govern

Descripción: La gestión de identidades y accesos (IAM, *Identity and Access Management*) comprende el conjunto de políticas, procesos y capacidades técnicas orientadas a definir, administrar, revisar y retirar los permisos de acceso a los sistemas, aplicaciones, datos y servicios de la organización. Su propósito es asegurar que cada

persona, cuenta o entidad disponga únicamente de los accesos necesarios para desempeñar sus funciones, bajo criterios de trazabilidad, segregación de funciones y control continuado del ciclo de vida de las identidades. En entornos industriales, la IAM resulta especialmente relevante por la coexistencia de usuarios internos, personal de operación, mantenimiento, ingeniería, terceros, cuentas de servicio y accesos híbridos entre entornos IT y OT.



Funciones principales de un sistema IAM. Fuente: Fortinet (n.d.)

Objetivo: Reducir el riesgo de acceso indebido, privilegios excesivos, cuentas no gubernadas o permanencia innecesaria de permisos, reforzando el principio de mínimo privilegio y la coherencia del modelo de acceso de la organización. En el ámbito industrial, su objetivo incluye también limitar la exposición derivada de cuentas con acceso a servicios sensibles, sistemas intermedios, plataformas de supervisión, infraestructuras de mantenimiento y recursos desde los que pueda alcanzarse el entorno operativo.

Cómo funciona / cómo se implanta: Su implantación se basa en la definición de un modelo de identidades y permisos asociado a las funciones reales de la organización, a los perfiles de usuario, a las responsabilidades operativas y a las necesidades de acceso a sistemas y servicios. Esto incluye el alta, modificación y baja de cuentas; la asignación de roles; la revisión periódica de permisos; el control de las cuentas compartidas, técnicas y de servicio; la federación cuando proceda; y la integración con mecanismos como MFA, políticas de acceso condicional, registro de actividad y procedimientos de

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

autorización. En entornos industriales, la IAM debe adaptarse a realidades específicas, como personal de planta por turnos, acceso temporal de proveedores, cuentas vinculadas a aplicaciones de fabricante, servicios intermedios, HMI, estaciones de ingeniería o entornos de administración que conectan IT y OT. Su eficacia depende de que el modelo de acceso refleje la realidad operativa y no se limite a una visión puramente corporativa.

Ventajas:

- Reduce la acumulación de privilegios innecesarios y el acceso no gobernado.
- Mejora la coherencia entre funciones reales, permisos asignados y trazabilidad.
- Facilita la aplicación del principio de mínimo privilegio y de la segregación de funciones.
- Refuerza el control sobre cuentas internas, de terceros, técnicas y de servicio.
- Complementa el MFA, el PAM y el control de sesiones con una base sólida de gobernanza de acceso.

Limitaciones y consideraciones:

- Su utilidad disminuye si los roles y permisos no reflejan la operativa real de la organización.
- En entornos industriales, pueden existir cuentas legadas, compartidas o dependientes de software de fabricante difíciles de gobernar a corto plazo.
- No sustituye al PAM, el control de sesiones ni la segmentación del acceso entre dominios.
- Se requiere revisión continua del ciclo de vida de las identidades, especialmente en entornos con terceros, turnos y cambios frecuentes de personal.
- Debe evitarse que la necesidad operativa justifique de forma permanente cuentas genéricas, privilegios excesivos o excepciones sin trazabilidad.

Relación con otros controles: Se relaciona con el MFA, el PAM, el acceso remoto seguro, la gestión de sesiones y trazabilidad, el control de accesos de terceros y proveedores, el MDM, la seguridad en el email y la monitorización y operación de seguridad. Constituye la base de gobernanza sobre la que se apoyan el resto de los controles de acceso y administración segura.

Casos habituales de uso: Se emplea para definir roles de acceso a sistemas corporativos y operativos, revisar permisos de personal interno y terceros, retirar

accesos obsoletos, controlar cuentas de servicio, aplicar políticas de segregación de funciones, gestionar identidades en plataformas cloud y reforzar el modelo de acceso a recursos intermedios con impacto potencial sobre IT y OT.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la IAM resulta especialmente útil como medida estructural para reducir riesgo acumulado en organizaciones con cuentas antiguas, privilegios excesivos o accesos poco gobernados. También puede actuar como medida compensatoria parcial cuando no es viable modificar de inmediato la arquitectura o reducir toda la exposición existente, ya que permite acotar mejor quién puede acceder, a qué recursos y en qué condiciones.

5.8.3 PAM

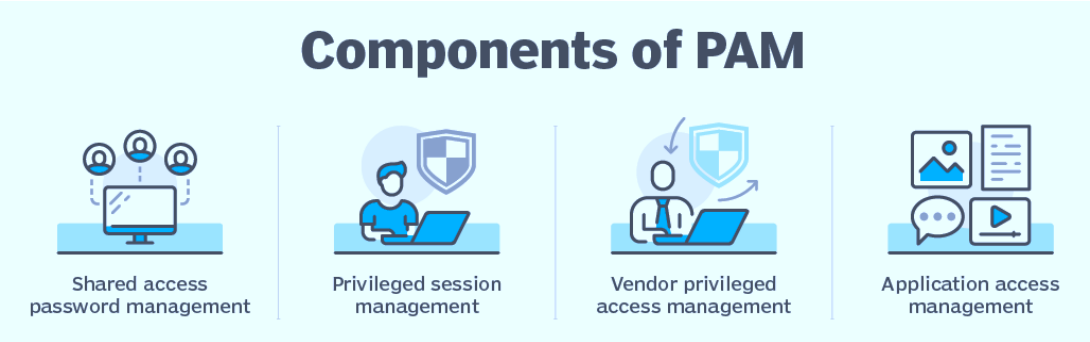
Categoría: Identidad, acceso y administración segura

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect, Govern

Descripción: La gestión de accesos privilegiados (PAM, *Privileged Access Management*) comprende el conjunto de mecanismos destinados a controlar, limitar, supervisar y proteger el uso de cuentas, credenciales y sesiones con privilegios elevados sobre sistemas, aplicaciones, infraestructura y entornos de administración. Su propósito es reducir el riesgo asociado al abuso, compromiso o uso indebido de accesos con capacidad de modificación, configuración, administración o ejecución de acciones críticas. En entornos industriales, el PAM resulta especialmente relevante porque determinadas cuentas privilegiadas permiten acceder a servidores de supervisión, estaciones de ingeniería, sistemas intermedios, herramientas de mantenimiento, servidores de salto, servicios remotos y otros recursos desde los que puede impactarse de forma directa o indirecta sobre la operación.



Elementos de solución PAM. Fuente: Techtarget (2025)

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

Objetivo: Reducir la exposición derivada del uso de cuentas privilegiadas, reforzando el control sobre quién accede, en qué condiciones, durante cuánto tiempo, con que permisos y con qué nivel de trazabilidad. En el ámbito industrial, su objetivo incluye también limitar el riesgo asociado a intervenciones de administración, mantenimiento o soporte sobre sistemas con relevancia operativa, especialmente cuando participan terceros o se accede a recursos de alta criticidad.

Cómo funciona / cómo se implanta: Su implantación suele basarse en la identificación de las cuentas privilegiadas existentes, en su clasificación según criticidad y uso, y en la incorporación de mecanismos como gestión segura de credenciales, rotación periódica de contraseñas, acceso justo a tiempo (JIT), autorización previa, bóvedas de credenciales, registro de sesiones, restricción de uso directo de cuentas administrativas y control del acceso a recursos críticos a través de canales o componentes específicos. En entornos industriales, el PAM debe adaptarse a realidades como accesos de mantenimiento, cuentas compartidas heredadas, intervención de fabricantes o integradores, administración de sistemas OT, herramientas de ingeniería y necesidades de disponibilidad. Su eficacia depende de que exista una gobernanza clara sobre qué cuentas son privilegiadas, quiénes puede utilizarlas, en qué condiciones operativas y cómo se revisa su utilización a lo largo del tiempo.

Ventajas:

- Reduce el riesgo asociado a cuentas con altos privilegios y el acceso a recursos críticos.
- Mejora la trazabilidad sobre el uso de credenciales y sesiones administrativas.
- Dificulta el abuso de cuentas compartidas, permanentes o poco gobernadas.
- Resulta especialmente útil para controlar intervenciones de terceros y accesos de mantenimiento.
- Complementa la IAM, el MFA y el control de sesiones con una capa específica sobre accesos de mayor impacto.

Limitaciones y consideraciones:

- Su utilidad disminuye si no se identifican correctamente todas las cuentas privilegiadas relevantes.
- En entornos industriales, pueden existir cuentas heredadas, credenciales incrustadas o dependencias de software de fabricante que dificulten la implantación completa.

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

- No sustituye la segmentación, el acceso remoto seguro ni la revisión de la arquitectura.
- Se requiere coordinación estrecha con operación, mantenimiento, seguridad y terceros para evitar bloqueos o excepciones permanentes.
- Debe evitarse una implantación sólo formal que no modifique el uso real de cuentas administrativas ni reduzca la dependencia de credenciales compartidas.

Relación con otros controles: Se relaciona con la IAM, con el MFA, con el acceso remoto seguro, con la gestión de sesiones y trazabilidad, con el control de accesos de terceros y proveedores, con la segmentación de red, con la monitorización y operación de seguridad y con los procedimientos de cambio y mantenimiento. Constituye una capa esencial para gobernar los accesos de mayor riesgo dentro de la administración segura.

Casos habituales de uso: Se emplea para controlar cuentas administrativas en servidores, HMI, estaciones de ingeniería, sistemas intermedios, infraestructuras de acceso remoto, servicios cloud, herramientas de gestión, intervención de fabricantes o integradores y entornos en los que el uso de credenciales privilegiadas puede tener impacto significativo sobre la seguridad o la operación.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el PAM es una de las medidas más valiosas para reducir riesgo cuando no es viable eliminar completamente ciertos accesos administrativos o dependencias de terceros. Su utilidad aumenta cuando se combina con MFA, servidores de salto, registro de sesiones, permisos temporales, revisión periódica de uso y segmentación del acceso a sistemas críticos.

5.8.4 Acceso remoto seguro

Categoría: Identidad, acceso y administración segura

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: El acceso remoto seguro (*Secure Remote Access*), comprende el conjunto de mecanismos, procedimientos y condiciones técnicas destinados a permitir la conexión a sistemas, servicios y entornos de la organización desde localizaciones externas sin comprometer la seguridad de los recursos accesibles ni la integridad del entorno. Su relevancia es especialmente alta en organizaciones industriales, donde el soporte remoto, el mantenimiento, la supervisión distribuida, la intervención de

terceros y la necesidad de continuidad operativa hacen que determinadas conexiones remotas sean inevitables. Su propósito no es simplemente permitir conectividad desde fuera, sino hacerlo de forma controlada, limitada, trazable y compatible con la criticidad de los activos y con las necesidades del proceso.

Objetivo: Reducir el riesgo asociado a las conexiones remotas, limitando la posibilidad de acceso indebido, movimiento lateral, abuso de credenciales o exposición excesiva de servicios internos. En el ámbito industrial, su objetivo incluye también permitir tareas legítimas de soporte, mantenimiento y administración sin abrir vías de acceso amplias o poco gobernadas hacia sistemas operativos, de supervisión o de control.

Cómo funciona / cómo se implanta: Su implantación se basa en la combinación de múltiples capas de protección: autenticación reforzada, segmentación del acceso, limitación de servicios expuestos, uso de servidores de salto, trazabilidad de las sesiones, permisos mínimos, validación previa de las conexiones, restricción temporal del acceso y monitorización de las actividades realizadas. En entornos industriales, el acceso remoto seguro debe evitar esquemas amplios y permanentes que concedan visibilidad o conectividad innecesaria sobre la red OT. Por el contrario, conviene estructurarlo en torno a recursos intermedios, autorización previa, acceso justo en el momento necesario, revisión de sesiones y políticas específicas para terceros y personal de mantenimiento. Su eficacia depende no sólo de la tecnología utilizada, sino también de la definición clara de quién puede conectarse, a qué recurso en concreto, en qué condiciones, durante cuánto tiempo y con qué supervisión.

Ventajas:

- Permite mantener capacidades de soporte, mantenimiento y administración sin presencia física continua.
- Reduce el riesgo frente a accesos remotos amplios, permanentes o poco gobernados.
- Mejora la trazabilidad sobre quién accede, cuándo, desde dónde y con qué finalidad.
- Refuerza la protección de recursos intermedios y de alta criticidad frente a terceros o usuarios externos.
- Resulta esencial en entornos con distribución geográfica, servicios remotos o dependencia de fabricantes e integradores.

Limitaciones y consideraciones:

- Su utilidad disminuye si se mantiene acceso amplio a la red en lugar de acceso granular a recursos concretos.
- En entornos industriales, las excepciones permanentes o los accesos no revisados pueden convertirse en una de las principales vías de exposición.
- No sustituye al MFA, el PAM, la segmentación ni el control de sesiones, sino que depende de ellos para ser realmente seguro.
- Se requiere coordinación entre seguridad, operación, mantenimiento y terceros para definir procedimientos compatibles con la continuidad.
- Debe evitarse que la urgencia operativa justifique accesos informales, credenciales compartidas o conexiones sin trazabilidad suficiente.

Relación con otros controles: Se relaciona con el MFA, con la IAM, con el PAM, con la gestión de sesiones y trazabilidad, con el control de accesos de terceros y proveedores, con la segmentación de red y separación IT/OT, con la DMZ industrial, con los servidores de salto, con la monitorización y operación de seguridad y con los procedimientos de mantenimiento y cambio.

Casos habituales de uso: Empleado para mantenimiento remoto, soporte técnico de terceros, administración puntual de sistemas, acceso a recursos intermedios en DMZ, supervisión distribuida, asistencia de fabricantes, intervención de integradores y operación de servicios que requieren conectividad desde localizaciones externas sin exponer directamente la red OT.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el acceso remoto seguro es una de las medidas más críticas y, al mismo tiempo, una de las más frecuentemente mal resueltas. Puede actuar como medida compensatoria cuando no es posible eliminar la necesidad de conexión remota, siempre que se combine con MFA, PAM, servidores de salto, registro de sesiones, permisos temporales, segmentación y revisión periódica de las conexiones autorizadas.

5.8.5 Gestión de sesiones y trazabilidad

Categoría: Identidad, acceso y administración segura

Tipología: Técnica / mixta

Función defensiva predominante: Detectiva

Función en NIST CSF: Detect

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

Descripción: La gestión de sesiones y trazabilidad comprende el conjunto de mecanismos orientados a controlar, registrar, supervisar y revisar las sesiones de acceso a sistemas, servicios y recursos críticos, así como a conservar evidencia suficiente sobre quien accedió, cuándo, desde dónde, con qué privilegios y qué acciones realizó. Su propósito es reforzar la rendición de cuentas, mejorar la capacidad de análisis e investigación y reducir el riesgo derivado de sesiones no monitorizadas, mal utilizadas o difíciles de atribuir. En entornos industriales, este control resulta especialmente relevante en accesos administrativos, intervenciones de mantenimiento, conexiones remotas, operaciones realizadas por terceros y sesiones sobre sistemas con impacto operativo directo o indirecto.

Objetivo: Asegurar que las sesiones con acceso a recursos sensibles sean controladas y atribuibles, reduciendo el riesgo de actuaciones no autorizadas, dificultando el abuso de cuentas privilegiadas y mejorando la capacidad de la organización para reconstruir eventos, investigar incidentes y revisar actuaciones con impacto potencial sobre el entorno. En el ámbito industrial, su objetivo incluye también reforzar la seguridad de las intervenciones remotas o administrativas sobre sistemas críticos, especialmente cuando participan terceros, personal técnico o cuentas de alto privilegio.

Cómo funciona / cómo se implanta: Su implantación se basa en la incorporación de mecanismos que permitan establecer sesiones bajo condiciones controladas y dejar registro suficiente de su actividad. Ello puede incluir identificación unívoca del usuario, asociación de la sesión con el recurso y con el momento temporal, registro de eventos relevantes, grabación o transcripción de sesiones cuando proceda, conservación de evidencias, revisión posterior e integración con los procesos de análisis y respuesta. En entornos industriales, resulta especialmente importante aplicar estos mecanismos a accesos remotos, intervenciones de mantenimiento, uso de servidores de salto, cuentas privilegiadas, sistemas de supervisión, estaciones de ingeniería y otros puntos de administración desde los que puedan ejecutarse cambios sensibles. Su eficacia depende de que los registros sean útiles, completos, consultables y alineados con los procedimientos reales de operación y seguridad.

Ventajas:

- Mejora la atribución de las acciones realizadas sobre sistemas y recursos críticos.
- Refuerza la trazabilidad de accesos remotos, administrativos y privilegiados.
- Facilita la investigación de incidentes, errores operativos y usos indebidos.

- Resulta especialmente útil en intervenciones de terceros, mantenimiento y administración sensible.
- Complementa el MFA, el PAM y el acceso remoto seguro con una capa de evidencia y supervisión.

Limitaciones y consideraciones:

- Su valor disminuye si los registros no son completos, no se revisan o no pueden correlacionarse con otros eventos.
- En entornos industriales, la grabación o supervisión de sesiones debe compatibilizarse con las necesidades operativas y con la protección de información sensible.
- No sustituye la segmentación, el control de identidades ni la limitación de privilegios.
- Puede generar volumen significativo de evidencia que requiere conservación, consulta y criterio de revisión.
- Debe evitarse que la trazabilidad se reduzca a una formalidad sin utilidad real para análisis, auditoría o respuesta.

Relación con otros controles: Se relaciona con el MFA, la IAM, el PAM, el acceso remoto seguro, el control de accesos de terceros y proveedores, la monitorización y operación de seguridad, la respuesta ante incidentes, el SIEM y los procedimientos de cambio y mantenimiento. Constituye una capa esencial para reforzar la seguridad y la auditabilidad de las sesiones con impacto relevante.

Casos habituales de uso: Se emplea para registrar intervenciones remotas, sesiones administrativas, accesos a servidores de salto, operaciones sobre estaciones de ingeniería, actuaciones de proveedores, administración de sistemas críticos, revisión de cambios sensibles e investigación posterior de eventos con posible impacto sobre la operación o la seguridad.

Observaciones / medidas compensatorias asociadas: en entornos industriales, la gestión de sesiones y trazabilidad resulta especialmente útil como medida compensatoria cuando no es viable eliminar ciertos accesos administrativos o remotos, ya que al menos permite reforzar el control, la atribución y la revisión posterior de las actuaciones realizadas. Su utilidad aumenta cuando se combina con MFA, PAM, permisos temporales, servidores de salto y procedimientos claros de revisión de las sesiones con mayor criticidad.

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

5.8.6 Control de accesos de terceros y proveedores

Categoría: Identidad, acceso y administración segura

Tipología: Organizativa / técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Govern, Protect

Descripción: El control de accesos de terceros y proveedores comprende el conjunto de medidas orientadas a regular, limitar, supervisar y revisar la conexión de entidades ajenas a la organización con sus sistemas, servicios, aplicaciones y entornos operativos. En entornos industriales, este control resulta especialmente relevante por la elevada dependencia de fabricantes, integradores, mantenedores, proveedores tecnológicos, servicios de soporte y empresas auxiliares que, con frecuencia, precisan acceder de forma puntual o recurrente a recursos con impacto directo o indirecto sobre la operación. Su propósito es asegurar que estas interacciones se produzcan bajo criterios de necesidad, mínimo privilegio, autorización formal, trazabilidad y compatibilidad con la continuidad y con la seguridad del proceso.

Objetivo: Reducir el riesgo derivado del acceso de terceros a recursos de la organización, limitando la exposición, evitando permisos excesivos y asegurando que toda conexión externa se produzca en condiciones controladas, temporales y auditables. En el ámbito industrial, su objetivo incluye también minimizar el riesgo de que proveedores o personal externo se conviertan en un vector de acceso, propagación, error operativo o alteración no autorizada sobre sistemas críticos.

Ejemplo de riesgos de la cadena de suministro. Fuente: ssl2buy (n.d.)

Cómo funciona / cómo se implanta: Su implantación se basa en la definición de políticas específicas para terceros, diferenciando tipos de proveedor, alcance funcional del acceso, duración, recursos autorizados, canales de conexión, requisitos de autenticación y mecanismos de supervisión. Ello incluye procesos de alta y baja, autorización previa, revisión periódica de permisos, uso de cuentas nominativas, acceso justo a tiempo cuando proceda, restricción de conexión a través de recursos intermedios, registro de sesiones, limitación por horario o finalidad e integración con procedimientos de mantenimiento y cambio. En entornos industriales, este control debe adaptarse a escenarios habituales como soporte remoto de fabricante, intervenciones de integradores, mantenimiento correctivo o preventivo, actualizaciones, supervisión de servicios y acceso puntual a estaciones de ingeniería, servidores de supervisión o componentes intermedios. Su eficacia depende de que los terceros no se integren en la organización mediante cuentas genéricos, canales informales o accesos permanentes sin revisión.

Ventajas:

- Reduce la exposición derivada de la conexión de entidades externas con acceso a recursos sensibles.
- Mejora la trazabilidad y la gobernanza sobre intervenciones de terceros.
- Facilita la aplicación de mínimo privilegio, temporalidad y control de alcance.

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

- Resulta especialmente útil en entornos con fuerte dependencia de fabricantes, integradores o soporte remoto.
- Complementa el MFA, el PAM, el acceso remoto seguro y la gestión de sesiones con criterios específicos para accesos externos.

Limitaciones y consideraciones:

- Su eficacia disminuye si la organización mantiene accesos permanentes, cuentas compartidas o excepciones no revisadas para terceros.
- En entornos industriales, las urgencias operativas pueden llevar a relajar controles si no existen procedimientos realistas y asumibles.
- No sustituye la segmentación, el control de sesiones ni la revisión técnica de las actuaciones ejecutadas por terceros.
- Se requiere coordinación contractual, técnica y operativa entre la organización y los proveedores implicados.
- Debe evitarse que la dependencia de terceros derive en una pérdida de gobernanza efectiva sobre los accesos críticos.

Relación con otros controles: Se relaciona con el MFA, con la IAM, con el PAM, con el acceso remoto seguro, con la gestión de sesiones y trazabilidad, con los servidores de salto, con la segmentación de red y separación IT/OT, con la monitorización y operación de seguridad y con los procedimientos de mantenimiento y cambio. Constituye una capa de control esencial en organizaciones industriales con alta interacción con entidades externas.

Casos habituales de uso: Empleado para acceso remoto de fabricantes, mantenimiento por parte de integradores, soporte técnico de terceros, actualizaciones puntuales sobre sistemas industriales, intervenciones sobre HMI o estaciones de ingeniería, análisis de incidencias por proveedores y conexión temporal a recursos intermedios o plataformas de soporte con impacto potencial sobre la operación.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el control de accesos de terceros y proveedores es una de las medidas más importantes para reducir exposición acumulada en organizaciones con fuerte dependencia de soporte externo. También puede actuar como medida compensatoria cuando no es viable eliminar ciertos accesos necesarios para mantenimiento o continuidad, siempre que se combine con MFA, PAM, permisos temporales, servidores de salto, registro de sesiones y revisión periódica de las autorizaciones concedidas.

5.8.7 Programa de gestión de vulnerabilidades

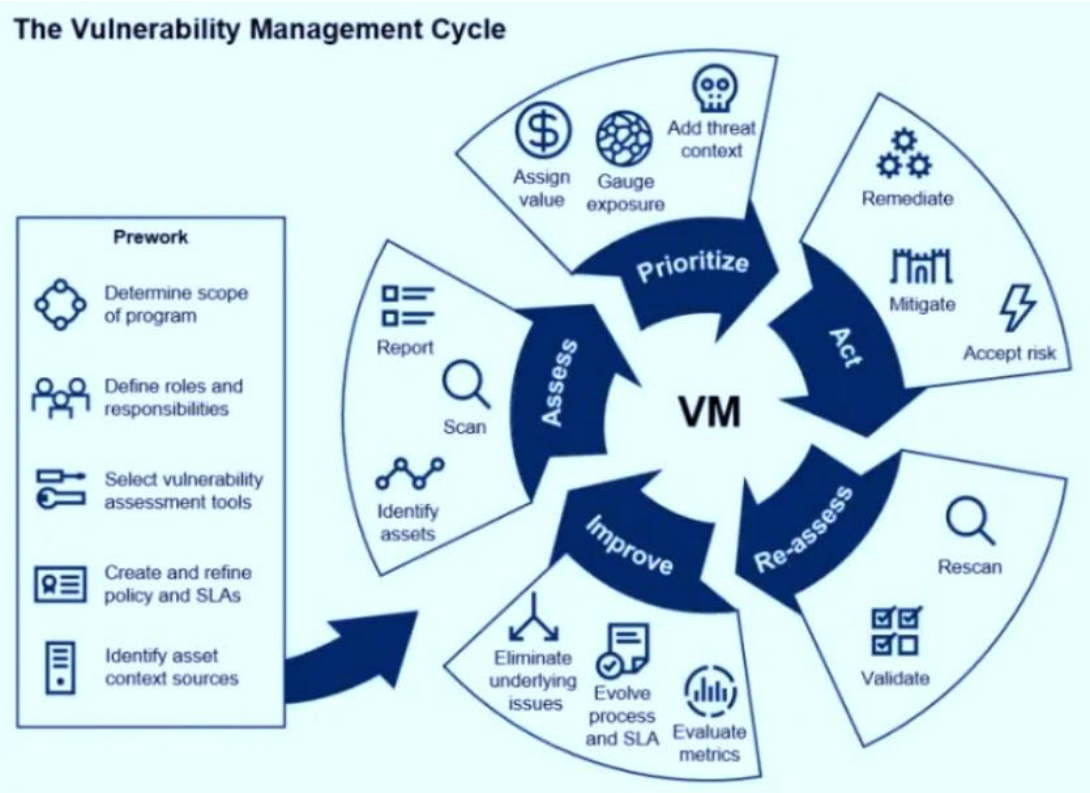
Categoría: Identidad, acceso y administración segura

Tipología: Organizativa / técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Identify, Govern

Descripción: El programa de gestión de vulnerabilidades es el conjunto estructurado de políticas, procesos, responsabilidades y capacidades técnicas destinadas a identificar, evaluar, priorizar, tratar y revisar las vulnerabilidades que afectan a los activos, sistemas, aplicaciones y servicios de la organización. Su finalidad no es sólo detectar debilidades aisladas, sino establecer una disciplina continuada para comprender la exposición real del entorno y decidir de manera proporcionada cómo reducirla a lo largo del tiempo. En entornos industriales, este control resulta especialmente crítico porque la presencia de activos legados, software de fabricante, restricciones de mantenimiento y dependencia de la continuidad operativa hace que la gestión de la vulnerabilidad no pueda limitarse a un enfoque estándar basado únicamente en severidad técnica.



Ciclo de gestión de vulnerabilidades. Fuente: Gartner (n.d.)

Objetivo: Dotar a la organización de un modelo continuo para gobernar la exposición a vulnerabilidades, reduciendo el riesgo de explotación mediante procesos de

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

identificación, priorización y tratamiento alineados con la criticidad de los activos y con el impacto potencial sobre la operación. En el ámbito industrial, su objetivo incluye también asegurar que la decisión sobre cómo tratar cada vulnerabilidad tenga en cuenta la disponibilidad, la seguridad funcional, la dependencia de terceros y la viabilidad real de las medidas correctivas o compensatorias.

Cómo funciona / cómo se implanta: Su implantación parte de la definición de un marco de gobernanza: alcance, roles, fuentes de información, activos incluidos, criterios de criticidad, metodología de evaluación, tiempos objetivo de tratamiento y mecanismos de revisión. Sobre esa base, se regulan actividades como recepción de avisos de seguridad, análisis de vulnerabilidades, correlación con inventarios de activos, evaluación del impacto potencial, priorización según riesgo, definición de medidas de tratamiento y seguimiento del estado de remediación. En entornos industriales, el programa debe incorporar elementos específicos como clasificación de activos OT, dependencia de fabricantes, validación previa de cambios, bastionado, segmentación, medidas compensatorias, coordinación con mantenimiento y revisión del riesgo residual cuando la remediación directa no sea viable. Su eficacia depende de que la organización trate la vulnerabilidad como un proceso continuo de gobernanza y no como una actividad puntual o puramente técnica.

Ventajas:

- Permite gobernar la exposición a vulnerabilidades de forma continuada y estructurada.
- Mejora la priorización de las actuaciones según riesgo real y criticidad del activo.
- Facilita la coordinación entre seguridad, sistemas, operación, mantenimiento y terceros.
- Ayuda a combinar remediación, bastionado y medidas compensatorias de manera coherente.
- Refuerza la trazabilidad de las decisiones adoptadas y el seguimiento del riesgo residual.

Limitaciones y consideraciones:

- Su utilidad disminuye si no existe un inventario fiable de activos y una buena contextualización de su criticidad.
- En entornos industriales, la severidad técnica de una vulnerabilidad no siempre refleja la prioridad real de tratamiento.

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

- No sustituye el análisis de riesgos, la segmentación, el parcheado ni el bastionado, sino que debe coordinarlos.
- Se requiere implicación de múltiples áreas y capacidad real para revisar, decidir y hacer seguimiento de las medidas.
- Debe evitarse que el programa derive en un registro estático de vulnerabilidades sin decisiones operativas ni revisión del estado real de la exposición.

