CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridade Industrial

Catálogo de boas prácticas e controis de seguridade para entornos ICS/OT

Xuño 2026

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

Edita: Xunta de Galicia

Axencia para a Modernización Tecnolóxica de Galicia (AMTEGA)

Lugar: Santiago de Compostela

Ano: 2026

Índice

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

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

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

1 Introdución

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

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

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

--

O presente traballo intégrase na liña de xeración de coñecemento especializado orientado a **apoiar a mellora da protección das organizacións industriais, das infraestruturas críticas e das administracións públicas con contornos operativos e tecnolóxicos de carácter híbrido** (a grande maioría), nos que conviven activos e procesos de **tecnoloxía da información (IT)** e de **tecnoloxía de operación (OT)**.

A progresiva dixitalización da industria, a automatización dos procesos produtivos, a crecente conectividade dos sistemas de control e supervisión e a incorporación de tecnoloxías como o **IoT industrial**, a analítica avanzada ou a monitorización remota están a transformar profundamente a realidade operativa de múltiples sectores. Esta evolución está a achegar **ganancias de eficiencia, trazabilidade, flexibilidade e capacidade de xestión**, mais tamén está a ampliar de maneira significativa a **superficie de exposición fronte a incidentes de ciberseguridade**. A **converxencia entre IT e OT**, lonxe de ser unha hipótese de futuro, constitúe xa unha **realidade consolidada** en contornos como a enerxía, a auga, a automoción, a alimentación, a loxística, o ámbito farmacéutico ou os servizos públicos esenciais.

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

Neste contexto, a protección dos contornos industriais esixe un enfoque específico, **máis alá da simple translación de controis tradicionais de seguridade da información ao ámbito operativo**. Os sistemas OT presentan **particularidades propias** que condicionan a selección e a implantación de medidas de seguridade: **longos ciclos de vida dos activos**, presenza de sistemas legados, restricións de parada e mantemento, dependencia de fabricantes e integradores, requisitos estritos de dispoñibilidade e continuidade, así como a necesidade de preservar en todo momento a **seguridade das persoas**, a **integridade do proceso** e a **estabilidade da operación**. Por este motivo, calquera aproximación eficaz á ciberseguridade industrial debe combinar criterios técnicos, organizativos e operativos, e facelo dende unha perspectiva de **defensa en profundidade**, xestión do risco e compatibilidade coa realidade do negocio.

O obxectivo deste informe é ofrecer un **catálogo de boas prácticas e controis de seguridade lóxica** que sirva como guía para a súa selección, priorización, implantación e mellora progresiva en contornos industriais. O documento recolle **controis de natureza organizativa, técnica e procedemental**, cun enfoque deliberadamente práctico e por motivos de espazo, sintetizado. Non se limita a describir tecnoloxías illadas, senón que procura presentar as diferentes capacidades de protección como parte dun **conxunto coherente de medidas complementarias**, aplicables en función do **nivel de madurez**, do **perfil de risco**, do sector de actividade e das características da arquitectura tecnolóxica de cada organización.

A vocación do catálogo é, ademais, **integradora**. A realidade da maior parte das empresas industriais non responde a unha separación estanca entre o mundo corporativo e o operativo, senón a unha convivencia continua entre sistemas de oficina, infraestruturas de comunicación, plataformas cloud, aplicacións de xestión, sistemas MES, estacións de enxeñaría, HMI, redes industriais, activos de control e servizos remotos de mantemento. Por iso, este documento adopta unha **visión combinada IT/OT**, na que teñen cabida tanto controis claramente asociados á protección da rede e da operación industrial como outras capacidades que, sendo máis habituais no ámbito IT, resultan igualmente relevantes para a **seguridade global da organización**.

Do mesmo xeito, o informe concede unha atención especial ás **medidas compensatorias**, especialmente necesarias en contornos nos que a remediación inmediata non sempre é viable. En numerosos escenarios industriais, a aplicación dun parche, a substitución dun activo ou a modificación dunha configuración poden non ser posibles a curto prazo por razóns operativas, contractuais, técnicas ou de seguridade funcional. Nestes casos, resulta imprescindible dispoñer dun **marco que permita**

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

reducir o risco mediante segmentación, restrición de accesos, endurecemento, monitorización reforzada, control de soportes externos, visibilidade de rede ou mecanismos de detección temperá, entre outras opcións.

En definitiva, este catálogo pretende constituír unha **ferramenta de apoio á revisión e á implantación progresiva de capacidades de ciberseguridade industrial**, útil tanto para organizacións que están a iniciar o seu proceso de madurez como para aquelas que desexan revisar, ampliar ou reorganizar os seus controis existentes. A súa finalidade última é contribuír a unha **protección máis robusta, proporcionada e sostible** dos contornos industriais galegos, reforzando a súa **resiliencia fronte ás ameazas actuais e futuras** e favorecendo unha **evolución segura da súa transformación dixital**.

2 Resumo executivo

O presente documento constitúe un **catálogo estruturado de boas prácticas e controis de seguridade lóxica** orientado a apoiar a **selección, priorización e posterior implantación de medidas de ciberseguridade** en contornos industriais reais nos que xeralmente conviven sistemas e procesos de **tecnoloxía da información (IT)** e de **tecnoloxía de operación (OT)**. A súa finalidade é proporcionar unha referencia práctica e ordenada que facilite a toma de decisións, a definición de follas de ruta de mellora e a adopción dun enfoque de protección máis coherente, progresivo e adaptado á realidade operativa das organizacións.

O catálogo está dirixido a un **abano amplo de perfís profesionais e organizativos**: empresas industriais, operadores de servizos esenciais, infraestruturas críticas, administracións públicas con instalacións técnicas ou industriais, responsables de ciberseguridade, equipos de operación e mantemento, persoal de enxeñaría, responsables de continuidade e resiliencia, así como provedores e integradores que participen no deseño, operación ou protección destes contornos. O seu valor principal reside en ofrecer unha visión integrada que **non separa artificialmente os ámbitos IT e OT**, senón que os aborda como partes interdependentes dunha mesma realidade tecnolóxica e operativa.

O documento recolle controis distribuídos en **grandes bloques funcionais**, que abranguen dende a **consultoría, gobernanza e análise**, as **auditorías técnicas** e a **identificación de debilidades**, ata a **defensa perimetral e a segmentación**, a **detección de ameazas e protección activa**, a **monitorización, visibilidade e operación de seguridade**, a **protección do posto, dos activos e dos soportes de operación**, a **identidade e o acceso seguro**, a **xestión de vulnerabilidades**, a **resposta e recuperación**, así como capacidades ligadas ao **DevSecOps** (operación e desenvolvemento seguro do software), ao **software conectado** e ás **tendencias emerxentes**. Esta estrutura permite combinar controis organizativos, procedementais e técnicos nun marco común de aplicación práctica.

Entre as mensaxes principais que se desprenden do catálogo, destacaríamos as seguintes.

- **Non existe un control único suficiente** para protexer de forma efectiva un entorno industrial. A seguridade real constrúese a partir da **combinación de medidas complementarias**, despregadas de maneira coherente e sostidas no

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

tempo. Neste sentido, a **defensa en profundidade** constitúe un principio esencial: segmentar, limitar accesos, reforzar a visibilidade, detectar anomalías, endurecer sistemas, dispoñer de capacidade de resposta e asegurar a recuperación son accións que se reforzan mutuamente e que deben entenderse como partes dun mesmo sistema de protección.

- **A priorización dos controis debe basearse no risco e na viabilidade operativa**, e non unicamente na dispoñibilidade de tecnoloxía ou na severidade teórica dunha ameaza. En contornos industriais, a criticidade do proceso, a dependencia da continuidade de servizo, as restricións de mantemento, a presenza de activos legados e a interacción entre seguridade lóxica e seguridade funcional obrigan a adoptar unha visión pragmática, contextualizada e gradual. Por iso, o catálogo non debe interpretarse como unha listaxe pechada de obrigas, senón como unha ferramenta para **ordenar prioridades e orientar decisións de implantación realistas**.
- **Subliñar o papel central das medidas compensatorias**, especialmente no ámbito OT. En moitos contornos industriais, a aplicación inmediata dun parche, a substitución dun equipo ou a modificación dun sistema poden non ser viables a curto prazo. Neses casos, resulta necesario reducir a exposición mediante outras medidas, como a **segmentación**, a **restrición de accesos**, o **hardening** ou **bastionado**, a **monitorización reforzada**, a **visibilidade de rede**, o **control de dispositivos externos** ou a **detección temperá de anomalías**. A capacidade de articular este tipo de respostas proporcionadas forma parte esencial dunha estratexia madura de ciberseguridade industrial.

Finalmente, o documento destaca que a protección dos contornos industriais require incorporar tamén **capacidades tradicionalmente asociadas ao ámbito IT**, sempre que resulten relevantes para a seguridade global da organización. Elementos como a xestión de identidades, a protección do correo electrónico, a seguridade de aplicacións, os servizos cloud, o desenvolvemento seguro ou a xestión centralizada de eventos poden desempeñar un papel decisivo na redución do risco cando existen interdependencias reais entre contornos corporativos e operativos. O catálogo adopta así unha visión **integradora, práctica e orientada á resiliencia**, pensada para servir de apoio tanto a organizacións que comezan a estruturar as súas capacidades como a aquelas que buscan reforzar ou reordenar os controis xa existentes.

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

3 Metodoloxía e fontes

O presente catálogo foi elaborado a partir dun **enfoque de síntese, estruturación e contextualización funcional de capacidades de ciberseguridade**, apoiado no **coñecemento experto do mercado, das boas prácticas e das solucións dispoñibles** por parte dos consultores de seguridade da información que participan na elaboración dos contidos técnicos do Observatorio, complementado con fontes especializadas de referencia no ámbito da ciberseguridade industrial.

O seu propósito non é ofrecer unha recompilación exhaustiva de solucións dispoñibles no mercado nin un inventario comercial de produtos, senón construír unha **guía técnico-funcional**, que permita identificar, contextualizar e relacionar as principais familias de controis e boas prácticas relevantes para a protección de contornos industriais con compoñentes **IT** e **OT**.

Unha das decisións metodolóxicas máis importantes foi a de **organizar o catálogo por tipoloxías funcionais e non por fabricantes, marcas ou solucións comerciais concretas**. Aínda que se tivo en conta un conxunto de capacidades existentes no mercado para contrastar a pertinencia dalgúns controis, o documento adopta deliberadamente unha formulación neutral, centrada en categorías como firewall, NDR, EDR, SIEM, PAM, acceso remoto seguro, escáner de vulnerabilidades, honeypots, monitorización ciberfísica ou copias de seguridade e restauración. Esta decisión reforza o carácter técnico do informe, evita unha lectura promocional ou prescritiva de tecnoloxías concretas e facilita que o catálogo poida ser utilizado por organizacións con distintos niveis de madurez, recursos e preferencias tecnolóxicas.

A metodoloxía empregada incorporou tamén, de forma explícita, o **enfoque de medidas compensatorias**, especialmente relevante en contornos industriais nos que a remediación inmediata non sempre é viable. A selección e descrición de controis tivo en conta que, en moitos escenarios, a redución do risco non depende exclusivamente da eliminación directa dunha vulnerabilidade ou da substitución dun activo, senón da combinación de medidas complementarias como a segmentación, a restrición de accesos, o endurecemento, a monitorización reforzada, a visibilidade de rede, a detección temperá ou o control de soportes de almacenamento externos.

Neste sentido, o catálogo recolle e consolida un enfoque xa presente, de maneira parcial ou implícita, noutras publicacións técnicas da serie do Observatorio, especialmente nos informes de ciberalertas [1] [2] e de intelixencia de ameazas [3] [4], nos que moitas

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

destas capacidades aparecen xa como recomendacións, mecanismos de mitigación ou ámbitos de mellora recorrentes.

Como base documental e técnica complementaria, empregáronse **estándares, marcos de boas prácticas, guías técnicas e bibliografía especializada** no ámbito da seguridade da información, da ciberseguridade industrial e da resiliencia ciberfísica. Con todo, este informe presenta deliberadamente un **peso relativamente maior do coñecemento experto aplicado** e un uso máis contido da bibliografía explícita que outros entregables da serie, precisamente pola súa natureza de **catálogo técnico-funcional orientado á práctica**.

Co obxectivo de ofrecer ao lector unha visión máis ampla, o documento remite indirectamente a outras publicacións da serie do Observatorio que desenvolven con maior profundidade cuestións relacionadas co catálogo de controis. Como diciamos, resulta especialmente recomendable a consulta dos informes xa publicados sobre **ciberalertas**, **intelixencia de ameazas, e tendencias e regulamento** [5], que achegan contexto, exemplos e desenvolvemento adicional para algunhas das tendencias emerxentes recollidas.

Dende o punto de vista metodolóxico, cómpre sinalar tamén algunhas **limitacións inherentes** ao tipo de exercicio realizado. En primeiro lugar, o tecido industrial presenta unha notable **heteroxeneidade sectorial**, o que implica que non todos os controis terán a mesma relevancia nin a mesma viabilidade en sectores como a enerxía, a auga, a alimentación, a automoción, a saúde, a loxística ou a administración pública. En segundo lugar, existen **diferenzas significativas de madurez organizativa e técnica** entre entidades, tanto no referente á súa capacidade interna de seguridade como á arquitectura e gobernanza dos seus activos. En terceiro lugar, a propia **diversidade de arquitecturas, tecnoloxías, protocolos, modelos de operación e relacións con terceiros** fai que a aplicabilidade concreta de cada control deba ser interpretada sempre en función do contexto.

Polo tanto, **este catálogo non debe entenderse como unha prescrición uniforme**, senón como unha base estruturada para orientar análises, decisións e follas de ruta adaptadas á realidade 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 e guía de uso do catálogo

4.1 Particularidades da ciberseguridade en contornos industriais IT/OT

A ciberseguridade en contornos industriais require unha aproximación diferenciada respecto da que habitualmente se aplica en contornos corporativos convencionais. Aínda que ambos os dous ámbitos comparten principios xerais da seguridade da información, como a necesidade de preservar a **confidencialidade**, a **integridade** e a **dispoñibilidade**, a realidade operativa das organizacións industriais introduce condicionantes específicos que afectan de maneira directa á selección, ao deseño e á implantación dos controis de seguridade. En consecuencia, a protección destes contornos non pode basearse nunha simple traslación de medidas propias do ámbito IT, senón nunha adaptación consciente ás particularidades técnicas, operativas e organizativas dos sistemas industriais [6].

- Un primeiro elemento diferencial reside na propia **finalidade dos sistemas implicados**. Mentres que en IT os activos adoitan estar orientados principalmente ao tratamento, almacenamento e intercambio de información, en OT os sistemas tecnolóxicos interactúan de maneira directa co **proceso físico**, coa **operación industrial** e, en moitos casos, coa **seguridade das persoas e das instalacións**. Isto significa que un incidente de ciberseguridade non só pode traducirse en perda de información, indispoñibilidade de servizos ou impacto reputacional, senón tamén en alteracións do proceso produtivo, danos materiais, perda de calidade, afectación á continuidade da actividade ou, nos casos máis graves, consecuencias sobre a seguridade física.
- Derivado do anterior, **os criterios de prioridade tamén adoitan diferir**. Nos contornos industriais, a **dispoñibilidade**, a **continuidade da operación** e a **estabilidade do proceso** adoitan ter un peso especialmente elevado. En determinados escenarios, a aplicación dunha medida que en IT se consideraría habitual —como un parche inmediato, un reinicio programado, unha actualización forzosa ou a instalación dun axente de protección— pode resultar inviable ou mesmo contraproducente se compromete o funcionamento normal dunha liña, dun sistema de control ou dun servizo esencial. Este feito obriga a valorar a seguridade nun equilibrio permanente entre a redución do risco e a preservación da operación.

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

- Outro factor distintivo é a presenza frecuente de **activos legados**, sistemas propietarios, protocolos industriais específicos e compoñentes cun ciclo de vida moi superior ao habitual no mundo IT. Moitos equipos industriais permanecen en servizo durante longos períodos, ás veces durante décadas, e poden depender de versións antigas de software, firmware ou sistemas operativos sen soporte actualizado. A isto engádese, en numerosas ocasións, unha forte dependencia de fabricantes, integradores ou provedores de mantemento, o que condiciona tanto a capacidade de intervención técnica como os tempos e marxes de actuación ante unha vulnerabilidade ou incidente.