Relación con otros controles: Se relaciona con el análisis de vulnerabilidades, el análisis de riesgos tecnológicos, la revisión de arquitectura, la segmentación, el bastionado de sistemas y servicios, la gestión de parcheado, las validaciones previas y ventanas de mantenimiento, con la visibilidad de activos y comunicaciones OT y las medidas compensatorias. Constituye el marco de gobernanza desde el que se ordenan y priorizan buena parte de las actuaciones técnicas del Catálogo.

Casos habituales de uso: Se emplea para gestionar vulnerabilidades detectadas en activos IT y OT, analizar avisos de fabricantes, priorizar actuaciones en sistemas críticos, coordinar medidas entre áreas técnicas y operativas, revisar exposición acumulada en activos legados, justificar excepciones temporales y dar seguimiento a planes de tratamiento y mitigación.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el programa de gestión de vulnerabilidades es especialmente útil para fundamentar decisiones proporcionadas cuando no es viable aplicar de inmediato una corrección directa. En esos casos, permite documentar la exposición, priorizar activos, definir medidas compensatorias —como segmentación, bastionado, limitación de acceso o refuerzo de la monitorización— y revisar periódicamente si el riesgo residual continúa siendo asumible.

5.8.8 Gestión de parcheado

Categoría: Identidad, acceso y administración segura

Tipología: Organizativa / técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect, Govern

Descripción: La gestión de parcheado comprende el conjunto de políticas, procesos y medidas orientadas a planificar, evaluar, priorizar, aplicar y verificar actualizaciones de seguridad, correcciones y cambios asociados a software, firmware, sistemas operativos, aplicaciones y componentes tecnológicos. Su finalidad es reducir la exposición derivada

de vulnerabilidades conocidas mediante la incorporación controlada de correcciones que mejoren la protección de los activos sin comprometer la estabilidad del entorno. En entornos industriales, este control resulta especialmente delicado, ya que el parcheado no puede tratarse como una actividad automática o indiscriminada: debe compatibilizarse con la continuidad de la operación, con la seguridad funcional, con el soporte de fabricante y con la disponibilidad de ventanas de intervención aceptables.

Ciclo de vida de parcheo. Fuente: Hexnode (2025)

Objetivo: Reducir el riesgo asociado a vulnerabilidades conocidas mediante la aplicación controlada de actualizaciones y correcciones, asegurando que el parcheado se realice con criterio, priorización y verificación suficientes. En el ámbito industrial, su objetivo incluye también minimizar el riesgo de que una actualización introduzca inestabilidad, incompatibilidades o alteraciones no deseadas sobre sistemas críticos para la operación.

Cómo funciona / cómo se implanta: Su implantación parte de la identificación de los activos parcheables, de la recepción y análisis de preavisos de seguridad, de la evaluación de relevancia de las actualizaciones y de la definición de criterios para decidir cuándo, cómo y sobre qué sistemas aplicar cada corrección. Ello incluye priorización (se plantean estrategias para ello en [2]) según criticidad, compatibilidad, exposición y riesgo, así como procedimientos de validación, autorización, planificación y verificación posterior. En entornos industriales, la gestión de parcheado debe estar estrechamente ligada al inventario de activos, a la dependencia de fabricantes, las recomendaciones del proveedor, a la disponibilidad de entornos de prueba, a las

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

ventanas de mantenimiento y medidas compensatorias aplicables cuando la actualización no sea viable a corto plazo. Su eficacia depende de tratar al parcheado como un proceso gubernado, coordinado y revisable, y no como una simple tarea técnica de aplicación de actualizaciones.

Ventajas:

- Reduce la exposición de vulnerabilidades conocidas cuando las actualizaciones son viables y adecuadas.
- Mejora la disciplina de mantenimiento y la trazabilidad sobre el estado de actualización de los activos.
- Facilita la coordinación entre seguridad, sistemas, operación, mantenimiento y terceros.
- Permite integrar criterios de riesgo, compatibilidad y criticidad en la decisión de actualización.
- Complementa el programa de gestión de vulnerabilidades con una vía estructurada de remediación directa.

Limitaciones y consideraciones:

- En entornos industriales, no todas las actualizaciones pueden aplicarse inmediatamente ni con seguridad.
- La compatibilidad con el software de fabricante, la estabilidad y la disponibilidad deben validarse previamente.
- No sustituye la segmentación, el bastionado ni otras medidas compensatorias cuando el parcheado no es viable.
- Se requiere coordinación estrecha con mantenimiento, operación y proveedores para evitar impactos no deseados sobre el proceso.
- Debe evitarse una visión simplista basada sólo en la disponibilidad del parche, sin evaluar el contexto real del activo y el riesgo de cambio.

Relación con otros controles: Se relaciona con el programa de gestión de vulnerabilidades, el análisis de vulnerabilidades, el bastionado de sistemas y servicios, las validaciones previas y ventanas de mantenimiento, la segmentación, la visibilidad de activos y comunicaciones OT, la monitorización y las medidas compensatorias orientadas a reducir exposición cuando no es posible actualizar.

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

Casos habituales de uso: Se emplea para planificar la actualización de servidores, estaciones de trabajo, HMI, componentes software, firmware, sistemas operativos, aplicaciones industriales y equipos de soporte cuando existen parches disponibles, evaluando su relevancia según la criticidad del activo, la exposición y el impacto operativo esperado.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la gestión de parcheado es especialmente útil cuando se integra con un proceso formal de decisión que permita diferenciar entre actualización inmediata, actualización diferida y tratamiento compensatorio. En esos casos, si el parche no puede aplicarse, la organización debe recurrir a medidas como segmentación, bastionado, limitación de accesos, refuerzo de la monitorización o aislamiento funcional del activo afectado, manteniendo trazabilidad sobre el riesgo residual y revisión periódica de la decisión adoptada.

5.8.9 Bastionado de sistemas y servicios

Categoría: Identidad, acceso y administración segura

Tipología: Organizativa / técnica / mixta

Función defensiva predominante: Preventiva

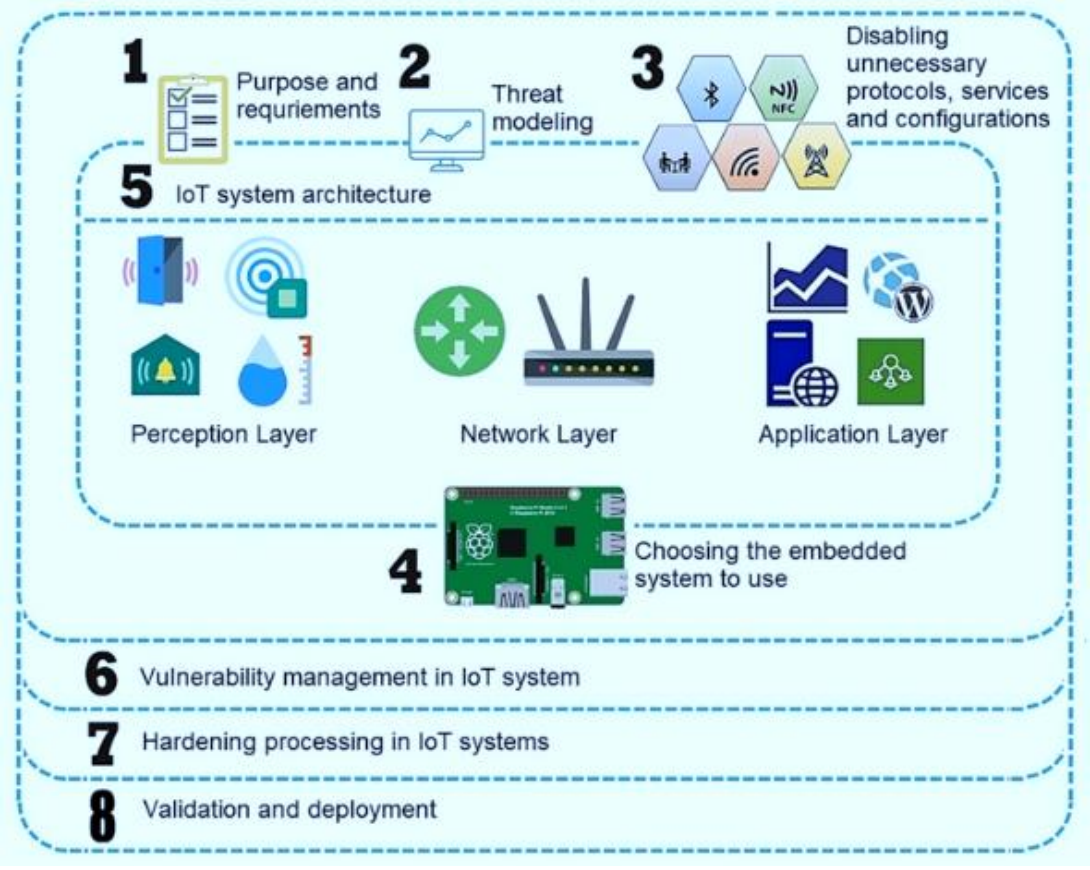
Función en NIST CSF: Protect

Descripción: El bastionado de sistemas y servicios comprende el conjunto de medidas orientadas a reducir la superficie de exposición de los activos mediante la configuración segura de sus componentes, la desactivación de funciones innecesarias, la eliminación de servicios no requeridos, el endurecimiento de parámetros de seguridad y la limitación de las posibilidades de abuso o explotación. Su finalidad es que los sistemas operen con una configuración más controlada, previsible y resistente frente a errores, usos indebidos, compromiso de credenciales, ejecución no autorizada o explotación de vulnerabilidades conocidas. En entornos industriales, este control resulta especialmente importante porque muchos activos no pueden actualizarse con frecuencia, dependen de software de fabricante o permanecen durante largos períodos en servicio, por lo que la reducción de la exposición mediante configuración segura adquiere un valor central.

Objetivo: Reducir el riesgo asociado a la configuración insegura de los sistemas y servicios, limitando la superficie de ataque y dificultando la explotación de debilidades existentes. En el ámbito industrial, su objetivo incluye también reforzar la protección de

activos con soporte limitado, sistemas legados, componentes de operación y servicios intermedios cuyo nivel de exposición no puede reducirse únicamente mediante parcheado o renovación tecnológica.

Cómo funciona / cómo se implanta: Su implantación se basa en la revisión y ajuste de las configuraciones de los sistemas para asegurar que sólo permanezcan activos los componentes, servicios, protocolos, puertos, permisos y funcionalidades estrictamente necesarios para su finalidad. Esto incluye, entre otras medidas, desactivar servicios no utilizados, reforzar políticas de autenticación, limitar privilegios, configurar registro y auditoría, proteger ficheros y directorios sensibles, eliminar software innecesario, aplicar configuraciones seguras por defecto y revisar parámetros que puedan incrementar la exposición del sistema. En entornos industriales, el bastionado debe aplicarse con especial prudencia, ya que ciertos cambios pueden afectar a la compatibilidad con aplicaciones de fabricante, protocolos específicos, herramientas de mantenimiento o necesidades del proceso. Su eficacia depende de conocer bien la función del activo, de validar previamente los cambios y de diferenciar entre activos en los que puede aplicase un bastionado más intenso y aquellos en los que sólo son viables medidas más graduales.



Propuesta de modelo de bastionado en IoT. Fuente: Echeverría, Ceballos et al. (2021)

Ventajas:

- Reduce la superficie de exposición de los sistemas y dificulta la explotación de debilidades.
- Mejora la previsibilidad y control de las configuraciones de los activos.
- Resulta especialmente útil en sistemas legados o con limitaciones de actualización.
- Complementa el parcheado y la segmentación con medidas directas sobre el propio activo.
- Ayuda a limitar software innecesario, servicios expuestos y permisos excesivos.

Limitaciones y consideraciones:

- Su aplicación puede verse limitada por la compatibilidad con software de fabricante o las condiciones de soporte.
- En entornos industriales, un cambio de configuración mal validado puede introducir inestabilidad o impacto operativo.
- No sustituye al parcheado, la segmentación ni la gestión de accesos, sino que debe complementarse con ellos.
- Se requiere conocimiento técnico detallado del activo y de su función en el proceso para evitar cambios contraproducentes.
- Debe evitarse tanto el bastionado insuficiente como la aplicación indiscriminada de guías genéricas no adaptadas al entorno.

Relación con otros controles: Se relaciona con el programa de gestión de vulnerabilidades, la gestión de parcheado, las validaciones previas y ventanas de mantenimiento, la protección del puesto de trabajo, la detección de integridad de ficheros, la segmentación, la monitorización y con las medidas compensatorias orientadas a reducir exposición en activos críticos o con soporte limitado.

Casos habituales de uso: Se emplea en servidores, estaciones de trabajo, HMI, estaciones de ingeniería, sistemas intermedios, servicios remotos, componentes de supervisión y otros activos en los que se precisa reducir funcionalidad innecesaria, reforzar configuraciones y limitar la exposición sin modificar sustancialmente la arquitectura.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el bastionado es una de las medidas compensatorias más útiles cuando no resulta viable

aplicar de inmediato actualizaciones, sustituir componentes o reestructurar la arquitectura. Su utilidad aumenta cuando se combina con segmentación, limitación de acceso, monitorización reforzada, control de cambios y validación previa de las modificaciones antes de su aplicación en sistemas con impacto operativo.

5.8.10 Validaciones previas y ventanas de mantenimiento

Categoría: Identidad, acceso y administración segura

Tipología: Organizativa / técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect, Govern

Descripción: Las validaciones previas y las ventanas de mantenimiento comprenden el conjunto de prácticas orientadas a comprobar de manera anticipada la compatibilidad, viabilidad e impacto de los cambios técnicos antes de su aplicación en sistemas en producción, así como a delimitar períodos específicos en los que dichas intervenciones pueden ejecutarse con menor riesgo para la operación. Su propósito es evitar que actualizaciones, modificaciones de configuración, cambios de componentes, tareas de bastionado o actuaciones correctivas se realicen sin evaluación previa suficiente ni en momentos incompatibles con la continuidad del servicio. En entornos industriales, este control resulta especialmente relevante porque la introducción de cambios no validados puede afectar a la disponibilidad, a la estabilidad del proceso, a la seguridad funcional o a la coordinación entre sistemas y operación.

Objetivo: Reducir el riesgo asociado a la aplicación de cambios en sistemas y servicios, asegurando que las intervenciones técnicas se ejecuten tras una validación suficiente y dentro de períodos controlados que minimicen el impacto operativo. En el ámbito industrial, su objetivo incluye también evitar que actuaciones orientadas a la mejora de la seguridad introduzcan indisponibilidad, incompatibilidades o alteraciones no deseadas sobre activos con función crítica.

Cómo funciona / cómo se implanta: Su implantación se basa en establecer procedimientos para revisar previamente los cambios propuestos, evaluar su compatibilidad con el entorno, comprobar dependencias, identificar riesgos asociados y definir condiciones de ejecución y reversión. Ello puede incluir el uso de entornos de prueba, simulaciones, revisión documental, validación con fabricantes, contraste con mantenimiento y operación, planificación de tareas y definición de criterios de aceptación. La ventana de mantenimiento, por su parte, delimita el período temporal en

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

el que la intervención puede realizarse con menor impacto sobre la actividad normal, contando con los recursos necesarios y con los equipos implicados preparados para supervisar, validar y, si es preciso, revertir el cambio. En entornos industriales, su eficacia depende de que estas prácticas no se reduzcan a una formalidad, sino que reflejen la criticidad real del activo, el momento operativo, el impacto potencial sobre el proceso y la disponibilidad de medios para validar el comportamiento posterior del sistema.

Ventajas:

- Reduce el riesgo de introducir cambios técnicos con impacto no previsto sobre la operación.
- Mejora la coordinación entre seguridad, sistemas, operación, mantenimiento y terceros.
- Facilita la planificación ordenada de actualizaciones, bastionado, correcciones e intervenciones técnicas.
- Refuerza la capacidad de anticipar incompatibilidades y definir medidas de reversión.
- Resulta esencial en entornos industriales en los que la continuidad del proceso condiciona fuertemente la aplicación de cambios.

Limitaciones y consideraciones:

- Su utilidad disminuye si no existen entornos de prueba, documentación suficiente o participación real de las áreas implicadas.
- En entornos industriales, no siempre es sencillo disponer de ventanas amplias o replicar con fidelidad las condiciones de la producción.
- No sustituye el análisis de riesgos, el programa de gestión de vulnerabilidades ni la gestión de parcheado, sino que debe coordinarlos.
- Puede ralentizar la aplicación de medidas correctivas si el proceso no está bien diseñado o resulta excesivamente burocrático.
- Debe evitarse que la presión operativa lleve a omitir validaciones necesarias o a ejecutar cambios fuera de los períodos previstos sin control suficiente.

Relación con otros controles: Se relaciona con el programa de gestión de vulnerabilidades, la gestión de parcheado, el bastionado de sistemas y servicios, el análisis de riesgos tecnológicos, la revisión de arquitectura, la continuidad de negocio y

resiliencia operativa, la respuesta ante incidentes y los procedimientos de cambio y mantenimiento. Constituye una capa de gobernanza esencial para aplicar medidas técnicas de forma compatible con la operación.

Casos habituales de uso: Se emplea antes de aplicar parches, cambios de configuración, modificaciones en HMI o estaciones de ingeniería, actualizaciones de software de fabricante, intervenciones sobre sistemas de supervisión, tareas de bastionado, cambios de conectividad, actuaciones correctivas sobre activos críticos y cualquier otra modificación con potencial impacto sobre la continuidad o la seguridad del proceso.

Observaciones / medidas compensatorias asociadas: En entornos industriales, las validaciones previas y la ventana de mantenimiento son especialmente útiles para reducir el riesgo de que medidas de seguridad bien intencionadas generen efectos adversos sobre la operación. También pueden actuar como soporte esencial de las medidas compensatorias, permitiendo decidir cuándo un cambio puede ejecutarse con seguridad y cuándo, por el contrario, debe diferirse y acompañarse temporalmente de segmentación, bastionado, refuerzo de monitorización o limitación adicional del acceso.

5.9 Respuesta, recuperación y continuidad

La resiliencia de una organización no se mide sólo por su capacidad de evitar incidentes, sino también por la rapidez y eficacia con la que puede contener, investigar, restaurar y recuperar la operación. Este bloque recoge **controles y servicios orientados a la respuesta ante incidentes, al análisis forense, a la restauración de sistemas y datos y a la continuidad operativa**, reforzando la capacidad de la entidad para resistir y superar eventos adversos.

5.9.1 Soporte a la respuesta ante incidentes

Categoría: Respuesta, recuperación y continuidad

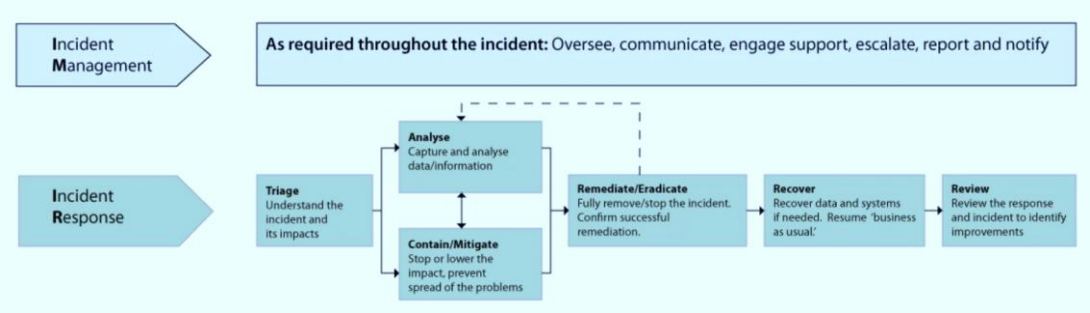
Tipología: Organizativa / técnica / mixta

Función defensiva predominante: Correctiva / de recuperación

Función en NIST CSF: Respond, Recover

Descripción: El soporte a la respuesta ante incidentes comprende el conjunto de capacidades, procedimientos, roles y medios técnicos destinados a preparar, coordinar y ejecutar actuaciones frente a eventos de seguridad que puedan afectar a los sistemas, servicios, activos o procesos de la organización. Su finalidad es asegurar que, una vez detectado un incidente, existan mecanismos claros para analizar la situación, contener

su impacto, escalar decisiones, coordinar a los equipos implicados y recuperar el control del entorno afectado. En entornos industriales, este control resulta especialmente relevante porque la respuesta no puede formularse sólo desde la óptica tecnológica, sino que debe considerar también la continuidad de la operación, la seguridad del proceso, la dependencia de terceros, la seguridad funcional y el riesgo de que una actuación incorrecta agrave la situación.



Etapas de la respuesta ante incidentes. Fuente: NCSC (2019)

Objetivo: Dotar a la organización de una capacidad estructurada para responder de forma ordenada y eficaz ante incidentes de seguridad, reduciendo el tiempo de reacción, limitando el impacto y mejorando la coordinación entre las áreas implicadas. En el ámbito industrial, su objetivo incluye también asegurar que las decisiones de contención, aislamiento, análisis o recuperación se adopten con un conocimiento suficiente del impacto potencial sobre la producción, servicios y los sistemas ciberfísicos.

Cómo funciona / cómo se implanta: Su implantación se basa en la definición de un modelo operativo de respuesta: procedimientos, roles, canales de comunicación, criterios de escalado, tipologías de incidente, mecanismos de coordinación interna y relación con terceros u organismos externos cuando proceda. Ello incluye la identificación de los equipos responsables, la disponibilidad de medios técnicos para análisis y contención, la preparación de guías de actuación, la coordinación con operación y mantenimiento y la realización de ejercicios o revisiones periódicas. En entornos industriales, el soporte a la respuesta debe contemplar escenarios específicos como acceso remoto comprometido, manipulación de cuentas privilegiadas, propagación entre IT y OT, indisponibilidad de sistemas de supervisión, afectación a HMI o estaciones de ingeniería, alteración de configuraciones, interacción con terceros e incidentes con impacto sobre la continuidad del proceso. Su eficacia depende de que el modelo esté adaptado al entorno real y de que las decisiones no se tomen aisladamente desde seguridad sin coordinación con las áreas operativas.

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

Ventajas:

- Mejora la capacidad de reacción frente a incidentes y reduce el tiempo de respuesta.
- Facilita la coordinación entre seguridad, sistemas, operación, mantenimiento y dirección.
- Ayuda a contener incidentes y limitar su impacto sobre los servicios y la operación.
- Refuerza la trazabilidad y la toma de decisiones bajo procedimientos conocidos.
- Resulta esencial para responder de manera segura en entornos con impacto operativo o ciberfísico.

Limitaciones y consideraciones:

- Su utilidad disminuye si se reduce la documentación formal sin capacidad real de ejecución.
- En entornos industriales, una respuesta técnicamente correcta puede resultar operativamente inadecuada si no se evalúa el impacto sobre el proceso.
- No sustituye la detección temprana, la segmentación ni la preparación previa del entorno.
- Se requiere coordinación continuada, adiestramiento y revisión de los procedimientos para que resulten realmente aplicables.
- Debe evitarse la dependencia exclusiva de personas concretas o conocimiento no documentado para la gestión de las primeras actuaciones.

Relación con otros controles: Se relaciona con el SOC, el MDR, el SIEM, el IDS/IPS, el NDR, la monitorización ciberfísica / MES, la visibilidad de activos y comunicaciones OT, los servicios forenses, las copias de seguridad y restauración, la recuperación de operación y continuidad y el plan de continuidad de negocio y resiliencia operativa.

Casos habituales de uso: Se emplea para coordinar la respuesta frente a accesos remotos comprometidos, infecciones por malware o ransomware, propagación entre dominios IT/OT, actividad anómala en cuentas privilegiadas, afectación de sistemas de supervisión, intervenciones no autorizadas de terceros, alteración de configuraciones e incidentes que requieren análisis, contención y recuperación bajo presión operativa.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el soporte a la respuesta ante incidentes es especialmente valioso cuando la organización

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

no puede eliminar totalmente ciertas exposiciones, pero sí prepararse mejor para detectarlas y gestionarlas con rapidez. Su utilidad aumenta cuando se combina con procedimientos específicos para OT, vías de escalado claras, inventario de activos críticos, trazabilidad de accesos, medios de análisis disponibles y coordinación previa con operación, mantenimiento y terceros.

5.9.2 Servicios forenses

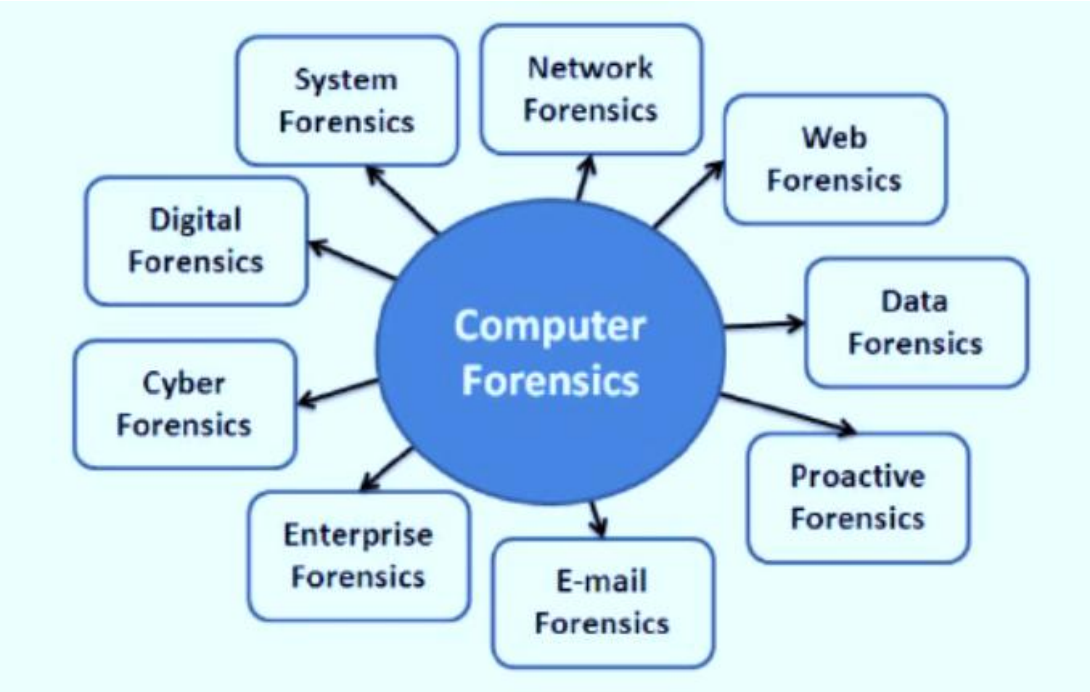
Categoría: Respuesta, recuperación y continuidad

Tipología: Técnica / mixta

Función defensiva predominante: Correctiva / de recuperación

Función en NIST CSF: Respond

Descripción: Los servicios forenses comprenden el conjunto de capacidades, técnicas y procedimientos destinados a la identificación, preservación, recogida, análisis e interpretación de evidencias digitales relacionadas con un incidente de seguridad. Su finalidad es reconstruir lo ocurrido, determinar vectores de acceso, alcance, impacto, persistencia y posibles responsabilidades, así como apoyar la toma de decisiones técnicas, organizativas y, cuando proceda, legales o regulatorias. En entornos industriales, esta capacidad resulta especialmente relevante porque los incidentes pueden afectar no sólo a sistemas informáticos convencionales, sino también a componentes OT, estaciones de ingeniería, HMI, servidores de supervisión, registros operativos, cuentas de terceros y evidencias asociadas al comportamiento del proceso.



Actividades del ámbito forense digital. Fuente: Sridhar N. et al. (2011)

Objetivo: Obtener y analizar evidencias fiables que permitan comprender la naturaleza y el alcance de un incidente, apoyar su contención y recuperación, y preservar información útil para aprendizaje posterior, revisión interna o actuaciones legales y de cumplimiento. En el ámbito industrial, su objetivo incluye también identificar si ha existido impacto sobre sistemas con función operativa, manipulación de configuraciones, alteración de parámetros, acceso indebido de terceros o efectos indirectos sobre la continuidad del proceso.

Cómo funciona / cómo se implanta: Su implantación requiere procedimientos claros para preservar evidencias, delimitar cadena de custodia, decidir cuándo y cómo intervenir sobre los sistemas afectados y coordinar el análisis con las necesidades de continuidad operativa. Ello puede incluir la adquisición de registros, imágenes de disco, memoria, eventos de red, evidencias de endpoints, sesiones administrativas, configuraciones, ficheros de proyecto, registros de HMI, datos de supervisión o información de plataformas de monitorización. En entornos industriales, el enfoque forense debe adaptarse a las restricciones propias del entorno: no siempre es viable aislar o apagar un sistema para capturarlo, ni todos los activos OT permiten técnicas forenses estándar sin riesgo operativo. Por ello, suele ser necesario combinar análisis tradicional con revisión de registros, telemetría, trazabilidad de accesos, copia de configuraciones, correlación con eventos de red y conocimiento del proceso. Su eficacia depende de actuar con rapidez, criterio y coordinación entre seguridad, operación, mantenimiento y, cuando proceda, terceros especializados.

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

Ventajas:

- Permiten comprender con mayor precisión lo que ocurrió durante un incidente.
- Ayudan a identificar vectores de entrada, persistencia, alcance y posibles movimientos laterales.
- Refuerzan la capacidad de mejora posterior, revisión de controles y aprendizaje organizativo.
- Aportan evidencias útiles para auditoría, cumplimiento y posibles actuaciones legales.
- Resultan especialmente valiosos en incidentes con impacto operativo, terceros implicados o dudas sobre manipulación de sistemas críticos.

Limitaciones y consideraciones:

- Su utilidad disminuye si la preservación de evidencias no se activa con rapidez o si se alteraran sistemas antes de analizarlos.
- En entornos industriales, algunas técnicas forenses convencionales pueden ser incompatibles con la continuidad o con la seguridad funcional.
- No sustituyen la respuesta operativa ni la contención, aunque deben integrarse con ambas.
- Se requiere conocimiento técnico especializado y, en ocasiones, apoyo externo con experiencia específica en OT.
- Debe evitarse que la urgencia por restaurar la operación elimine evidencias clave sin realizar al menos una preservación mínima y trazable.

Relación con otros controles: Se relaciona con el soporte a la respuesta ante incidentes, el SIEM, el SOC, el MDR, el NDR, el EDR, la gestión de sesiones y trazabilidad, la monitorización ciberfísica / MES, las copias de seguridad y restauración y con la recuperación de operación y continuidad. Funciona como capacidad de análisis profundo para apoyar tanto la respuesta inmediata como la mejora posterior.

Casos habituales de uso: Se emplea tras incidentes de malware o ransomware, accesos remotos comprometidos, uso indebido de cuentas privilegiadas, sospecha de manipulación de configuraciones, actividad anómala en HMI o estaciones de ingeniería, intervenciones de terceros con resultado no previsto, exfiltración de información técnica y cualquier escenario en el que sea necesario reconstruir lo ocurrido en base a evidencias.

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

Observaciones / medidas compensatorias asociadas: En entornos industriales, los servicios forenses resultan especialmente útiles cuando es necesario reconstruir un incidente sin comprometer la continuidad de la operación y cuando las decisiones posteriores dependen de conocer con precisión el alcance real del compromiso. Su utilidad aumenta cuando existen registros suficientes, trazabilidad de accesos, coordinación con el proceso de respuesta y criterios previos para preservar evidencias mínimas antes de proceder a la recuperación o a la reconfiguración de los sistemas afectados.

5.9.3 Copias de seguridad y restauración

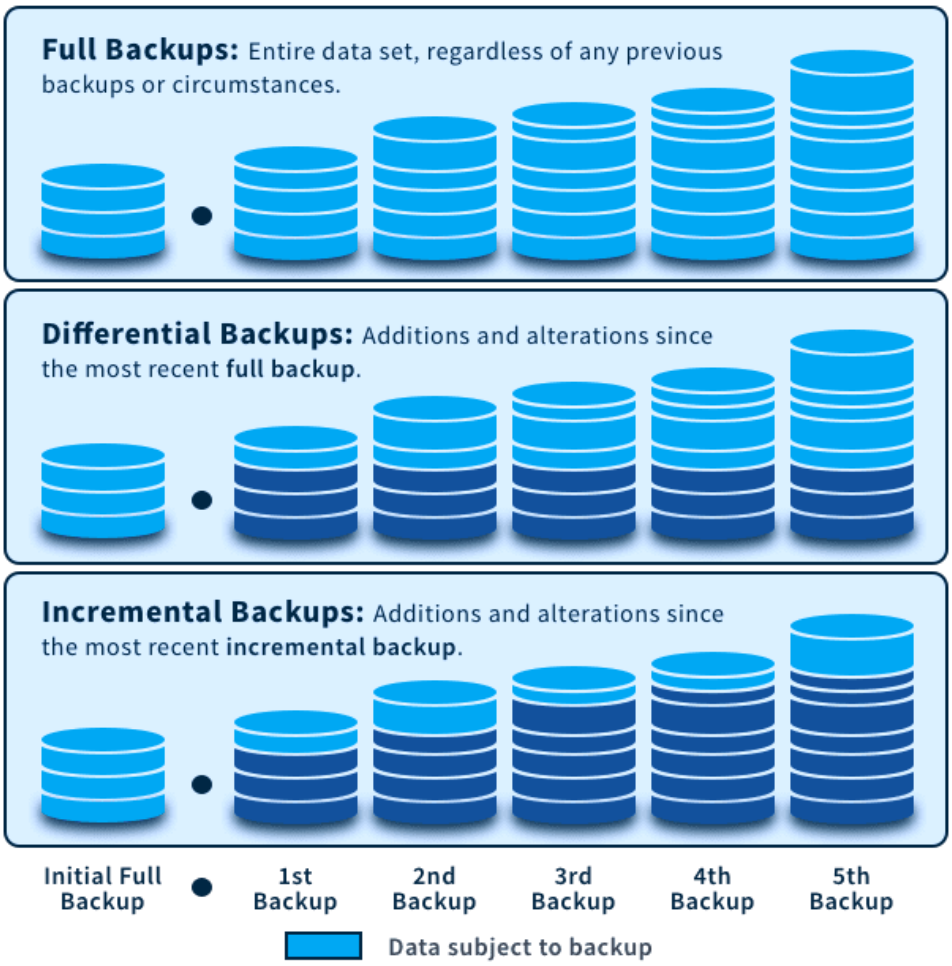
Categoría: Respuesta, recuperación y continuidad

Tipología: Técnica / mixta

Función defensiva predominante: Correctiva / de recuperación

Función en NIST CSF: Recover

Descripción: Las copias de seguridad y restauración comprenden el conjunto de medidas orientadas a preservar información, configuraciones, sistemas y componentes críticos mediante réplicas controladas que permitan su recuperación tras un incidente, error, fallo o pérdida de disponibilidad. Su finalidad no es únicamente conservar datos, sino asegurar que la organización pueda restaurar capacidades esenciales en un tiempo y con un nivel de integridad compatibles con la continuidad de la actividad. En entornos industriales, este control abarca no sólo ficheros corporativos o servidores convencionales, sino también proyectos de ingeniería, configuraciones de HMI, recetas, bases de datos operativas, historiadores, parámetros de sistema, máquinas virtuales, registros relevantes y otros componentes cuya pérdida o corrupción podría afectar a la producción, la supervisión o a la seguridad del proceso.



Tipos de copia de seguridad. Fuente: Spanning.com (2020)

Objetivo: Garantizar que la organización disponga de copias fiables, íntegras y recuperables de los activos de información y de los componentes tecnológicos necesarios para restablecer la operación tras un incidente. En el ámbito industrial, su objetivo incluye también asegurar que la restauración pueda realizarse sin introducir configuraciones incoherentes, pérdida de trazabilidad o riesgo adicional sobre sistemas con impacto operativo.

Cómo funciona / cómo se implanta: Su implantación parte de la identificación de lo que debe copiarse, de qué forma y con qué frecuencia, durante cuánto tiempo debe conservarse y bajo qué condiciones debe poder restaurarse. Ello incluye definir alcances, prioridades, periodicidad, tipos de copia, segregación del almacenamiento, protección frente a manipulación, control de acceso a las copias y procedimientos de restauración verificada. En entornos industriales, este control debe contemplar tanto datos como configuraciones y componentes técnicos específicos: proyectos de automatización, imágenes de sistemas, configuraciones de dispositivos, servidores de supervisión, parámetros de aplicaciones industriales, documentación operativa y otros

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

elementos necesarios para reconstruir el entorno de manera coherente. Su eficacia depende no sólo de hacer copias, sino de comprobar periódicamente que pueden restaurarse, que son utilizables y que están alineadas con la realidad actual del proceso y de la arquitectura.

Ventajas:

- Permiten recuperar información y sistemas tras incidentes, errores o corrupción de datos.
- Refuerzan la resiliencia frente a ransomware, fallo técnico, error humano o pérdida de disponibilidad.
- Ayudan a reducir tiempos de recuperación e impacto sobre la actividad.
- Resultan esenciales para restaurar configuraciones y componentes críticos en entornos industriales.
- Complementan los planes de continuidad y los procedimientos de respuesta con una capacidad técnica de recuperación.

Limitaciones y consideraciones:

- Su utilidad disminuye si las copias no se prueban, no están actualizadas o no incluyen los componentes realmente críticos.
- En entornos industriales, no basta con copiar datos: también deben preservarse configuraciones, dependencias y elementos necesarios para la restauración funcional del entorno.
- No sustituyen la prevención, la segmentación ni la respuesta temprana ante incidentes.
- Se requiere protección frente a borrado, cifrado o manipulación de las propias copias.
- Debe evitarse una falsa sensación de seguridad basada en la existencia de copias no verificadas o sin procedimientos claros de restauración.

Relación con otros controles: Se relaciona con el soporte a la respuesta ante incidentes, los servicios forenses, la recuperación de operación y continuidad, el plan de continuidad de negocio y resiliencia operativa, la detección de integridad de ficheros, el bastionado de sistemas y servicios y los procedimientos de cambio y mantenimiento. Constituye una de las capacidades técnicas más relevantes dentro de la recuperación.

Casos habituales de uso: Se utiliza para restaurar servidores, puestos críticos, configuraciones de HMI, proyectos de ingeniería, bases de datos operativas, historiadores, documentación técnica, servicios de supervisión, entornos virtualizados y otros componentes afectados por ransomware, error humano, corrupción de datos, fallo de infraestructura o intervención técnica fallida.

Observaciones / medidas compensatorias asociadas: En entornos industriales, las copias de seguridad y restauración resultan especialmente útiles cuando se integran en una estrategia más amplia de continuidad y recuperación, y no como mecanismo aislado. Su utilidad aumenta cuando se combinan con segmentación, protección de las copias frente a manipulación, pruebas periódicas de restauración, validación posterior del estado del sistema y coordinación con operación y mantenimiento antes de la puesta en servicio del entorno restaurado.

5.9.4 Recuperación de operación y continuidad

Categoría: Respuesta, recuperación y continuidad

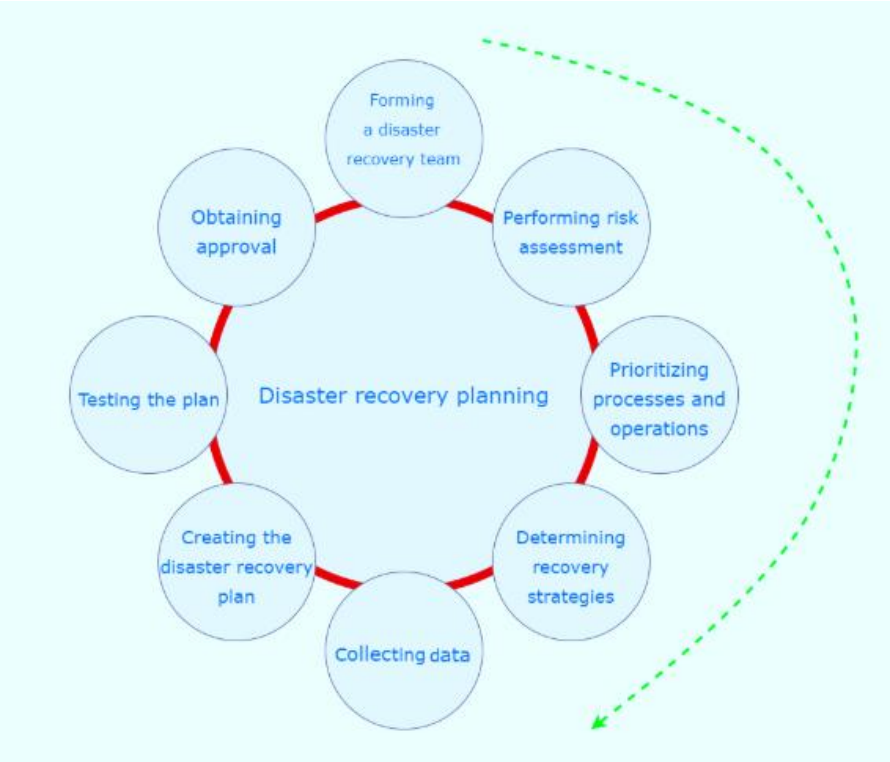
Tipología: Organizativa / técnica / mixta

Función defensiva predominante: Correctiva / de recuperación

Función en el NIST CSF: Recover, Govern

Descripción: La recuperación de operación y continuidad comprende el conjunto de medidas, procedimientos y decisiones orientadas a restablecer de manera segura y ordenada la actividad de la organización tras un incidente, fallo o interrupción que afecte a sus sistemas, servicios o procesos críticos. Su finalidad va más allá de la mera restauración técnica de componentes: implica que la operación pueda retomarse bajo condiciones aceptables de seguridad, integridad, trazabilidad y coordinación entre áreas. En entornos industriales, este control resulta especialmente relevante porque la recuperación no debe centrarse sólo en la disponibilidad de los sistemas, sino también en la coherencia del proceso, en la validación del estado de los activos, en la continuidad del servicio y en la protección de las personas, de las instalaciones y de la producción.

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



Planificación de recuperación ante desastres. Fuente: Cybersecurity - Attack and Defense Strategies (2018)

Objetivo: Restablecer la operación y los servicios esenciales de la organización de forma progresiva, segura y controlada tras un incidente, minimizando el tiempo de interrupción y reduciendo el riesgo de reintroducir fallos, configuraciones incoherentes o condiciones de inseguridad. En el ámbito industrial, su objetivo incluye también asegurar que la vuelta a la operación se produzca con validación técnica y operativa suficiente, evitando recuperaciones apresuradas que puedan comprometer el proceso o generar nuevos incidentes.

Cómo funciona / cómo se implanta: Su implantación parte de la identificación previa de las funciones críticas, de los activos necesarios para sostenerlas, de las prioridades de restauración y de los criterios de aceptación para considerar que la operación puede retomarse. Ello incluye procedimientos de recuperación, dependencias entre sistemas, órdenes de restauración, validación del estado de los componentes, coordinación con copias de seguridad, revisión de configuraciones, comprobación de comunicaciones y definición de responsables para cada fase. En entornos industriales, este control debe contemplar también la verificación de HMI, estaciones de ingeniería, sistemas de supervisión, conexiones de red, parámetros de proceso, recetas, sistemas intermedios, dependencias con terceros y condiciones de seguridad funcional. Su eficacia depende de que la recuperación esté planificada, probada y alineada con el funcionamiento real de

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

la operación, y de que exista coordinación entre seguridad, sistemas, operación, mantenimiento, producción y Dirección.

Ventajas:

- Ayuda a reducir el tiempo de interrupción y a restaurar servicios esenciales con mayor orden y control.
- Mejora la coordinación entre áreas técnicas y operativas durante la vuelta a la normalidad.
- Refuerza la seguridad de la recuperación evitando restauraciones improvisadas o incoherentes.
- Resulta especialmente útil en entornos industriales con fuerte dependencia de activos, secuencias y estados operativos.
- Complementa las copias de seguridad y los planes de continuidad con un enfoque orientado a la puesta en servicio real.

Limitaciones y consideraciones:

- Su utilidad disminuye si no existen prioridades claras, procedimientos definidos o pruebas previas suficientes.
- En entornos industriales, la recuperación técnica de un sistema no garantiza por sí sola la recuperación funcional del proceso.
- No sustituye la preparación previa, la respuesta ante incidentes ni la resiliencia de la arquitectura.
- Se requiere coordinación estrecha con operación, mantenimiento y responsables del proceso para validar la vuelta al servicio.
- Debe evitarse una recuperación precipitada que reintroduzca sistemas comprometidos, configuraciones defectuosas o estados no verificados.

Relación con otros controles: Se relaciona con el soporte a la respuesta ante incidentes, los servicios forenses, las copias de seguridad y restauración, el plan de continuidad de negocio y resiliencia operativa, la monitorización ciberfísica / MES, la gestión de cambios y las validaciones previas y en la ventana de mantenimiento. Constituye la capa que transforma la restauración técnica en recuperación operativa efectiva.

Casos habituales de uso: Se emplea tras incidentes de ransomware, caída de sistemas de supervisión, corrupción de configuraciones, fallos en servidores o plataformas

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

críticas, indisponibilidad de entornos intermedios, recuperación de líneas o servicios industriales, reactivación de operación tras aislamiento preventivo y escenarios en los que se necesita una puesta en servicio gradual y validada.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la recuperación de operación y continuidad resulta especialmente útil cuando se formula como un proceso gradual, con validación técnica y operativa antes de cada paso de restablecimiento. Su utilidad aumenta cuando se combina con copias fiables, trazabilidad de las intervenciones, revisión del estado del sistema, coordinación con mantenimiento y operación y criterios claros para decidir cuándo la actividad puede considerarse restablecida en condiciones aceptables.

5.9.5 Ciberseguros

Categoría: Respuesta, recuperación y continuidad

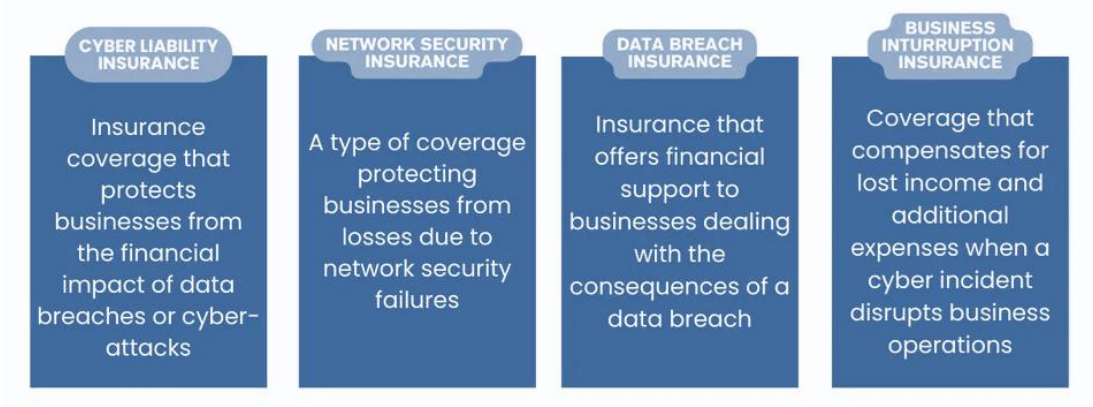
Tipología: Organizativa / mixta

Función defensiva predominante: Correctiva / de recuperación

Función en el NIST CSF: Recover, Govern

Descripción: Los ciberseguros son instrumentos de transferencia y mitigación financiera del riesgo de ciberseguridad que permiten a la organización contar con una cobertura económica y, en algunos casos, con servicios asociados para hacer frente a los costes derivados de un incidente. Su finalidad no es sustituir los controles técnicos y organizativos de prevención, detección y respuesta, sino complementar la capacidad de la organización para absorber el impacto económico, operativo, legal y reputacional de un incidente grave. En entornos industriales, esta figura puede adquirir especial relevancia cuando una interrupción, un ransomware, una afectación a la producción, un incidente con terceros o una degradación prolongada de los servicios tiene potencial para generar pérdidas significativas, costes de recuperación elevados o responsabilidades contractuales y regulatorias adicionales.

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



Tipo de ciberseguros. Fuente: onsurity.com (2024)

Objetivo: Reducir la exposición financiera de la organización ante incidentes cibernéticos graves, aportando un mecanismo de cobertura y apoyo que complemente la preparación técnica y organizativa frente a eventos de alto impacto. En el ámbito industrial, su objetivo incluye también mejorar la capacidad de la entidad para afrontar costes asociados a la interrupción de la operación, a la recuperación de sistemas, la asistencia especializada, a la gestión legal y la comunicación posterior al incidente.

Cómo funciona / cómo se implanta: Su implantación requiere analizar el perfil de riesgo de la organización, el tipo de coberturas necesarias, los límites de la póliza, las exclusiones aplicables, las condiciones de activación y los servicios complementarios asociados, como apoyo legal, respuesta técnica, comunicación o peritaje. En entornos industriales, este análisis debe tener en cuenta aspectos como dependencia de la producción, impacto de una parada, uso de terceros, exposición remota, criticidad de los sistemas, requisitos contractuales, posibles afectaciones a la cadena de suministro y costes derivados de la recuperación de activos y servicios. Su eficacia depende de que la póliza esté alineada con el riesgo real de la organización y de que los equipos responsables conozcan las condiciones de cobertura, los procedimientos de notificación y los límites de lo que puede esperarse del seguro. No se trata sólo de contratar una póliza, sino de integrarla dentro de la gobernanza del riesgo y de la continuidad.

Ventajas:

- Ayudan a absorber parte del impacto económico derivado de un incidente de ciberseguridad grave.
- Pueden facilitar acceso a servicios especializados de apoyo técnico, legal o comunicativo.
- Refuerzan la planificación financiera ante escenarios de alta severidad.

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

- Resultan útiles en organizaciones con elevada dependencia de la continuidad o de la prestación de servicios.
- Complementan los planes de continuidad y respuesta con una capa de cobertura económica y contractual.

Limitaciones y consideraciones:

- No sustituyen la necesidad de controles preventivos, detectivos y correctivos sólidos.
- Su cobertura puede incluir exclusiones, límites o condiciones que reduzcan su valor real si no se analizan con detalle.
- En entornos industriales, los costes e impactos relevantes no siempre encajan de manera simple en las coberturas estándar.
- Se requiere conocimiento previo de la póliza y de los procesos de activación para evitar errores o retrasos durante un incidente.
- Debe evitarse una falsa sensación de seguridad basada en la transferencia del riesgo financiero sin mejora paralela del nivel de protección real.

Relación con otros controles: Se relaciona con el análisis de riesgos tecnológicos, el plan de continuidad de negocio y resiliencia operativa, el soporte a la respuesta ante incidentes, los servicios forenses, las copias de seguridad y restauración, la recuperación de operación y continuidad y los procedimientos de gobernanza del riesgo. Funciona como mecanismo complementario de absorción y gestión del impacto, no como control técnico de seguridad.

Casos habituales de uso: Se emplea para cubrir costes asociados a eventos de ransomware, interrupción de la actividad, recuperación técnica, asistencia forense, asesoramiento legal, notificaciones, reclamaciones, afectación de terceros, pérdidas por indisponibilidad de servicios u otros incidentes con impacto económico relevante sobre la organización.

Observaciones / medidas compensatorias asociadas: En entornos industriales, los ciberseguros resultan especialmente útiles cuando la organización tiene una exposición significativa a interrupciones operativas, dependencia de terceros o impacto económico elevado ante incidentes prolongados. Su utilidad aumenta cuando se integran con un análisis de riesgo realista, con un conocimiento claro de las condiciones de la póliza y con una preparación previa que permita activar la cobertura sin interferir en la respuesta técnica, en la continuidad ni en la recuperación del proceso.

5.10 DevsecOps, software y entornos digitales conectados

La creciente digitalización de la industria y la integración entre software, operación y conectividad hace necesario incorporar la seguridad al propio ciclo de vida de las aplicaciones y componentes digitales (desarrollo y operación, o DevSecOps). Esta subsección aborda **capacidades destinadas a mejorar la seguridad del desarrollo, de la integración y del software vinculado a la operación, reduciendo el riesgo introducido por errores de diseño, vulnerabilidades y dependencias tecnológicas**.

5.10.1 SAST

Categoría: DevSecOps, software y entornos digitales conectados

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Identify

Descripción: El análisis estático de seguridad del código (SAST, *Static Application Security Testing*) es una práctica orientada a la identificación temprana de debilidades y patrones inseguros en el código fuente, en los componentes de la aplicación y en otros artefactos de desarrollo, antes de su puesta en ejecución. Su finalidad es detectar errores de programación, usos inseguros de funciones, fallos de validación, gestión incorrecta de entradas, problemas de autenticación, exposición de secretos y otras vulnerabilidades potenciales durante las fases iniciales del ciclo de vida del software. En entornos industriales, esta práctica resulta especialmente relevante cuando la organización desarrolla o adapta software propio ligado a la operación, integra componentes de supervisión, crea aplicaciones de soporte al proceso o mantiene capas digitales conectadas con sistemas productivos, de monitorización o de gestión operativa.

Objetivo: Reducir el riesgo de introducir vulnerabilidades en el software antes de su implantación, mejorando la calidad del código y reforzando la seguridad desde fases tempranas del desarrollo. En el ámbito industrial, su objetivo incluye también limitar la incorporación de debilidades en aplicaciones, integraciones o componentes software que puedan influir sobre la operación, la supervisión o la exposición de información técnica y operativa sensible.

Cómo funciona / cómo se implanta: Su implantación se basa en el análisis automatizado o asistido del código fuente, de las bibliotecas empleadas y de otros componentes del desarrollo para localizar patrones asociados a prácticas inseguras o a

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

vulnerabilidades conocidas. Este análisis puede integrarse en el repositorio de código, en los flujos de integración continua, en las revisiones de cambios o en las fases previas a la puesta en producción. En entornos industriales, el valor del SAST aumenta cuando se aplica de manera temprana y recurrente sobre software propio, scripts de automatización, componentes de integración, aplicaciones de soporte a la operación y herramientas desarrolladas internamente o adaptadas al contexto de la organización. Su eficacia depende de que los resultados se revisen con criterio, se prioricen según riesgo y se integren en un proceso de desarrollo seguro y gobernado.

Ventajas:

- Permite detectar vulnerabilidades antes de que el software entre en producción.
- Reduce el coste de corrección al actuar en fases iniciales del ciclo de desarrollo.
- Mejora la calidad del código y la disciplina de desarrollo seguro.
- Resulta útil para reforzar aplicaciones y componentes software con impacto sobre la operación.
- Puede integrarse de forma continua en los flujos DevSecOps y de revisión técnica.

Limitaciones y consideraciones:

- No todas las debilidades detectadas tienen la misma relevancia real ni el mismo impacto en el contexto de la aplicación.
- Puede generar falsos positivos o alertas poco accionables si no existe revisión técnica suficiente.
- En entornos industriales, el valor del análisis depende de que el software examinado esté bien identificado y del conocimiento de su papel operativo.
- No sustituye las pruebas dinámicas, la revisión funcional ni la protección de la aplicación una vez desplegada.
- Se requiere integración con los equipos de desarrollo, mantenimiento y seguridad para que las detecciones se conviertan en mejoras reales del software.

Relación con otros controles: Se relaciona con el DAST, con el RASP, con las prácticas seguras de desarrollo e integración, con la protección de software ligado a la operación, con la gestión de vulnerabilidades, con el bastionado de sistemas y servicios y con los procedimientos de validación previa antes de la puesta en producción. Constituye una de las capas preventivas más relevantes en el desarrollo seguro.

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

Casos habituales de uso: Se emplea para revisar aplicaciones internas, portales de gestión, componentes de integración, scripts de automatización, APIs, herramientas de soporte, software desarrollado para monitorización u operación y otros componentes en los que se necesita reducir la presencia de vulnerabilidades antes de su implantación o actualización.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el SAST resulta especialmente útil cuando la organización desarrolla o adapta software con relación directa o indirecta con la operación y necesita anticipar riesgos antes de introducir cambios en producción. Su utilidad aumenta cuando se combina con revisión técnica manual, DAST, validación en entornos de prueba, gestión de cambios y procedimientos de liberación que tengan en cuenta la criticidad del entorno en el que el software será ejecutado.

5.10.2 DAST

Categoría: DevSecOps, software y entornos digitales conectados

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Identify

Descripción: El análisis dinámico de seguridad de aplicaciones (DAST, *Dynamic Application Security Testing*) es una práctica orientada a la identificación de vulnerabilidades y comportamientos inseguros mediante la evaluación de una aplicación en ejecución, observando cómo responde a peticiones, interacciones y entradas maliciosas o no previstas. A diferencia del SAST, que actúa sobre el código fuente y otros artefactos antes de la ejecución, el DAST se centra en el comportamiento efectivo de la aplicación desplegada en real o en entorno de prueba, permitiendo detectar debilidades visibles desde el exterior, errores de validación, exposición de componentes, configuraciones inseguras o fallos en la gestión de sesiones y parámetros. En entornos industriales, esta práctica resulta especialmente relevante cuando existen aplicaciones web, portales de gestión, APIs, componentes de integración o servicios software que, directa o indirectamente, se conectan con sistemas de supervisión, operación, mantenimiento o intercambio de información técnica.

Objetivo: Detectar vulnerabilidades y fallos de seguridad en el comportamiento real de una aplicación antes de su puesta en producción o durante su ciclo de vida, reduciendo el riesgo de explotación externa o interna sobre servicios software accesibles. En el

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

ámbito industrial, su objetivo incluye también identificar exposiciones en aplicaciones e interfaces que puedan actuar como punto de entrada hacia servicios técnicos, datos operativos o componentes con impacto indirecto sobre la operación.

Cómo funciona / cómo se implanta: Su implantación se basa en la ejecución de pruebas sobre la aplicación en funcionamiento, enviando peticiones e interacciones diseñadas para comprobar cómo gestiona entradas, sesiones, autenticación, autorización, errores, navegación, exposición de componentes y otras condiciones de riesgo. Este análisis puede realizarse en entornos de desarrollo, preproducción o, con mucha cautela, sobre aplicaciones ya desplegadas cuando exista control suficiente del alcance. En entornos industriales, el DAST debe aplicarse preferentemente sobre entornos de prueba o réplicas representativas, especialmente cuando la aplicación tiene relación con sistemas de mantenimiento, supervisión, gestión técnica o intercambio de información operativa. Su eficacia depende de que el alcance esté bien definido, de que las pruebas reflejen el comportamiento real de la aplicación y de que los resultados se integren en un proceso de mejora y validación previa antes de la puesta en servicio.

Ventajas:

- Permite identificar vulnerabilidades observables en el comportamiento real de la aplicación.
- Complementa el SAST al analizar la aplicación en ejecución y no sólo el código.
- Resulta útil para detectar exposiciones en sesiones, entradas, errores y configuraciones visibles.
- Ayuda a evaluar servicios web, APIs y componentes de integración antes de su despliegue definitivo.
- Puede integrarse en procesos de convalidación y liberación de software con enfoque DevSecOps.