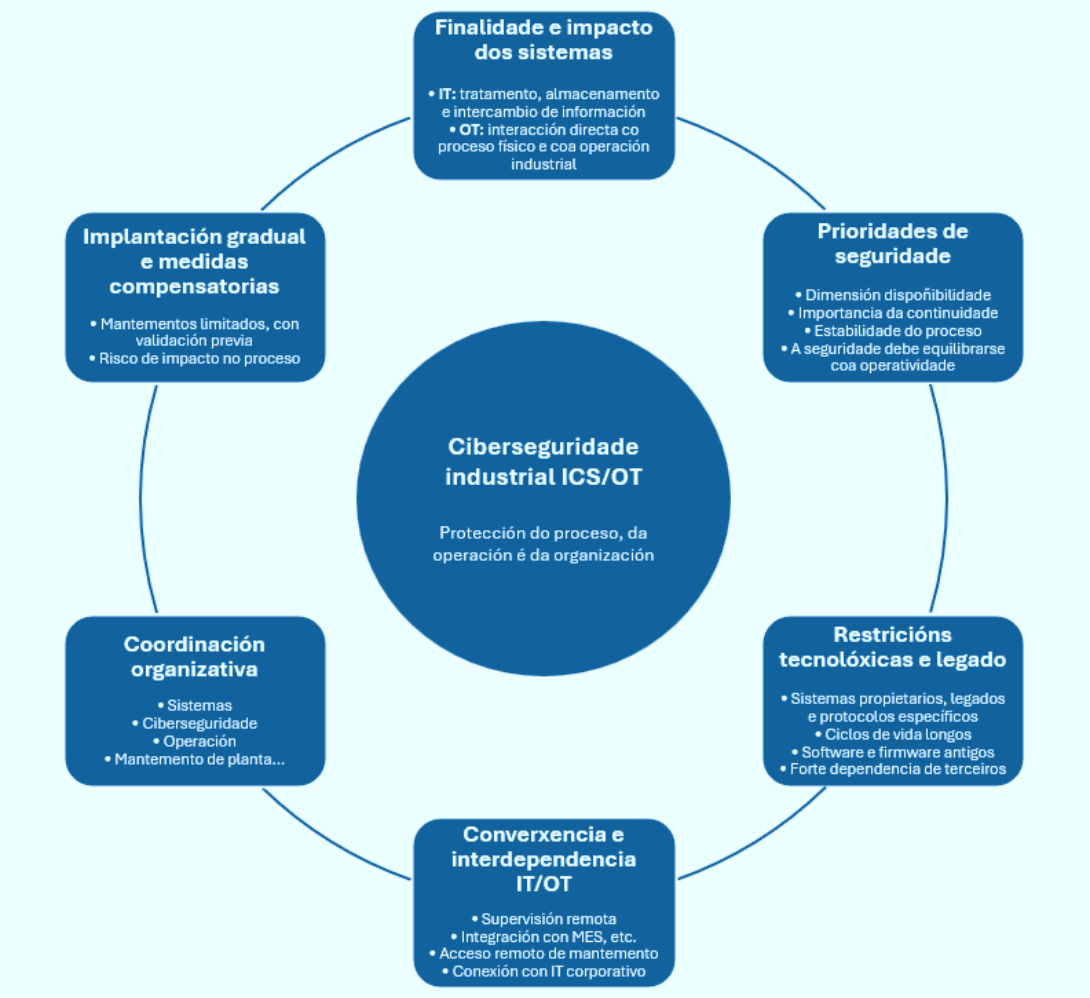
- A todo iso súmase a crecente **converxencia entre IT e OT**, que constitúe unha das características máis relevantes do panorama industrial actual. A incorporación de sistemas de supervisión remota, plataformas de analítica, solucións MES, acceso remoto para soporte, integración con servizos cloud, intercambio de datos en tempo real ou conexión con sistemas corporativos de xestión fai que os límites tradicionais entre a rede corporativa e a rede operativa sexan cada vez máis porosos. Esta interdependencia xera oportunidades evidentes en termos de eficiencia e capacidade de control, pero tamén amplía a superficie de exposición e multiplica os puntos de contacto a través dos cales pode producirse unha intrusión, unha propagación lateral ou unha afectación indirecta ao proceso industrial.

- A diferenza doutros ámbitos, ademais **os contornos industriais esixen unha coordinación máis estreita entre perfís que tradicionalmente operaron con lóxicas distintas**: responsables de sistemas, especialistas en ciberseguridade, persoal de operación, equipos de mantemento, enxeñaría de procesos, fabricantes, integradores e responsables de continuidade ou de seguridade física. A madurez da protección depende, en boa medida, da capacidade de aliñar estes perfís arredor de criterios comúns, procedementos compatibles e prioridades compartidas. A ciberseguridade industrial non é, por tanto, un problema exclusivamente tecnolóxico, senón tamén **organizativo, procedemental e de coordinación interfuncional**.

- Por outra banda, cómpre ter presente que a **implantación de controis en contornos industriais adoita estar suxeita a restricións prácticas significativas**: fiestras de mantemento limitadas, necesidade de validación previa, risco de impacto non desexado sobre o proceso, requisitos de seguridade funcional, dependencia de terceiros e limitacións de capacidade interna. Estas

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

restricións explican por que, en moitas ocasións, a xestión do risco descansa en combinacións graduais de medidas, e non nunha remediación inmediata e completa. Deste xeito, cobran especial relevancia mecanismos como a segmentación, o control de accesos, a visibilidade de rede, o endurecemento, a monitorización reforzada, a restrición de dispositivos externos ou o uso de medidas compensatorias.



Particularidades da ciberseguridade en contornos ICS/OT. Fonte: elaboración propia (2026)

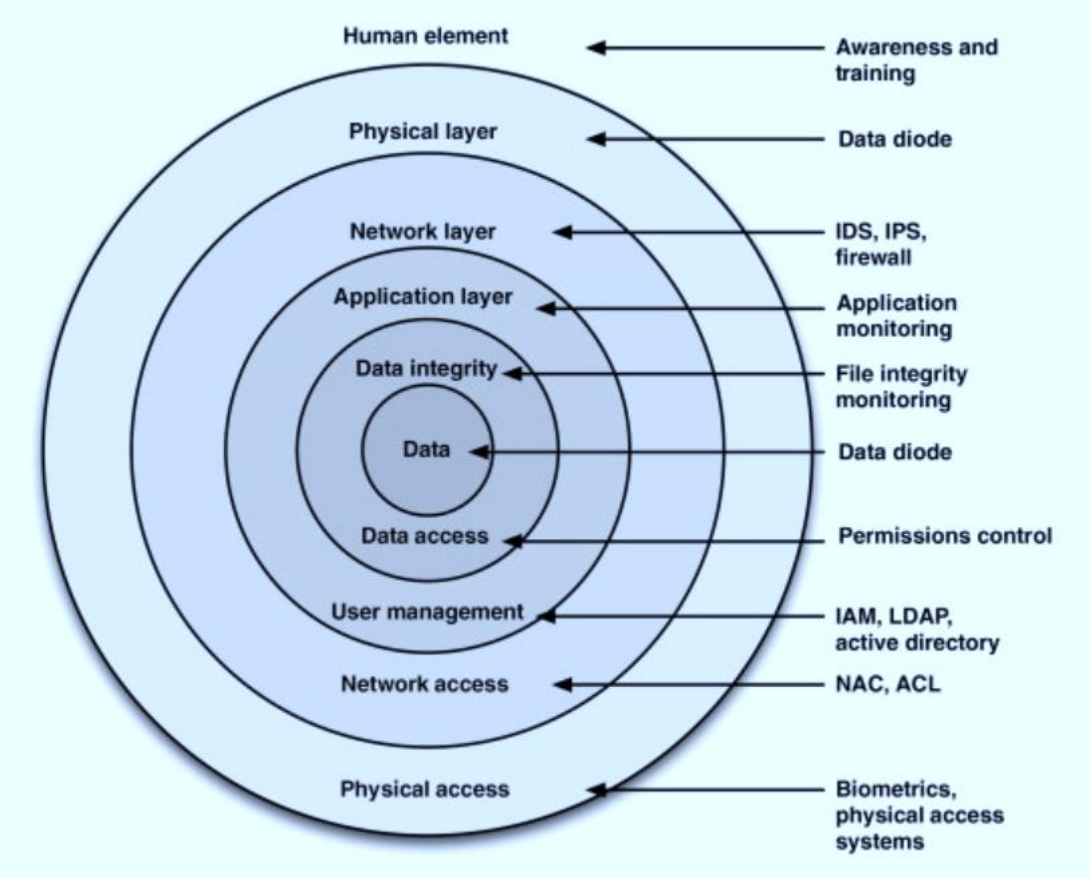
4.2 Principios xerais de protección e defensa en profundidade

A protección eficaz dos contornos industriais IT/OT non pode descansar nun único mecanismo nin nunha capa illada de seguridade. A experiencia acumulada no ámbito da ciberseguridade industrial, tanto dende a perspectiva normativa como dende a análise de incidentes reais, mostra que a redución do risco require combinar **controis organizativos, técnicos e operativos** de maneira coordinada, graduada e sostida no tempo. Esta aproximación coñécese habitualmente como **defensa en profundidade**, e

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

constitúe un dos principios máis asentados para a protección de sistemas industriais e infraestruturas críticas [7].

A defensa en profundidade parte dunha idea sinxela: asumir que ningunha medida de seguridade é perfecta nin suficiente por si mesma. Un cortalumes mal configurado, unha credencial comprometida, unha vulnerabilidade non parcheada, un equipo legado ou un acceso remoto deficiente poden abrir a porta a unha intrusión mesmo en organizacións que dispoñen de controis maduros noutros ámbitos. Por iso, a protección debe articularse en **capas complementarias**, de forma que a debilidade ou a quebra dunha delas non implique automaticamente o compromiso do conxunto [8].



Defensa en profundidade. Fonte: Science Direct (n.d.)

Esta lóxica é especialmente importante en contornos industriais, onde as consecuencias dun incidente poden transcender o plano estritamente dixital e afectar á **continuidade da operación**, á **calidade do proceso**, aos **equipamentos físicos** ou á **seguridade das persoas**.

Aplicada ao ámbito IT/OT, a defensa en profundidade tradúcese na combinación de medidas que actúan en distintos niveis: o **goberno e a xestión do risco**, a **segmentación da arquitectura**, o **control de identidades e accesos**, a **protección**

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

perimetral, a **detección de ameazas**, a **visibilidade sobre os activos e as comunicacións**, o **endurecemento de sistemas**, a **xestión de vulnerabilidades**, a **resposta ante incidentes** e a **capacidade de recuperación e continuidade**. O valor desta aproximación non reside unicamente en sumar tecnoloxías, senón en **establecer relacións lóxicas entre capacidades**, de maneira que cada control reforce ou complemente os demais.

Un primeiro principio xeral é a necesidade de partir dun **coñecemento suficiente do entorno a protexer**. Non é posible defender adecuadamente aquilo que non se coñece: activos non inventariados, comunicacións non documentadas, accesos de terceiros pouco gobernados ou dependencias tecnolóxicas mal comprendidas introducen puntos cegos que debilitan calquera estratexia defensiva. A visibilidade, por tanto, non é só unha capacidade operativa, senón unha condición previa para a xestión do risco, a segmentación, a detección e a resposta.

O segundo principio é o de **mínimo privilexio e control de acceso proporcional ao risco**. Nun entorno industrial, isto implica limitar os permisos ao estritamente necesario, separar funcións cando proceda, controlar os accesos privilexiados, reforzar a autenticación e establecer mecanismos seguros para o acceso remoto e a intervención de terceiros. A exposición innecesaria de contas, sesións ou canles de administración continúa sendo un dos vectores máis habituais de compromiso, especialmente en contornos interconectados e con dependencia de mantemento remoto.

O terceiro principio é a **segmentación e segregación das comunicacións**. A separación entre dominios con diferentes necesidades de seguridade —por exemplo, entre a rede corporativa e a rede OT, ou entre diferentes zonas funcionais dentro do entorno operativo— constitúe unha medida esencial para limitar a propagación lateral, conter incidentes e reducir a exposición dos activos máis sensibles. A segmentación, ademais, non debe entenderse só como unha decisión de deseño de rede, senón como unha medida transversal que condiciona o acceso remoto, a monitorización, a xestión de vulnerabilidades e a resposta ante incidentes.

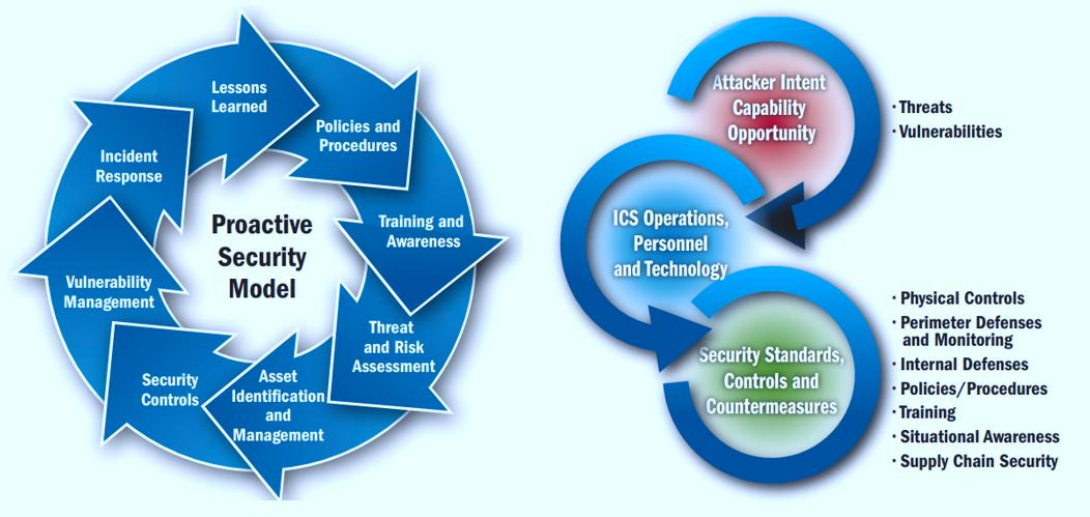
O cuarto principio é o de **seguridade adaptada á operación**. Os controis deben ser compatibles coa realidade do proceso industrial e coas restricións de mantemento, validación e continuidade. Isto significa que a implantación de medidas debe priorizar solucións proporcionadas, tecnicamente viables e operativamente sostibles. En moitos casos, a seguridade efectiva non depende dunha remediación inmediata, senón da combinación gradual de mecanismos como o bastionado, a monitorización reforzada, a

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

restrición de servizos, a limitación de accesos ou o despregue de medidas compensatorias.

O quinto principio é a necesidade de incorporar **capacidades de detección e resposta**, asumindo que a prevención absoluta non existe. A protección moderna de contornos industriais require non só impedir accesos indebidos, senón tamén detectar comportamentos anómalos, correlacionar eventos, analizar desviacións e actuar con rapidez para conter ou mitigar un incidente. Isto reforza o papel de capacidades como o SIEM, o SOC, o NDR, a monitorización ciberfísica, a visibilidade de activos e a resposta planificada.

O sexto principio é a **resiliencia**, entendida non só como recuperación tras un incidente, senón como capacidade da organización para anticipar, resistir, absorber, responder e restaurar a operación en condicións aceptables. Nun entorno industrial, esta visión é particularmente relevante, xa que a protección non se esgota na prevención nin na detección, senón que debe incluír copias de seguridade, restauración probada, continuidade operativa, procedementos de crise e coordinación entre áreas técnicas e funcionais. A resiliencia constitúe, así, a expresión máis completa da defensa en profundidade aplicada a sistemas con impacto físico e operativo.



Modelo de seguridade proactiva e deseño de defensa en profundidade. Fonte: CISA (2016)

Estes fundamentos permiten comprender que a seguridade industrial non debe formularse como unha acumulación desordenada de produtos ou medidas illadas, senón como unha **arquitectura coherente de controis**, aliñada co risco, co nivel de exposición, coa criticidade do proceso e coa madurez da organización. Este enfoque é o que dá sentido ao catálogo que se desenvolve neste informe: non como unha simple

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

listaxe de solucións posibles, senón como unha estrutura para apoiar decisións informadas, graduais e sostibles no tempo.