Limitaciones y consideraciones:

- No sustituye la revisión del código ni detecta todos los problemas internos no visibles desde la aplicación en ejecución.
- Puede generar resultados incompletos si el entorno de prueba no reproduce adecuadamente el comportamiento real.
- En entornos industriales, debe evitarse la ejecución indiscriminada de pruebas dinámicas sobre servicios en producción con impacto potencial sobre la operación.

- Se requiere interpretación técnica de los aportes para distinguir entre exposición real, error de configuración y vulnerabilidad explotable.
- Debe complementarse con procedimientos de convalidación, gestión de cambios y revisión funcional de la aplicación.

Relación con otros controles: Se relaciona con el SAST, el RASP, el WAF, las prácticas seguras de desarrollo e integración, la protección de software ligado a la operación, la gestión de vulnerabilidades y las validaciones previas antes de la puesta en producción. Constituye una capa muy útil para evaluar la seguridad observable de las aplicaciones desplegadas.

Casos habituales de uso: Se emplea para revisar portales web, servicios de administración, APIs, componentes de integración, aplicaciones de soporte a la operación, interfaces técnicas publicadas en entornos de prueba y otros servicios software en los que se necesita detectar vulnerabilidades antes del despliegue o de una actualización relevante.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el DAST resulta especialmente útil cuando existen aplicaciones conectadas a procesos de mantenimiento, supervisión o integración y se requiere validar su comportamiento antes de su exposición o actualización. Su utilidad aumenta cuando se combina con SAST, revisión manual, entornos de prueba representativos, WAF, gestión de cambios y procedimientos de liberación adaptados a la criticidad del entorno en el que la aplicación va a operar.

5.10.3 RASP

Categoría: DevSecOps, software y entornos digitales conectados

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect, Detect

Descripción: La autoprotección de aplicaciones en tiempo de ejecución (RASP, *Runtime Application Self-Protection*) es un conjunto de capacidades orientadas a supervisar y proteger el comportamiento de una aplicación mientras está en funcionamiento, a fin de detectar y bloquear interacciones maliciosas, explotaciones de vulnerabilidades o usos indebidos en el propio momento en que se producen. A diferencia de controles externos como el WAF, que observan el tráfico desde fuera de la aplicación, el RASP opera con mayor proximidad al contexto interno de la ejecución, lo que le permite interpretar

mejor ciertas llamadas, flujos lógicos, entradas y patrones de comportamiento. En entornos industriales, esta capacidad puede resultar especialmente útil en aplicaciones web, servicios de integración, interfaces técnicas, componentes software de apoyo a la operación y otras piezas digitales conectadas que requieren protección adicional sin depender exclusivamente del perímetro.

Objetivo: Reducir el riesgo de explotación de vulnerabilidades o de uso indebido de las aplicaciones en ejecución, aportando una capa adicional de protección capaz de detectar y, cuando proceda, bloquear acciones maliciosas en tiempo real. En el ámbito industrial, su objetivo incluye también reforzar la protección de aplicaciones ligadas a la gestión, la supervisión, la integración o al soporte técnico cuando éstas tienen relación con información operativa, servicios sensibles o entornos con impacto indirecto sobre la operación.

Cómo funciona / cómo se implanta: Su implantación se basa en la integración de componentes de observación y protección dentro de la aplicación o en su entorno inmediato de ejecución, de manera que puedan analizar llamadas, flujos, entradas, sesiones y comportamiento interno con contexto suficiente para identificar acciones sospechosas. Esto permite detectar explotaciones que pueden pasar desapercibidas para otros mecanismos más externos y, en determinados casos, interrumpir la acción antes de que se complete. En entornos industriales, el RASP debe aplicarse principalmente a aplicaciones desarrolladas o mantenidas por la organización, o a componentes software en los que exista capacidad real de integración y validación. Su eficacia depende de compatibilidad con el entorno de ejecución, impacto asumible sobre rendimiento y mantenimiento, e integración con un proceso de desarrollo seguro en el que los resultados puedan analizarse e incorporarse de manera ordenada.

Ventajas:

- Añade protección sobre la aplicación en el propio momento de la ejecución.
- Puede detectar y bloquear explotaciones con mayor contexto que otros controles externos.
- Complementa SAST, DAST y WAF con una capa próxima a la lógica interna de la aplicación.
- Resulta útil para aplicaciones con exposición relevante o función sensible.
- Puede mejorar la visibilidad sobre comportamientos anómalos e intentos de abuso de funcionalidades.

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

Limitaciones y consideraciones:

- Su aplicabilidad depende del tipo de aplicación, del entorno de ejecución y de la posibilidad real de integración.
- Puede introducir impacto en rendimiento, compatibilidad o mantenimiento si no se valida adecuadamente.
- En entornos industriales, no resulta igualmente adecuado para todos los componentes software, especialmente si son muy cerrados o dependen de proveedores externos.
- No sustituye el desarrollo seguro, el SAST, el DAST ni la revisión de la arquitectura de la aplicación.
- Se requiere control del ciclo de vida de la aplicación y criterio técnico suficiente para interpretar y ajustar el comportamiento de la protección en ejecución.

Relación con otros controles: Se relaciona con el SAST, el DAST, el WAF, las prácticas seguras de desarrollo e integración, la protección de software ligado a la operación, la gestión de vulnerabilidades y la monitorización y operación de seguridad. Constituye una capa avanzada de protección orientada al comportamiento real de la aplicación en ejecución.

Casos habituales de uso: Se emplea en aplicaciones web de gestión, APIs, componentes de integración, portales técnicos, servicios conectados a información sensible y otras aplicaciones en las que se busca añadir una capa adicional de protección frente a explotaciones en tiempo real sin depender sólo de controles perimetrales.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el RASP puede resultar especialmente útil cuando una aplicación debe permanecer accesible o expuesta y no es viable rediseñarla de inmediato ni eliminar completamente determinadas debilidades. Su utilidad aumenta cuando se combina con SAST, DAST, WAF, validación en entornos de prueba, gestión de cambios y revisión continua del impacto de la protección sobre el comportamiento funcional de la aplicación.

A continuación, se muestran las diferencias y similitudes de los tres últimos controles descritos.

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

Característica	SAST	DAST	RASP
Método de funcionamiento	Examina el código fuente sin ejecutarlo	Evalúa aplicaciones en ejecución simulando ataques	Se ejecuta en la aplicación para detectar y defenderse contra ataques en tiempo real
Fase en el SDLC	En las primeras fases del ciclo de desarrollo	Después del desarrollo, en preproducción	En producción / en tiempo de ejecución
Tipo de problemas detectados	Errores de sintáxis, fallos de seguridad como desbordamientos de búffer e inyecciones SQL	Problemas en tiempo de ejecución, errores de autenticación/autorización, problemas de gestión de sesiones	Ataques en tiempo real, entradas maliciosas, vulnerabilidades en ejecución
Integración	Integrado en el proceso de desarrollo	Parte de una estrategia AST más amplia, usada en entornos de staging	Integrado dentro de la aplicación; funciona en un entorno de producción
Granularidad	Examina el código a un nivel detallado	Evalúa la aplicación en su conjunto	Supervisa y protege en tiempo de ejecución, proporcionando información contextual
Asistencia para la corrección	Permite la detección temprana y la corrección de problemas	Identifica problemas en un estado de ejecución, proporcionando contexto para las vulnerabilidades en tiempo de ejecución	Proporciona protección y mitigación inmediatas
Cobertura	Código fuente, ficheros de configuración	Solicitudes HTTP, respuestas y datos de sesión	Flujo de datos, flujo de control, información de conexión interna
Falsos positivos	Pueden ser más numerosos debido a la falta de contexto de ejecución	Generalmente menos, ya que evalúa el comportamiento real en ejecución	Bajos, ya que opera en el entorno real de ejecución

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

Ventajas	Detección temprana de una amplia gama de problemas detectables	Eficaz para identificar vulnerabilidades específicas de ejecución	Protección inmediata y continua, defensa con conocimiento del contexto
Desventajas	Puede no detectar problemas específicos en tiempo de ejecución	Requiere una aplicación en ejecución, con posible dependencia del entorno	Sobrecarga en el rendimiento de la aplicación y complejidad en la integración

Comparativa SAST, DAST, RASP. Fuente: Somi, Vivek (2024)

5.10.4 Prácticas seguras de desarrollo SW e integración

Categoría: DevSecOps, software y entornos digitales conectados

Tipología: Organizativa / técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect, Govern

Descripción: Las prácticas seguras de desarrollo e integración comprenden el conjunto de principios, procedimientos, controles y rutinas orientados a incorporar la seguridad de manera continua a lo largo del ciclo de vida del software, desde el análisis de requisitos hasta el desarrollo, integración, validación, despliegue y mantenimiento evolutivo. Su propósito es evitar que la seguridad aparezca como una revisión tardía y aislada, convirtiéndola en un criterio transversal de diseño, implementación y entrega. En entornos industriales, esta aproximación resulta especialmente relevante cuando la organización desarrolla software propio, adapta componentes, para integraciones con sistemas de supervisión u operación, automatizar procesos o mantener entornos digitales conectados con impacto potencial sobre servicios, datos técnicos o procesos productivos.

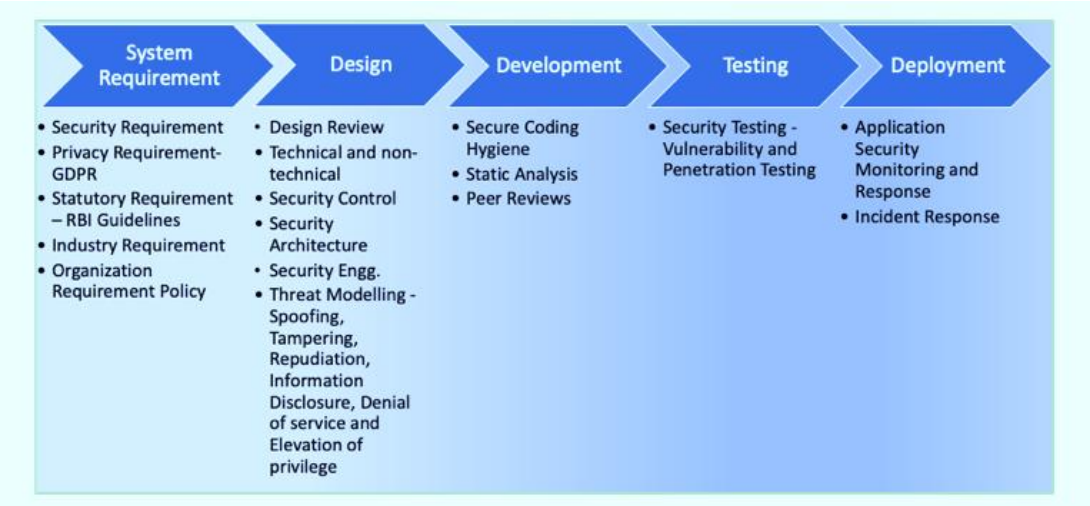


Diagrama del ciclo de vida de desarrollo de software seguro (S-SDLC). Fuente: Digisec360 (2020)

Objetivo: Reducir la incorporación de riesgos y vulnerabilidades al software y a sus integraciones mediante prácticas sistemáticas de diseño seguro (S-SDLC), revisión técnica, control de cambios y validación continua. En el ámbito industrial, su objetivo incluye también asegurar que las integraciones entre aplicaciones, sistemas corporativos, componentes técnicos y servicios ligados a la operación se realicen bajo criterios compatibles con la continuidad, la trazabilidad y la protección del entorno.

Cómo funciona / cómo se implanta: Su implantación se basa en la incorporación de controles y rutinas de seguridad al flujo habitual de desarrollo y entrega: definición de requisitos de seguridad, revisión de arquitectura, uso de buenas prácticas de codificación, gestión segura de dependencias, revisión por pares, control de secretos, análisis automatizado, pruebas de seguridad, validación previa al despliegue y gobernanza del cambio. En entornos industriales, estas prácticas deben extenderse también a las integraciones entre software y sistemas técnicos, a los scripts de automatización, a las APIs, a los componentes de intercambio de datos, a las aplicaciones de soporte a la operación y a cualquier pieza digital que pueda afectar a la supervisión, mantenimiento, producción o gestión operativa. Su eficacia depende de que la seguridad se integre en los procedimientos reales de los equipos y de que exista coordinación entre desarrollo, operación, seguridad, mantenimiento y responsables funcionales.

Ventajas:

- Reduce la incorporación de vulnerabilidades desde fases tempranas del ciclo de vida del software.
- Mejora la calidad técnica de las aplicaciones y de las integraciones y reduce costes.

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

- Refuerza la coherencia entre desarrollo, cambio, validación y despliegue.
- Resulta útil para controlar riesgos en componentes conectados a la operación o la información sensible.
- Complementa SAST, DAST y RASP con un marco más amplio de gobernanza y buenas prácticas.

Limitaciones y consideraciones:

- Su utilidad disminuye si se formula como conjunto teórico de principios sin integración real en el flujo de trabajo.
- En entornos industriales, las integraciones con software legado, componentes de fabricante o servicios poco documentados pueden dificultar su aplicación completa.
- No sustituye las pruebas técnicas ni la validación previa a la puesta en producción.
- Se requiere madurez organizativa, disciplina de cambio y participación coordinada de varios perfiles.
- Debe evitarse que la presión por entregar cambios rápidos relegue la seguridad a una revisión final sin capacidad real de corrección.

Relación con otros controles: Se relaciona con el SAST, con el DAST, con el RASP, con la protección de software ligado a la operación, con la gestión de vulnerabilidades, con las validaciones previas y en la ventana de mantenimiento, con el bastionado de sistemas y servicios y con los procedimientos de cambio y liberación. Constituye el marco de trabajo que integra la seguridad en el desarrollo y entrega continua de software.

Casos habituales de uso: Se emplea en equipos que desarrollan aplicaciones internas, scripts de automatización, APIs, integraciones con plataformas industriales, servicios de soporte técnico, componentes de intercambio de datos, portales de gestión y otros elementos software que necesitan control de seguridad a lo largo de todo su ciclo de vida.

Observaciones / medidas compensatorias asociadas: En entornos industriales, estas prácticas resultan especialmente útiles cuando la organización mantiene software propio o integraciones críticas y precisa reducir el riesgo antes del despliegue. Su utilidad aumenta cuando se combinan con revisión técnica manual, SAST, DAST, entornos de prueba representativos, gestión de cambios, validación funcional y criterios

claros de liberación adaptados a la criticidad del entorno en el que el software va a operar.

5.10.5 Protección de software ligado a la operación

Categoría: DevSecOps, software y entornos digitales conectados

Tipología: Técnica / mixta

Función defensiva predominante: Preventiva

Función en NIST CSF: Protect

Descripción: La protección de software ligado a la operación comprende el conjunto de medidas orientadas a asegurar aplicaciones, componentes, integraciones y herramientas software que, sin formar parte necesariamente del núcleo de control industrial, tienen una relación directa o indirecta con el funcionamiento operativo de la organización. Esto incluye software de supervisión, gestión técnica, integración de datos, apoyo al mantenimiento, interfaces con sistemas industriales, componentes de analítica, servicios intermedios, scripts de automatización y otras piezas digitales que pueden influir sobre la visibilidad, la coordinación, trazabilidad o la ejecución de tareas críticas. En entornos industriales, este tipo de software adopta constituir un puente entre los dominios IT y OT, por lo que su protección adquiere un valor especial dentro de la superficie de riesgo global.

Objetivo: Reducir el riesgo de que el software vinculado a la operación introduzca vulnerabilidades, exposiciones o dependencias inseguras que puedan afectar a la continuidad, a la integridad del proceso, a la gestión técnica o acceso a información y servicios críticos. En el ámbito industrial, su objetivo incluye también reforzar la protección de las aplicaciones e integraciones que, sin ser controladores o componentes OT puros, pueden servir como vía de acceso, manipulación o degradación del entorno operativo.

Cómo funciona / cómo se implanta: Su implantación se basa en la identificación de los componentes software que tienen relación con la operación y en la aplicación sobre ellos de un conjunto combinado de medidas: desarrollo seguro cuando proceda, revisión de configuración, control de accesos, gestión de dependencias, bastionado, protección frente a la explotación, validación previa al despliegue, monitorización, trazabilidad y revisión continua de su ciclo de vida. En entornos industriales, este control debe aplicarse con especial atención a aplicaciones propias, componentes adaptados, integraciones con MES o sistemas de supervisión, portales técnicos, herramientas de

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

gestión de activos, servicios de intercambio de datos, APIs, software de apoyo al mantenimiento y otras piezas que conectan la operación con servicios corporativos o externos. Su eficacia depende de que la organización identifique este software como parte de su entorno crítico, y no como un conjunto de aplicaciones auxiliares ajenas a la gobernanza de la seguridad.

Ventajas:

- Reduce la exposición derivada de aplicaciones y componentes conectados con la operación.
- Mejora el control sobre piezas software que suelen actuar como puente entre IT y OT.
- Ayuda a limitar vulnerabilidades, configuraciones inseguras y dependencias poco gestionadas.
- Resulta útil para reforzar servicios técnicos, integraciones y herramientas con impacto operativo indirecto.
- Complementa el desarrollo seguro y los controles de protección de aplicaciones con enfoque más orientado a la operación.

Limitaciones y consideraciones:

- Su eficacia disminuye si no se identifican correctamente todas las aplicaciones e integraciones con relevancia operativa.
- En entornos industriales, algunos componentes pueden depender de software de fabricante o de terceros con poca capacidad de modificación local.
- No sustituye la segmentación, la gestión de accesos, las validaciones previas ni la protección del entorno en el que ese software se ejecuta.
- Se requiere coordinación entre desarrollo, seguridad, operación, mantenimiento y responsables funcionales para contextualizar el riesgo real.
- Debe evitarse tratar como "auxiliar" un software que, en la práctica, condiciona el acceso a la información operativa o la ejecución de procesos relevantes.

Relación con otros controles: Se relaciona con el SAST, el DAST, el RASP, las prácticas seguras de desarrollo e integración, el WAF, la gestión de vulnerabilidades, el bastionado de sistemas y servicios, las validaciones previas y ventanas de mantenimiento y con la monitorización y operación de seguridad. Constituye una capa orientada a reducir el riesgo específico del software conectado con la actividad operativa.

Casos habituales de uso: Se emplea en software de supervisión, portales técnicos, herramientas de soporte al mantenimiento, aplicaciones de integración con sistemas industriales, servicios de intercambio de datos, componentes MES auxiliares, APIs internas, scripts de automatización y otras soluciones software que, sin controlar directamente el proceso, tienen impacto sobre su visibilidad, coordinación o continuidad.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la protección de software ligado a la operación resulta especialmente útil cuando la organización depende de múltiples capas digitales intermedias entre IT y OT y precisa reducir el riesgo sin aguardar a una renovación completa de la arquitectura. Su utilidad aumenta cuando se combina con desarrollo seguro, validación en entornos de prueba, bastionado, segmentación, control de acceso, monitorización y revisión periódica de las dependencias e integraciones que mantienen estos componentes.

5.11 Tendencias emergentes y capacidades avanzadas

La evolución de la industria conectada está introduciendo nuevas tecnologías, nuevos modelos de operación y también nuevos escenarios de riesgo que no siempre encajan en los esquemas tradicionales de protección. Este último bloque reúne **capacidades asociadas a ámbitos emergentes como el IoT industrial, las comunicaciones avanzadas, la inteligencia artificial o la resiliencia ciberfísica**, con la finalidad de ofrecer una **visión prospectiva sobre controles o tecnologías que ya comienzan a ser relevantes en muchos entornos industriales**. Dado este enfoque híbrido, se permite una mayor libertad en el formato de la ficha descriptiva.

5.11.1 IoT industrial

Categoría: Tendencias emergentes y capacidades avanzadas

Tipología: -

Función defensiva predominante: -

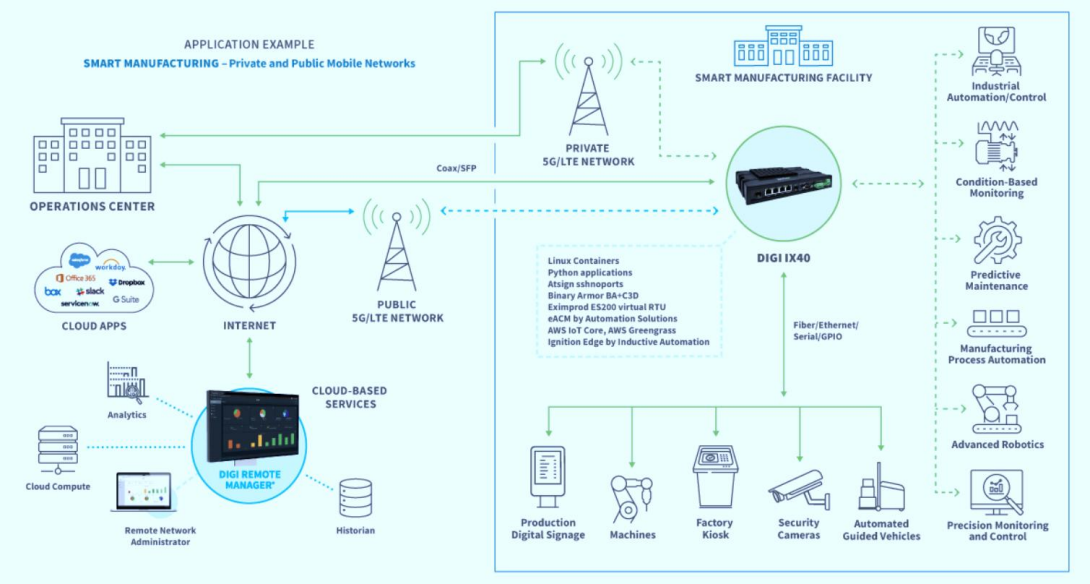
Función en NIST CSF: -

Descripción y alcance: El IoT industrial (IIoT, *Industrial Internet of Things*) se refiere al uso de sensores, actuadores, dispositivos conectados, pasarelas, módulos de comunicación y plataformas asociadas para recoger datos, intercambiar información, automatizar tareas y mejorar la visibilidad sobre procesos, activos y condiciones operativas. Su relevancia en el ámbito industrial no reside sólo en la conectividad de nuevos dispositivos, sino en la capacidad de incorporar capas adicionales de medición,

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

supervisión, trazabilidad y análisis sobre procesos físicos e infraestructuras que tradicionalmente funcionaban con menor nivel de observabilidad o integración digital.

En un sentido amplio, el IoT industrial abarca desde sensores ambientales o de condición hasta dispositivos de mantenimiento predictivo, componentes de telemetría, soluciones de localización, equipos de comunicación avanzada, instrumentación conectada, pasarelas de integración o elementos que alimentan plataformas de analítica, mantenimiento, trazabilidad o gestión energética. Esta evolución abre oportunidades relevantes en eficiencia, conocimiento del proceso y resiliencia operativa, pero también introduce nuevos activos, más software embebido, más firmware, más comunicaciones y más dependencias tecnológicas que deben ser gobernadas con criterios de ciberseguridad desde el inicio.



Ejemplo de uso de IIoT en fabricación inteligente. Fuente: Digi (2023)

Objetivo: Aprovechar las capacidades del IoT industrial para mejorar la visibilidad, la automatización y toma de decisiones sobre la operación, incorporando al mismo tiempo medidas suficientes para limitar el riesgo derivado de la proliferación de dispositivos conectados, de la expansión de la superficie de exposición y de la aparición de nuevas interdependencias entre sistemas físicos y digitales.

Cómo se materializa en un entorno industrial: En la práctica, el IoT industrial suele introducirse de forma progresiva en torno a casos de uso concretos: monitorización de condición, mantenimiento predictivo, eficiencia energética, sensorización de activos, trazabilidad de operaciones, supervisión remota, control ambiental, localización de elementos críticos o integración de datos en plataformas analíticas y de decisión. Su implantación requiere normalmente la combinación de dispositivos de campo, redes de

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

comunicación, pasarelas, plataformas de gestión, mecanismos de integración y, en muchos casos, servicios cloud o entornos híbridos.

Desde la perspectiva de la seguridad, el valor del IIoT depende de que estos componentes no se traten como elementos "auxiliares" o de baja criticidad sólo porque no formen parte del núcleo tradicional del control industrial. Un sensor, una pasarela o una plataforma asociada pueden convertirse en fuente de visibilidad muy valiosa, pero también en un vector de acceso, en un punto de fuga de información, en una dependencia insegura o en un elemento de degradación del proceso si no existe inventario, control de acceso, segmentación, actualización, bastionado y supervisión suficientes.

Principales ventajas:

- Mejora la visibilidad sobre activos, condiciones y comportamiento del proceso.
- Permite ampliar capacidades de monitorización, trazabilidad y mantenimiento.
- Facilita la integración de datos para analítica, optimización y soporte a la decisión.
- Puede contribuir a la detección temprana de anomalías operativas o técnicas.
- Favorece la evolución hacia entornos más conectados, medibles y adaptativos.

Principales riesgos y limitaciones:

- Incrementa el número de activos conectados y la superficie global de exposición.
- Introduce componentes con firmware, software embebido y ciclos de actualización a menudo complejos.
- Puede generar dependencias nuevas con proveedores, plataformas cloud o pasarelas de integración.
- En entornos industriales, muchos dispositivos IIoT no tienen el mismo nivel de robustez o gobernanza que otros activos más maduros.
- Su valor disminuye rápidamente si la conectividad crece más rápido que la capacidad de inventariar, segmentar, supervisar y mantener el entorno.

Elementos de seguridad especialmente relevantes: En este ámbito cobran especial importancia controles como la visibilidad de activos y comunicaciones OT, la segmentación de red, el control de accesos, el NAC cuando aplique, la gestión de vulnerabilidades, el bastionado, la monitorización de red, la seguridad en el acceso remoto, la protección de las pasarelas de integración, la gobernanza de dispositivos externos y la revisión de dependencias cloud o SaaS asociadas al caso de uso.

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

Casos habituales de uso: Se emplea en sensorización de activos industriales, monitorización ambiental, mantenimiento predictivo, eficiencia energética, localización de componentes, trazabilidad de operaciones, recogida distribuida de datos, supervisión de condiciones de proceso y ampliación de la observabilidad en infraestructuras con elevada dispersión física o necesidad de medición fina.

Enfoque recomendado en el catálogo: Dentro de este catálogo, el IoT industrial debe interpretarse menos como un "producto" y más como una capacidad habilitadora que transforma la arquitectura y la superficie de riesgo del entorno. Por lo tanto, su valoración debe hacerse siempre atendiendo a tres dimensiones combinadas: utilidad operativa, grado de exposición introducido y capacidad real de la organización para gobernar los nuevos activos y flujos. En organizaciones maduras, puede actuar como acelerador de visibilidad y resiliencia; en organizaciones con poca gobernanza técnica, puede ampliar de forma significativa la complejidad y el riesgo.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el despliegue de IoT industrial resulta más seguro cuando se realiza de forma gradual, con inventario previo, segmentación específica, autenticación adecuada, protección de las pasarelas, limitación de accesos y monitorización continua de los flujos introducidos. Cuando no sea viable asegurar de inmediato todos los componentes del ecosistema IIoT, conviene reforzar medidas compensatorias como la separación de redes, el control estricto de conectividad, la revisión de las integraciones externas y la supervisión intensificada de los nuevos dispositivos y canales de comunicación.

5.11.2 Redes privadas y comunicaciones avanzadas

Categoría: Tendencias emergentes y capacidades avanzadas

Tipología: -

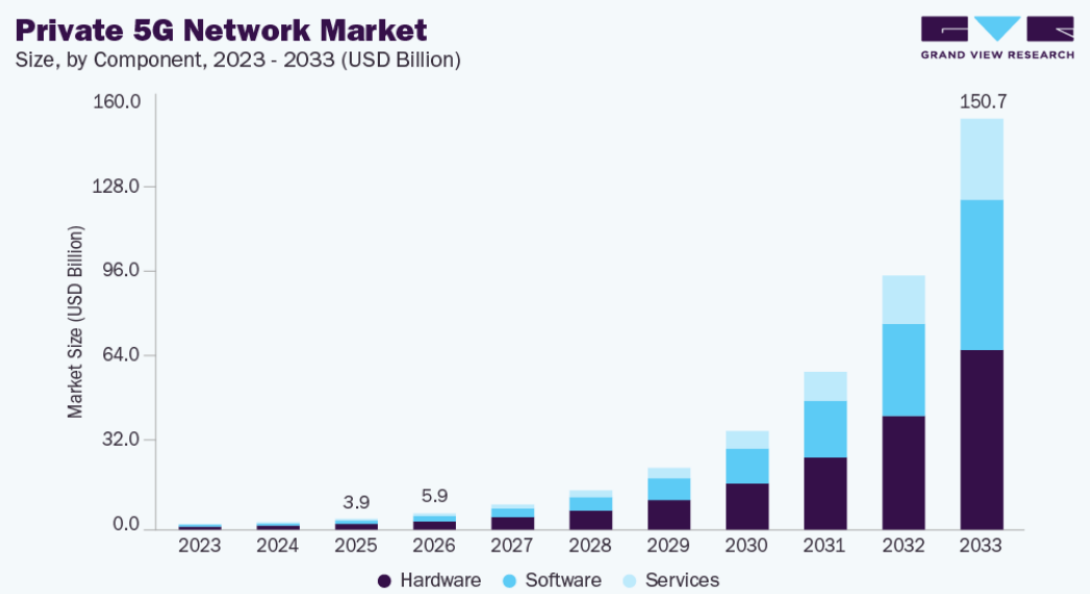
Función defensiva predominante: -

Función en NIST CSF: -

Descripción y alcance: Las redes privadas y comunicaciones avanzadas abarcan el conjunto de tecnologías y arquitecturas de conectividad orientadas a proporcionar comunicaciones más segmentadas, resilientes, de baja latencia, con mayor control operativo y con capacidad de adaptación a las necesidades específicas del entorno industrial. En esta categoría pueden incluirse redes privadas móviles (por ejemplo 5G), soluciones avanzadas de comunicación sin hilos, infraestructuras dedicadas para operación crítica, mecanismos de conectividad distribuida con control reforzado y, en

general, modelos de comunicación que superan la lógica tradicional de red plana o conectividad genérica.

En el ámbito industrial, estas capacidades resultan relevantes porque la digitalización, la sensorización distribuida, la movilidad operativa, la supervisión remota, la automatización flexible y el uso creciente de entornos conectados exigen comunicaciones más previsibles, más gobernables y mejor alineadas con las necesidades del proceso. Al mismo tiempo, la introducción de estas tecnologías modifica la topología de conectividad, incorpora nuevos componentes de red, nuevos planos de gestión y nuevas dependencias con proveedores y servicios, por lo que debe abordarse también desde una perspectiva clara de ciberseguridad.



Previsiones de crecimiento del mercado de las redes 5G privadas. Fuente: Grand View Research (2025)

Objetivo: Mejorar la conectividad del entorno industrial mediante arquitecturas de comunicación más robustas, adaptadas y controladas, asegurando al mismo tiempo que la incorporación de estas capacidades no amplíe de manera desordenada la superficie de exposición ni introduzca nuevas dependencias mal gobernadas.

Cómo se materializa en un entorno industrial: En la práctica, estas capacidades suelen implantarse para soportar casos de uso como movilidad en planta, conectividad de sensores y dispositivos distribuidos, comunicación entre áreas extensas, integración de equipos móviles o autónomos, supervisión remota, intercambio intensivo de datos, control más granular de la conectividad o despliegue de servicios con requisitos estrictos de latencia y disponibilidad. También pueden resultar útiles para separar mejor determinados flujos, crear dominios de comunicación con mayor control y reducir la dependencia de redes compartidas o poco adecuadas para ciertas funciones críticas.

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

Desde la perspectiva de la seguridad, el valor de estas redes depende de que la organización no las interprete únicamente como una mejora de capacidad o rendimiento, sino como un cambio de arquitectura que debe ir acompañado de segmentación, gobernanza de identidades, protección del plano de gestión, visibilidad de activos, control de dispositivos conectados, revisión de integraciones y mecanismos de monitorización acordes al nuevo modelo de comunicación. En entornos industriales, una comunicación más avanzada no es necesariamente una comunicación más segura si no se acompaña de control técnico y procedimental suficiente.

Principales ventajas:

- Permiten adaptar mejor la conectividad a las necesidades reales del proceso y de la operación.
- Pueden mejorar la resiliencia, la previsibilidad y el control de la comunicación entre componentes distribuidos.
- Resultan útiles para entornos con movilidad, dispersión física o alta necesidad de observabilidad.
- Facilitan la incorporación de nuevos casos de uso digital sin depender exclusivamente de redes tradicionales menos flexibles.
- Pueden contribuir a una mejor separación funcional de flujos cuando se diseñan con criterio arquitectónico.

Principales riesgos y limitaciones:

- Introducen nuevos componentes, planos de gestión, dependencias y superficies de exposición.
- Pueden generar una falsa sensación de control si se prioriza la capacidad técnica sobre la gobernanza de la seguridad.
- En entornos industriales, la integración con redes existentes puede aumentar la complejidad y la dificultad de supervisión.
- La dependencia de proveedores, tecnologías especializadas o servicios externos puede convertirse en un factor crítico de riesgo.
- Su valor disminuye si no existe inventario claro de los dispositivos conectados ni visibilidad suficiente de los flujos habilitados.

Elementos de seguridad especialmente relevantes: En este ámbito cobran especial importancia la segmentación de red y separación IT/OT, el NAC cuando aplique, la

visibilidad de activos y comunicaciones OT, la monitorización de red, el control de accesos, el MFA para los planos de gestión, la seguridad en el acceso remoto, el bastionado de los componentes de comunicación, la revisión de las dependencias con terceros y la integración con capacidades como NDR, SIEM o SOC.

Casos habituales de uso: Se emplea en plantas con alta dispersión física, entornos con movilidad técnica u operativa, comunicación con sensores distribuidos, integración de activos IIoT, soporte a plataformas de monitorización avanzada, conectividad de equipos autónomos o móviles, y escenarios en los que la arquitectura de comunicación tradicional no responde adecuadamente a los nuevos requisitos de digitalización y control.

Enfoque recomendado en el catálogo: Dentro de este catálogo, las redes privadas y comunicaciones avanzadas deben interpretarse como una capacidad arquitectónica habilitadora, no como una medida de seguridad por sí misma. Su valor dependerá de la capacidad de la organización para incorporarlas dentro de un diseño segmentado, visible y gobernado, en el que la conectividad no se expanda más rápido que los controles necesarios para protegerla. En organizaciones maduras, pueden reforzar la resiliencia y la flexibilidad; en organizaciones con poca gobernanza, pueden aumentar la opacidad y la dificultad de control.

Observaciones / medidas compensatorias asociadas: En entornos industriales, el despliegue de estas redes resulta más seguro cuando se acompaña desde el inicio de inventario de dispositivos, segmentación por función, protección reforzada del plano de gestión, control de accesos, monitorización de los flujos y revisión de las dependencias externas. Cuando no sea viable asegurar plenamente todos los componentes de la nueva arquitectura, conviene reforzar medidas compensatorias como separación adicional de dominios, restricción de conectividad, supervisión intensificada y validación progresiva de los casos de uso antes de ampliar el despliegue.

5.11.3 Entornos industriales conectados

Categoría: Tendencias emergentes y capacidades avanzadas

Tipología: -

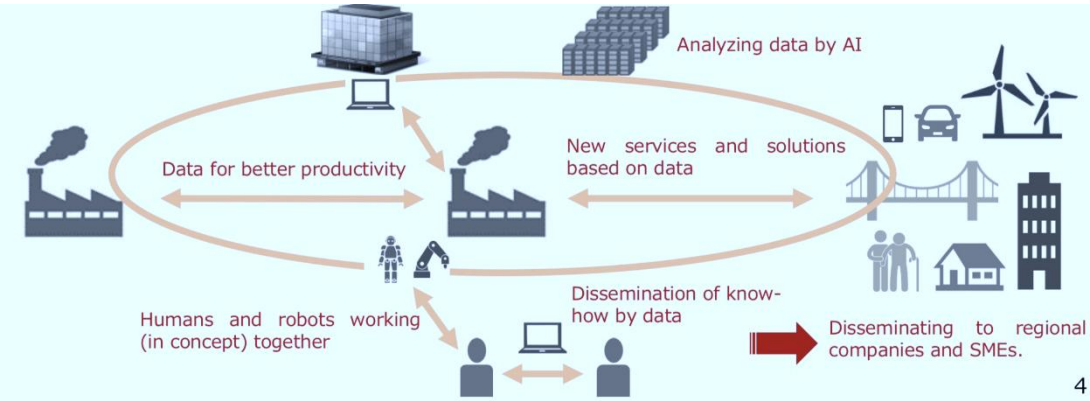
Función defensiva predominante:-

Función en NIST CSF: -

Descripción y alcance: Los entornos industriales conectados representan una evolución de la arquitectura industrial tradicional hacia modelos en los que los sistemas

de operación, supervisión, análisis, mantenimiento, gestión y soporte intercambian información de manera más continua, distribuida e interdependiente. Esta conectividad puede producirse entre activos de planta, sistemas corporativos, plataformas cloud, servicios de terceros, entornos de mantenimiento remoto, componentes IIoT, soluciones de analítica, herramientas de trazabilidad o infraestructuras de apoyo a la decisión. Más que una tecnología concreta, se trata de un modelo de funcionamiento en el que la conectividad pasa a ser un elemento central de la operación, de la visibilidad y de la eficiencia.

En el ámbito industrial, esta evolución permite mejorar la integración de datos, la capacidad de supervisión, la coordinación entre áreas, la optimización del proceso y el soporte a la toma de decisiones. Sin embargo, también introduce una característica crítica desde el punto de vista de la ciberseguridad: la progresiva desaparición de fronteras rígidas entre dominios que antes estaban más separados. Esto hace que el riesgo deje de concentrarse sólo en el perímetro y pase a distribuirse a través de múltiples relaciones, dependencias y superficies de exposición que afectan tanto a la capa digital como al comportamiento operativo.



Concepto de industria conectada. Fuente: METI "Connected Industries Tokyo Initiative" (2017)

Objetivo: Aprovechar los beneficios de la conectividad industrial —mayor visibilidad, integración, eficiencia y capacidad de supervisión— asegurando al mismo tiempo que esa conectividad se produce bajo criterios de segmentación, control, trazabilidad, resiliencia y gobernanza suficientes para no incrementar de forma desordenada la exposición del entorno.

Cómo se materializa en un entorno industrial: En la práctica, los entornos industriales conectados suelen manifestarse a través de la integración entre OT y sistemas corporativos, del uso de plataformas compartidas para analítica o gestión, de la conexión con servicios externos, del acceso remoto para mantenimiento, la incorporación de IIoT, la supervisión distribuida, el intercambio de datos en tiempo real

y la interrelación creciente entre operación, cadena de suministro y servicios digitales. Esta realidad permite mejorar la observabilidad y la capacidad de respuesta de la organización, pero también implica que una incidencia en un punto periférico o aparentemente auxiliar pueda propagarse, directa o indirectamente, hacia funciones de mayor criticidad.

Desde la perspectiva de la seguridad, lo más relevante no es sólo la presencia de más conectividad, sino el hecho de que esa conectividad transforma la arquitectura del riesgo. Los activos ya no pueden analizarse aisladamente: deben comprenderse como parte de un ecosistema de relaciones en el que la identidad, el acceso remoto, los flujos de datos, los terceros, las plataformas intermedias, la nube, los servidores de salto y las integraciones pasan a tener un papel estructural. Esto obliga a reforzar la defensa en profundidad y a pasar de una lógica de protección puntual a otra basada en la gobernanza continuada del entorno conectado.

Principales ventajas:

- Mejoran la integración de información entre operación, mantenimiento, supervisión y gestión.
- Permiten aumentar la visibilidad del proceso y la capacidad de análisis.
- Facilitan nuevos modelos de mantenimiento, soporte, trazabilidad y optimización.
- Favorecen la coordinación entre dominios antes más aislados.
- Pueden contribuir a la eficiencia, a la resiliencia y a la capacidad de respuesta de la organización.

Principales riesgos y limitaciones:

- Ampliación de la superficie de exposición y de las vías de propagación entre dominios.
- Mayor dependencia de integraciones, terceros servicios externos y plataformas intermedias.
- Dificultad para mantener una visión clara de activos, flujos y relaciones cuando la conectividad crece rápidamente.
- Incremento del impacto potencial de una credencial comprometida, de una integración insegura o de un acceso remoto mal gobernado.

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

- Riesgo de asumir que la conectividad aporta eficiencia sin acompañarla de una gobernanza proporcional al riesgo.

Elementos de seguridad especialmente relevantes: En este ámbito cobran especial importancia la segmentación de red y separación IT/OT, la DMZ industrial, la visibilidad de activos y comunicaciones OT, el acceso remoto seguro, el MFA, la IAM, el PAM, el control de accesos de terceros, la monitorización y operación de seguridad, la protección de las integraciones software, la revisión de las dependencias cloud y SaaS y la existencia de procedimientos de cambio y continuidad adaptados a la realidad conectada.

Casos habituales de uso: Se emplea para integración de datos OT con plataformas corporativas, supervisión remota de procesos, mantenimiento distribuido, analítica operativa, conexión con cadena de suministro, incorporación de servicios cloud, trazabilidad en tiempo real, integración con plataformas MES, soporte remoto de fabricantes y arquitecturas en las que la operación depende crecientemente de servicios y relaciones digitales interconectadas.

Enfoque recomendado en el catálogo: Dentro de este catálogo, los entornos industriales conectados deben interpretarse como un marco estructural de evolución de la industria, no como un control concreto. Su valor dependerá de la capacidad de la organización para acompañar a la conectividad con arquitectura segura, control de accesos, gobernanza de las integraciones, visibilidad continua y preparación para responder a incidentes que ya no afectan a componentes aislados, sino a ecosistemas interdependientes. En organizaciones maduras, pueden reforzar muchas capacidades; en organizaciones con gobernanza débil, pueden convertirse en el principal multiplicador del riesgo.

Observaciones / medidas compensatorias asociadas: En entornos industriales, la evolución hacia modelos más conectados resulta más segura cuando se produce de manera gradual, con inventario actualizado, segmentación explícita, control de accesos, trazabilidad de las integraciones y monitorización suficiente de los nuevos flujos. Cuando no sea posible asegurar plenamente todos los elementos del ecosistema conectado, conviene reforzar medidas compensatorias como separación adicional de dominios, limitación de conectividad entre componentes, validación previa de integraciones, revisión periódica de permisos y supervisión intensificada de las relaciones entre sistemas y servicios.

5.11.4 Uso de inteligencia artificial en seguridad

Categoría: Tendencias emergentes y capacidades avanzadas

Tipología: Técnica / organizativa / mixta

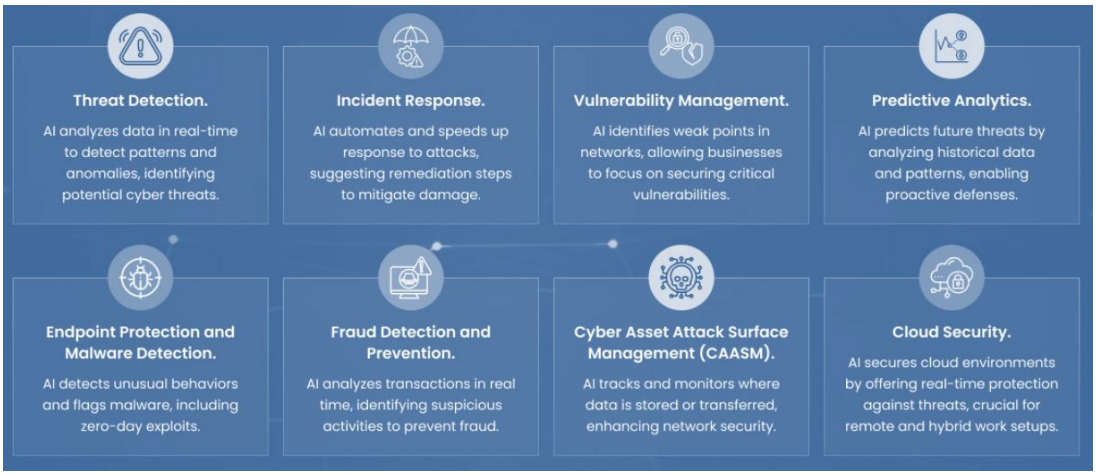
Función defensiva predominante: Detectiva / preventiva

Función en NIST CSF: Detect, Respond

Descripción y alcance: El uso de inteligencia artificial en seguridad se refiere a la aplicación de técnicas de analítica avanzada, aprendizaje automático, correlación automatizada, modelos de predicción, asistencia a la decisión y automatización contextual para mejorar la capacidad de la organización de identificar, interpretar, priorizar y responder frente a riesgos e incidentes de ciberseguridad. En el ámbito industrial, esta tendencia no debe entenderse sólo como un fenómeno tecnológico emergente, sino como una capa potencial de amplificación de las capacidades ya existentes de monitorización, análisis y resiliencia, especialmente en entornos con grandes volúmenes de telemetría, alta complejidad operativa y necesidad de detectar patrones poco evidentes.

La inteligencia artificial puede emplearse, entre otros fines, para detectar anomalías en tráfico y comportamiento de activos, correlacionar señales de múltiples fuentes, apoyar tareas de caza de amenazas, mejorar el análisis de eventos, reducir ruido en operaciones de seguridad, priorizar alertas, identificar desviaciones en parámetros de proceso, reforzar el mantenimiento predictivo o asistir en la simulación de escenarios y en el análisis forense. Al mismo tiempo, su incorporación introduce nuevos riesgos: dependencia de datos de calidad, opacidad de los modelos, falsas conclusiones, automatización excesiva de decisiones y exposición a manipulación o uso indebido de la propia IA.

Objetivo: Aprovechar la inteligencia artificial para aumentar la capacidad de la organización de interpretar grandes volúmenes de información, identificar patrones relevantes y mejorar la eficacia de la detección, análisis y respuesta frente a riesgos de seguridad, sin perder control humano ni contexto operativo sobre las decisiones más sensibles. En el ámbito industrial, su objetivo incluye también reforzar la comprensión de relaciones complejas entre actividad digital, comportamiento de red y señales operativas que, de otro modo, resultarían más difíciles de analizar con rapidez y precisión.



Casos de uso de IA en ciberseguridad. Fuente: IS Partners (2024)

Cómo se materializa en un entorno industrial: En la práctica, el uso de IA en seguridad suele aparecer integrado en otras capacidades ya conocidas: plataformas NDR, SIEM, SOC, monitorización ciberfísica, detección de anomalías, correlación de eventos, análisis de comportamiento de usuarios o activos, priorización automática de incidentes y soporte a la investigación. También puede emplearse en entornos más avanzados para apoyar simulaciones, predicción de fallos, análisis de telemetría industrial, clasificación de riesgos o automatización parcial de respuestas controladas.

En entornos industriales, su valor depende especialmente de la calidad de las fuentes de datos, de la correcta contextualización de los activos y del conocimiento del proceso. La IA puede resultar muy útil para señalar desviaciones, relaciones anómalas o hipótesis de riesgo, pero difícilmente sustituye por completo el criterio técnico y operativo humano cuando están en juego la continuidad de la producción, la seguridad funcional o la interpretación de variaciones legítimas del proceso. Por ello, el enfoque más sólido suele ser el de la inteligencia artificial como capacidad de asistencia y refuerzo, más que como sustitución automática del análisis experto.

Principales ventajas:

- Mejora la capacidad para analizar grandes volúmenes de eventos y telemetría.
- Puede ayudar a identificar anomalías y correlaciones poco evidentes con mayor rapidez.
- Resulta útil para reducir ruido y priorizar alertas en operaciones de seguridad complejas.
- Puede reforzar la detección y la interpretación de señales procedentes de múltiples dominios IT/OT.

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

- Favorece la evolución hacia modelos de monitorización y análisis más adaptativos.

Principales riesgos y limitaciones:

- Su eficacia depende fuertemente de la calidad, cobertura y contexto de los datos disponibles.
- Puede generar falsas conclusiones, sesgos o automatizaciones inadecuadas si se aplica sin supervisión suficiente.
- En entornos industriales, el contexto operativo y las variaciones legítimas del proceso pueden dificultar la interpretación correcta de los modelos.
- La opacidad de los algoritmos puede reducir la trazabilidad y la explicabilidad de ciertas decisiones.
- Su valor disminuye si se emplea como argumento comercial o de modernización sin un caso de uso claro y bien gobernado.

Elementos de seguridad especialmente relevantes: En este ámbito cobran especial importancia la calidad del inventario y de la telemetría, la visibilidad de activos y comunicaciones OT, la monitorización ciberfísica / MES, el NDR, el SIEM, el SOC, el MDR, la caza de amenazas, la gobernanza del dato, la revisión humana de las decisiones automatizadas y la definición clara de qué tareas pueden asistirse con IA y cuáles requieren validación experta obligatoria.

Casos habituales de uso: Se emplea para correlación avanzada de eventos, detección de anomalías de comportamiento, priorización de alertas, apoyo a la investigación de incidentes, análisis de telemetría industrial, mantenimiento predictivo con impacto en seguridad, detección temprana de desviaciones operativas, apoyo a la caza de amenazas y análisis de grandes volúmenes de información procedente de entornos híbridos y conectados.

Enfoque recomendado en el catálogo: Dentro de este catálogo, el uso de inteligencia artificial en seguridad debe interpretarse como una capacidad de refuerzo transversal, y no como un control autónomo suficiente. Su valor real dependerá de la madurez de la organización, de la calidad del dato, de la existencia de procesos de monitorización ya estructurados y de la capacidad para integrar la IA como apoyo al análisis, y no como sustitución acrítica del criterio humano. En organizaciones maduras, puede amplificar mucho la visibilidad y la detección; en organizaciones poco maduras, puede añadir complejidad, opacidad y dependencia tecnológica sin mejora proporcional del control.

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

Observaciones / medidas compensatorias asociadas: En entornos industriales, el uso de IA en seguridad resulta más robusto cuando se introduce de forma gradual, ligado a casos de uso concretos y acompañado de mecanismos de supervisión humana, validación de resultados y revisión periódica del rendimiento del modelo. Cuando no exista madurez suficiente para automatizar decisiones sensibles, conviene emplear la IA como apoyo al análisis y la priorización, manteniendo como medidas compensatorias el refuerzo de la monitorización convencional, la revisión experta de los eventos relevantes y la limitación de las acciones automáticas sobre sistemas con impacto operativo.

5.11.5 Monitorización avanzada y resiliencia ciberfísica

Categoría: Tendencias emergentes y capacidades avanzadas

Tipología: Técnica / organizativa / mixta

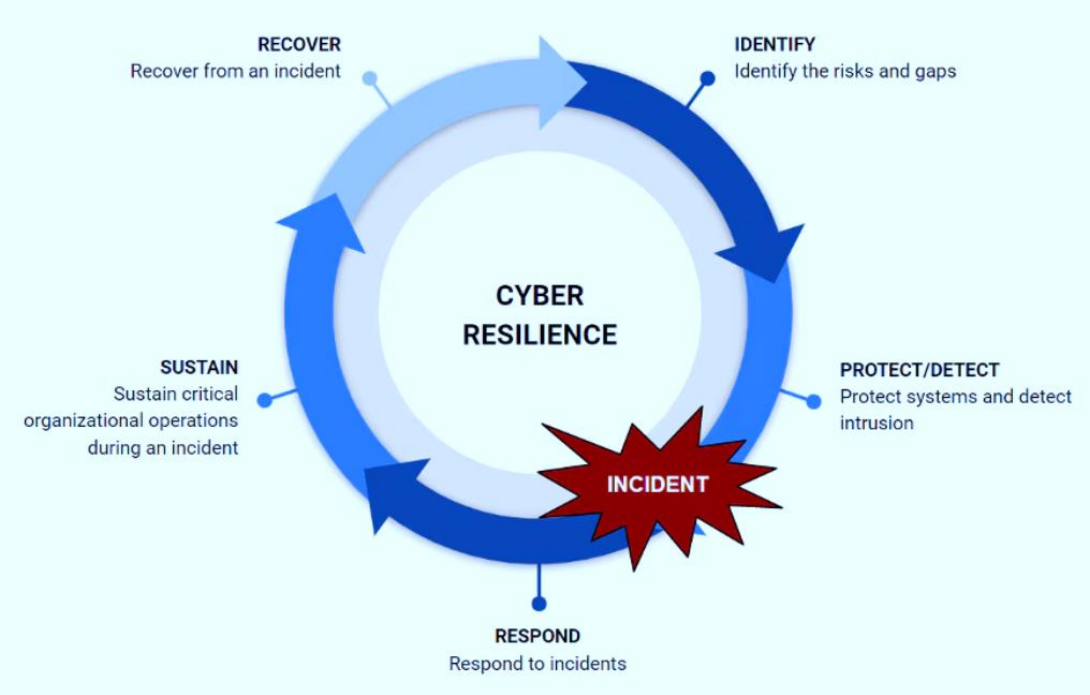
Función defensiva predominante: Detectiva / correctiva

Función en NIST CSF: Detect, Recover

Descripción y alcance: La monitorización avanzada y resiliencia ciberfísica comprende el conjunto de capacidades orientadas a observar, interpretar y reforzar el comportamiento combinado de los sistemas digitales, de las comunicaciones, de los activos físicos y del propio proceso industrial, a fin de anticipar desviaciones, detectar condiciones de riesgo, resistir mejor impactos y recuperar la operación con mayor seguridad y control. Más que un control aislado, se trata de una evolución hacia modelos en los que la protección ya no se limita a detectar eventos informáticos o a restaurar componentes técnicos, sino que incorpora una lectura más integral del funcionamiento real del sistema ciberfísico y de su capacidad para mantener condiciones aceptables de operación bajo perturbación, fallo o incidente.

Esta perspectiva combina elementos de monitorización técnica, observación de señales de proceso, análisis de comportamiento operativo, correlación de eventos, conocimiento del estado de los activos y preparación para absorber degradaciones sin pérdida inmediata de control. En entornos industriales, donde la relación entre la capa digital y la física es directa, esta capacidad resulta especialmente valiosa porque permite pasar de una visión fragmentada del riesgo a otra más próxima a la realidad del proceso, de la producción y continuidad operativa.

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



Etapas de la resiliencia en ciberseguridad. Fuente: Foro Económico Mundial (2022)

Objetivo: Reforzar la capacidad de la organización para detectar de forma más temprana condiciones de riesgo con impacto ciberfísico, interpretar mejor su evolución y sostener la operación o recuperarla bajo criterios más seguros y resilientes. En el ámbito industrial, su objetivo incluye también reducir el riesgo de que un incidente digital, un fallo técnico o una alteración de comunicaciones se derive en una pérdida abrupta de control, visibilidad o capacidad de respuesta sobre el proceso físico.

Cómo se materializa en un entorno industrial: En la práctica, esta capacidad suele materializarse mediante la integración de múltiples planos de observación y preparación: telemetría de red, estado de activos, datos de proceso, alarmas, variables industriales, eventos de sistemas, información de plataformas de supervisión, monitorización ciberfísica, análisis de comportamiento y procedimientos de respuesta y recuperación adaptados al entorno real. Su valor no está sólo en la cantidad de datos disponibles, sino en la capacidad de interpretarlos de manera conjunta para identificar degradaciones, condiciones anómalas, señales débiles de compromiso o patrones que puedan afectar a la estabilidad del sistema ciberfísico.

En entornos industriales maduros, esta aproximación suele complementarse con ejercicios de resiliencia, revisión de dependencias críticas, análisis de modos degradados de operación, validación de capacidades de recuperación y diseño de mecanismos que permitan mantener cierta funcionalidad incluso en escenarios adversos. De esta forma, la monitorización avanzada no se limita a "ver más", sino que

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

contribuye también a responder mejor y a recuperar con mayor conocimiento de las condiciones reales del entorno.

Principales ventajas:

- Mejora la comprensión del estado real del sistema ciberfísico y de sus condiciones de riesgo.
- Permite detectar anomalías con mayor contexto operativo y técnico.
- Refuerza la capacidad de anticipar degradaciones o evoluciones peligrosas del entorno.
- Ayuda a planificar respuestas y recuperaciones más coherentes con el comportamiento del proceso.
- Favorece una visión más integrada de la continuidad, de la seguridad y de la resiliencia industrial.

Principales riesgos y limitaciones:

- Se requiere una base sólida de visibilidad, telemetría y conocimiento del proceso para que sea realmente útil.
- Puede generar complejidad elevada si se incorporan demasiadas fuentes sin capacidad suficiente de interpretación.
- En entornos industriales, la correlación entre señal digital y comportamiento físico no siempre es directa ni trivial.
- Su valor disminuye si se limita a paneles de observación sin procedimientos claros de actuación, escalado y recuperación.
- Puede depender de tecnologías avanzadas o especializadas que exigen madurez organizativa y técnica para ser sostenibles.

Elementos de seguridad especialmente relevantes: En este ámbito cobran especial importancia la visibilidad de activos y comunicaciones OT, la monitorización ciberfísica / MES, el NDR, el SIEM, el SOC, el MDR, el soporte a la respuesta ante incidentes, las copias de seguridad y restauración, la recuperación de operación y continuidad, el conocimiento de las dependencias críticas y la coordinación entre seguridad, operación, mantenimiento y responsables del proceso.

Casos habituales de uso: Se emplea para reforzar la observación de procesos críticos, identificar modos degradados de operación, correlacionar señales digitales y físicas, mejorar la detección temprana de desviaciones, apoyar la respuesta ante incidentes con

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

impacto operativo, verificar la recuperación de sistemas industriales y avanzar hacia modelos de operación más resistentes frente a perturbaciones tecnológicas y ciberfísicas.