4.3 Medidas compensatorias en contornos industriais

Un dos trazos máis característicos da ciberseguridade en contornos industriais é a necesidade frecuente de recorrer a **medidas compensatorias** como parte da xestión do risco. A diferenza do que sucede en moitos contornos corporativos, nos que a remediación técnica adoita asociarse a actualizacións rápidas, substitución de compoñentes ou cambios de configuración relativamente asumibles, no ámbito IT/OT existen múltiples situacións nas que a eliminación inmediata dunha vulnerabilidade ou a implantación do control ideal non é viable no curto prazo. Esta realidade non implica aceptar pasivamente a exposición, senón adoptar un enfoque pragmático no que a redución do risco se apoia en combinacións alternativas de controis, procedementos e restricións operativas.

As medidas compensatorias poden definirse como **controis alternativos ou complementarios** que permiten diminuír a probabilidade de explotación ou reducir o impacto dun incidente cando a medida correctiva directa non pode aplicarse de forma inmediata ou completa. No contexto industrial, isto pode responder a motivos moi diversos: dependencia de fabricantes, ausencia de parches estables, risco de impacto sobre o proceso, fiestras de mantemento moi limitadas, requisitos de seguridade funcional, validación previa obrigatoria, incompatibilidades con sistemas legados ou limitacións de capacidade técnica e organizativa. En todos estes casos, a lóxica de protección debe orientarse a **compensar a exposición existente** mentres non sexa posible abordar unha remediación definitiva.

A relevancia destas medidas increméntase en contornos nos que a **dispoñibilidade**, a **continuidade operativa** e a **estabilidade do proceso** constitúen prioridades irrenunciables. Nunha planta industrial, nunha infraestrutura crítica ou nun servizo esencial, a aplicación dun parche sen validación, a substitución dun activo sensible ou a modificación dun sistema de control poden introducir riscos superiores aos que se pretenden mitigar. Por iso, a xestión prudente da ciberseguridade industrial require aceptar que, en determinados momentos, a opción máis razoable non é actuar de maneira inmediata sobre o compoñente vulnerable, senón reforzar o seu entorno, limitar a súa exposición e aumentar a capacidade de detección e resposta.

Entre as medidas en ocasións consideradas compensatorias máis habituais empregadas en contornos industriais poden incluírse, de maneira illada ou combinada, a

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

segmentación de rede, a creación dunha **DMZ industrial ou dun bordo IT/OT controlado**, o **parcheo virtual** ou o uso de mecanismos de filtrado en capa de aplicación, a **monitorización pasiva e detección de anomalías**, o **logging inmutable** ou rexistro inviolable, o **control de acceso robusto e a separación de funcións**, o **acceso remoto seguro para mantemento**, as **estratexias compensatorias de xestión de parches**, as **copias de seguridade e recuperación orientadas a OT**, o **bastionado de HMI e sistemas de enxeñaría**, a **xestión da cadea de subministración e do firmware**, o reforzo da **resiliencia e da seguridade funcional**, así como os **procedementos operativos e de formación do persoal** [9] [10]. A súa eficacia, con todo, non depende de cada medida por separado, senón da capacidade de combinalas segundo a criticidade do activo, a natureza do risco, a arquitectura existente e o nivel de madurez da organización.

É importante subliñar que as medidas compensatorias **non deben entenderse como solucións improvisadas nin como substitutos permanentes por defecto** das medidas correctivas estruturais. O seu valor reside en formar parte dun proceso ordenado de xestión do risco, no que a exposición se identifica, se avalía, se prioriza e se trata mediante mecanismos proporcionados ao contexto. Isto require documentar as decisións adoptadas, definir responsabilidades, establecer prazos de revisión e manter unha visión clara do **risco residual** que continúa asumindo a organización.

Outro aspecto clave é que as medidas compensatorias adoitan ter un forte compoñente **arquitectónico e operativo**, ademais de tecnolóxico. A súa eficacia depende tanto da existencia de certos controis como da forma en que se implantan e gobernan. Por exemplo, a segmentación só cumpre adecuadamente a súa función se vai acompañada de regras coherentes, control de accesos, supervisión de tráfico e revisión periódica. Do mesmo xeito, a limitación do acceso remoto require autenticación reforzada, control de sesións, trazabilidade e gobernanza de terceiros. E a monitorización intensificada só achega valor se existen capacidades reais de análise, correlación e resposta. Isto reforza a idea de que compensar non é simplemente engadir un produto, senón **reorganizar a protección ao redor dun risco concreto**.

Dende unha perspectiva metodolóxica, a implantación de medidas compensatorias debería responder, cando menos, a catro preguntas básicas: **que risco se pretende mitigar**, **por que a remediación directa non é viable nese intre**, **que combinación de medidas permite reducir razoablemente a exposición** e **cando se revisará a necesidade de manter ou substituír esa compensación**, cando o control é temporal ou mellorable. Esta formulación é especialmente útil en contornos industriais con gran

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

dependencia de terceiros e con activos heteroxéneos, xa que obriga a facer explícita a racionalidade técnica e operativa da decisión.

A práctica amosa, ademais, que moitas organizacións industriais melloran substancialmente a súa postura de seguridade non tanto por aplicar de forma inmediata grandes transformacións, senón por introducir **melloras compensatorias ben priorizadas e sostibles**: separar redes, endurecer configuracións, limitar canles remotas, controlar soportes externos, reforzar a detección ou mellorar a trazabilidade. Estas medidas, aínda que ás veces percibidas como menos ambiciosas que outras iniciativas, son con frecuencia as que permiten reducir máis rapidamente a superficie de exposición real e crear condicións máis seguras para futuras actuacións de maior alcance.

Neste sentido, as medidas compensatorias gardan unha relación directa coa **madurez da organización**. Non só constitúen unha resposta a limitacións inmediatas, senón tamén un mecanismo para transitar dende escenarios de baixa visibilidade ou alta exposición cara a estados de control progresivamente máis robustos. Un programa de seguridade industrial maduro non elimina a necesidade de compensar; ao contrario, intégrana como parte dun modelo racional de decisión, priorización e resiliencia.

4.4 Como utilizar este catálogo

O presente catálogo foi concibido como unha **ferramenta práctica de referencia**, e non como unha relación pechada, lineal ou uniforme de medidas de obrigada implantación. A súa utilidade reside precisamente en permitir que cada organización poida interpretar os controis dende a súa realidade específica, tendo en conta a criticidade dos seus procesos, o grao de exposición, a arquitectura tecnolóxica existente, as restricións operativas, o nivel de madurez alcanzado e a dispoñibilidade real de recursos técnicos, humanos e económicos.

Neste sentido, o catálogo debe empregarse cunha lóxica de **selección contextualizada e implantación progresiva**. Non todos os controis serán igualmente necesarios, viables ou prioritarios en todos os contornos. Unha planta industrial con alto nivel de automatización, múltiples accesos remotos de terceiros e dependencia intensiva de sistemas OT terá necesidades distintas ás dunha organización con menor complexidade operativa ou cun maior peso do entorno corporativo. Do mesmo xeito, unha entidade que xa dispoña de visibilidade de rede, procedementos maduros e capacidades internas de resposta poderá orientar o catálogo cara a capas máis avanzadas, mentres que outras

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

organizacións deberán comezar por medidas máis básicas, pero de alto impacto na redución do risco.

Un primeiro modo de utilizar o catálogo consiste en empregalo como **guía de diagnóstico ou autoavaliación**. Neste caso, os diferentes bloques e sub-bloques permiten revisar de forma estruturada que capacidades están presentes, cales existen só parcialmente e cales non están aínda desenvolvidas. Esta lectura resulta especialmente útil para organizacións que precisan identificar carencias, ordenar capacidades ou establecer unha secuencia de mellora. O catálogo pode servir así como referencia para análises GAP, revisións internas, exercicios de madurez, propostas técnicas ou esquemas de priorización.

Un segundo uso posible é como **instrumento de planificación e estruturación de medidas**. Os controis recollidos non deben interpretarse de forma illada, senón como compoñentes dun sistema de protección máis amplo. Por iso, durante a súa utilización convén analizar non só se unha capacidade existe ou non, senón tamén como se relaciona co resto. Por exemplo, a segmentación de rede gaña eficacia cando vai acompañada de control de accesos, visibilidade de comunicacións e procedementos de mantemento seguro; a monitorización reforzada perde parte do seu valor se non existen capacidades reais de análise e resposta; e a xestión de vulnerabilidades resulta insuficiente se non se integra con criterios de criticidade operativa, validación previa e medidas compensatorias. O catálogo, por tanto, debe lerse tamén como unha **estrutura de relacións entre controis**, non só como unha listaxe temática.

Un terceiro enfoque de uso é o da **lectura baseada en risco**. O catálogo permite identificar que medidas ofrecen unha maior redución da exposición en función dos escenarios máis probables ou máis gravosos para a organización. En contornos industriais, esta lectura é especialmente relevante, xa que a presión por implantar medidas de seguridade debe convivir coa necesidade de manter a operación, respectar restricións de mantemento e evitar impactos non desexados sobre o proceso. Por iso, a aplicación do catálogo debería estar sempre vinculada á análise de riscos, á criticidade dos activos e á avaliación do impacto potencial sobre a continuidade, a seguridade física, a calidade ou o servizo.

Tamén pode empregarse como **marco común entre perfís distintos**, algo especialmente relevante en contornos industriais. Un dos problemas habituais na implantación de controis é que os diferentes equipos —ciberseguridade, sistemas, operación, mantemento, enxeñaría, dirección ou provedores— non sempre comparten a mesma linguaxe nin a mesma percepción das prioridades. A estrutura do catálogo

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

pode facilitar unha visión común, permitindo analizar medidas non dende unha perspectiva puramente tecnolóxica, senón en termos de finalidade, dependencia, impacto e viabilidade. Nese sentido, o documento pode cumprir tamén unha función de apoio á gobernanza e á coordinación interfuncional.

Ademais, o catálogo pode utilizarse como **soporte para a elaboración de follas de ruta graduais**, algo particularmente útil en organizacións cun punto de partida heteroxéneo. A madurez en ciberseguridade industrial non adoita construírse mediante transformacións abruptas, senón a través de iteracións sucesivas nas que se consolidan capacidades, se revisan decisións previas e se introducen melloras de maior profundidade unha vez fortalecida a base. A lectura do catálogo dende esta óptica permite distinguir entre medidas iniciais, melloras intermedias e capacidades máis avanzadas, sen perder de vista que a prioridade non debe ser a sofisticación do control, senón a súa contribución real á protección do entorno.

É importante insistir en que este documento **non substitúe unha análise técnica ou de risco específica**, nin resolve por si mesmo a adecuación concreta de cada control a unha arquitectura determinada. O catálogo proporciona unha base ordeada de referencia, pero a súa aplicabilidade debe interpretarse sempre á luz do contexto da organización, do sector, das obrigas reguladoras que resulten de aplicación, da arquitectura dispoñible, das dependencias de terceiros e do nivel de exposición asumido. O seu valor está en **ordenar e contextualizar os controis**, non en substituír a análise específica.

Finalmente, recoméndase que a utilización do catálogo siga unha secuencia lóxica. En primeiro lugar, resulta conveniente comprender as **particularidades dos contornos industriais IT/OT** e os **principios xerais de protección e defensa en profundidade** expostos nos apartados anteriores. En segundo lugar, debe revisarse o papel das **medidas compensatorias**, xa que estas condicionan unha parte importante da implantación real en contornos industriais. Só despois resulta plenamente útil abordar o bloque central do catálogo, no que cada familia de controis pode interpretarse de xeito máis preciso. Desta forma, o documento funciona non só como repositorio de capacidades, senón como unha guía estruturada para apoiar análises máis informadas, coherentes e sostibles no tempo.

En definitiva, este catálogo debe entenderse como un **instrumento de referencia flexible e acumulativo**, útil para diagnosticar, priorizar, estruturar, coordinar e mellorar a postura de seguridade das organizacións industriais. A súa eficacia dependerá, en último termo, da capacidade de cada entidade para empregalo con

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

criterio, adaptándoo ao seu contexto e integrándoo nunha visión máis ampla de risco, operación e resiliencia.

4.5 Criterios de clasificación dos controis

A utilidade dun catálogo como o presente depende, en boa medida, da súa capacidade para **ordenar os controis de maneira comprensible, coherente e funcional**. Nun documento que reúne mais de setenta medidas diferentes de natureza diversa —organizativas, técnicas, operativas e procedementais— a clasificación non cumpre un papel meramente formal, senón que condiciona a forma en que o lector interpreta o contido, identifica relacións entre capacidades e localiza máis facilmente os elementos relevantes para o seu contexto. Por este motivo, o catálogo estrutúrase seguindo criterios de clasificación que combinan unha lóxica funcional coas particularidades propias dos contornos industriais IT/OT.

O primeiro criterio empregado é o da **familia funcional do control**. Isto significa que os controis non se agrupan segundo tecnoloxías illadas, fabricantes concretos ou marcos normativos específicos, senón segundo a función principal que desempeñan dentro da protección global da organización. Así, o catálogo distingue entre bloques ligados á gobernanza e á análise, ás auditorías técnicas e identificación de debilidades, á enxeñería social, á defensa perimetral e segmentación, á detección de ameazas, á monitorización e operación de seguridade, á protección de postos e activos, á identidade e acceso seguro, á xestión de vulnerabilidades, á resposta e recuperación, ao desenvolvemento seguro e ás tendencias emerxentes. Esta estrutura permite ler o documento como un **mapa de capacidades**, no que cada bloque representa un ámbito de protección cunha finalidade específica.

O segundo criterio é o da **natureza do control**, xa que non todos os mecanismos de seguridade teñen a mesma expresión nin o mesmo modo de implantación. Algúns controis son eminentemente **organizativos**, como a análise de riscos, a definición de procedementos ou a continuidade de negocio; outros son principalmente **técnicos**, como o firewall, o NDR, o PAM ou o SIEM; e outros presentan unha natureza **mixta**, ao combinar tecnoloxía, procedemento e operación, como ocorre coa xestión de accesos de terceiros, a monitorización, a xestión de parches ou a resposta ante incidentes. Esta distinción resulta útil para evitar unha visión reducionista da ciberseguridade industrial entendida só como adquisición de ferramentas, e para poñer en valor o peso que teñen a gobernanza, os procedementos e a coordinación na eficacia real dos controis.

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

O terceiro criterio de clasificación é o da **función defensiva predominante**. Dende esta perspectiva, os controis poden cumprir un papel principalmente:

- **preventivo**, cando buscan reducir a probabilidade de compromiso;
- **detectivo**, cando permiten identificar anomalías, eventos ou incidentes;
- **correctivo ou de recuperación**, cando facilitan conter, restaurar ou retornar a condicións aceptables de operación;
- **compensatorio**, cando se empregan para mitigar un risco ante a imposibilidade de implantar de forma inmediata a medida correctiva ideal.

Na práctica, moitos controis poden participar en máis dunha destas funcións. Por exemplo, a segmentación é claramente preventiva, pero tamén contribúe á contención dun incidente; a monitorización reforzada é detectiva, pero pode cumprir un papel compensatorio; e o bastionado é preventivo, aínda que tamén pode utilizarse para reducir exposición en contextos con vulnerabilidades non remediadas. O criterio adoptado no catálogo non pretende encadrar de forma ríxida cada control nunha única categoría, senón destacar a súa **función principal dentro do conxunto**.

O cuarto criterio é o da **función do control dentro do NIST Cybersecurity Framework (NIST CSF)**, un dos marcos máis utilizados internacionalmente para estruturar programas de ciberseguridade de forma comprensible e transversal [11] [12]. Esta norma organiza a protección arredor de **seis funcións principais**, que permiten describir que papel cumpre cada capacidade dentro dun sistema máis amplo.

- A función **Govern** refírese ao goberno da ciberseguridade, incluíndo políticas, roles, supervisión, xestión de risco e cadea de subministración.
- A función **Identify** céntrase no coñecemento do entorno, dos activos, das dependencias e dos riscos existentes.
- A función **Protect** abrangue as medidas destinadas a limitar ou reducir a probabilidade de impacto, como o control de acceso, a formación, o bastionado ou a protección de datos.
- A función **Detect** recolle as capacidades orientadas a identificar eventos, anomalías ou sinais de compromiso.
- A función **Respond** inclúe a xestión do incidente unha vez detectado, dende a análise ata a contención e a comunicación.
- Finalmente, a función **Recover** refírese á restauración de servizos e capacidades, á continuidade e á aprendizaxe posterior ao incidente.