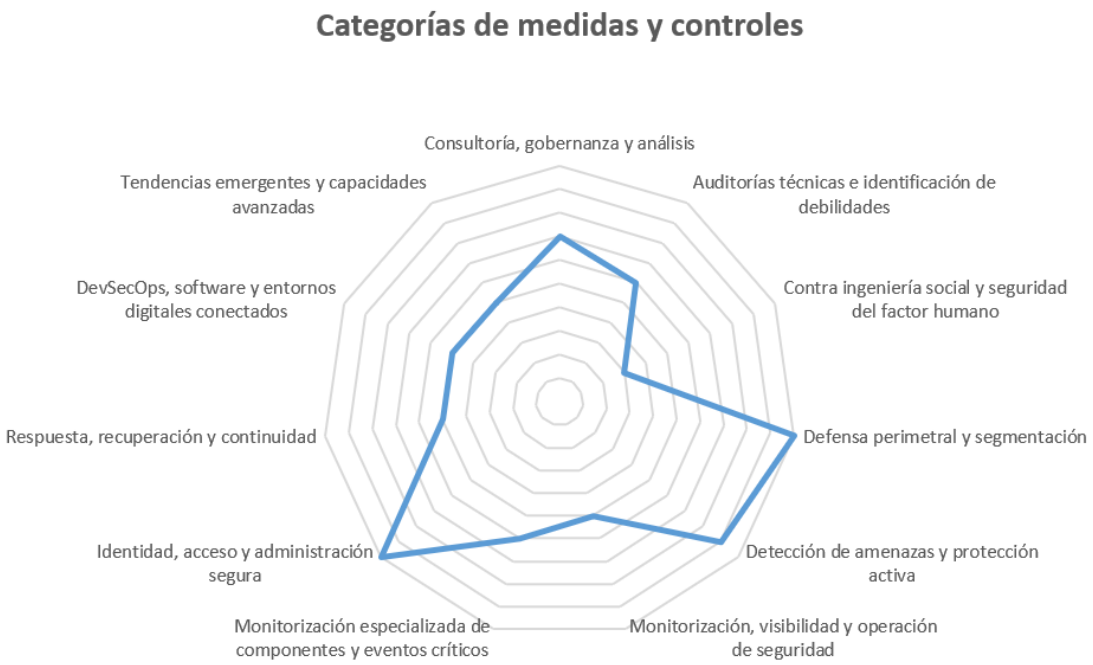
Enfoque recomendado en el catálogo: Dentro de este catálogo, la monitorización avanzada y resiliencia ciberfísica debe interpretarse como una capacidad avanzada de madurez del entorno, especialmente útil en organizaciones que ya disponen de una base razonable de visibilidad, segmentación, control de acceso y operación de seguridad. Su valor no reside en sustituir a los controles básicos, sino en amplificarlos mediante una comprensión más profunda del comportamiento del sistema y de su capacidad de resistir, adaptarse y recuperarse. En organizaciones con baja madurez, conviene priorizar primero la base; en organizaciones más avanzadas, esta capacidad puede marcar una diferencia clara en antelación y resiliencia.

Observaciones / medidas compensatorias asociadas: En entornos industriales, esta capacidad resulta más útil cuando se construye de manera progresiva, partiendo de fuentes fiables, conocimiento operativo y procedimientos claros de actuación. Cuando no exista todavía madurez suficiente para una resiliencia ciberfísica avanzada, conviene reforzar como medidas compensatorias la visibilidad OT, la segmentación, la monitorización de red, la coordinación entre operación y seguridad, las pruebas de recuperación y la preparación de modos degradados de funcionamiento bajo control.

5.12 Resumen del catálogo

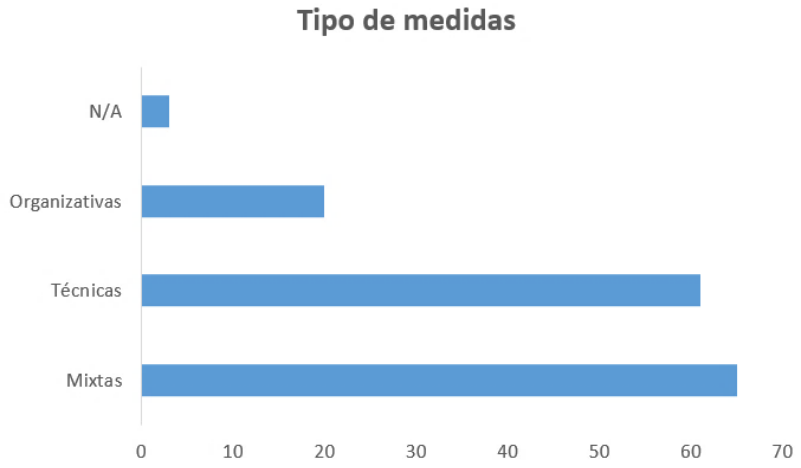
Con el objetivo de facilitar una lectura de conjunto del catálogo y complementar la descripción individual de cada control, se incluye a continuación una síntesis gráfica de su composición. Estas representaciones permiten visualizar de manera agregada la naturaleza de las medidas propuestas, su orientación funcional predominante, su alineamiento con las funciones del marco NIST CSF y la distribución interna del catálogo por grandes bloques temáticos.

La representación por categorías funcionales permite observar su distribución interna y el peso relativo de cada bloque. Destacan especialmente las áreas de **defensa perimetral y segmentación**, **identidad, acceso y administración segura y detección de amenazas y protección activa**, que concentran una parte relevante de las medidas propuestas. Este reparto es coherente con la necesidad de reforzar, en los entornos industriales conectados, **los mecanismos de separación entre dominios, el control del acceso a activos críticos y la capacidad de identificar comportamientos anómalos o maliciosos en una fase temprana**.



Volumen de controles por categoría en el catálogo. Fuente: elaboración propia (2026)

El análisis por tipología confirma el **claro predominio de medidas de carácter técnico y mixto**, lo que resulta coherente con la naturaleza del ámbito ICS/OT y con la finalidad práctica de este documento. La presencia de controles organizativos, aunque menor en términos absolutos, **sigue siendo relevante**, ya que aporta la capa de gobernanza, procedimiento y coordinación necesaria para que las medidas técnicas puedan implantarse, sostenerse y revisarse con criterios de riesgo y continuidad.

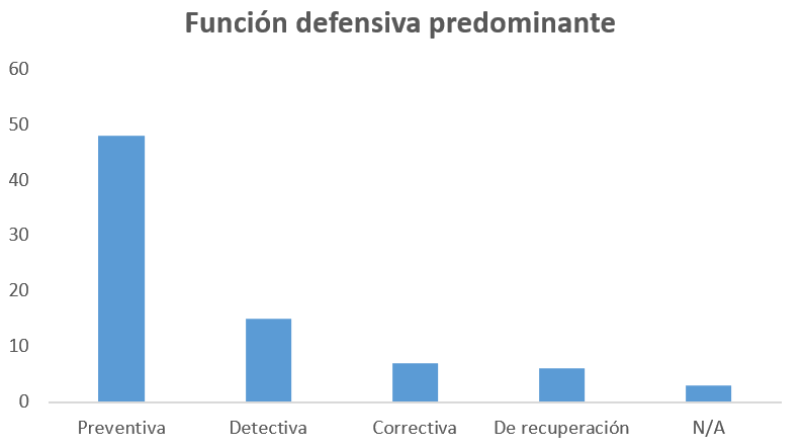


Tipología de medidas en el catálogo. Fuente: elaboración propia (2026)

Por otro lado, la distribución según la función defensiva predominante muestra una **orientación mayoritariamente preventiva**. Este resultado era esperable en un catálogo concebido como instrumento de mejora progresiva de la postura de seguridad,

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

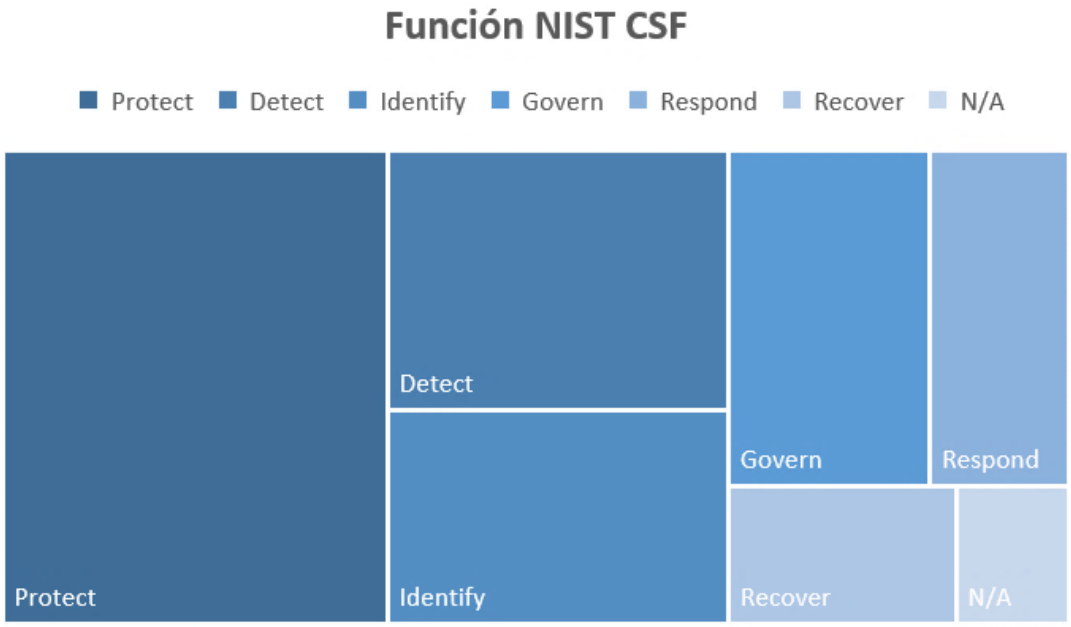
ya que una parte muy significativa de los controles descritos persigue **reducir exposición, limitar superficies de ataque, reforzar el acceso, mejorar la segmentación y disminuir la probabilidad de compromiso**. Junto a esta base preventiva, se observa también la presencia de capacidades detectivas y, en menor medida, de controles correctivos y de recuperación, lo que refuerza la idea de **defensa en profundidad y de resiliencia operativa**.



Funciones defensivas del catálogo. Fuente: elaboración propia (2026)

Por último, la lectura agregada según las funciones del marco NIST CSF evidencia una concentración principal en las funciones **Protect**, **Detect** e **Identify**, acompañadas por una representación también significativa de **Govern**. Ello indica que el catálogo **no se limita a proponer medidas de protección aisladas**, sino que incorpora también capacidades de visibilidad, análisis, inventario, contextualización del riesgo y estructuración de la gobernanza. Por su parte, las funciones **Respond y Recover** presentan un menor peso relativo, pero siguen estando presentes para cubrir la respuesta a incidentes, la restauración de capacidades y la continuidad de la operación.

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



Funciones del NIST CSF representadas en el catálogo. Fuente: elaboración propia (2026)

En su conjunto, esta información permite concluir que el catálogo presenta una **orientación eminentemente práctica, con fuerte peso técnico, predominio preventivo y alineamiento claro con los pilares fundamentales de la protección, la detección y gobernanza**. Al mismo tiempo, la distribución por bloques muestra que el documento procura ofrecer una **cobertura amplia del ciclo de defensa**, integrando medidas de análisis, bastionado, supervisión, administración segura, respuesta y recuperación, aunque con diferente densidad según la naturaleza de cada dominio funcional.

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

6 Estrategia de priorización e implantación

6.1 Criterios de priorización

La utilidad real de un catálogo de controles como el presente **no depende únicamente de la calidad o amplitud de las medidas descritas**, sino también de la capacidad de la organización para **priorizar su implantación con criterios realistas, proporcionados y sostenibles**. En entornos industriales, esta cuestión resulta especialmente relevante, ya que la mejora de la ciberseguridad debe convivir con la continuidad de la operación, con la estabilidad del proceso, con las restricciones de mantenimiento, con la presencia de sistemas legados y con la dependencia habitual de fabricantes, integradores y proveedores de servicios. Por este motivo, la selección del orden de implantación no debería responder a una lógica de acumulación de tecnologías ni a una visión puramente normativa, sino a un análisis contextualizado del riesgo y de la viabilidad.

En este marco, la priorización de los controles puede apoyarse en un conjunto de criterios complementarios que permiten ordenar las actuaciones según su valor real para la organización. Entre ellos, destacan especialmente el **riesgo**, **la criticidad, la exposición, el impacto operativo, la facilidad de implantación y la dependencia de terceros**. La combinación de estos factores permite construir una secuencia de despliegue más sólida que la que resultaría de atender exclusivamente a la severidad teórica de una vulnerabilidad, al coste de la solución o a su popularidad en el mercado [13] [14] [15].

- El primer criterio, y probablemente lo más relevante, es el del **riesgo**. Priorizar en función del riesgo implica **valorar la probabilidad de que una amenaza pueda materializarse sobre un activo o proceso y el impacto que ese hecho tendría sobre la organización**. Esta aproximación obliga a tener en cuenta no sólo la existencia de una debilidad técnica, sino también el nivel de exposición del activo, su papel dentro de la arquitectura, la existencia o no de medidas compensatorias, la accesibilidad desde otros dominios y el tipo de consecuencias que podrían producirse. En un entorno industrial, este riesgo no puede medirse únicamente en términos de pérdida de información, sino también de interrupción de la operación, degradación de la calidad, daño físico, afectación a la seguridad de las personas o incumplimiento de servicios esenciales.

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

- Un segundo criterio clave es la **criticidad** del activo, del sistema o del proceso afectado. **No todos los componentes tienen el mismo peso dentro de la organización, ni todos los incidentes producen consecuencias equivalentes.** Existen activos que, por su función, por los servicios que soportan o por su relación con el proceso industrial deben considerarse prioritarios desde el punto de vista de la protección. Ello incluye, por ejemplo, sistemas de supervisión y control, estaciones de ingeniería, servicios de acceso remoto, repositorios de configuración, sistemas de autenticación, componentes de comunicación entre zonas, activos ligados a la seguridad funcional o infraestructuras sin las que no sería posible mantener una operación segura y estable. La criticidad, además, puede no ser visible en un inventario puramente tecnológico, por lo que resulta esencial interpretarla con el apoyo de operación, mantenimiento y responsables de proceso.
- El tercer criterio es la **exposición**, entendida como el **grado en el que un activo, servicio o comunicación se encuentra accesible, directa o indirectamente, a interacciones no deseadas**. Un sistema altamente expuesto —por ejemplo, un servicio publicado, una conexión remota ancha, un dispositivo con acceso desde la red corporativa o un activo ubicado en un segmento poco compartimentado— tiende a requerir mayor prioridad que otro con una debilidad semejante pero fuertemente aislado o bien compensado. La exposición también debe valorarse de manera dinámica: no depende sólo de si un activo está "en red", sino de quien puede llegar al mismo, por qué canales, con que privilegios, mediante que dependencias y bajo qué grado de trazabilidad y control.
- Un cuarto criterio esencial es el **impacto operativo** de la medida a implantar. **En ciberseguridad industrial no basta con saber que un control sería deseable; también es necesario valorar qué consecuencias puede tener su aplicación sobre la continuidad, el rendimiento, la seguridad funcional, la disponibilidad o el mantenimiento del proceso**. Algunas medidas pueden reducir el riesgo de manera muy significativa, pero resultar inviables a corto plazo por obligar a paradas prolongadas, introducir incertidumbre técnica, generar incompatibilidades con software de fabricante o requerir validaciones que no pueden ejecutarse de inmediato. En estos casos, la priorización debe distinguir entre el valor teórico del control y su viabilidad real, articulando si es preciso secuencias graduales y medidas compensatorias intermedias.

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

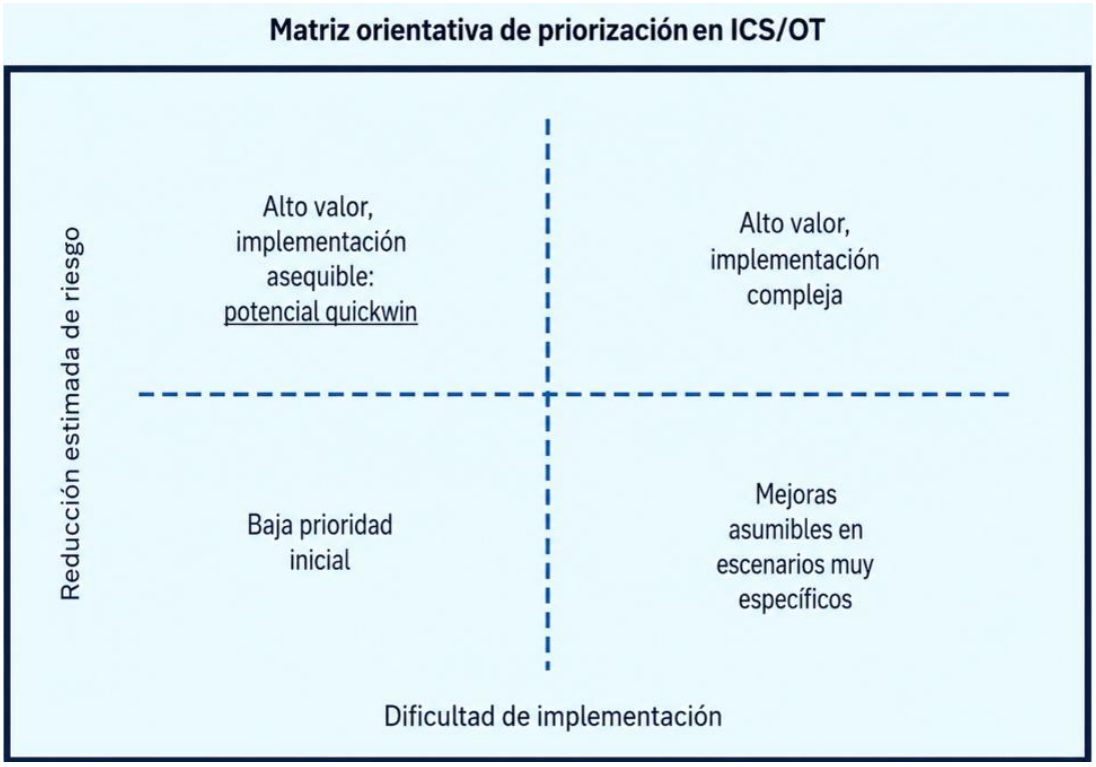
- El quinto criterio es **la facilidad de implantación**, que permite **identificar aquellos controles que, con un esfuerzo asumible, pueden producir una reducción de riesgo significativa**. Este criterio no debe confundirse con una visión simplista basada en escoger siempre lo más fácil, pero sí resulta útil para detectar actuaciones de alto valor y baja complejidad relativa. En muchas organizaciones industriales, existen mejoras que pueden ejecutarse sin transformaciones profundas de la arquitectura, como reforzar accesos remotos, mejorar copias de seguridad, limitar privilegios, inventariar activos, endurecer configuraciones o introducir mayor trazabilidad en conexiones de terceros. Priorizar este tipo de medidas puede generar un efecto tractor positivo, al permitir ganar protección real mientras se preparan iniciativas de mayor complejidad.
- El sexto criterio es la **dependencia de terceros**, particularmente relevante en el ámbito industrial. **Muchas decisiones de seguridad no dependen exclusivamente de la voluntad o capacidad interna de la organización, sino de la intervención de fabricantes, integradores, mantenedores, operadores de servicios, proveedores cloud o empresas externas con acceso al entorno**. Cuando un control requiere coordinación contractual, actualizaciones de firmware, cambios validados por fabricante, reconfiguración de sistemas mantenidos por terceros o alteraciones en servicios externalizados, su implantación puede verse condicionada por tiempos, costes, autorizaciones y restricciones que se deben incorporar explícitamente a la priorización. Ignorar este factor adopta conducir a hojas de ruta poco realistas y a expectativas de ejecución difíciles de cumplir.

A partir de estos criterios, la organización puede construir una **matriz de priorización** en la que cada control se valore según el riesgo que mitiga, la criticidad del activo asociado, su nivel de exposición, el impacto operativo de su implantación, su facilidad de despliegue y la dependencia de terceros. El resultado no debe interpretarse como un algoritmo automático ni como una fórmula cerrada, sino como un instrumento de apoyo a la decisión. Lo más importante no es obtener una puntuación exacta, sino hacer explícita la racionalidad con la que se decide qué medidas se implantan primero, cuáles se difieren, cuáles requieren condiciones previas y cuáles deben acompañarse de medidas compensatorias.

Desde una perspectiva práctica, esta priorización suele conducir a un equilibrio entre tres tipos de actuaciones.

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

- En primer lugar, medidas de **alto riesgo y alta criticidad**, que deben abordarse con carácter preferente, aunque su implantación sea más compleja.
- En segundo lugar, medidas de **alto valor y baja complejidad**, que permiten reducir exposición con rapidez y generar mejoras visibles a corto plazo.
- En tercer lugar, medidas de **mayor madurez o sofisticación**, que pueden ofrecer gran valor en un escenario más avanzado, pero que no deberían desplazar la implantación previa de una base mínima de control, visibilidad, segmentación, acceso seguro y capacidad de recuperación.



Matriz bidimensional de priorización de controles ICS/OT. Fuente: elaboración propia (2026)

La priorización de los controles debe entenderse como un ejercicio continuo y revisable, no como una decisión única adoptada al inicio de un programa. La evolución de la arquitectura, de los procesos, de las amenazas, de los requisitos regulatorios y de las dependencias externas puede alterar el orden razonable de implantación a lo largo del tiempo. Por ello, conviene revisar periódicamente los criterios aplicados y adaptar la hoja de ruta según cambien el riesgo real, la madurez alcanzada o la capacidad de ejecución de la organización.

Priorizar bien significa **implantar primer aquello que más reduce el riesgo real en las condiciones concretas de la organización**, y no necesariamente aquello que resulta más avanzado, más visible o más próximo al ideal teórico. Este enfoque es

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

especialmente importante en entornos industriales, donde la seguridad efectiva tiende a construirse mediante decisiones graduales, bien fundamentadas y compatibles con la operación.

6.2 Implantación por niveles de madurez

La implantación de los controles descritos en este catálogo no debería abordarse como un ejercicio uniforme ni como un itinerario idéntico para todas las organizaciones. La realidad industrial muestra situaciones de partida muy diversas: entidades con escasa visibilidad sobre sus activos y comunicaciones conviven con organizaciones que ya disponen de segmentación parcial, monitorización avanzada o procedimientos maduros de continuidad y respuesta. Por este motivo, una aproximación basada en **niveles de madurez** resulta especialmente útil para orientar la adopción progresiva de medidas, establecer expectativas realistas y evitar tanto la inacción por exceso de ambición como la implantación desordenada de capacidades aisladas.

La lógica de madurez permite ordenar los controles **no sólo por su valor teórico, sino también por su relación con el punto de partida de la organización**. En lugar de asumir que todas las entidades deben aspirar de inmediato a las mismas capacidades avanzadas, este enfoque propone **construir la seguridad en capas sucesivas, consolidando primero una base mínima de conocimiento, control y resiliencia antes de acometer despliegues de mayor sofisticación técnica u operativa**. De esta forma, la madurez no debe entenderse como una etiqueta estática, sino como una guía práctica para estructurar una hoja de ruta de mejora graduaL.

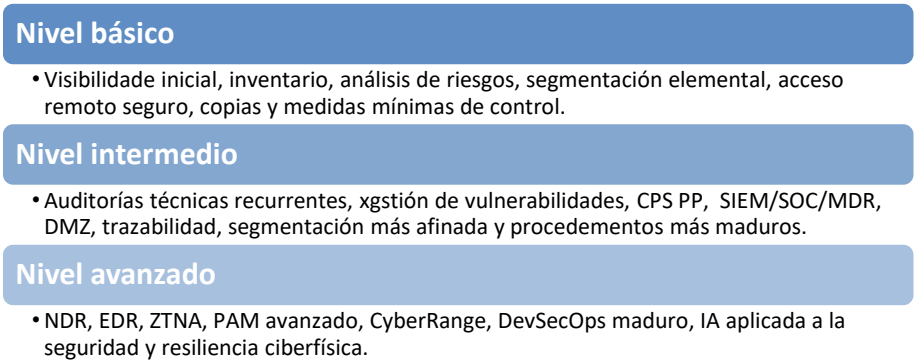
Con carácter orientativo, puede distinguirse entre **tres niveles principales de implantación**: **medidas básicas**, **medidas intermedias** y **medidas avanzadas**. Esta clasificación no pretende ser rígida ni universal, ya que la misma capacidad puede situarse en un nivel distinto según el sector, la arquitectura, la criticidad del proceso o la existencia de dependencias externas. Con todo, ofrece una base útil para interpretar el catálogo y traducirlo a programas de mejora más asumibles.

- El primer peldaño estaría constituido por las **medidas básicas**, esto es, aquellas capacidades que deberían considerarse prioritarias en organizaciones con baja madurez inicial o con escasa formalización previa de su seguridad industrial. Se trata de medidas que permiten conocer mejor el entorno, limitar exposiciones evidentes, reforzar accesos y asegurar una capacidad mínima de continuidad y recuperación. En este nivel suelen situarse, entre otras, el análisis de riesgos tecnológicos, la recomendación de controles, el inventario y la visibilidad básica

de activos y comunicaciones, la segmentación elemental entre IT y OT, el acceso remoto seguro, el refuerzo del control de identidades, el bastionado básico, el control de dispositivos externos, protección del puesto y de los endpoints más expuestos, las copias de seguridad y restauración, así como determinadas medidas de concienciación y procedimientos formales de validación. Son controles que, sin requerir necesariamente una gran sofisticación, **pueden producir una reducción significativa del riesgo cuando se implantan con criterio**.

- El segundo nivel correspondería a las **medidas intermedias**, orientadas a organizaciones que ya disponen de una base razonable de control y que precisan mejorar su capacidad de detección, trazabilidad, análisis y coordinación operativa. En este nivel pueden incorporarse controles como auditorías técnicas más frecuentes, revisiones de arquitectura, programas de gestión de vulnerabilidades, gestión de parches estructurada, segmentación más detallada, DMZ industriales, plataformas CPS PP, SIEM, SOC o MDR, NAC en puntos sensibles, protección reforzada del correo electrónico, trazabilidad de sesiones, control más granular de accesos de terceros y primeros mecanismos de monitorización OT más avanzados. Su valor principal **es consolidar la capacidad de la organización para pasar de una seguridad básicamente preventiva a un modelo en el que la observación, el análisis y la respuesta comienzan a tener un papel más relevante**.
- El tercer nivel agruparía las medidas **avanzadas**, propias de entornos con una madurez ya consolidada, con una arquitectura más ordenada y con una cierta capacidad de operación de la seguridad. En este nivel se situarían controles como ZTNA, PAM muy estructurado, NDR, EDR en los activos compatibles, threat hunting, integración avanzada de señales IT/OT, validaciones en CyberRange, prácticas maduras de DevSecOps, protección de software ligado a la operación, uso de capacidades de IA aplicadas al análisis de riesgos e incidentes, y mecanismos avanzados de resiliencia ciberfísica. Estas medidas pueden aportar un valor muy alto, pero **habitualmente dependen de la existencia previa de inventario fiable, segmentación razonable, identidad gobernada, procedimientos claros, telemetría útil y capacidad real de análisis y respuesta**. **Sin esa base, corren el riesgo de quedar infrautilizadas, mal configuradas o desconectadas de la realidad operativa**.

La principal ventaja de este enfoque por niveles es que permite **adaptar la hoja de ruta a la situación real de la organización**. Una empresa industrial pequeña o mediana, con una arquitectura poco documentada y escasa capacidad interna de seguridad, obtendrá normalmente más valor introduciendo visibilidad, acceso remoto seguro, segmentación básica y copias convalidadas que incorporando de inmediato tecnologías avanzadas de detección sin contexto suficiente. Por el contrario, una organización ya madura, con una base preventiva consolidada, puede encontrar más beneficio relativo en la mejora de la correlación, de la detección temprana, de la respuesta estructurada y de la resiliencia operativa.



Resumen simplificado de controles por nivel de madurez en ICS/OT. Fuente: elaboración propia (2026)

Con todo, este modelo también requiere cautela. La clasificación por madurez **no debe emplearse para posponer indefinidamente medidas necesarias ni para asumir que todos los controles avanzados son siempre secundarios**. En ciertos contextos, un control habitualmente avanzado puede ser prioritario si responde a un riesgo muy expuesto o a una obligación específica del proceso. Del mismo modo, una medida básica mal implantada o insuficientemente gobernada puede ofrecer menos valor que otra aparentemente más sofisticada pero bien contextualizada. La madurez, por lo tanto, debe leerse como **criterio de orientación, no como regla automática**.

Otra ventaja relevante es que esta estructura facilita la **comunicación entre áreas técnicas, operativas y directivas**. Presentar la implantación en niveles permite explicar mejor **por qué determinadas capacidades se incorporan antes que otras, qué dependencias existen entre ellas y qué condiciones previas deben consolidarse antes de avanzar hacia escenarios más complejos**. Ello favorece la elaboración de hojas de ruta comprensibles, compatibles con el presupuesto, con la disponibilidad de personal y con las restricciones operativas de la organización.

Desde una perspectiva práctica, la implantación por niveles de madurez puede emplearse de varias maneras. En primer lugar, como instrumento de **autoevaluación**,

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

permitiendo a la entidad identificar en que estadio se encuentran sus capacidades actuales. En segundo lugar, como base para **priorizar inversiones**, orientando los recursos hacia las medidas que más contribuyen a consolidar el siguiente escalón razonable de madurez. En tercer lugar, como marco para **ordenar el despliegue temporal**, distinguiendo entre controles que pueden abordarse en el corto plazo, medidas que requieren preparación previa y capacidades que sólo tendrán sentido cuando la organización disponga de una base mínima sólida. Finalmente, también puede servir como apoyo para procesos de adecuación a marcos como NIST CSF [11], ISO 27001 [26], IEC 62443 [27] o ENS [28], en los que la progresividad y la trazabilidad de la mejora tienen un papel central. Más detalle de cumplimiento normativo en [25].

La implantación por niveles de madurez, en definitiva, debe entenderse como una **herramienta para hacer más realista, sostenible y eficaz la adopción del catálogo**. Su valor no reside en clasificar organizaciones de forma rígida, sino en ofrecer una estructura que permita construir capacidades de manera ordenada, progresiva y coherente con la realidad del riesgo y de la operación industrial.

6.3 Quick wins en entornos industriales

En un programa de mejora de la ciberseguridad industrial, no todas las medidas tienen el mismo tiempo de maduración ni requieren el mismo nivel de inversión, transformación arquitectónica o coordinación interna. Junto a actuaciones de mayor alcance y complejidad, existen también **controles y decisiones que, bien seleccionados, pueden producir una reducción relevante del riesgo en un plazo relativamente corto y con un esfuerzo asumible**. **A estas actuaciones se ha adoptado denominar como *quick wins***: medidas de impacto alto, implantación comparativamente viable y capacidad para mejorar de manera visible la postura de seguridad sin depender necesariamente de proyectos largos o de transformaciones profundas de la arquitectura.

En entornos industriales, este enfoque tiene una utilidad especial. La presencia de sistemas legados, la dificultad para ejecutar cambios en producción, las restricciones de mantenimiento, la dependencia de terceros y la necesidad de preservar la continuidad hacen que muchas organizaciones perciban la mejora de la ciberseguridad como un proceso complejo, costoso y lento. **Identificar *quick wins* permite romper esa inercia inicial y demostrar que es posible reducir exposición y ganar control mediante actuaciones graduales, proporcionadas y muy orientadas a la realidad operativa**. Además, estas medidas suelen generar un efecto tractor positivo: mejoran la base de

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

control del entorno y crean condiciones más favorables para abordar posteriormente capacidades de mayor madurez.

Es importante subrayar que un *quick win* no es sinónimo de medida superficial ni de acción meramente cosmética. Su principal característica no es la simplicidad abstracta, sino la **buena relación entre esfuerzo de implantación y reducción efectiva del riesgo**. Un control puede considerarse un *quick win* cuando, partiendo de la situación real de la organización, permite resolver exposiciones evidentes, introducir una capa de seguridad significativa o reforzar de inmediato la gobernanza de un ámbito especialmente sensible. Por el contrario, una medida técnicamente atractiva pero con poca aplicación práctica, con escaso alcance real o con fuerte dependencia de condiciones previas, no debería tratarse como tal.

- **Entre los *quick wins* más habituales** en entornos industriales destacan, en primer lugar, el **inventario y la visibilidad básica de activos y comunicaciones**. No es posible proteger adecuadamente aquello que no se conoce, y muchas organizaciones siguen teniendo carencias relevantes en la identificación de equipos, flujos y relaciones entre sistemas IT y OT. Mejorar esta visibilidad —aunque sea inicialmente de manera parcial y progresiva— tiende a generar un beneficio inmediato: permite identificar puntos ciegos, reducir incertidumbre, apoyar el análisis de riesgos y fundamentar mejor la priorización de otros controles. Esto puede hacerse manualmente, o de la mano de la integración por ejemplo con una plataforma CPS PP que adquiera tráfico pasivamente sin interferir con la producción.
- Otro ámbito en el que existen mejoras de implantación asumible es el de la **segmentación básica**. Sin necesidad de acometer de inicio una arquitectura extremadamente sofisticada, muchas organizaciones pueden reducir exposición introduciendo separaciones mínimas entre la red corporativa y la red OT, limitando flujos innecesarios, controlando mejor los accesos de terceros o aislando activos especialmente sensibles o legados. Estas actuaciones, cuando se basan en un conocimiento razonable de los flujos necesarios y se ejecutan con criterio, suelen proporcionar una mejora clara en la capacidad de contención y en la reducción del movimiento lateral.
- Siguiendo con los *quick win* de alto valor, otra muestra es **el acceso remoto seguro**. En muchos entornos industriales, el mantenimiento, la asistencia técnica y la operación distribuida dependen de conexiones remotas, muchas veces con fuerte presencia de terceros. Reforzar este ámbito mediante MFA,

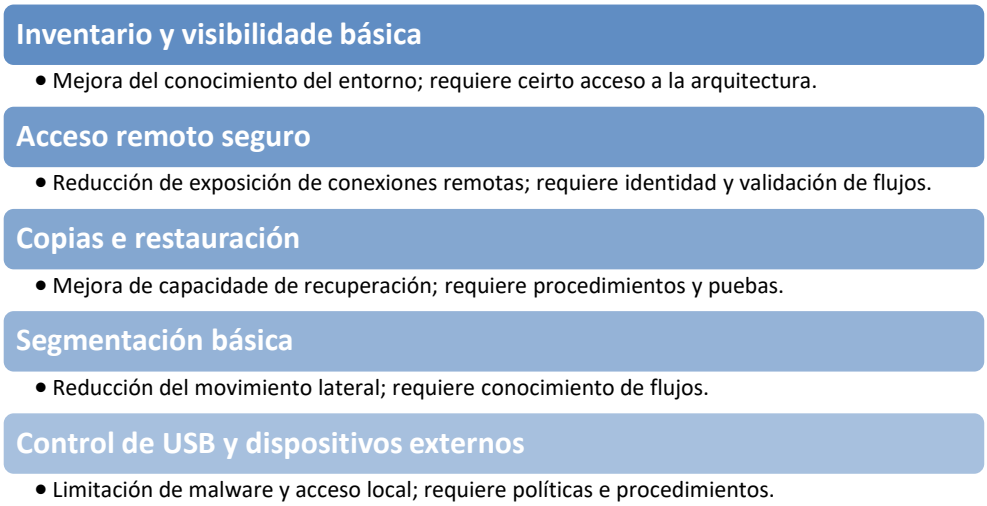
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

segmentación del acceso, servidores de salto, limitación de permisos, trazabilidad de sesiones y procedimientos formales de convalidación ofrecen una mejora muy significativa de la seguridad sin requerir necesariamente una transformación integral de la arquitectura. Dado que el acceso remoto sigue siendo uno de los vectores más relevantes de exposición, cualquier avance en este ámbito produce beneficios rápidos y claramente visibles.

- También deben considerarse *quick wins* las **copias de seguridad y las pruebas de restauración**, especialmente cuando la organización depende de sistemas cuya indisponibilidad puede comprometer la continuidad de la operación (por ejemplo ante un ataque de ransomware). Disponer de copias no solo existentes sino también estructuradas, actualizadas, protegidas y periódicamente verificadas es una de las medidas con mejor relación entre coste y valor práctico. En entornos industriales, este enfoque debe extenderse no sólo a servidores y datos corporativos, sino también a configuraciones, proyectos, recetas, sistemas de supervisión, estaciones de ingeniería y componentes cuya recuperación resulte crítica para volver a condiciones operativas aceptables.
- De la misma manera, el **control de USB y de otros dispositivos externos** han adecuado constituir un *quick win* relevante. En numerosos entornos industriales, el uso de soportes extraíbles, portátiles de mantenimiento y equipos de terceros continúa siendo una vía de interacción habitual con los sistemas. Introducir políticas de restricción, trazabilidad, escaneo previo, convalidación de dispositivos autorizados y procedimientos de conexión controlada puede reducir de forma muy significativa el riesgo asociado a la introducción de malware, la fuga de información o a la modificación no autorizada de componentes sensibles.

Además de estas medidas, existen otros *quick wins* frecuentes según el contexto: refuerzo de privilegios administrativos, eliminación de cuentas por defecto, revisión de exposición de servicios innecesarios, bastionado básico en HMI y estaciones de ingeniería, mejora de la seguridad en el correo electrónico, revisión de los accesos de terceros, formalización de procedimientos de cambio, endurecimiento de credenciales o introducción de mecanismos simples de monitorización y trazabilidad.

El carácter de *quick win* dependerá siempre del punto de partida de la organización, pero la idea central permanece: identificar actuaciones que puedan ejecutarse con relativa rapidez y que aporten valor inmediato.



Ejemplo de potenciales Quick Wins en entornos ICS/OT. Fuente: elaboración propia (2026)

La selección de estos *kick wins* debe hacerse con criterio. No se trata de escoger sólo lo más fácil, sino lo que **más contribuye a reducir el riesgo real con menor fricción de implantación**. Para ello, conviene combinar los criterios expuestos en la sección inicial del bloque: riesgo, criticidad, exposición, impacto operativo, facilidad de implantación y dependencia de terceros. Un *quick win* deja de serlo si su ejecución requiere largos ciclos de validación, cambios profundos de arquitectura o coordinación contractual compleja; del mismo modo, una medida simple pero de valor marginal tampoco debería ocupar el lugar de actuaciones más relevantes.

Desde una perspectiva de gestión, los *quick wins* tienen también una función pedagógica y organizativa. Permiten demostrar resultados tempranos, mejorar la percepción interna del programa de seguridad, facilitar la implicación de áreas operativas y justificar nuevas fases de inversión o despliegue. En un entorno en el que la seguridad industrial puede percibirse como un ámbito especialmente técnico o distante de la operación diaria, estas actuaciones visibles y asumibles contribuyen a hacer más tangible el valor de la mejora continua.

Con todo, hay que evitar una interpretación reducionista. Los *kick wins* son útiles para iniciar o acelerar una hoja de ruta, pero **no sustituyen la necesidad de construir capacidades estructurales y sostenibles en el tiempo**. Su función es reforzar la base, no agotar la estrategia. Un programa maduro no se limita a acumular medidas rápidas, sino que utiliza esas primeras mejoras para crear las condiciones que permitan abordar después segmentación más avanzada, operación de seguridad más madura, detección contextualizada, respuesta estructurada y resiliencia ciberfísica más optimizada.

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

6.4 Secuencia recomendada de despliegue

La implantación de un catálogo amplio de controles de ciberseguridad industrial requiere **no sólo priorizar medidas según riesgo o madurez, sino también establecer un orden lógico de despliegue** que evite dependencias mal resueltas, proyectos desconectados entre sí o inversiones prematuras en capacidades que no cuentan aún con una base suficiente. En entornos industriales IT/OT, esta necesidad es especialmente importante, ya que muchos controles sólo alcanzan su valor pleno cuando se apoyan sobre conocimiento previo del entorno, gobernanza mínima, acceso razonablemente ordenado y cierta estabilidad arquitectónica.

Por este motivo, la implantación no debería formularse como una simple sucesión de productos o iniciativas aisladas, sino como una secuencia progresiva en la que cada etapa prepara las condiciones para la siguiente. Esto no significa que exista un orden universal e inmutable aplicable a todas las organizaciones, pero sí una lógica general que tiende a resultar válida en la mayoría de los entornos: primero **conocer y visualizar,** después **controlar y limitar el acceso**, a continuación **segmentar y reducir exposición**, más tarde **mejorar la detección y la contextualización del riesgo**, y finalmente **consolidar capacidades de gestión de vulnerabilidades, respuesta y continuidad**. Esta progresión reduce el riesgo de desplegar capacidades avanzadas en un entorno poco conocido o escasamente gobernado.

1. Un primer escalón de la secuencia debería centrarse en la **visibilidad y en el conocimiento del entorno**. Sin inventario, sin comprensión de los activos y de las comunicaciones, y sin un análisis mínimo de riesgos y dependencias, la implantación del resto de los controles tiende a basarse en supuestos incompletos. En esta fase resultan especialmente relevantes capacidades como el análisis de riesgos tecnológicos, la recomendación de controles, las evaluaciones técnicas y revisiones de arquitectura, la visibilidad de activos y comunicaciones OT y, según el caso, auditorías de infraestructura o revisiones de perímetro físico-lógico. Su propósito es crear una base factual que permita entender que debe protegerse, con qué prioridad y a través de qué relaciones técnicas y operativas.
2. Una vez alcanzado un nivel razonable de visibilidad, la siguiente prioridad suele ser el **control del acceso y de la identidad**. En muchos incidentes industriales, el acceso remoto excesivamente amplio, las credenciales mal gobernadas, los privilegios innecesarios o la falta de

trazabilidad sobre sesiones y terceros actúan como multiplicadores del riesgo. Por ello, en una secuencia de despliegue realista, suele tener sentido reforzar pronto controles como MFA, IAM, PAM, acceso remoto seguro, gestión de sesiones y trazabilidad y control de accesos de terceros y proveedores. El valor de esta etapa reside en reducir la confianza implícita, limitar la superficie de acceso y crear condiciones más seguras para el funcionamiento del resto de la arquitectura.

3. El tercer momento lógico es el de la **segmentación y separación de dominios**. Una vez conocido el entorno y minimizado en cierta medida el riesgo derivado del acceso, la organización se encuentra en mejor posición para estructurar la arquitectura en zonas y conductos, introducir DMZ industriales, reforzar la compartimentación entre IT y OT y limitar flujos innecesarios. En esta fase cobran protagonismo controles como firewall, NGFW/UTM, segmentación de red y separación IT/OT, DMZ industrial, NAC, proxy, ZTNA o, cuando proceda, mecanismos más avanzados de control de conectividad. La segmentación no debería ser el primer movimiento si los flujos no están bien comprendidos, pero tampoco debería aplazarse en exceso, ya que constituye una de las bases más eficaces para limitar movimiento lateral, contener incidentes y proteger activos legados o de alta criticidad.

4. Un cuarto bloque de la secuencia debería centrarse en la **detección, monitorización y contextualización de la actividad**. Una vez existen visibilidad básica, control de acceso y cierta compartimentación, la organización puede extraer mucho más valor de controles orientados a la observación y análisis de eventos. Aquí se sitúan capacidades como IDS/IPS, NDR, SIEM, SOC, MDR, monitorización ciberfísica / MES, EDR en los activos compatibles, CPS PP, detección de integridad de ficheros, honeypots o threat hunting. Su valor es mucho mayor cuando se despliegan sobre una arquitectura ya razonablemente conocida y estructurada, pues las alertas pueden interpretarse con más contexto y con menos ruido. Esta fase permite avanzar desde una seguridad fundamentalmente preventiva hacia una postura más consciente, capaz de detectar indicios de compromiso y apoyar investigaciones de manera más temprana.

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

5. A continuación, resulta recomendable consolidar de manera más estructurada **la gestión de vulnerabilidades, el bastionado y el control del cambio**. Cuando la organización ya dispone de mejor visibilidad, de una arquitectura más ordenada y de una cierta capacidad de identificación y detección, está en mejor disposición para organizar un programa sostenible de gestión de vulnerabilidades, gestión de parcheado, bastionado de sistemas y servicios y pruebas previas y ventanas de mantenimiento. Este momento es especialmente importante en entornos industriales, ya que la remediación no puede basarse en decisiones aisladas ni en parcheado indiscriminado, sino en un proceso gobernado, compatible con la operación y apoyado en criterios de criticidad, exposición y medidas compensatorias.

6. Finalmente, la secuencia debería culminar con la consolidación de las capacidades de **respuesta, recuperación y continuidad**. Esto no significa que estas medidas deban posponerse hasta el final absoluto; de hecho, ciertos elementos como las copias de seguridad deberían abordarse pronto. Pero sí que su desarrollo más robusto requiere cierta base previa de conocimiento, inventario, acceso gobernado, arquitectura razonablemente estructurada y visibilidad operativa. En esta etapa se sitúan controles como soporte a la respuesta ante incidentes, servicios forenses, copias de seguridad y restauración, recuperación de operación y continuidad y, cuando proceda, instrumentos complementarios como los ciberseguros. Su propósito es asegurar que la organización no sólo pueda prevenir y detectar mejor, sino también contener, restaurar y volver a condiciones operativas aceptables con mayor rapidez y menor impacto.

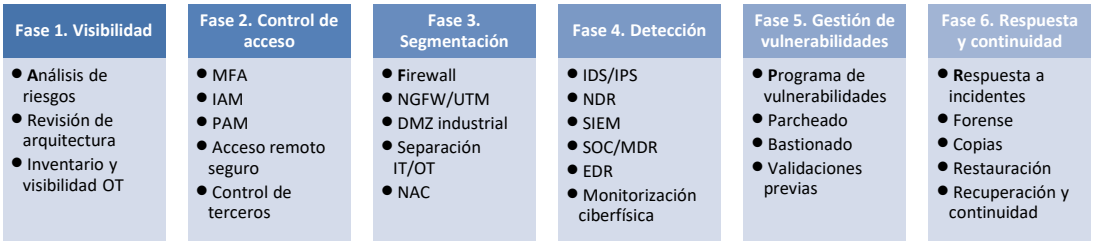
Esta secuencia general puede resumirse de forma simplificada, en la siguiente cadena:

Propuesta de priorización de controles en entornos ICS/OT. Fuente: elaboración propia (2026)

Esta formulación tiene la ventaja de ser intuitiva y útil para la elaboración de hojas de ruta. No obstante, **debe interpretarse como una guía flexible y no como una prescripción rígida. En la práctica, algunas medidas pueden avanzar en paralelo y otras deberán anticiparse o retrasarse según el contexto**. Por ejemplo, las copias de seguridad pueden merecer una atención inmediata incluso antes de completar la fase de detección, y ciertas organizaciones pueden necesitar abordar muy pronto la protección del acceso remoto o el control de terceros por tener en ese ámbito su principal exposición. La clave no está en seguir una secuencia mecánica, sino en mantener la coherencia entre dependencias, capacidad de implantación y reducción efectiva del riesgo.

Otra cuestión importante es que este orden de despliegue **no debe confundirse con el orden de importancia absoluta de los controles**. Un control puede ser muy relevante y, con todo, necesitar condiciones previas para ser implantado con sentido. Esto ocurre con frecuencia con tecnologías avanzadas de detección, correlación o acceso contextualizado, que pueden aportar gran valor pero requieren inventario fiable, identidad razonablemente gubernada, arquitectura segmentada y procesos operativos maduros para ofrecer resultados consistentes. Distinguir entre "control muy importante" y "qué debe implantarse primero" es esencial para construir una hoja de ruta realista.

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



Medidas de seguridad específicas por bloque de controles. Fuente: elaboración propia (2026)

Desde una perspectiva de gobernanza, esta secuencia también facilita la coordinación entre áreas. Ayuda a explicar por qué determinadas inversiones tienen más sentido en un momento concreto, qué dependencias deben resolverse antes de avanzar y cómo se relacionan los controles entre sí. Esto resulta especialmente útil en entornos industriales en los que sistemas, operación, mantenimiento, ingeniería, seguridad y dirección deben compartir una visión común sobre el orden lógico de las actuaciones.

En entornos industriales suele resultar más eficaz **desplegar primero aquello que permite conocer, ordenar y limitar el entorno**, para después **añadir observación, capacidad de respuesta y mecanismos más avanzados de mejora y resiliencia**.

6.5 Relación entre controles base y controles avanzados

Uno de los **errores más habituales** en los programas de mejora de la ciberseguridad industrial consiste en **asumir que la incorporación de controles más sofisticados o tecnológicamente avanzados permite compensar la ausencia de una base mínima suficientemente consolidada**. En la práctica, esto suele traducirse en entornos en los que se despliegan soluciones de alto valor potencial —por ejemplo—, NDR, EDR, ZTNA, PAM avanzado, threat hunting o capacidades de análisis asistida por IA— sin disponer aún de inventario fiable, segmentación suficiente, control riguroso del acceso remoto, políticas de identidad maduras o procedimientos claros de respuesta y continuidad. El resultado suele ser una arquitectura de seguridad desequilibrada, en la que ciertas capacidades existen formalmente, pero no alcanzan el valor esperado o quedan infrautilizadas por la falta de condiciones previas.

Por este motivo, resulta esencial explicar la **relación de complementariedad y dependencia entre controles base y controles avanzados**. Los primeros son aquellos que proporcionan los fundamentos mínimos para conocer, ordenar, limitar y estabilizar el entorno; los segundos introducen capacidades de mayor profundidad, contextualización, automatización o especialización, pero suelen necesitar esa base para funcionar de manera eficaz. Esta relación no debe interpretarse como una oposición

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

entre dos mundos separados, sino como una progresión lógica: los controles avanzados no sustituyen a base, sino que la amplían, la refinan y la hacen más eficaz cuando ésta existe.

Los **controles base** suelen incluir, entre otros, el análisis de riesgos tecnológicos, el inventario y la visibilidad básica de activos y comunicaciones, la segmentación elemental entre IT y OT, el firewall, el acceso remoto seguro, el refuerzo de identidades y autenticación, el control de terceros, el bastionado básico, el control de dispositivos externos, las copias de seguridad y restauración y una capacidad mínima de procedimientos para gestionar cambios, incidencias y continuidad. Estas medidas no siempre resultan espectaculares ni representan el nivel máximo de sofisticación técnica, pero son las que permiten reducir exposiciones evidentes, limitar el movimiento lateral, conocer el entorno y establecer un marco operativo mínimamente gobernado.

Los **controles avanzados**, por su parte, suelen añadir una capa adicional de profundidad analítica, granularidad, automatización o contexto. En ese grupo pueden situarse capacidades como ZTNA frente a esquemas remotos más tradicionales, PAM avanzado con control detallado de sesiones privilegiadas, NDR, EDR, funciones avanzadas de plataformas CPS PP, threat hunting, CyberRange, prácticas maduras de DevSecOps, integración avanzada de señales IT/OT, detección contextualizada y mecanismos más sofisticados de resiliencia ciberfísica. Su valor potencial es elevado, pero su eficacia depende mucho más de que existan condiciones previas: activos conocidos, arquitectura razonablemente segmentada, identidad gubernada, flujos comprendidos, telemetría útil, procedimientos claros y capacidad real de análisis y respuesta.

Un primer aspecto que es destacar es que **un control avanzado no corrige automáticamente las carencias de un control base ausente o mal implantado**. Por ejemplo, un NDR puede mejorar mucho la visibilidad sobre comportamientos anómalos en la red, pero no sustituye la necesidad de segmentar adecuadamente ni de limitar accesos remotos amplios. De la misma manera, un PAM muy sofisticado pierde gran parte de su valor si la organización no tiene una gobernanza mínima de las identidades, si existen cuentas compartidas sin control o si el acceso remoto sigue siendo excesivamente amplio y poco trazable. Una plataforma CPS PP puede aportar un contexto muy valioso sobre el comportamiento ciberfísico, pero no resolverá por sí sola la exposición arquitectónica de un entorno escasamente compartimentado. Esta lógica es esencial: el control avanzado mejora, refina o amplifica la protección; no la sustituye desde cero.

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

Un segundo aspecto importante es que la existencia de **una base sólida aumenta exponencialmente el valor de los controles avanzados**. Cuando la organización ya dispone de inventario fiable, acceso remoto gobernado, segmentación razonable, fuentes de telemetría útiles y procedimientos claros, entonces capacidades como SIEM avanzado, NDR, EDR, ZTNA, threat hunting o monitorización ciberfísica pueden ofrecer resultados mucho más consistentes. En ese escenario, la tecnología avanzada no opera en el vacío, sino sobre un entorno más conocido y estable, en el que las alertas son más interpretables, las decisiones más accionables y la relación entre control y riesgo más visible.

También es importante subrayar que **la distinción entre base y avanzado no es absoluta ni fija**. Un mismo control puede conllevarse como capacidad avanzada en una organización con un nivel inicial muy bajo y, por el contrario, pasar a considerarse parte de la base operativa en una entidad ya madura. El relevante no es tanto la etiqueta, sino la función que cumple dentro de la arquitectura y las dependencias que arrastra. Por ejemplo, un SIEM puede parecer avanzado para una organización sin inventario ni procedimientos de análisis, pero convertirse en un componente casi básico en una organización que ya opera con un SOC estructurado. Lo mismo ocurre con el NAC, con el ZTNA o con las capacidades de visibilidad OT: su lugar real en la hoja de ruta depende del punto de partida y del contexto.

Otra cuestión clave es que la relación entre controles y avanzados no debe leerse sólo en términos tecnológicos. También existe una dependencia fuerte en el plano **organizativo y procedimental**. La respuesta ante incidentes, por ejemplo, puede apoyarse en tecnologías muy avanzadas de detección y análisis, pero seguirá siendo débil si no existen roles definidos, criterios de escalado, coordinación entre áreas técnicas y operativas, procedimientos validados y capacidad de restauración. De la misma manera, la mejor herramienta de acceso contextualizado perderá valor si la organización no tiene claro quién debe acceder, a qué recursos, en qué condiciones y bajo qué aprobación. La madurez real deriva tanto de la tecnología como de la forma en que ésta se integra con procesos, responsabilidades y práctica operativa.

Desde una perspectiva de implantación, esta relación sugiere una regla práctica muy útil: **antes de invertir en un control avanzado, conviene preguntarse qué condiciones previas debe cumplir la organización para obtener valor del mismo**. Si esas condiciones no existen, puede ser más eficiente reforzar primero los controles base de los que depende. Esta pregunta ayuda a evitar despliegues prematuros, expectativas irreales e inversiones que terminan ofreciendo menos retorno de lo

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

esperado. También ayuda a construir hojas de ruta más coherentes, en las que cada capacidad nueva se apoya sobre una base ya parcialmente consolidada.

La utilidad de esta diferenciación es también comunicativa. Permite explicar a la dirección, a los equipos técnicos y áreas operativas por las que determinadas medidas, aun siendo menos vistosas, deben consolidarse antes de dar el salto a tecnologías más avanzadas. Ayuda a ordenar el discurso: primero conocer, limitar y gobernar; después observar mejor, correlacionar, automatizar y especializar. En un contexto en el que la ciberseguridad industrial puede percibirse como una sucesión de herramientas o proyectos independientes, esta visión contribuye a reforzar la idea de arquitectura de capacidades y no de acumulación de soluciones.

La relación entre controles y controles avanzados debe formularse como un principio de acumulación coherente. Los controles avanzados son deseables y pueden ofrecer un valor muy alto, pero su eficacia depende de que exista previamente un nivel mínimo de control del entorno, de gobernanza de la identidad, de compartimentación, de visibilidad y de capacidad de respuesta. Sin esa base, la sofisticación puede convertirse en una ilusión de seguridad más que en una mejora real de la postura defensiva.

Podemos cerrar diciendo que, en una hoja de ruta madura, los controles avanzados deben entenderse como mecanismos para **reforzar y expandir una base ya construida**, no como atajos para sustituir los fundamentos que aún no existen.

7 Conclusiones

Este informe reúne un **catálogo amplio, ordenado y conciso** para seleccionar, priorizar e implantar medidas de ciberseguridad en entornos industriales en las que conviven activos, procesos y dependencias de naturaleza **IT y OT**. Su interés principal no está sólo en el listado de controles, sino en ofrecer una lectura estructurada del conjunto: **qué capacidades existen, cómo se relacionan entre sí y con qué criterios tiene sentido incorporarlas** en un entorno marcado por la complejidad técnica, la criticidad operativa y la necesidad de preservar la continuidad.

La primera idea que se desprende del documento es que **la ciberseguridad industrial requiere un tratamiento específico**. No basta con trasladar al entorno operativo controles pensados para sistemas corporativos convencionales. Los ciclos de vida largos, la presencia de sistemas legados, la dependencia de fabricantes e integradores, las limitaciones de mantenimiento, los requisitos de disponibilidad y la creciente interdependencia entre dominios corporativos e industriales obligan a trabajar con una lógica distinta. Por ello, **proteger un entorno industrial exige combinar perspectiva técnica, conocimiento operativo y criterio organizativo,** y no resolver la seguridad como una suma de herramientas.

La segunda conclusión es igual de relevante: **no existe una medida única capaz de resolver por sí sola el riesgo industrial**. La protección real depende de la combinación de controles complementarios: gobernanza, segmentación, control de acceso, visibilidad, detección, respuesta y recuperación. El catálogo deja ver con claridad esa idea de fondo: **cada capacidad** tiene sentido por separado, pero **gana valor cuando forma parte de un conjunto coherente**, bien relacionado y construido sobre una base mínima suficiente.

En ese sentido, el informe insiste con razón en que **la visibilidad es un punto de partida imprescindible**. Inventariar activos, comprender flujos, revisar arquitectura, identificar dependencias y contextualizar el riesgo no son tareas accesorias, sino condiciones necesarias para decidir con criterio. Sin ese conocimiento, las organizaciones tienden a aplicar medidas genéricas, a invertir en capacidades poco aprovechadas o a incorporar controles sofisticados sin una base suficientemente conocida.

También **resulta significativo el peso que adquieren los controles preventivos y capacidades de protección**, acompañados por funciones de identificación, detección y

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

gobernanza. Esta distribución encaja con la realidad de muchas organizaciones industriales, en las que sigue siendo prioritario reducir exposición, ordenar accesos, reforzar la segmentación, controlar terceros y mejorar la disciplina de cambio. Ahora bien, el informe deja claro que **esa base preventiva no es suficiente por sí sola**. Debe completarse con capacidades de observación, correlación, investigación y respuesta, porque la prevención absoluta no existe y porque, en un entorno industrial, detectar tarde puede traducirse en consecuencias mucho más graves.

Otro de los puntos fuertes del documento es la manera de abordar la **priorización**. El informe sostiene que el orden de implantación de los controles debe responder al **riesgo real y a la viabilidad operativa**, y no sólo a la severidad teórica de una amenaza o a la disponibilidad de una tecnología. Ello significa incorporar a la decisión factores como la criticidad del proceso, la exposición efectiva, el impacto operativo de la medida, la facilidad de implantación y la dependencia de terceros. Esta lectura permite pasar de una aproximación abstracta a una hoja de ruta más realista y sostenible.

En la misma línea, la propuesta de **organizar la implantación según niveles de madurez** —básico, intermedio y avanzado— **resulta especialmente útil**. No todas las organizaciones parten del mismo apartado ni tienen las mismas condiciones para avanzar. Esta estructura ayuda a evitar dos errores frecuentes: por una parte, la parálisis que produce querer llegar de inmediato a un estado demasiado ambicioso; por la otra, la tendencia a incorporar capacidades avanzadas sin haber consolidado previamente lo esencial. El mensaje de fondo es claro: **la madurez no depende de acumular tecnologías, sino de construir una base sólida y evolucionar sobre ella con sentido**.