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

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

Funcións NIST CSF e relación con categorías. Fonte: NIST (2024)

Empregar este criterio complementa os anteriores, porque permite **situar cada control dentro dunha lóxica de ciclo completo da ciberseguridade**, e non só dentro dunha categoría técnica ou organizativa.

Cómpre sinalar tamén que os criterios de clasificación adoptados **non son excluíntes entre si**. Un mesmo control pode localizarse nun bloque determinado pola súa familia funcional, ter unha natureza técnica ou mixta, cumprir unha función defensiva predominantemente preventiva ou detectiva, e encaixar ademais nunha ou varias das funcións do NIST CSF. Esta superposición non debe entenderse como un defecto do modelo, senón como unha expresión da propia complexidade da ciberseguridade industrial. De feito, unha das finalidades do catálogo é precisamente facer visible que os controis non existen de forma illada nin poden comprenderse axeitadamente dende unha única dimensión.

En consecuencia, a clasificación recollida neste informe responde a un equilibrio entre **claridade expositiva** e **fidelidade á realidade operativa**. Non se busca construír unha taxonomía académica exhaustiva, nin replicar literalmente a estrutura dun estándar concreto, senón ofrecer un marco de lectura suficientemente robusto para organizar o catálogo e, ao mesmo tempo, suficientemente flexible como para ser útil a organizacións con perfís, sectores e arquitecturas moi diferentes.

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

5 Catálogo de boas prácticas e controis

5.1 Consultoría, gobernanza e análise

Este primeiro bloque reúne **capacidades de carácter organizativo, estratéxico e técnico-funcional que permiten establecer as bases dunha ciberseguridade industrial madura**. Inclúe actividades orientadas a comprender o risco, definir prioridades, aliñar decisións co negocio e estruturar programas de protección adaptados á realidade operativa dos contornos ICS/OT, servindo así como punto de partida para unha implantación coherente do resto de controis.

5.1.1 Análise de riscos tecnolóxicos

Categoría: Consultoría, gobernanza e análise

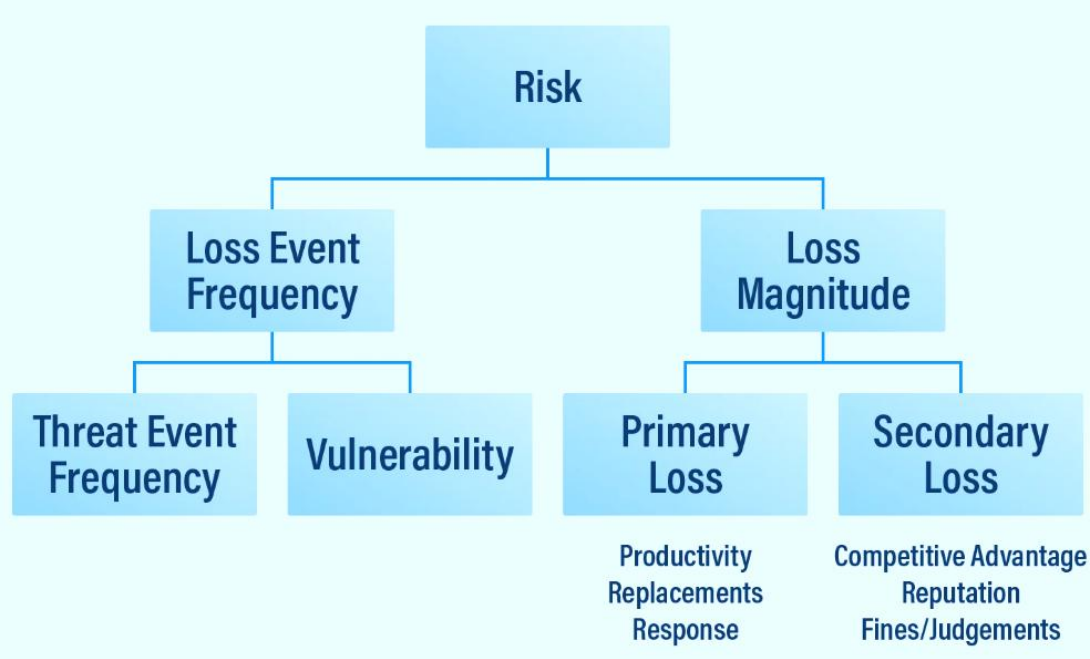
Tipoloxía: Organizativo / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Govern, Identify

Descrición: A análise de riscos tecnolóxicos é o proceso sistemático mediante o cal unha organización identifica, avalía e trata os riscos derivados das ameazas que poden afectar aos seus activos, procesos, servizos e dependencias tecnolóxicas. No contexto industrial, esta análise debe considerar tanto os compoñentes propios da infraestrutura corporativa como os elementos operativos e de control que interveñen na produción, a supervisión, o mantemento e a continuidade do proceso. O seu valor reside en proporcionar unha visión estruturada da exposición real da organización, permitindo relacionar activos, ameazas, vulnerabilidades, impactos e medidas de tratamento nun marco coherente [13] [14].

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



Análise de riscos cuantitativa. Fonte: FAIR Institute (n.d.)

Obxectivo: Establecer unha base formal para comprender que riscos afectan á organización, que activos son máis críticos, que escenarios de ameaza resultan máis relevantes e que medidas de protección, mitigación ou compensación deben implantarse. A análise de riscos non persegue só cuantificar exposición, senón tamén facilitar unha visión priorizada e contextualizada da seguridade, aliñada coa operativa do negocio e coa criticidade dos procesos industriais.

Como funciona / como se implanta: A súa implantación adoita comezar coa definición do alcance, a identificación dos activos e procesos incluídos, a caracterización das ameazas e vulnerabilidades relevantes e a estimación do impacto e da probabilidade de materialización dos distintos escenarios. A partir desa base, establécense criterios de aceptación do risco, priorízanse tratamentos (evitar, mitigar, transferir ou aceptar os riscos) e documéntanse as medidas previstas. En contornos industriais, este exercicio debe incorporar non só activos dixitais clásicos, senón tamén sistemas de control, redes OT, compoñentes de campo, dependencias de terceiros, accesos remotos, seguridade funcional, continuidade operativa e posibles efectos físicos, produtivos ou reputacionais. O proceso pode apoiarse en marcos como ISO 27005, NIST SP 800-30, MAGERIT, IEC 62443 ou metodoloxías adaptadas ao sector.

Vantaxes:

- Permite priorizar os esforzos de seguridade en función da criticidade real dos activos e procesos.

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

- Facilita a selección proporcionada de controis técnicos, organizativos e procedementais.
- Axuda a xustificar investimentos, excepcións e medidas compensatorias.
- Mellora a trazabilidade entre ameazas, exposición, impacto e tratamento previsto.
- Serve de base para auditorías, plans directores, continuidade e gobernanza da seguridade.

Limitacións e consideracións:

- A súa utilidade depende da calidade do inventario de activos e do coñecemento real da arquitectura.
- Pode perder valor se se formula como exercicio puramente documental e non como proceso vivo.
- En contornos industriais, unha avaliación insuficientemente adaptada pode infravalorar impactos operativos, físicos ou de seguridade funcional.
- Require participación de perfís diversos: sistemas, ciberseguridade, operación, mantemento, enxeñaría e responsables de proceso.
- Debe revisarse periodicamente, especialmente tras cambios de arquitectura, incorporación de terceiros, novas interconexións ou aparición de ameazas relevantes.

Relación con outros controis: Relaciónase de forma directa coa recomendación de controis de seguridade, coa implantación de marcos normativos, coa segmentación de rede, coa xestión de vulnerabilidades, co acceso remoto seguro, co patch management, coas medidas compensatorias, coa resposta ante incidentes e cos plans de continuidade. Constitúe, en termos prácticos, un control vertebrador do resto do catálogo, xa que permite contextualizar e priorizar a súa implantación.

Casos habituais de uso: Emprégase para elaborar plans directores de seguridade, definir follas de ruta de mellora, preparar auditorías ou certificacións, xustificar excepcións en contornos OT, priorizar activos críticos, revisar dependencias de terceiros, orientar medidas compensatorias ou avaliar o impacto de cambios tecnolóxicos e normativos.

Observacións / medidas compensatorias asociadas: Nun entorno industrial, a análise de riscos tecnolóxicos resulta especialmente relevante para fundamentar a

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 cando un control non pode implantarse de forma inmediata. Tamén é o mecanismo máis adecuado para xustificar por que determinados activos legados, accesos remotos, sistemas sen soporte ou arquitecturas herdadas deben tratarse cun enfoque gradual e proporcional, en lugar de mediante remediacións inmediatas potencialmente incompatibles coa operación.

5.1.2 Recomendación de controis de seguridade

Categoría: Consultoría, gobernanza e análise

Tipoloxía: Organizativo / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Govern, Protect

Descrición: A recomendación de controis de seguridade consiste na definición estruturada das medidas técnicas, organizativas e procedementais que resultan máis adecuadas para reducir os riscos identificados nunha organización. Non se trata dunha simple enumeración de solucións posibles, senón dun exercicio de contextualización no que os controis se seleccionan en función da arquitectura existente, da criticidade dos activos, das ameazas relevantes, das obrigas normativas aplicables e das limitacións operativas do entorno. No ámbito industrial, esta actividade require traducir os achados procedentes da análise de riscos, das auditorías ou das revisións técnicas a un conxunto coherente de actuacións priorizadas e compatibles coa realidade IT/OT. Podería realizarse o exercicio inspirado neste catálogo, ou nas propostas de CISA Cybersecurity Performance Goals [15] ou ISO 27002 (mais xeneralistas neste caso [16]).

Obxectivo: Determinar que controis deben implantarse, reforzarse, combinarse ou revisarse para mellorar a postura de seguridade da organización de forma proporcionada, realista e sostible. O seu propósito é conectar a análise coa acción, evitando tanto a implantación indiscriminada de medidas como a dependencia de recomendacións xenéricas pouco adaptadas ao contexto industrial.

Como funciona / como se implanta: Habitualmente, a recomendación de controis parte dun conxunto previo de entradas: análise de riscos, resultados de auditoría, avaliacións técnicas, revisión de arquitectura, requisitos regulatorios ou incidentes observados. A partir desa base, establécese unha proposta de medidas que pode incluír controis preventivos, detectivos, correctivos e compensatorios, ordenados segundo criterios de criticidade, viabilidade e relación co resto da arquitectura de seguridade. En contornos industriais, esta recomendación debe considerar aspectos como a

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

segmentación IT/OT, o acceso remoto de terceiros, a presenza de activos legados, a necesidade de validación previa, o impacto potencial sobre a operación, a seguridade funcional e a dependencia de fabricantes ou integradores. O resultado adoita materializarse en informes técnicos, plans de acción, follas de ruta ou propostas de mellora.

Vantaxes:

- Traducir achados técnicos ou de risco a actuacións concretas e ordenadas.
- Evitar enfoques xenéricos ou pouco adaptados ao contexto real da organización.
- Facilitar a priorización de medidas segundo impacto e viabilidade.
- Mellorar a coherencia entre controis, arquitectura, procedementos e operación.
- Servir de base para plans directores, auditorías, investimentos e revisións de seguridade.

Limitacións e consideracións:

- Perde valor se se formula como listaxe estándar de medidas sen contexto nin priorización.
- Require coñecemento suficiente do entorno, das dependencias operativas e das restricións de implantación.
- En contornos industriais, unha recomendación tecnicamente correcta pode resultar inviable se non se considera o impacto sobre a dispoñibilidade e o proceso.
- Debe evitar unha visión excesivamente centrada en ferramentas, incorporando tamén medidas organizativas, procedementais e compensatorias.
- Convén revisar as recomendacións cando cambian a arquitectura, o marco normativo, a exposición ou o modelo de operación.

Relación con outros controis: Relaciónase directamente coa análise de riscos tecnolóxicos, coa implantación e auditoría de marcos e normas de seguridade, coas auditorías técnicas, coa xestión de vulnerabilidades, coa segmentación, co acceso remoto seguro, co hardening, coa monitorización, coa resposta ante incidentes e cos plans de continuidade. Funciona como ponte entre o diagnóstico e a estruturación do resto de controis do catálogo.

Casos habituais de uso: Utilízase para elaborar plans de mellora, propostas técnicas, follas de ruta de implantación, adecuacións a marcos como ENS, ISO 27001, IEC 62443

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

ou NIST CSF, revisións de arquitectura, procesos de compra ou contratación, e para definir medidas compensatorias cando un control non pode implantarse de forma inmediata.

Observacións / medidas compensatorias asociadas: Nun entorno industrial, a recomendación de controis resulta especialmente útil cando debe equilibrarse a redución do risco coa preservación da operación. Por iso, non debería formularse unicamente en termos de control ideal, senón tamén contemplando secuencias graduais de implantación, dependencias entre medidas e alternativas compensatorias cando existan restricións técnicas, operativas ou de seguridade funcional.

5.1.3 Implantación e auditoría de marcos e normas de seguridade

Categoría: Consultoría, gobernanza e análise

Tipoloxía: Organizativo / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Govern

Descrición: A implantación e auditoría de marcos e normas de seguridade consiste na adopción estruturada de referencias recoñecidas para organizar, avaliar e mellorar a ciberseguridade dunha organización. Estes marcos poden ter natureza xeral, como ISO 27001, ENS ou NIST CSF [11], ou unha orientación máis específica a contornos industriais, como IEC 62443 ou NIST SP 800-82. A súa utilidade reside en proporcionar unha linguaxe común, un conxunto de requisitos ou boas prácticas e unha metodoloxía de revisión que permita pasar dunha xestión ad hoc da seguridade a un modelo máis ordenado, trazable e verificable.

Obxectivo: Dotar á organización dun marco de referencia coherente para estruturar os seus controis, revisar o seu grao de adecuación, identificar desviacións, establecer prioridades de mellora e demostrar un determinado nivel de madurez, cumprimento ou capacidade de xestión da seguridade. No ámbito industrial, isto resulta especialmente útil para aliñar a ciberseguridade co risco operativo, coa gobernanza interna e coas esixencias regulamentarias e sectoriais aplicables.

Como funciona / como se implanta: A implantación adoita comezar coa selección do marco ou combinación de marcos máis axeitados ao contexto da organización, en función do sector, da arquitectura, do alcance e das obrigas de cumprimento. A partir dese punto, realízase un exercicio de análise GAP ou de avaliación inicial, no que se compara a situación real cos requisitos ou principios do marco escollido. Sobre esa base,

establécense medidas de adecuación, documentos de gobernanza, procedementos, evidencias e controis técnicos ou organizativos. A auditoría, pola súa parte, verifica o grao de cumprimento ou adecuación mediante revisión documental, entrevistas, análise técnica e comprobación de evidencias. En contornos industriais, a implantación non debería limitarse a trasladar requisitos IT de forma mecánica, senón adaptalos á realidade OT, á seguridade funcional, á dispoñibilidade, aos sistemas legados, á segmentación, ao acceso remoto e ás necesidades de coordinación entre operación e seguridade.

Vantaxes:

- Proporciona unha estrutura ordenada e recoñecible para a xestión da seguridade.
- Facilita a identificación de carencias e a planificación de melloras.
- Axuda a aliñar a organización con requisitos normativos, contractuais ou sectoriais.
- Mellora a trazabilidade documental e a capacidade de auditoría.
- Permite integrar gobernanza, risco, operación e control técnico nun mesmo marco de referencia.

Limitacións e consideracións:

- A súa implantación perde valor se se orienta só ao cumprimento formal e non á eficacia real dos controis.
- Non todos os marcos teñen o mesmo nivel de adecuación a contornos industriais, polo que a súa selección debe ser contextualizada.
- En OT, unha interpretación demasiado literal de certos requisitos pode resultar pouco viable ou incluso contraproducente se non se adapta ao proceso.
- Require participación de múltiples áreas: seguridade, sistemas, operación, enxeñaría, continuidade, cumprimento e dirección.
- A auditoría debe valorar non só a existencia documental dun control, senón tamén a súa aplicación efectiva e sostibilidade.

Relación con outros controis: Relaciónase directamente coa análise de riscos tecnolóxicos, coa recomendación de controis de seguridade, coas auditorías técnicas, coa xestión de vulnerabilidades, coa segmentación, coa resposta ante incidentes, cos

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

plans de continuidade e coas medidas compensatorias. Funciona como marco vertebrador para ordear e dar consistencia ao resto dos controis do catálogo.

Casos habituais de uso: Utilízase para procesos de adecuación ao ENS, implantación de SGSI baseados en ISO 27001, revisións fronte a NIST CSF, programas sectoriais de seguridade, marcos OT como IEC 62443, procesos de certificación, auditorías internas ou externas, licitacións, requirimentos de clientes e iniciativas de mellora continua con alcance corporativo e industrial.

Observacións / medidas compensatorias asociadas: En contornos industriais, a implantación de marcos e normas de seguridade resulta especialmente valiosa cando se emprega cun criterio de aplicabilidade e adaptación ao risco, e non como exercicio de cumprimento abstracto. Neste sentido, marcos como o ENS, IEC 62443 ou NIST CSF poden servir tamén para fundamentar excepcións xustificadas e a utilización de medidas compensatorias, sempre que exista trazabilidade, avaliación do risco residual, validación e revisión periódica.

5.1.4 Plan de continuidade de negocio e resiliencia operativa

Categoría: Consultoría, gobernanza e análise

Tipoloxía: Organizativo / mixto

Función defensiva predominante: Correctivo / de recuperación

Función no NIST CSF: Govern, Recover

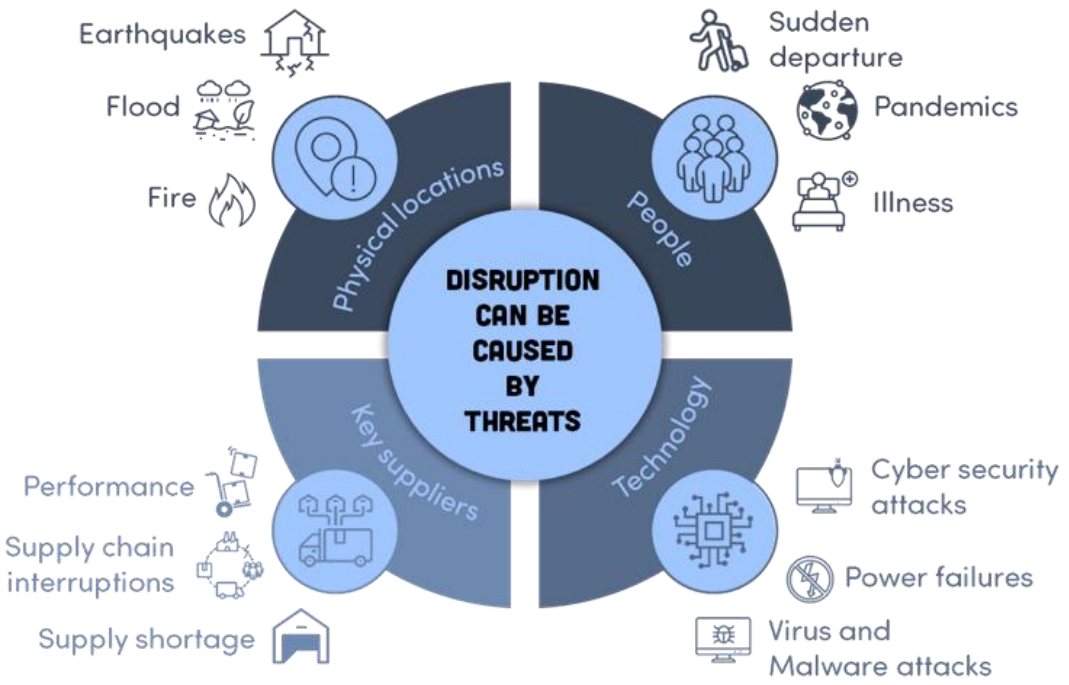
Descrición: O plan de continuidade de negocio e resiliencia operativa é o conxunto estruturado de políticas, procedementos, roles e medidas técnicas e organizativas destinadas a garantir que a organización poida manter, restablecer ou adaptar as súas funcións críticas ante incidentes disruptivos que afecten á súa actividade [17] [18]. No contexto industrial, este control abrangue non só a continuidade dos servizos corporativos, senón tamén a preservación da operación, a recuperación dos procesos produtivos, a restauración de sistemas OT e a coordinación entre áreas técnicas, operativas e directivas. A súa finalidade vai máis alá da mera recuperación tras un fallo, integrando tamén a capacidade de absorción, adaptación e resposta fronte a interrupcións con impacto operativo (xa sexan de natureza humana, por causas naturais ou técnicas).

Obxectivo:

Minimizar o impacto de incidentes, fallos, ataques ou interrupcións sobre os procesos esenciais da organización, asegurando que existan criterios previos para priorizar

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

servizos, restaurar capacidades, coordinar actuacións e manter a continuidade en condicións aceptables. En contornos industriais, o obxectivo inclúe tamén reducir o risco de paradas prolongadas, preservar a seguridade das persoas e do proceso, e asegurar que a recuperación non comprometa a integridade dos sistemas nin introduza novos riscos operativos.



Exemplo de causas de disrupción en industria. Fonte: DigitalTransformation.org (n.d.)

Como funciona / como se implanta: A súa implantación parte da identificación das funcións críticas de negocio e dos procesos operativos esenciais, así como das dependencias que os soportan: sistemas, redes, persoal clave, provedores, instalacións, enerxía, comunicacións, servizos externos e compoñentes OT. Sobre esa base establécense escenarios de interrupción, tempos obxectivo de recuperación, prioridades e puntos de restauración de datos e servizos e procedementos específicos para distintos tipos de incidente. Nun entorno industrial, o plan debe contemplar a recuperación de sistemas de supervisión e control, HMI, estacións de enxeñaría, comunicacións industriais, receitas, configuracións, copias de seguridade, acceso remoto, relación con terceiros e interacción coa seguridade funcional. A súa eficacia depende tamén da realización de probas, simulacros, revisións periódicas e actualizacións tras cambios significativos na arquitectura ou na operación.

Vantaxes:

- Reduce o tempo e o impacto das interrupcións sobre a actividade.

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

- Mellora a preparación da organización ante incidentes operativos e ciberincidentes.
- Facilita a coordinación entre áreas técnicas, operación, mantemento, dirección e terceiros.
- Axuda a priorizar a recuperación en función da criticidade real dos procesos e servizos.
- Reforza a resiliencia organizativa e a capacidade de recuperación sostible no tempo.

Limitacións e consideracións:

- Perde valor se se formula como documento estático sen probas, actualización nin integración coa realidade operativa.
- A súa eficacia depende da calidade do inventario de activos críticos e da identificación de dependencias.
- En contornos industriais, unha visión excesivamente centrada en TI pode deixar fóra compoñentes esenciais da recuperación OT.
- Require coordinación real con operación, mantemento, enxeñaría, provedores e, cando proceda, responsables de seguridade funcional.
- Debe manter coherencia cos plans de resposta ante incidentes, coas copias e restauración e cos procedementos de crise.

Relación con outros controis: Relaciónase directamente coa análise de riscos tecnolóxicos, coa recomendación de controis de seguridade, coa implantación de marcos e normas, coa resposta ante incidentes, cos servizos forenses, coas copias de seguridade e restauración, coa xestión de vulnerabilidades, coa segmentación e coas medidas compensatorias. Constitúe unha capa esencial para dar continuidade práctica ao resto dos controis cando a prevención non resulta suficiente.

Casos habituais de uso: Emprégase para preparar escenarios de recuperación fronte a ransomware, fallo de sistemas críticos por múltiples causas, perda de comunicacións industriais, indispoñibilidade de persoal clave, problemas en cadea de subministración, interrupcións prolongadas de servizos tecnolóxicos, ataques con impacto físico ou degradación de procesos produtivos e servizos esenciais.

Observacións / medidas compensatorias asociadas: En contornos industriais, a continuidade e a resiliencia operativa non deben limitarse á restauración técnica dun

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

sistema, senón contemplar a volta segura á operación, a verificación do estado do proceso, a dispoñibilidade de configuracións válidas, a coordinación cos responsables de operación e a revisión das condicións de seguridade antes da reanudación completa. Tamén resulta especialmente relevante para xustificar medidas compensatorias temporais cando a recuperación definitiva dun activo ou proceso non pode executarse de inmediato.

5.1.5 Avaliacións técnicas e revisión de arquitectura

Categoría: Consultoría, gobernanza e análise

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Identify

Descrición: As avaliacións técnicas e a revisión de arquitectura consisten na análise estruturada dos compoñentes tecnolóxicos, das comunicacións, das interdependencias e do deseño xeral dun entorno para identificar debilidades, exposicións innecesarias, erros de segmentación, puntos únicos de fallo e carencias de protección. No ámbito industrial, este control abrangue tanto a arquitectura corporativa relacionada cos servizos de apoio á operación como a infraestrutura OT propiamente dita, incluíndo redes, accesos remotos, sistemas de supervisión, estacións de enxeñaría, HMI, integracións con terceiros, activos legados e interconexións entre dominios IT e OT.

Obxectivo: Comprobar se a arquitectura tecnolóxica existente responde a criterios adecuados de seguridade, resiliencia e compatibilidade operativa, detectando deseños inseguros, exposicións evitables e relacións de dependencia que poidan incrementar o risco. A súa finalidade é proporcionar unha visión técnica e estrutural do entorno, permitindo corrixir debilidades de deseño antes de que deriven en incidentes, auditorías desfavorables, degradación da operación ou dificultades de recuperación.

Como funciona / como se implanta: A súa execución adoita partir da recompilación de información sobre a arquitectura existente: diagramas de rede, inventarios de activos, fluxos de comunicación, políticas de acceso, integracións con terceiros, procedementos operativos e configuracións relevantes. Sobre esa base, revísanse aspectos como a separación entre dominios, a existencia e coherencia da segmentación, os accesos administrativos e remotos, a exposición de servizos, os mecanismos de autenticación, a protección de activos críticos, a resiliencia de comunicacións, a dependencia de sistemas sen soporte e a trazabilidade das comunicacións. En contornos

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

industriais, este exercicio debe ter en conta tamén a seguridade funcional, a dispoñibilidade, a latencia, a compatibilidade cos protocolos industriais, os requisitos de mantemento e o impacto potencial sobre o proceso. O resultado adoita materializarse en informes de situación, propostas de mellora arquitectónica, plans de adecuación ou recomendacións específicas de reforzo.

Vantaxes:

- Permite detectar debilidades estruturais antes de que se materialicen en incidentes.
- Mellora a coherencia entre seguridade, arquitectura e operación.
- Facilita a revisión de segmentación, accesos, exposicións e dependencias críticas.
- Axuda a xustificar cambios de deseño, reforzos de protección e medidas compensatorias.
- Serve de base para auditorías, adecuación normativa e follas de ruta de mellora.

Limitacións e consideracións:

- A súa calidade depende da dispoñibilidade e fiabilidade da documentación técnica existente.
- Pode ofrecer unha visión incompleta se non se incorpora coñecemento operativo e de proceso.
- En contornos industriais, unha revisión exclusivamente orientada a IT pode ignorar restricións críticas de OT.
- Require participación coordinada de sistemas, ciberseguridade, operación, mantemento e enxeñaría.
- Debe actualizarse cando se producen cambios relevantes de arquitectura, novas interconexións, incorporación de terceiros ou evolución de procesos.

Relación con outros controis: Relaciónase de maneira directa coa análise de riscos tecnolóxicos, coa recomendación de controis de seguridade, coa segmentación de rede e separación IT/OT, coa DMZ industrial, co acceso remoto seguro, coa visibilidade de activos e comunicacións OT, coa xestión de vulnerabilidades, co bastionado e coas medidas compensatorias. Actúa como soporte técnico para moitos dos controis posteriores do catálogo.

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

Casos habituais de uso: Emprégase en proxectos de revisión de arquitectura IT/OT, procesos de adecuación a IEC 62443 ou ENS, implantación de segmentación, incorporación de acceso remoto de terceiros, migracións tecnolóxicas, revisión de redes industriais, análises previas a auditorías, integración de novos sistemas ou avaliación de exposición de activos críticos e legados.

Observacións / medidas compensatorias asociadas: Nun entorno industrial, a revisión de arquitectura é especialmente útil para identificar medidas compensatorias de carácter estrutural, como a reorganización de zonas e condutos (IEC 62443), a limitación de fluxos innecesarios, o reforzo de controis de acceso, o despregue de DMZ industriais, a mellora da visibilidade ou a redución da exposición de activos que non poden ser actualizados ou substituídos a curto prazo.

5.1.6 Análise de vulnerabilidades hardware

Categoría: Consultoría, gobernanza e análise

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Identify

Descrición: A análise de vulnerabilidades hardware consiste na identificación, avaliación e contextualización de debilidades que afectan a compoñentes físicos, dispositivos embebidos, firmware, electrónica de control, interfaces de comunicación e outros elementos materiais que forman parte da infraestrutura tecnolóxica dunha organización. No ámbito industrial, este control resulta especialmente relevante porque boa parte da exposición non se concentra só en software convencional, senón tamén en PLC, RTU, sensores, gateways, equipos de rede industrial, HMI, dispositivos IIoT, controladores e compoñentes propietarios cuxa superficie de risco pode estar vinculada ao deseño físico, ao firmware, á configuración de baixo nivel ou á cadea de subministración.

Obxectivo: Detectar debilidades de seguridade en compoñentes hardware ou firmware que poidan comprometer a integridade, a dispoñibilidade ou a fiabilidade dun sistema, e establecer medidas de mitigación, compensación ou control que reduzan a exposición real da organización. O seu propósito é ampliar a análise clásica de vulnerabilidades software cara a elementos físicos e embebidos que, en contornos industriais, poden ter un impacto directo sobre a operación e o proceso.

Como funciona / como se implanta:

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

A súa implantación parte habitualmente da identificación dos activos físicos máis relevantes e da recompilación de información técnica sobre modelos, versións, firmware, interfaces dispoñibles, funcións críticas e relacións de dependencia. A partir desa base, poden revisarse advisories de fabricantes, boletíns de seguridade (véxase [1] [2]), bases de datos de vulnerabilidades, documentación técnica, configuracións de baixo nivel e, cando resulta viable, realizar probas específicas de análise ou validación sobre laboratorio, banco de probas ou contornos controlados. En contornos industriais, este exercicio debe executarse con especial prudencia, xa que determinados métodos de análise intensiva poden non ser compatibles coa operación en produción. Por iso, adoita combinar revisión documental, correlación con intelixencia de vulnerabilidades, contraste con fabricantes ou integradores e, cando procede, ensaios controlados sobre compoñentes equivalentes ou contornos illados.

Vantaxes:

- Permite identificar riscos que non serían visibles nunha análise centrada só en software.
- Axuda a comprender mellor a exposición real de dispositivos embebidos e compoñentes propietarios.
- Facilita a priorización de medidas compensatorias en activos que non poden ser parcheados facilmente.
- Reforza a visión sobre firmware, interfaces físicas e cadea de subministración.
- Resulta especialmente útil en contornos con elevada dependencia de activos industriais legados ou específicos.

Limitacións e consideracións:

- A dispoñibilidade de información técnica ou de advisories detallados pode ser limitada en certos dispositivos industriais.
- Moitos equipos propietarios dificultan a análise directa ou a validación independente.
- En contornos de produción, algunhas probas poden resultar inviables polo risco de impacto na operación.
- Require coñecemento especializado sobre firmware, electrónica, protocolos industriais e arquitectura de dispositivo.

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

- A súa eficacia mellora cando se integra con xestión de activos, intelixencia de ameazas, revisión de arquitectura e xestión de vulnerabilidades.

Relación con outros controis: Relaciónase coa análise de riscos tecnolóxicos, coa xestión de vulnerabilidades en software clásica (ver sección seguinte), co hardening de HMI e sistemas de enxeñaría, coa xestión da cadea de subministración e do firmware, coa segmentación, coa monitorización de activos OT, coas medidas compensatorias e coas estratexias de parcheo ou substitución gradual.

Casos habituais de uso: Emprégase na revisión de PLC, RTU, equipos IIoT, sensores, gateways industriais, dispositivos de comunicación, HMI, firmware de equipos de planta, compoñentes de fabricantes específicos, sistemas con ciclos de vida longos ou contornos nos que se detectan advisories recorrentes asociados a dispositivos físicos críticos.

Observacións / medidas compensatorias asociadas: En contornos industriais, é frecuente que as vulnerabilidades hardware ou firmware non poidan ser tratadas mediante actualización inmediata. Por iso, este control adoita desembocar na adopción de medidas compensatorias como segmentación reforzada, illamento de activos, limitación de servizos expostos, control estrito de accesos, monitorización específica, xestión da cadea de subministración ou substitución planificada a medio prazo. A súa utilidade é especialmente alta cando se emprega para fundamentar decisións de contención e priorización sobre activos críticos con soporte limitado.