El informe también acierta al destacar el papel de los **quick wins**, entendidos como medidas con una buena **relación entre esfuerzo y reducción efectiva del riesgo**. En muchos entornos industriales, mejoras como el inventario de activos, el acceso remoto seguro, las copias de seguridad verificadas, la segmentación básica o el control de dispositivos externos pueden generar beneficios claros en un plazo relativamente corto. Su valor no está sólo en el resultado inmediato, sino en que **permiten ganar control sobre el entorno y preparar el terreno para actuaciones posteriores más exigentes**.

Muy relacionada con esto está la idea de que el **orden de implantación importa**. El documento muestra que suele tener más sentido avanzar desde **la visibilidad** hacia el **control de acceso**, la **segmentación**, la **detección**, **la gestión de vulnerabilidades y**, finalmente, la **respuesta y continuidad**, que intentar desplegar desde el primer momento capacidades avanzadas sin base suficiente. No se trata de una secuencia rígida,

pero sí de una lógica sensata que ayuda a evitar proyectos desconectados, dependencias mal resueltas y expectativas poco realistas.

Otra conclusión importante es que **los controles avanzados no sustituyen los controles base**. Tecnologías como NDR, EDR, ZTNA, PAM avanzado, threat hunting o capacidades más sofisticadas de resiliencia pueden ser muy valiosas, pero suelen depender de una base previa de inventario, acceso gobernado, segmentación, telemetría útil, procedimientos claros y capacidad de análisis. Sin esos fundamentos, existe el riesgo de proyectar una imagen de madurez que luego no se corresponde con la capacidad real de la organización para operar, interpretar y aprovechar esos controles.

El catálogo también destaca por el lugar que concede a las **medidas compensatorias**, algo especialmente relevante en el ámbito industrial. En muchas organizaciones no es viable parchear, sustituir o reconfigurar de inmediato ciertos activos. En esos casos, reducir el riesgo pasa por medidas como la segmentación, el bastionado, la limitación de accesos, la monitorización reforzada, la trazabilidad o el aislamiento de componentes. El valor del informe está en tratar esta realidad con naturalidad y sin simplificaciones: **compensar no es renunciar a la seguridad, sino gestionar el riesgo con criterio y de forma compatible con la operación**.

Desde una perspectiva más transversal, el documento refuerza una idea que suele pasarse por alto: **la ciberseguridad industrial no puede sostenerse sólo desde el área técnica**. Se requiere coordinación entre gobernanza, operación, mantenimiento, ingeniería, seguridad y terceros. La claridad procedimental, la definición de responsabilidades y la existencia de un lenguaje común son condiciones tan importantes como los propios controles técnicos. En este sentido, el catálogo también cumple una función útil como **marco compartido de lectura y decisión** entre perfiles muy distintos.

Es destacable, además, que se adopta una **visión amplia y realista de la seguridad industrial**. No se limita a los controles más próximos a la red OT, sino que incorpora también cuestiones ligadas a la identidad, al acceso remoto, a la seguridad del correo, a la protección de aplicaciones, a la gestión de vulnerabilidades, al DevSecOps, la continuidad o a la resiliencia ciberfísica. Esta elección responde a una evidencia cada vez más clara: las **organizaciones industriales ya no operan en compartimentos estancos**, y la exposición puede proceder tanto de un PLC como de un portátil de mantenimiento, de un servicio SaaS mal gobernado o de una conexión remota excesivamente abierta.

El trabajo deja una conclusión principal bastante nítida: **la mejora de la ciberseguridad industrial depende menos de incorporar una tecnología concreta que de construir una arquitectura de controles coherente, gradual y sostenible en el tiempo**. Eso implica conocer mejor el entorno, priorizar con criterio, reforzar primero la base, emplear medidas compensatorias cuando sea necesario y avanzar hacia capacidades más sofisticadas sólo cuando existan condiciones reales para aprovecharlas.

Así, **el catálogo** puede funcionar como **herramienta de referencia para la autoevaluación, la planificación y la revisión de capacidades**, tanto en organizaciones que están comenzando como en aquellas que necesitan reorganizar o reforzar lo ya existente. Su valor principal reside en **convertir un conjunto amplio y heterogéneo de controles en una guía comprensible y aplicable a situaciones reales**.

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

Bibliografía

[1] Observatorio de Ciberseguridad Industrial de Galicia (2026). *Informe de Ciberalertas - I*. Recuperado de https://ciberseguridadegalicia.gal/es

[2] Observatorio de Ciberseguridad Industrial de Galicia (2026). *Informe de Ciberalertas - II*. Recuperado de https://ciberseguridadegalicia.gal/es

[3] Observatorio de Ciberseguridad Industrial de Galicia (2026). *Informe de Inteligencia de Amenazas - I*. Recuperado de https://ciberseguridadegalicia.gal/es

[4] Observatorio de Ciberseguridad Industrial de Galicia (2026). *Informe de Inteligencia de Amenazas - II*. Recuperado de https://ciberseguridadegalicia.gal/es

[5] Observatorio de Ciberseguridad Industrial de Galicia (2026). *Informe de tendencias y reglamento*. Recuperado de https://ciberseguridadegalicia.gal/es

[6] Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC). (2024). *Principles of operational technology cyber security*. Recuperado de https://www.cyber.gov.au/business-government/secure-design/operational-technology-environments/principles-of-operational-technology-cyber-security

[7] CISA (2016). *ICS-CERT Recommended Practices: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*. Recuperado de https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[8] ScienceDirect (n.d.). *Defense in Depth*. Recuperado de https://www.sciencedirect.com/topics/computer-science/defense-in-depth

[9] Centro de Ciberseguridad Industrial (CCI). (2025). *Llevando el reglamento a la realidad 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/

[10] Centro de Ciberseguridad Industrial (CCI). (2025). *Llevando el reglamento a la realidad 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/

[11] NIST (2024). *Cybersecurity Framework 2.0*. Recuperado de https://www.nist.gov/cyberframework

[12] NIST (2024). *Cybersecurity Framework 2.0 Quick Start Guides*. Recuperado de https://www.nist.gov/cyberframework/quick-start-guides

[13] NIST (2012). *Guide for Conducting Risk Assessments (SP 800-30 Rev. 1).* Recuperado de https://csrc.nist.gov/pubs/sp/800/30/r1/final

[14] ISO (2018). *ISO 31000:2018 Risk management — Guidelines.* Recuperado de https://www.iso.org/standard/65694.html

[15] CISA (n.d.). *Cybersecurity Performance Goals 2.0 (CPG 2.0).* Recuperado de https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0

[16] ISO/IEC (2022). *ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls.* Recuperado de https://www.iso.org/standard/75652.html

[17] NIST (2010). *Contingency Planning Guide for Federal Information Systems (SP 800-34 Rev. 1).* Recuperado de https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final

[18] ISO (2019). ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements. Recuperado de https://www.iso.org/standard/75106.html

[19] ENISA (2026). *The ENISA Cybersecurity Exercise Methodology.* Recuperado de https://www.enisa.europa.eu/publications/the-enisa-cybersecurity-exercise-methodology

[20] CISA (n.d.). *Vulnerability Scanning, Analysis, and Reporting.* Recuperado de https://www.cisa.gov/resources-tools/services/vulnerability-management-vulnerability-scanning-analysis-and-reporting

[21] DragonJAR (n.d.). *OSSTMM, Manual de la Metodología Abierta de Testeo de Seguridad.* Recuperado de https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml

[22] OWISAM (wayback machine, 2016). *Página principal.* Recuperado de https://web.archive.org/web/20160503094556/https://www.owisam.org/es/P%C3%A1gina_principal

[23] NIST (2023). *Guidelines for Managing the Security of Mobile Devices in the Enterprise (SP 800-124 Rev. 2).* Recuperado de https://csrc.nist.gov/pubs/sp/800/124/r2/final

[24] Council of the European Union (2025). *Cybersecurity: social engineering.* Recuperado de https://www.consilium.europa.eu/en/policies/cybersecurity-social-engineering/

[25] Observatorio de Ciberseguridad Industrial de Galicia (2026). *Guía normativa de ciberseguridad industrial*. Recuperado de https://ciberseguridadegalicia.gal/es

[26] ISO/IEC (2022). *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* Recuperado de https://www.iso.org/es/norma/27001

[27] IEC. – International Electrotechnical Commission (n.d.). *IEC 62443 – Security for Industrial Automation and Control Systems*. Recuperado de: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[28] Centro Criptológico Nacional (2022). *ENS Navegable – Revisión visual e interactiva de las medidas de seguridad del Real Decreto 311/2022.* Recuperado de https://gobernanza.ccn-cert.cni.es/ens-navegable

Glosario

Acceso remoto seguro

Conjunto de medidas y mecanismos destinados a permitir conexiones remotas a sistemas y servicios bajo condiciones controladas, trazables y proporcionadas al riesgo. En entornos industriales suele apoyarse en MFA, segmentación, servidores de salto, permisos limitados y registro de sesiones.

ACL (Access Control List / Lista de control de acceso)

Conjunto de reglas que determinan qué comunicaciones, usuarios o dispositivos están autorizados a acceder a un recurso, a una interfaz o a un segmento de red. Se utiliza con frecuencia como apoyo a la segmentación y control de flujos.

Activo OT

Elemento tecnológico con función directa o indirecta sobre la operación industrial, como PLC, HMI, estaciones de ingeniería, redes de control, sensores o sistemas de supervisión. Su protección debe tener en cuenta la criticidad del proceso, la disponibilidad y la seguridad funcional.

Análisis GAP

Ejercicio de comparación entre la situación real de una organización y el nivel objetivo definido por un marco, una norma o un conjunto de requisitos. Resulta útil para identificar carencias, priorizar mejoras y ordenar una hoja de ruta de implantación.

Análisis de riesgos tecnológicos

Proceso estructurado de identificación, evaluación y tratamiento de los riesgos que afectan a los activos, servicios, procesos y dependencias tecnológicas de una organización. En el ámbito industrial debe considerar tanto componentes IT como OT y los posibles impactos operativos, físicos y de continuidad.

API (Application Programming Interface / Interfaz de programación de aplicaciones)

Mecanismo que permite la comunicación entre aplicaciones, servicios o plataformas. Su protección es relevante cuando se emplea para integraciones, publicación de datos, servicios cloud o interacción entre sistemas corporativos y operativos.

Auditoría técnica

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

Revisión sistemática de un entorno, sistema, red o conjunto de controles con el objetivo de identificar debilidades, exposiciones, errores de configuración y carencias de protección. Puede abarcar arquitectura, infraestructura, dispositivos finales, redes sin hilos, perímetro o activos OT específicos.

BC/DR (Business Continuity / Disaster Recovery)

Conjunto de planes, procedimientos y capacidades orientados a garantizar la continuidad de la actividad y la recuperación tras un incidente grave. En entornos industriales incluye también la restauración de sistemas de control, comunicaciones y servicios ligados a la operación.

Bastionado

Proceso de refuerzo de la configuración de un sistema para reducir su superficie de ataque. Incluye la desactivación de servicios innecesarios, la limitación de privilegios, el endurecimiento de parámetros de seguridad y la eliminación de configuraciones por defecto inseguras.

CASB (Cloud Access Security Broker)

Capacidad orientada a dar visibilidad y control sobre el uso de aplicaciones y servicios cloud. Permite aplicar políticas de acceso, protección de datos y supervisión sobre interacciones con recursos SaaS y otros servicios externos.

CERT (Computer Emergency Response Team)

Equipo especializado en la gestión de incidentes de ciberseguridad, análisis de amenazas, publicación de alertas y emisión de recomendaciones técnicas. Pueden existir CERT nacionales, sectoriales, corporativos o vinculados a organismos públicos.

Control compensatorio

Medida alternativa o complementaria que permite reducir el riesgo cuando la remediación directa ideal no es viable de forma inmediata. En OT es especialmente relevante cuando no se puede parchear, sustituir o reconfigurar un activo sin afectar a la operación.

CPS (Cyber-Physical Systems / Sistemas ciberfísicos)

Sistemas en los que componentes digitales, comunicaciones y procesos físicos interactúan de forma estrecha. Los entornos OT e ICS son ejemplos característicos de sistemas ciberfísicos.

CPS PP (Cyber-Physical Systems Protection Platforms)

Plataformas de seguridad orientadas a entornos ciberfísicos que combinan información de red, activos, proceso y telemetría para detectar anomalías, mejorar la visibilidad y contextualizar riesgos. Resultan especialmente útiles cuando el análisis debe integrar señales digitales y comportamiento físico del sistema.

CSIRT (Computer Security Incident Response Team)

Equipo de respuesta ante incidentes de seguridad informática. Suele encargarse del análisis, contención, coordinación y seguimiento técnico de incidentes, de forma complementaria o integrada con un SOC.

CVE (Common Vulnerabilities and Exposures)

Sistema de identificación normalizada de vulnerabilidades conocidas mediante un código único. Se emplea habitualmente para referenciar debilidades técnicas en advisories, informes de seguridad y programas de gestión de vulnerabilidades.

CVSS (Common Vulnerability Scoring System)

Sistema estandarizado para valorar la severidad de una vulnerabilidad. Su puntuación resulta útil como referencia, pero no sustituye el análisis contextual del riesgo real en un entorno industrial.

CyberRange

Entorno controlado de prueba, simulación y adiestramiento en el que se pueden ensayar controles, convalidar cambios, ejecutar ejercicios y formar equipos sin afectar a la operación real. En industrial, puede recrear de forma parcial o completa arquitecturas IT/OT, activos y escenarios de incidente.

DAST (Dynamic Application Security Testing)

Técnica de análisis de seguridad que evalúa aplicaciones en ejecución para identificar vulnerabilidades observables desde su comportamiento real. Resulta útil para detectar fallos en la capa de aplicación antes de la puesta en producción o de una actualización relevante.

DCS (Distributed Control System / Sistema de control distribuido)

Arquitectura de control habitual en industrias de proceso continuo, formada por múltiples controladores coordinados y supervisados desde interfaces centrales. Tiene un papel relevante en sectores como energía, química, agua o fabricación avanzada.

Defensa en profundidad

Principio según el cual la seguridad debe construirse mediante capas complementarias de control y no con un único mecanismo aislado. En entornos industriales suele combinar gobernanza, segmentación, control de accesos, visibilidad, detección, respuesta y recuperación.

DLP (Data Loss Prevention)

Conjunto de capacidades orientadas a evitar la fuga, transferencia o copia no autorizada de información sensible. En entornos industriales puede aplicarse también a proyectos de automatización, configuraciones, recetas, documentación técnica y otros datos operativos críticos.

DMZ industrial

Zona de red intermedia entre IT y OT destinada a canalizar intercambios necesarios bajo control, evitando conexiones directas innecesarias entre ambos dominios. Puede alojar servicios compartidos, proxies, servidores de salto, historiadores o mecanismos de intercambio controlado.

EDR (Endpoint Detection and Response)

Capacidad de supervisión, detección, investigación y respuesta sobre la actividad de equipos finales. En entornos industriales tiende a aplicarse a estaciones de trabajo, portátiles de mantenimiento, servidores intermedios y otros activos compatibles con un agente sin riesgo operativo excesivo.

ENS (Esquema Nacional de Seguridad)

Marco normativo español que establece principios y medidas para garantizar la seguridad de la información en el sector público y en las entidades que prestan servicios relacionados. Puede ser una referencia útil para estructurar controles, gobernanza y adecuación documental también en entornos con componente industrial.

FAIR (Factor Analysis of Information Risk)

Metodología orientada al análisis y cuantificación del riesgo de la información. Puede emplearse como apoyo para estructurar escenarios, impacto y exposición de manera más formalizada.

Firewall

Mecanismo de filtrado que regula qué comunicaciones pueden establecerse entre redes, sistemas o segmentos. En entornos industriales constituye una pieza fundamental para

la separación IT/OT, la compartimentación interna y la limitación del movimiento lateral.

Firmware

Software embebido que controla el funcionamiento básico de un dispositivo, equipo o componente hardware. En entornos industriales suele tener un papel crítico en PLC, RTU, sensores, gateways, equipos de red y otros activos específicos.

GRC (Governance, Risk and Compliance / Gobierno, riesgo y cumplimiento)

Enfoque de gestión orientado a integrar gobernanza, análisis de riesgo y cumplimiento normativo en un mismo marco de decisión y control. Resulta útil para estructurar programas de seguridad de manera coordinada.

Hardening

Término empleado habitualmente como equivalente de bastionado. Se refiere al refuerzo de la configuración y de la superficie de exposición de un sistema para hacerlo más resistente frente a usos indebidos o explotaciones.

HMI (Human-Machine Interface / Interfaz hombre-máquina)

Sistema o pantalla a través de la cual los operadores visualizan el estado del proceso e interactúan con él. Su protección es crítica porque la misma está ligada a la supervisión, a la operación y a la ejecución de acciones con impacto directo sobre el entorno OT.

IAM (Identity and Access Management)

Conjunto de procesos y herramientas destinados a gestionar identidades, cuentas, roles, permisos y ciclo de vida del acceso. Su finalidad es garantizar que cada usuario o sistema disponga sólo de los privilegios necesarios y bajo condiciones trazables.

ICS (Industrial Control Systems / Sistemas de control industrial)

Conjunto de sistemas utilizados para supervisar, controlar y automatizar procesos industriales. Incluye componentes como PLC, DCS, SCADA, sensores, HMI, estaciones de ingeniería y redes de comunicación industrial.

IDS / IPS

Los IDS detectan patrones o tráficos sospechosos en la red; los IPS, además, pueden bloquear o limitar ciertas comunicaciones. En entornos industriales suelen utilizarse con prudencia, especialmente cuando la prevención activa puede afectar a la disponibilidad de la operación.

IEC 62443

Familia de normas internacionales de referencia para la ciberseguridad de sistemas de automatización y control industrial. Aporta conceptos, requisitos y buenas prácticas sobre gobernanza, zonas y conductos, sistemas, componentes y relaciones entre operadores, integradores y fabricantes.

IIoT (Industrial Internet of Things / IoT industrial)

Aplicación de sensorización, conectividad e intercambio de datos a activos, procesos y componentes del entorno industrial. Aporta la visibilidad y eficiencia, pero también amplía la superficie de exposición y las dependencias tecnológicas.

Inventario de activos

Relación estructurada de los activos tecnológicos presentes en un entorno, incluyendo identificación, función, localización, propietario, versiones y relaciones de dependencia. Es una base esencial para análisis de riesgos, segmentación, gestión de vulnerabilidades y respuesta ante incidentes.

IoT industrial

Conjunto de dispositivos, sensores, actuadores y componentes conectados que recogen, transmiten o procesan información relacionada con la operación. Su seguridad requiere prestar atención a inventario, autenticación, segmentación, firmware y canales de comunicación.

IT (Information Technology / Tecnología de la información)

Conjunto de sistemas, redes, aplicaciones y servicios orientados principalmente al tratamiento, almacenamiento e intercambio de información. En un entorno industrial convive cada vez más con OT, generando interdependencias que deben gobernarse con criterio.

MAGERIT

Metodología de análisis y gestión de riesgos promovida en el ámbito español para apoyar ejercicios de evaluación, tratamiento y documentación del riesgo. Puede emplearse como referencia en programas de seguridad y adecuación normativa.

MDR (Managed Detection and Response)

Servicio gestionado de detección y respuesta que aporta supervisión, análisis y apoyo operativo ante incidentes. Puede complementar o sustituir parcialmente capacidades internas, especialmente en organizaciones sin SOC propio maduro.

MDM (Mobile Device Management)

Capacidad orientada a la administración centralizada de dispositivos móviles, incluyendo configuración, políticas, control de acceso, cifrado y, cuando procede, borrado remoto. Resulta útil para reforzar la seguridad de smartphones, tablets y otros dispositivos portátiles.

MES (Manufacturing Execution System)

Sistema de ejecución de manufactura que actúa como capa intermedia entre la planificación y la operación, coordinando información de producción, trazabilidad, órdenes y control del proceso. Su protección es relevante por su posición de enlace entre dominios corporativos y operativos.

MFA (Multi-Factor Authentication / Autenticación multifactor)

Mecanismo de autenticación que requiere más de un factor de verificación para conceder acceso, como contraseña, token, certificado o biometría. Es especialmente recomendable en accesos remotos, cuentas privilegiadas e interacciones con activos sensibles.

NAC (Network Access Control)

Conjunto de mecanismos orientados a controlar qué dispositivos pueden conectarse a la red y en qué condiciones. Resulta útil para limitar la incorporación no autorizada de portátiles, equipos de terceros, dispositivos móviles o componentes no inventariados.

NDR (Network Detection and Response)

Capacidad orientada a la observación y análisis del tráfico de red para detectar anomalías, movimiento lateral, exploración o interacciones sospechosas. En OT es muy valiosa para ganar visibilidad sobre flujos, protocolos y relaciones entre activos.

NGFW (Next-Generation Firewall)

Firewall de nueva generación que añade al filtrado clásico capacidades como inspección más avanzada, identificación de aplicaciones, integración con inteligencia de amenazas o prevención de intrusiones. Debe configurarse con prudencia en entornos industriales.

NIST

National Institute of Standards and Technology de los Estados Unidos. Es una de las entidades de referencia internacional en la publicación de marcos, guías y buenas prácticas de ciberseguridad.

NIST CSF (Cybersecurity Framework)

Marco de referencia del NIST para estructurar programas de ciberseguridad en torno a las funciones Govern, Identify, Protect, Detect, Respond y Recover. Resulta útil para clasificar controles, orientar hojas de ruta y comunicar madurez de manera comprensible.

OT (Operational Technology / Tecnología de operación)

Conjunto de tecnologías empleadas para supervisar, controlar y mantener procesos físicos, industriales u operativos. Se diferencia de IT por su vínculo directo con la disponibilidad, la estabilidad del proceso y, en muchos casos, con la seguridad de las personas y de las instalaciones.

PAM (Privileged Access Management)

Capacidad orientada a controlar, limitar y supervisar el uso de cuentas y sesiones privilegiadas. Su valor es especialmente alto en entornos con acceso remoto de terceros, administración de sistemas críticos u operación sobre activos sensibles.

Patch management

Expresión habitual para referirse a la gestión de parcheado. Incluye planificación, convalidación, aplicación y seguimiento de las actualizaciones de seguridad y correcciones técnicas.

Pentesting

Ejercicio controlado de simulación de ataque destinado a comprobar si determinadas debilidades pueden ser explotadas y con qué consecuencias. En entornos industriales debe formularse con fuerte prudencia, alcance delimitado y autorización previa para evitar impacto en la operación.

Phishing

Técnica de ingeniería social basada normalmente en correo electrónico para engañar a una persona y conseguir credenciales, datos, ejecución de acciones o acceso inicial. Puede combinarse con suplantación de identidad, urgencia aparente o uso de enlaces y anexos maliciosos.

PLC (Programmable Logic Controller / Controlador lógico programable)

Dispositivo fundamental en muchos entornos industriales encargado de ejecutar lógicas de control sobre máquinas y procesos. Su criticidad hace que su seguridad, configuración y exposición deban tratarse con especial prudencia.

Proxy

Servicio intermediario que controla comunicaciones entre un cliente y un recurso de destino, evitando conexiones directas innecesarias. Puede utilizarse para canalizar acceso a servicios, filtrar tráfico, registrar actividad o publicar aplicaciones bajo control.

PRTR (Plan de Recuperación, Transformación y Resiliencia)

Marco de inversión pública vinculado a fondos europeos que financia, entre otras líneas, iniciativas de modernización, digtalización y ciberseguridad.

RASP (Runtime Application Self-Protection)

Capacidad de protección integrada en la aplicación o en su entorno de ejecución, diseñada para detectar y bloquear ciertos usos maliciosos en tiempo real. Complementa otros controles de seguridad de la aplicación, especialmente cuando existen servicios expuestos.

RETECH (Redes Territoriales de Especialización Tecnológica)

Programa de apoyo a proyectos de especialización tecnológica impulsado en el ámbito estatal y autonómico. Puede aparecer como marco institucional del Observatorio y de otros entregables asociados.

Resiliencia ciberfísica

Capacidad de un sistema o de una organización para anticipar, resistir, absorber, responder y recuperarse de incidentes que afectan simultáneamente a las capas digitales y físicas. En entornos industriales implica no sólo restaurar sistemas, sino volver a condiciones operativas seguras y aceptables.

RTU (Remote Terminal Unit / Unidad terminal remota)

Dispositivo empleado para recoger datos y ejecutar acciones de control en entornos distribuidos, especialmente en infraestructuras geográficamente dispersas. Es habitual en sectores como energía, agua o transporte.

SaaS (Software as a Service)

Modelo en el que una aplicación se consume como servicio a través de la red, normalmente gestionado por un proveedor externo. Su uso requiere controlar acceso, configuración, intercambio de datos, permisos e integraciones.

SANS

Organización internacional conocida por la publicación de estudios, buenas prácticas, formación e investigación aplicada en ciberseguridad. Sus guías y encuestas suelen utilizarse como referencia sectorial.

SASE (Secure Access Service Edge)

Modelo que combina conectividad y seguridad para controlar accesos distribuidos, servicios cloud y recursos híbridos bajo políticas coherentes. Puede integrar capacidades como acceso seguro, filtrado, inspección y control contextual.

SAST (Static Application Security Testing)

Técnica de análisis de seguridad aplicado al código fuente, binarios o componentes antes de la ejecución, con el fin de detectar vulnerabilidades y patrones inseguros. Resulta útil en procesos de desarrollo e integración de software.

SCADA (Supervisory Control and Data Acquisition)

Arquitectura de supervisión y adquisición de datos empleada para controlar procesos distribuidos y recoger información de campo. Es habitual en sectores como agua, energía, transporte y otras infraestructuras con operación remota o descentralizada.

Segmentación IT/OT

Separación arquitectónica y lógica entre dominios corporativos y operativos para limitar exposición, movimiento lateral y propagación de incidentes. Puede complementarse con zonas y conductos, DMZ industriales, firewalls y reglas de comunicación estrictamente definidas.

SGSI (Sistema de Gestión de la Seguridad de la Información)

Estructura organizativa, documental y operativa orientada a gestionar la seguridad de la información de forma continua y sistemática, habitualmente asociada a ISO/IEC 27001.

SIEM (Security Information and Event Management)

Plataforma orientada a la recogida, normalización, correlación y análisis de eventos de múltiples fuentes. Permite mejorar la detección y la investigación de incidentes a partir de una visión centralizada de la actividad de seguridad.

SOC (Security Operations Center)

Capacidad organizativa y operativa encargada de supervisar, analizar y coordinar la respuesta frente a incidentes de seguridad. Puede ser interno, externo o híbrido, y en entornos industriales debe integrar también el contexto operativo de las alertas relacionadas con OT.

SSID (Service Set Identifier)

Nombre identificador de una red WiFi. Su configuración, visibilidad y segregación pueden tener relevancia en auditorías de redes inalámbricas y control de acceso inalámbrico.

SW (Software)

Abreviatura habitual de software. En el catálogo aparece especialmente vinculada a desarrollo seguro, integración, análisis de aplicaciones y protección de software ligado a la operación.

Threat hunting

Actividad proactiva de búsqueda de indicios de compromiso o comportamiento malicioso que no ha sido detectado automáticamente por los mecanismos convencionales. Requiere visibilidad suficiente, hipótesis de investigación y capacidad analítica para contextualizar señales débiles.

UTM (Unified Threat Management)

Solución que integra en un mismo dispositivo o servicio varias capacidades de seguridad, como firewall, inspección, filtrado o prevención de intrusiones. En entornos industriales debe emplearse con criterio y convalidación previa del impacto.

Vishing

Técnica de ingeniería social basada en llamadas telefónicas o comunicación de voz para engañar a una persona y obtener información, credenciales o acciones indebidas.

VLAN (Virtual Local Area Network)

Mecanismo de segmentación lógica que permite separar redes o grupos de dispositivos dentro de la misma infraestructura física. Es un recurso frecuente para compartimentar tráfico y apoyar el diseño de zonas.

VPN (Virtual Private Network)

Tecnología que establece canales cifrado entre usuarios, sedes o sistemas para proteger las comunicaciones sobre redes potencialmente expuestas. En industrial debe emplearse con alcance limitado, autenticación fuerte e integración con segmentación y trazabilidad.

WAF (Web Application Firewall)

Control de seguridad orientado a proteger aplicaciones y servicios web frente a peticiones maliciosas y explotaciones en la capa de aplicación. Es útil cuando existen

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

portales, APIs o interfaces web que deben permanecer accesibles bajo condiciones de control reforzado.

Gestión de parcheado

Proceso de planificación, convalidación, aplicación y verificación de actualizaciones y correcciones de seguridad en sistemas y componentes tecnológicos. En entornos industriales debe conciliarse con la disponibilidad, la validación previa y el uso de medidas compensatorias cuando el parcheo directo no es viable.

Gestión de sesiones y trazabilidad

Conjunto de mecanismos orientados a registrar, supervisar y, cuando procede, revisar las sesiones de acceso a recursos sensibles. Es especialmente relevante en cuentas privilegiadas, mantenimiento remoto y accesos de terceros.

ZTNA (Zero Trust Network Access)

Modelo de acceso basado en la verificación explícita de la identidad, del dispositivo y del contexto antes de conceder acceso a un recurso concreto. Procura sustituir la confianza implícita por permisos granulares y limitados al mínimo necesario.

CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridad Industrial

Catálogo de buenas prácticas y controles de seguridad para entornos ICS/OT

AMTEGA – Xunta de Galicia 2026

Financiado pola Unión Europea NextGenerationEU

Plan de Recuperación, Transformación e Resiliencia

incibe_

AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA

Xacobeo 2027