5.1.7 CyberRange e contornos de proba

Categoría: Consultoría, gobernanza e análise

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: Os CyberRange e contornos de proba son infraestruturas controladas deseñadas para reproducir, con maior ou menor fidelidade, compoñentes tecnolóxicos, procesos, comunicacións e escenarios de seguridade co fin de validar controis, ensaiar procedementos, formar persoal e analizar o comportamento de sistemas e ameazas sen afectar á operación real, utilizando escenarios de propostas como a de ENISA [19].

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

Metodoloxía proposta para a execución de ciberexercicios. Fonte: ENISA (2026)

No ámbito industrial, estes contornos poden incluír simulación de redes IT/OT, representación de activos industriais, estacións de enxeñaría, HMI, PLC, protocolos específicos, accesos remotos, fluxos de datos e casos de uso de resposta ante incidentes. O seu valor principal reside en proporcionar un espazo seguro para probar, aprender e mellorar sen introducir risco directo sobre produción ou servizos esenciais.

Obxectivo: Dispoñer dun entorno controlado no que sexa posible validar medidas de seguridade, comprobar cambios técnicos, ensaiar escenarios de incidente, adestrar equipos e reducir a incerteza asociada á implantación de controis ou á resposta fronte a eventos reais. En contornos industriais, o obxectivo inclúe tamén mellorar a preparación operativa, validar a compatibilidade de medidas co proceso e reducir o risco de impacto sobre sistemas en produción.

Como funciona / como se implanta: A súa implantación pode adoptar diferentes formatos, dende laboratorios sinxelos con activos representativos ata plataformas avanzadas de simulación e adestramento que recrean arquitecturas industriais completas ou parciais. O deseño do entorno de proba debe partir dos obxectivos perseguidos: validación de configuracións, ensaio de segmentación, probas de acceso remoto, formación técnica, simulación de incidentes, adestramento de resposta, revisión de actualizacións ou comprobación de medidas compensatorias. En contornos industriais, resulta especialmente útil reproducir activos críticos, fluxos de comunicación, dependencias entre sistemas e interaccións co proceso, mesmo cando esa representación non sexa idéntica ao entorno real. Algunhas plataformas permiten hibridar elementos virtuais e físicos. A súa eficacia aumenta cando se integra con procedementos de proba, criterios de aceptación, rexistro de resultados e leccións aprendidas.

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

Vantaxes:

- Permite validar cambios e controis sen afectar directamente á operación.
- Reduce o risco asociado á implantación de medidas en produción.
- Mellora a formación práctica de perfís técnicos, operativos e de seguridade.
- Facilita exercicios de simulación, resposta e coordinación entre equipos.
- Resulta útil para probar medidas compensatorias, actualizacións, configuracións e escenarios de incidente.

Limitacións e consideracións:

- A súa representatividade depende do grao de semellanza co entorno real.
- Pode requirir investimento relevante en deseño, mantemento e actualización de compoñentes.
- Non sempre é viable replicar con exactitude sistemas propietarios, activos legados ou condicións reais de proceso.
- Debe evitarse asumir que unha proba satisfactoria en laboratorio elimina por completo o risco en produción.
- O seu valor diminúe se non se integra con procedementos, obxectivos claros e revisión dos resultados obtidos.

Relación con outros controis: Relaciónase coa análise de riscos tecnolóxicos, coa recomendación de controis de seguridade, coa revisión de arquitectura, co patch management, co hardening, co acceso remoto seguro, coa monitorización, coa resposta ante incidentes, coas copias e restauración e coas medidas compensatorias. Funciona como soporte transversal para validar ou adestrar boa parte dos controis do catálogo.

Casos habituais de uso: Emprégase para validar segmentación e fluxos de rede, probar actualizacións ou cambios de configuración, ensaiar accesos remotos, adestrar equipos SOC/CSIRT, simular escenarios de ransomware ou indispoñibilidade, comprobar procedementos de recuperación, avaliar ferramentas de detección e formar persoal de operación, mantemento e ciberseguridade en contextos industriais realistas.

Observacións / medidas compensatorias asociadas: En contornos industriais, os CyberRange e contornos de proba son especialmente valiosos cando a implantación directa dun cambio en produción implica incerteza elevada. Nese sentido, permiten validar previamente medidas compensatorias, secuencias de recuperación, procedementos de resposta ou controis novos antes do seu despregue real. Tamén

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

resultan útiles para mellorar a coordinación interfuncional e para reducir a dependencia de decisións tomadas exclusivamente sobre supostos teóricos, ademais de fins formativos.

5.2 Auditorías técnicas e identificación de debilidades

A mellora da seguridade require coñecer con suficiente precisión que debilidades existen realmente no entorno e como poden ser explotadas. Esta subsección recolle **servizos e capacidades orientados a avaliar tecnicamente a exposición, validar hipóteses de risco e identificar vulnerabilidades, erros de configuración, superficies de ataque e carencias de protección** en infraestruturas, redes, dispositivos e compoñentes industriais.

5.2.1 Análise de vulnerabilidades

Categoría: Auditorías técnicas e identificación de debilidades

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Identify

Descrición: A análise de vulnerabilidades consiste no proceso sistemático de identificación, clasificación e contextualización de debilidades técnicas presentes en sistemas, aplicacións, servizos, dispositivos e compoñentes de rede que poidan ser explotados por un atacante ou derivar en fallos de seguridade [20]. O seu propósito non se limita a detectar vulnerabilidades coñecidas, senón tamén a comprender a súa relevancia dentro do entorno real da organización, tendo en conta a exposición do activo, a súa criticidade, as dependencias operativas e a posibilidade efectiva de explotación. En contornos industriais, este control abrangue tanto activos IT como OT, aínda que a súa execución require cautelas específicas cando afecta a sistemas de control, supervisión ou operación.

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

Proceso de xestión de vulnerabilidades. Fonte: DataCypher (2025)

Obxectivo: Identificar debilidades técnicas que poidan comprometer a confidencialidade, integridade, dispoñibilidade ou resiliencia dun entorno, proporcionando unha base ordenada para priorizar medidas de mitigación, hardening, segmentación, parcheo ou compensación. No ámbito industrial, o seu obxectivo inclúe tamén reducir a exposición de activos críticos sen introducir riscos innecesarios para a continuidade da operación nin para a seguridade funcional.

Como funciona / como se implanta: A súa implantación adoita partir da identificación do alcance, do inventario de activos e da selección da metodoloxía de análise máis adecuada segundo a natureza do entorno. O proceso pode combinar revisión de configuracións, contraste con bases de datos de vulnerabilidades, correlación con advisories de fabricantes, identificación de software e firmware instalados e, cando resulta viable, uso de ferramentas de análise automatizada. En contornos IT, estas revisións poden ser máis intrusivas e frecuentes; en contornos OT, pola contra, deben adaptarse ao risco operativo, priorizando técnicas pasivas, revisión documental, coordinación con fabricantes ou ensaios en contornos controlados cando a análise activa poida afectar á estabilidade do sistema. O resultado adoita expresarse mediante informes que relacionan cada vulnerabilidade co activo afectado, o seu nivel de exposición, o impacto potencial e as posibles vías de tratamento.

Vantaxes:

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

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

- Facilita a priorización de actuacións sobre a base da exposición real dos activos.
- Axuda a orientar medidas de mitigación, parcheo, bastionado ou compensación.
- Mellora a visibilidade técnica sobre sistemas, versións, configuracións e compoñentes afectados.
- Serve de apoio a auditorías, revisións de arquitectura e programas de xestión de vulnerabilidades.

Limitacións e consideracións:

- A simple detección dunha vulnerabilidade non determina por si soa a prioridade real de tratamento.
- En contornos industriais, unha análise agresiva ou mal planificada pode xerar impacto na operación.
- Os resultados poden ser incompletos se non existe un inventario de activos axeitado ou se hai pouca visibilidade sobre compoñentes legados.
- Requírese interpretación contextual: non todas as vulnerabilidades teñen a mesma relevancia nin a mesma explotabilidade no entorno real.
- Debe combinarse con criterios de criticidade, exposición, arquitectura e continuidade, e non lerse como unha listaxe illada de CVEs.

Relación con outros controis: Relaciónase coa análise de riscos tecnolóxicos, coa revisión de arquitectura, coa propia xestión de vulnerabilidades, co patch management, co hardening, coa segmentación, coa monitorización, coas medidas compensatorias e coa intelixencia de ameazas. Constitúe un control técnico de entrada para boa parte das actuacións posteriores de mitigación e reforzo.

Casos habituais de uso: Emprégase en auditorías técnicas, revisións periódicas de exposición, adecuación a marcos normativos, análises previas a cambios de arquitectura, revisión de activos críticos, contornos con accesos remotos, sistemas expostos a advisories de fabricante ou escenarios nos que se precisa priorizar a mitigación de debilidades coñecidas.

Observacións / medidas compensatorias asociadas: En contornos industriais, a análise de vulnerabilidades non debe entenderse automaticamente como paso previo a un parcheo inmediato. En moitos casos, a súa utilidade principal reside en permitir a contextualización do risco e a adopción de medidas de priorización ou compensatorias como segmentación, limitación de accesos, monitorización reforzada, hardening ou

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

redución da exposición, especialmente cando existen activos legados, sistemas propietarios ou restricións de mantemento (mais detalle deste contexto en [2]).

5.2.2 Pentesting e probas de seguridade controladas

Categoría: Auditorías técnicas e identificación de debilidades

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Identify

Descrición: O pentesting e as probas de seguridade controladas consisten na simulación planificada de accións de ataque sobre sistemas, aplicacións, redes ou servizos co fin de comprobar se determinadas debilidades poden ser explotadas e con que consecuencias. A diferenza da análise de vulnerabilidades, que se centra principalmente na identificación de fallos coñecidos ou configuracións débiles, estas probas buscan verificar a explotabilidade real, o encadeamento de debilidades, a eficacia dos controis existentes e o impacto potencial dun compromiso. En contornos industriais, este tipo de exercicios require un nivel de prudencia e planificación superior ao habitual, dado que determinadas interaccións poden afectar á estabilidade da operación, á comunicación entre sistemas ou, nalgúns casos, á seguridade funcional. Poden empregarse diversas metodoloxías, como OSSTMM adaptadas [21].

Obxectivo: Comprobar de forma controlada se un sistema ou entorno pode ser efectivamente comprometido a partir de debilidades existentes, obtendo evidencias prácticas sobre exposición, movemento lateral, escalada de privilexios, eficacia dos controis e impacto potencial. No ámbito industrial, o seu propósito é achegar visibilidade realista sobre a superficie de ataque sen comprometer a dispoñibilidade nin introducir riscos desproporcionados para o proceso.

Como funciona / como se implanta: A súa implantación require definir con precisión o alcance, os activos afectados, as limitacións operativas, as regras do exercicio, os horarios, os mecanismos de parada segura e os criterios de éxito. En contornos convencionais, as probas poden incluír explotación de vulnerabilidades, movemento lateral, comprobación de credenciais, análise de servizos expostos ou revisión de aplicacións. En contornos industriais, pola contra, adoita ser necesario limitar técnicas intrusivas en produción, priorizar ensaios sobre laboratorios, contornos replicados, sistemas representativos ou activos non críticos, e contar coa validación previa de operación, mantemento e responsables técnicos. Nalgúns casos, o valor da proba reside

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

máis na simulación controlada de escenarios e no contraste de hipóteses de explotación ca nunha acción agresiva directa sobre sistemas de planta.

Vantaxes:

- Aporta evidencias prácticas sobre a explotabilidade real de determinadas debilidades.
- Permite validar a eficacia de controis preventivos, detectivos e de contención.
- Axuda a identificar cadeas de ataque que non son visibles nunha revisión puramente documental.
- Mellora a comprensión da exposición real do entorno e das posibles vías de compromiso.
- Pode apoiar a revisión de arquitectura, segmentación, acceso remoto e resposta ante incidentes.

Limitacións e consideracións:

- En contornos industriais, unha proba mal deseñada pode afectar á dispoñibilidade, á estabilidade do proceso ou á seguridade funcional.
- Non todas as técnicas habituais de pentesting son aceptables sobre activos OT en produción.
- Require coñecemento técnico especializado e coordinación estreita con operación, mantemento e enxeñaría.
- Os resultados son dependentes do alcance definido: unha proba limitada non representa necesariamente toda a exposición real.
- Debe executarse con autorización formal, regras claras e procedementos de contención ou reversión cando proceda.

Relación con outros controis: Relaciónase coa análise de vulnerabilidades, coa revisión de arquitectura, coa segmentación de rede, co acceso remoto seguro, coa monitorización e detección, coa resposta ante incidentes, co hardening e cos contornos de proba ou CyberRange. Funciona como mecanismo de validación práctica doutros controis e hipóteses de risco.

Casos habituais de uso: Emprégase na revisión de perímetros expostos, validación de segmentación, comprobación de accesos remotos, ensaio de escenarios de movemento lateral, revisión de aplicacións ou servizos concretos, auditorías previas a posta en

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

produción, avaliación de contornos replicados e exercicios controlados de verificación técnica en arquitectura IT/OT.

Observacións / medidas compensatorias asociadas: En contornos industriais, o pentesting debe formularse sempre dende un criterio de proporcionalidade, alcance limitado e control estrito do risco. En moitos casos, o exercicio máis recomendable non será unha explotación plena en produción, senón probas parciais, simulacións, validación en laboratorio ou revisión técnica reforzada. Tamén pode ser útil para comprobar a robustez de medidas compensatorias xa implantadas, como segmentación, restrición de accesos, limitación de servizos ou mecanismos de detección.

5.2.3 Auditorías de infraestrutura

Categoría: Auditorías técnicas e identificación de debilidades

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Identify

Descrición: As auditorías de infraestrutura consisten na revisión técnica e estruturada dos compoñentes que soportan a operación tecnolóxica dunha organización, incluíndo redes, servidores, sistemas, servizos, dispositivos de comunicación, activos de seguridade e elementos de interconexión entre dominios. O seu propósito é avaliar se a infraestrutura presenta unha configuración adecuada, se responde a criterios mínimos de seguridade e resiliencia e se existen debilidades de deseño, exposicións innecesarias ou dependencias críticas insuficientemente controladas. En contornos industriais, este tipo de auditoría abrangue tanto a infraestrutura corporativa vinculada á operación como os compoñentes de rede e comunicación que dan soporte aos sistemas OT, ás estacións de enxeñaría, aos HMI, ás comunicacións remotas e ás integracións con terceiros. Poden empregarse diferentes metodoloxías como OSSTMM [21].

Obxectivo: Verificar o estado real da infraestrutura tecnolóxica dende o punto de vista da seguridade, identificando configuracións incorrectas, exposicións evitables, carencias de protección, problemas de segmentación, dependencias non documentadas ou puntos únicos de fallo que poidan incrementar o risco da organización. No ámbito industrial, o obxectivo inclúe tamén comprobar que a infraestrutura que soporta a operación é compatible cun nivel axeitado de dispoñibilidade, control e trazabilidade.

Como funciona / como se implanta: A súa implantación adoita combinar revisión documental, análise de configuracións, inspección técnica, entrevistas con responsables

de sistemas e operación e, cando procede, verificación sobre os compoñentes en alcance. O exercicio pode abranguer elementos como topoloxía de rede, segmentación, firewalls, switches, routers, servidores, sistemas de virtualización, mecanismos de autenticación, servizos expostos, infraestrutura de acceso remoto, políticas de administración e dependencias entre sistemas. En contornos industriais, a auditoría debe estenderse tamén a compoñentes como redes de supervisión, comunicacións industriais, servidores OT, HMI, servidores de salto, enlaces con integradores, mecanismos de recollida de logs e soportes de continuidade. A análise debe adaptarse á realidade do entorno, evitando accións que poidan comprometer a operación e combinando, cando sexa necesario, observación pasiva e contraste con documentación e configuracións exportadas.

Vantaxes:

- Permite obter unha visión estruturada do estado real da infraestrutura.
- Axuda a detectar configuracións inseguras, exposicións innecesarias e dependencias críticas.
- Facilita a revisión de segmentación, accesos, servizos expostos e controis de base.
- Mellora a capacidade de priorizar reforzos de arquitectura e medidas de protección.
- Serve de apoio a auditorías normativas, análises de risco e revisións de continuidade.

Limitacións e consideracións:

- A súa profundidade depende da dispoñibilidade de documentación fiable e acceso aos compoñentes auditados.
- Pode ofrecer unha visión parcial se non se integra co coñecemento operativo e cos fluxos reais da organización.
- En contornos industriais, unha revisión deseñada só con criterios IT pode pasar por alto condicionantes críticos de OT.
- Debe executarse con coordinación suficiente para evitar interferencias co proceso e cos sistemas produtivos.
- O seu valor diminúe se os achados non se traducen despois en medidas concretas de corrección, reforzo ou compensación.

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

Relación con outros controis: Relaciónase coa revisión de arquitectura, coa análise de riscos tecnolóxicos, coa análise de vulnerabilidades, coa segmentación de rede, coa DMZ industrial, co acceso remoto seguro, coa visibilidade de activos e comunicacións OT, co hardening, coa monitorización e coa continuidade de negocio. Funciona como base técnica para comprender o estado xeral do entorno e ordenar melloras posteriores.

Casos habituais de uso: Emprégase en revisións previas a auditorías de cumprimento, programas de reforzo da arquitectura, proxectos de segmentación IT/OT, avaliación de infraestruturas de acceso remoto, revisión de redes industriais e corporativas, incorporación de novos servizos ou terceiros, análises tras incidentes ou exercicios periódicos de verificación da postura técnica do entorno.

Observacións / medidas compensatorias asociadas: En contornos industriais, as auditorías de infraestrutura son especialmente útiles para identificar medidas compensatorias de base arquitectónica, como reforzo da segmentación, limitación de servizos expostos, mellora do control de accesos, introdución de servidores de salto, illamento de compoñentes legados, mellora da visibilidade ou revisión de dependencias críticas que non poidan ser eliminadas a curto prazo.

5.2.4 Auditorías de redes inalámbricas

Categoría: Auditorías técnicas e identificación de debilidades

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Identify

Descrición: As auditorías de redes inalámbricas consisten na revisión técnica e funcional das tecnoloxías sen fíos empregadas por unha organización, co obxectivo de identificar configuracións inseguras, exposicións non controladas, deficiencias de segmentación, mecanismos de autenticación débiles, canles non autorizadas ou riscos asociados ao uso de comunicacións radio. No ámbito industrial, este control abrangue non só redes Wi-Fi convencionais, senón tamén outros medios sen fíos presentes en planta ou en infraestruturas operativas, como enlaces de radio, dispositivos móbiles, sensores conectados, compoñentes IIoT, redes de apoio loxístico ou solucións de mantemento e supervisión remota que empregan comunicación inalámbrica. Exemplo dunha metodoloxía proposta, aquí [22].

Obxectivo: Verificar que as comunicacións inalámbricas presentes no entorno non introducen unha superficie de exposición desproporcionada e que existen medidas

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

adecuadas para limitar accesos non autorizados, interferencias, movemento lateral, fuga de información ou incorporación non controlada de dispositivos. En contornos industriais, o obxectivo inclúe tamén comprobar que o uso de tecnoloxías sen fíos é compatible coa seguridade, a continuidade e a estabilidade da operación.

Como funciona / como se implanta: A súa implantación adoita partir da identificación das tecnoloxías inalámbricas existentes, do seu propósito operativo e da súa integración coa arquitectura xeral. A partir desa base, revísanse aspectos como cobertura, cifrado, autenticación, segregación, inventario de dispositivos, exposición a SSID non autorizados, mecanismos de xestión, políticas de acceso, presenza de puntos de acceso non controlados, uso de credenciais por defecto e interacción co resto da infraestrutura. En contornos industriais, a auditoría debe considerar ademais o papel que estas redes xogan na operación, no mantemento, na mobilidade de persoal, na sensorización ou na conectividade de equipos auxiliares, prestando especial atención a dependencias ocultas, uso informal de redes sen fíos e posibles impactos sobre a dispoñibilidade ou a integridade do proceso. O exercicio pode combinar revisión documental, inspección técnica, captura pasiva de tráfico, análise de cobertura e comprobación de configuracións e políticas.

Vantaxes:

- Permite identificar exposicións que adoitan pasar inadvertidas en revisións centradas só en rede cableada.
- Mellora o control sobre accesos, dispositivos e comunicacións sen fíos.
- Axuda a detectar configuracións débiles, redes non autorizadas ou segmentación insuficiente.
- Reforza a protección fronte a movemento lateral, acceso oportunista ou uso informal de conectividade inalámbrica.
- Achega visibilidade sobre compoñentes IIoT, mobilidade e canles radio presentes no entorno.

Limitacións e consideracións:

- Pode ofrecer unha visión incompleta se a organización non dispón dun inventario claro das tecnoloxías inalámbricas en uso.
- En contornos industriais, a conectividade sen fíos pode estar dispersa entre múltiples áreas e provedores, dificultando a súa gobernanza.

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

- Non todas as debilidades derivan da tecnoloxía; moitas proceden de usos informais, configuracións herdadas ou falta de segmentación.
- A análise debe ter en conta non só a seguridade, senón tamén cobertura, interferencias, estabilidade e compatibilidade coa operación.
- Debe integrarse co control de accesos, a xestión de dispositivos, a segmentación e a monitorización do entorno.

Relación con outros controis: Relaciónase coa auditoría de infraestrutura, coa segmentación de rede, co NAC, coa protección de endpoints industriais, coa conexión segura de dispositivos externos, coa monitorización de activos e comunicacións OT, coa xestión de identidades e accesos e coas medidas compensatorias orientadas a limitar exposición de canles sen fíos.

Casos habituais de uso: Emprégase na revisión de redes Wi-Fi corporativas e operativas, puntos de acceso en planta, dispositivos móbiles de mantemento, sensores inalámbricos, contornos IIoT, solucións de supervisión remota, redes temporais de soporte, radioenlaces ou escenarios nos que se sospeita da existencia de conectividade sen fíos non inventariada ou insuficientemente controlada.

Observacións / medidas compensatorias asociadas: En contornos industriais, as auditorías de redes inalámbricas son especialmente útiles para detectar canles de exposición pouco visibles e para fundamentar medidas compensatorias como segregación específica, reforzo de autenticación, limitación de dispositivos autorizados, illamento de SSID, desactivación de servizos innecesarios, control reforzado de acceso ou monitorización específica de comunicacións radio.

5.2.5 Auditorías de dispositivos móbiles e endpoints

Categoría: Auditorías técnicas e identificación de debilidades

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Identify

Descrición: As auditorías de dispositivos móbiles e endpoints consisten na revisión técnica e funcional dos equipos de usuario, dispositivos portátiles e terminais que interactúan coa infraestrutura tecnolóxica da organización, co fin de comprobar o seu nivel real de protección, configuración, control e exposición. Este control abrangue, entre outros, ordenadores corporativos, portátiles de mantemento, estacións de traballo, tablets, smartphones, equipos de soporte técnico e outros dispositivos que

poidan conectarse á rede, acceder a servizos corporativos ou intervir, directa ou indirectamente, na operación. Poden empregarse para este fin boas prácticas do NIST [23]. No ámbito industrial, esta revisión adquire especial relevancia porque moitos destes dispositivos constitúen unha ponte entre o entorno corporativo, os servizos remotos, o persoal de mantemento e os sistemas OT.

Obxectivo: Comprobar se os dispositivos finais e móbiles da organización presentan un nivel axeitado de seguridade, control e trazabilidade, identificando configuracións inseguras, carencias de protección, software non autorizado, xestión insuficiente de accesos, exposición innecesaria ou riscos de propagación cara a outros dominios. En contornos industriais, o obxectivo inclúe tamén reducir o risco de que un portátil de mantemento, un equipo de terceiros ou un dispositivo móbil se converta en vector de acceso, movemento lateral ou alteración de sistemas operativos e produtivos.

Como funciona / como se implanta: A súa implantación adoita partir do inventario dos dispositivos en alcance, da súa función dentro da organización e do grao de interacción que manteñen cos distintos contornos tecnolóxicos. A partir desa base, revísanse aspectos como sistema operativo, nivel de actualización, configuración de seguridade, cifrado, xestión de credenciais, mecanismos de autenticación, rexistro e monitorización, software instalado, políticas de uso, privilexios dispoñibles, protección antimalware, control de dispositivos externos e integración con solucións de administración centralizada. En contornos industriais, a auditoría debe prestar especial atención aos portátiles de enxeñaría e mantemento, aos equipos utilizados por integradores e provedores, aos dispositivos con acceso remoto, ás estacións de traballo que interactúan con HMI ou sistemas de supervisión, e aos terminais que operan en contornos mixtos IT/OT. O exercicio pode combinar revisión documental, análise de configuración, verificación técnica e contraste coas políticas corporativas e operativas.

Vantaxes:

- Permite detectar configuracións inseguras e debilidades de protección en equipos finais.
- Mellora o control sobre dispositivos que poden actuar como vector de acceso ou propagación.
- Axuda a reforzar a trazabilidade, o control de software e a xestión de privilexios.
- Achega visibilidade sobre portátiles de mantemento, equipos de terceiros e dispositivos móbiles con acceso relevante.

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

- Serve de apoio para reforzar políticas de acceso, hardening e administración centralizada.

Limitacións e consideracións:

- A súa eficacia depende da existencia dun inventario fiable e dunha gobernanza suficiente sobre os dispositivos.
- Pode verse limitada pola presenza de equipos non xestionados, legados ou pertencentes a terceiros.
- En contornos industriais, algúns portátiles ou estacións poden ter restricións de actualización ou compatibilidade con software específico de fabricante.
- Non debe analizarse só dende a óptica corporativa, xa que algúns endpoints teñen impacto directo ou indirecto sobre a operación.
- Debe combinarse con control de accesos, xestión de software, restrición de dispositivos externos e monitorización de actividade.

Relación con outros controis: Relaciónase coa protección do posto de traballo, coa protección de endpoints industriais, co MDM, coa seguridade no correo, coa conexión segura de dispositivos externos, coa xestión de identidades e accesos, co acceso remoto seguro, coa monitorización, co hardening e coas medidas compensatorias orientadas a limitar exposición de equipos con capacidade de interacción con contornos OT.

Casos habituais de uso: Emprégase na revisión de portátiles de mantemento e enxeñaría, equipos de terceiros con acceso a planta, dispositivos móbiles corporativos, estacións de traballo con acceso a sistemas críticos, terminais con acceso remoto, revisión de privilexios locais, control de software instalado e escenarios nos que se necesita avaliar o risco de propagación dende endpoints cara a redes industriais ou sistemas sensibles.

Observacións / medidas compensatorias asociadas: En contornos industriais, estas auditorías resultan especialmente útiles para fundamentar medidas compensatorias como limitación de privilexios, endurecemento específico, control reforzado de software, uso de servidores de salto, segmentación de accesos, restrición de portátiles autorizados, control de dispositivos USB, monitorización intensificada ou segregación de equipos utilizados por provedores e persoal de mantemento.

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

5.2.6 Revisión de perímetro físico-lóxico

Categoría: Auditorías técnicas e identificación de debilidades

Tipoloxía: Técnico/ mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Identify

Descrición: A revisión de perímetro físico-lóxico consiste na análise conxunta dos elementos de acceso, separación, conexión e control que delimitan a exposición dun entorno tecnolóxico tanto dende o punto de vista físico como dende o punto de vista lóxico. O seu propósito é identificar de que maneira os espazos, armarios, salas técnicas, portos, interfaces, conexións de rede, dispositivos de acceso, medios extraíbles e puntos de interconexión poden actuar como superficie de entrada, manipulación ou propagación dun incidente. En contornos industriais, este control resulta especialmente relevante porque a seguridade non depende só da rede ou do software, senón tamén da forma en que os activos están fisicamente despregados, protexidos e conectados á infraestrutura operativa.

Obxectivo: Verificar que os límites físicos e lóxicos do entorno están suficientemente definidos e protexidos, reducindo a posibilidade de accesos non autorizados, manipulación local de equipos, conexión de dispositivos indebidos, exposición de interfaces de administración ou interconexións inseguras entre dominios. No ámbito industrial, o obxectivo inclúe tamén reducir o risco derivado de accesos a sala, armarios de control, postos de mantemento, portos de comunicación, equipos de campo e outros puntos nos que unha interacción física pode traducirse nun compromiso lóxico con impacto operativo.

Como funciona / como se implanta: A súa execución adoita combinar revisión in situ, contraste con documentación de arquitectura, análise dos puntos de acceso físico e lóxico e verificación da protección existente sobre compoñentes clave. Isto inclúe, entre outros aspectos, control de acceso a salas e armarios, protección de postos de operación e mantemento, exposición de portos físicos, presenza de interfaces non utilizadas, conectividade de dispositivos externos, separación entre redes, acceso a consolas locais, uso de servidores de salto, protección de cuartos de comunicacións, trazabilidade de intervencións físicas e relación entre acceso local e privilexios lóxicos. En contornos industriais, esta revisión debe estenderse a PLC, HMI, estacións de enxeñaría, switches industriais, gateways, armarios de planta, compoñentes de campo e calquera outro

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

elemento no que unha interacción física poida alterar o proceso, introducir malware, modificar configuracións ou abrir unha vía de acceso cara á rede operativa.

Vantaxes:

- Permite detectar exposicións que non serían visibles nunha revisión puramente lóxica ou documental.
- Mellora a comprensión das relacións entre acceso físico e compromiso tecnolóxico.
- Axuda a identificar puntos de entrada local, interfaces innecesarias e conexións mal gobernadas.
- Reforza a protección de activos críticos, postos de mantemento e compoñentes de comunicación.
- Resulta útil para limitar accesos oportunistas, manipulacións locais e propagación a partir de dispositivos conectados fisicamente.

Limitacións e consideracións:

- Pode quedar incompleta se non se realiza con coñecemento do proceso e da realidade operativa do entorno.
- En contornos industriais, moitos puntos de acceso físico responden a necesidades de mantemento ou operación que non poden eliminarse sen máis.
- A existencia de protección física non garante por si soa un control lóxico axeitado, e viceversa.
- Requírese coordinación con operación, mantemento, infraestruturas, seguridade física e responsables técnicos.
- Debe integrarse con políticas de acceso, trazabilidade, xestión de dispositivos externos e segmentación da rede.

Relación con outros controis: Relaciónase coa auditoría de infraestrutura, coa segmentación de rede, co acceso remoto seguro, coa conexión segura de dispositivos externos, coa protección do posto de traballo, coa xestión de identidades e accesos, co hardening, coa monitorización e coas medidas compensatorias destinadas a reducir a exposición de activos e interfaces críticas.

Casos habituais de uso: Emprégase na revisión de salas técnicas e armarios de control, postos de operación e enxeñaría, equipos de mantemento, portos físicos en HMI e PLC, cuartos de comunicacións, interconexión entre redes corporativas e operativas, xestión

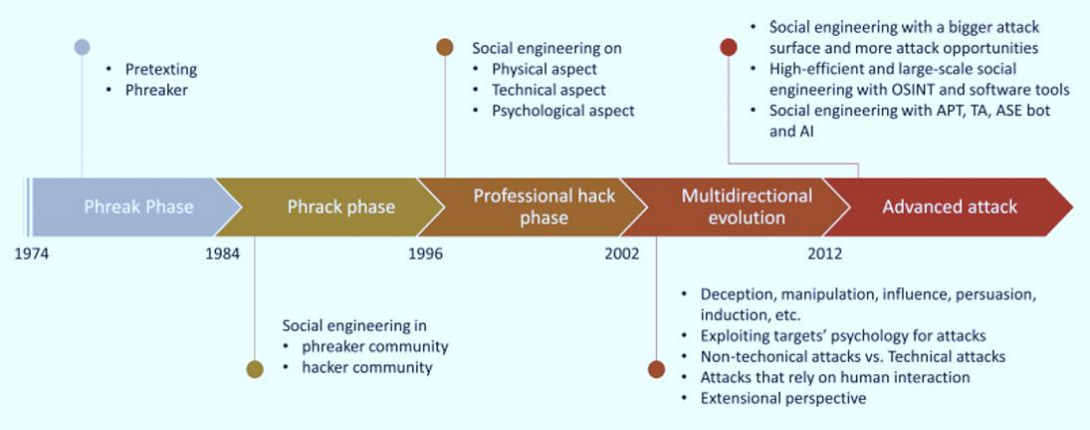
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

de USB e portátiles autorizados, e escenarios nos que se precisa avaliar a relación entre acceso local e capacidade de alteración do entorno tecnolóxico.

Observacións / medidas compensatorias asociadas: En contornos industriais, esta revisión resulta especialmente útil para fundamentar medidas compensatorias como selado ou desactivación de portos non necesarios, reforzo de control de acceso a armarios e salas, uso de servidores de salto, restrición de conexión de dispositivos externos, monitorización de intervencións locais, reforzo de trazabilidade ou segregación física e lóxica adicional en compoñentes con alta criticidade.

5.3 Contra enxeñaría social e seguridade do factor humano

A protección dos contornos industriais non depende só da robustez da arquitectura técnica, senón tamén do comportamento das persoas que interactúan cos sistemas, a información e os procesos. Este bloque aborda as **medidas destinadas a reducir o risco derivado da manipulación humana** (enxeñería social [24]), **da suplantación e do erro, combinando capacidades de prevención, concienciación, simulación e resposta** fronte a técnicas cada vez máis sofisticadas.



Evolución conceptual da historia da enxeñería social. Fonte: Wang, Sun & Zhu (2010)

5.3.1 Phishing, vishing, smishing e técnicas afíns

Categoría: Contra enxeñaría social e seguridade do factor humano

Tipoloxía: Organizativo / técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: O phishing, o vishing, o smishing e outras técnicas afíns forman parte do conxunto de tácticas de enxeñaría social orientadas a manipular ás persoas para obter información, credenciais, acceso inicial ou execución de accións que favorezan un

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

compromiso posterior. A súa diferenza principal reside na canle empregada: correo electrónico no caso do phishing, chamadas telefónicas no vishing, mensaxería móbil no smishing, aínda que todas comparten a mesma lóxica de explotación da confianza, da urxencia, da autoridade aparente ou do descoñecemento.

En contornos industriais, estas técnicas non afectan só ao persoal corporativo, senón tamén a perfís de operación, mantemento, enxeñaría, provedores e terceiros con acceso a sistemas ou procesos críticos.

Obxectivo: Reducir a probabilidade de que a manipulación do factor humano se converta nun vector de acceso, fraude, fuga de información ou alteración da operación, reforzando a capacidade da organización para identificar, bloquear, informar e responder fronte a interaccións maliciosas dirixidas a persoas con acceso ou influencia sobre o entorno tecnolóxico.

Como funciona / como se implanta: A súa abordaxe non se limita á detección de mensaxes fraudulentas, senón que require combinar concienciación, procedementos, protección técnica e canles de reporte. Isto inclúe formación adaptada a distintos perfís, mecanismos de dobre validación para accións sensibles, protección do correo e das identidades, procedementos de verificación de solicitudes críticas, revisión de canles de comunicación, simulacións controladas cando proceda e integración cos procesos de resposta. En contornos industriais, resulta especialmente importante adaptar o enfoque aos escenarios reais do entorno: mensaxes dirixidas a persoal de planta, chamadas fraudulentas a servizos de mantemento, suplantación de provedores, peticións urxentes de acceso remoto, cambios de credenciais, envío de ficheiros ou instrucións aparentando proceder de responsables internos ou fabricantes.

Vantaxes:

- Reduce un dos vectores de acceso inicial máis frecuentes en incidentes reais.
- Mellora a capacidade do persoal para identificar interaccións sospeitosas.
- Reforza a protección de identidades, credenciais e canles de comunicación.
- Axuda a limitar fraudes, acceso indebido e execución de accións non autorizadas.
- Favorece unha cultura de reporte e verificación fronte a solicitudes anómalas.

Limitacións e consideracións:

- A concienciación por si soa non elimina o risco nin substitúe os controis técnicos.

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

- Os atacantes adaptan rapidamente mensaxes, canles e elementos de suplantación ao contexto da organización.
- En contornos industriais, certos perfís poden non estar expostos con frecuencia á formación convencional de seguridade e seguir sendo un obxectivo relevante.
- Debe evitarse un enfoque excesivamente xenérico ou centrado só no correo electrónico, deixando fóra teléfono, mensaxería instantánea ou interaccións con terceiros.
- A súa eficacia depende de que existan procedementos claros para validar peticións e informar incidentes sospeitosos.

Relación con outros controis: Relaciónase coa seguridade no email, coa xestión de identidades e accesos, co acceso remoto seguro, coa conexión segura de dispositivos externos, coa monitorización, coa resposta ante incidentes e coas campañas de concienciación e simulación. Constitúe unha capa esencial para reducir risco humano e reforzar a protección dos accesos ao entorno IT/OT.

Casos habituais de uso: Emprégase na prevención de roubo de credenciais, suplantación de provedores, fraude en peticións urxentes, acceso remoto non autorizado, envío de ficheiros maliciosos, manipulación de persoal de mantemento ou enxeñaría, campañas dirixidas a usuarios con privilexios e escenarios de compromiso inicial por interacción humana.

Observacións / medidas compensatorias asociadas: En contornos industriais, este control gaña eficacia cando se combina con procedementos reforzados de validación, limitación de privilexios, MFA, monitorización de accesos e segregación de funcións. Tamén resulta útil establecer canles específicas para confirmar solicitudes de mantemento, cambios de configuración, intervencións remotas ou actuacións que poidan ter impacto sobre a operación.

5.3.2 Campañas de concienciación e simulación

Categoría: Contra enxeñaría social e seguridade do factor humano

Tipoloxía: Organizativo / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: As campañas de concienciación e simulación consisten no conxunto de accións planificadas destinadas a mellorar a percepción do risco, a capacidade de

identificación de ameazas e a resposta do persoal fronte a situacións que poidan comprometer a seguridade da organización. Inclúen tanto actividades formativas e divulgativas como exercicios prácticos, simulacións controladas e mecanismos de reforzo orientados a comprobar o comportamento real das persoas ante intentos de manipulación, fraude, acceso indebido ou execución de accións non autorizadas. En contornos industriais, este control resulta especialmente relevante porque o factor humano intervén non só na xestión da información, senón tamén no mantemento da continuidade operativa, no acceso a sistemas OT, na xestión de incidencias e na relación con provedores e terceiros.

Obxectivo: Incrementar a capacidade do persoal para recoñecer, evitar e reportar situacións de risco relacionadas coa enxeñaría social, co uso indebido de canles de comunicación, coa suplantación de identidade ou con comportamentos inseguros que poidan afectar aos contornos tecnolóxicos e operativos. O seu propósito é reducir a exposición derivada do factor humano e reforzar a cultura de seguridade da organización de maneira sostida e contextualizada.

Como funciona / como se implanta: A súa implantación adoita partir da identificación dos perfís de usuario, das súas funcións e do nivel de exposición de cada colectivo. Sobre esa base, deséñanse accións de concienciación adaptadas ao contexto real da organización, combinando contidos xerais de seguridade con escenarios específicos do entorno. Estas campañas poden incluír materiais formativos, sesións presenciais ou en liña, recordatorios periódicos, guías prácticas, cápsulas temáticas, simulacións de phishing ou outras técnicas de enxeñaría social, así como medición de resultados e reforzo sobre os comportamentos detectados. En contornos industriais, é importante adaptar o enfoque aos distintos perfís implicados —persoal de operación, mantemento, enxeñaría, administración, sistemas, provedores— e incorporar exemplos relacionados con acceso remoto, uso de portátiles de mantemento, suplantación de fabricantes, validación de cambios, procedementos críticos ou interacción con sistemas de control.

Vantaxes:

- Mellora a capacidade do persoal para identificar e evitar interaccións maliciosas.
- Reforza a cultura organizativa de seguridade e o hábito de reporte.
- Permite adaptar mensaxes e exercicios a colectivos con exposición e funcións distintas.
- Axuda a detectar debilidades de comportamento antes de que se materialicen en incidentes reais.

- Complementa os controis técnicos reforzando a primeira capa de defensa humana.

Limitacións e consideracións:

- A súa eficacia diminúe se se formula como acción puntual e non como proceso continuado.
- Non substitúe os controis técnicos nin elimina por si soa o risco de erro humano ou manipulación.
- As simulacións deben deseñarse con criterio proporcional, evitando efectos contraproducentes ou rexeitamento por parte do persoal.
- En contornos industriais, algúns perfís poden ter pouca exposición á formación corporativa tradicional e requirir enfoques específicos.
- Convén medir resultados non só en taxas de erro, senón tamén en mellora do reporte, comprensión do risco e adecuación dos procedementos.

Relación con outros controis: Relaciónase co phishing, vishing, smishing e técnicas afíns, co email security, coa xestión de identidades e accesos, co acceso remoto seguro, coa conexión segura de dispositivos externos, cos procedementos operativos e coa resposta ante incidentes. Funciona como capa complementaria para reducir a probabilidade de que o factor humano actúe como vector de entrada ou de propagación.

Casos habituais de uso: Emprégase en programas anuais de concienciación, campañas periódicas de simulación de phishing, formación específica para persoal de mantemento e enxeñaría, reforzo de boas prácticas en accesos remotos, sensibilización fronte a suplantación de terceiros, revisión de procedementos de validación e exercicios orientados a colectivos con acceso privilexiado ou con impacto operativo relevante.

Observacións / medidas compensatorias asociadas: En contornos industriais, estas campañas son especialmente útiles cando se combinan con procedementos formais de validación, segregación de funcións, MFA, restrición de privilexios e canles claras de reporte. Tamén poden actuar como medida compensatoria parcial en escenarios nos que non é posible reforzar de inmediato todos os controis técnicos, sempre que se integren nun programa máis amplo e sostido de protección do factor humano.

5.3.3 Outras técnicas anti-enxeñaría social

Categoría: Contra enxeñaría social e seguridade do factor humano

Tipoloxía: Organizativo / mixto

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

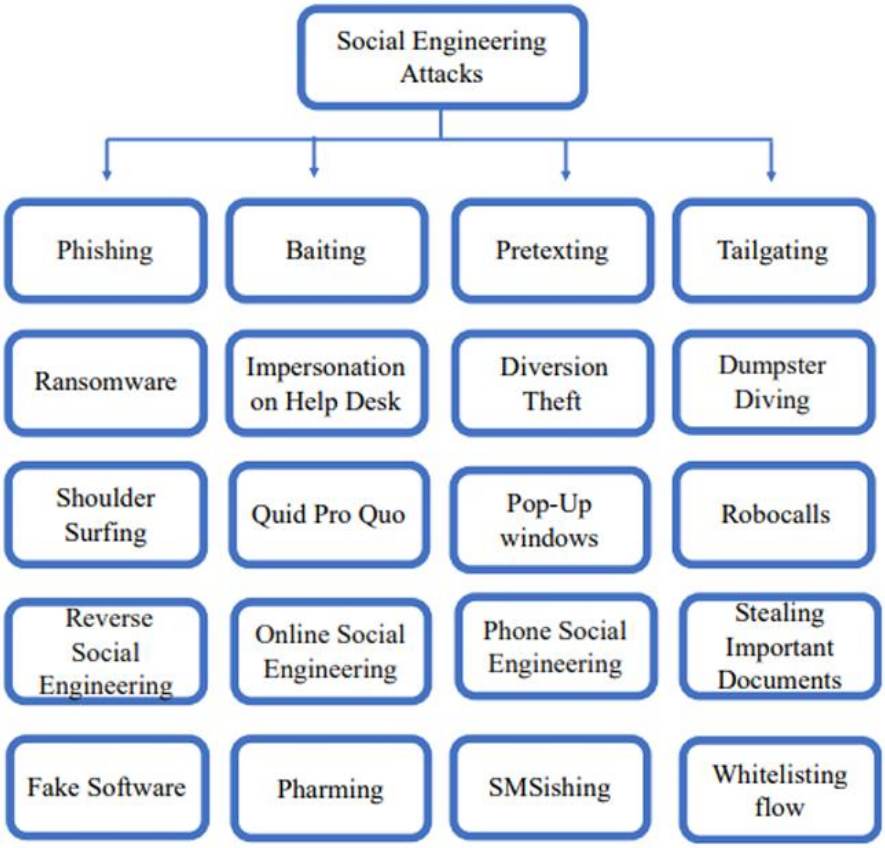
Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: As outras técnicas anti-enxeñaría social comprenden o conxunto de medidas organizativas, procedementais e de validación destinadas a reducir o risco de manipulación humana máis alá das campañas específicas de phishing, vishing ou smishing. Inclúen prácticas como a dobre verificación de solicitudes sensibles, a validación de identidade por canles independentes, os procedementos formais de autorización, a segregación de funcións, a restrición de accións críticas a roles determinados, os protocolos fronte a cambios urxentes ou non planificados e o uso de canles seguras para interaccións con terceiros. En contornos industriais, estas medidas son especialmente relevantes porque moitas accións de alto impacto non se executan a través dunha simple mensaxe maliciosa, senón mediante peticións aparentemente lexítimas de acceso, modificación, mantemento, cambio de configuración ou intervención operativa.

Obxectivo: Reducir a probabilidade de que unha interacción humana manipulada ou unha suplantación de identidade poida derivar en acceso indebido, execución de cambios non autorizados, entrega de información sensible, alteración do proceso ou activación de cadeas de risco con impacto operativo. O seu propósito é reforzar a seguridade a través de controis procedementais que introduzan verificación, trazabilidade e separación de responsabilidades nas accións máis sensibles.

A continuación, exemplos de ataques de enxeñería social, mais alá dos descritos antes.



Ataques de enxeñería social. Fonte: Salahdine & Kaabouch (2019)

Como funciona / como se implanta: A súa implantación parte da identificación das operacións e interaccións máis expostas a manipulación, como peticións urxentes de acceso remoto, cambios de credenciais, modificacións de configuración, envío de ficheiros, actuacións de mantemento, intervencións de terceiros ou solicitudes que impliquen impacto sobre a operación. Sobre esa base, establécense procedementos formais de validación, mecanismos de confirmación por segunda canle, requisitos de autorización, rexistro de actuacións, segregación de roles e controis de supervisión. En contornos industriais, resulta especialmente importante aplicar estas medidas a actividades como acceso de provedores, modificación de lóxicas ou parámetros, actualizacións, intervencións en planta, uso de portátiles de mantemento, conexión de dispositivos externos e actuacións sobre HMI, estacións de enxeñaría ou activos críticos. O valor destas técnicas depende de que sexan coñecidas, practicables e realmente integradas no funcionamento diario da organización.

Vantaxes:

- Introducen barreiras procedementais fronte á manipulación humana e á suplantación de identidade.

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

- Reducen a probabilidade de execución de accións críticas baseadas en peticións fraudulentas ou non validadas.
- Melloran a trazabilidade e a separación de responsabilidades.
- Resultan aplicables a múltiples escenarios, mesmo cando non existe unha mensaxe maliciosa evidente.
- Complementan os controis técnicos reforzando a seguridade das interaccións sensibles.

Limitacións e consideracións:

- Perden eficacia se non se interiorizan como práctica habitual e quedan reducidas a políticas formais.
- Poden xerar fricción operativa se se deseñan sen criterio de proporcionalidade ou sen adaptación ao contexto.
- En contornos industriais, os procesos urxentes de mantemento ou continuidade poden levar a relaxar estes controis se non están ben integrados.
- Requiren apoio da dirección, coñecemento dos equipos e revisión periódica para evitar bypass informais.
- Deben acompañarse de formación, concienciación e mecanismos claros de reporte e escalado.

Relación con outros controis: Relaciónase co phishing, vishing, smishing e técnicas afíns, coas campañas de concienciación e simulación, coa xestión de identidades e accesos, co acceso remoto seguro, coa segregación de funcións, coa conexión segura de dispositivos externos, cos procedementos operativos e coa resposta ante incidentes. Constitúe unha capa procedemental de protección moi relevante en escenarios de interacción con terceiros e operación sensible.

Casos habituais de uso: Emprégase para validar peticións de acceso remoto, cambios de configuración, actualizacións, uso de credenciais privilexiadas, actuacións de provedores, conexión de portátiles ou dispositivos externos, modificacións en sistemas de control, autorizacións de mantemento urxente e calquera outra acción que poida ter impacto sobre a operación ou a seguridade do entorno.

Observacións / medidas compensatorias asociadas: En contornos industriais, estas técnicas anti-enxeñaría social resultan especialmente valiosas cando se combinan con MFA, rexistro de sesións, segregación de funcións, control de privilexios e validación por

segunda canle. Tamén poden actuar como medida compensatoria parcial cando non é posible reforzar de inmediato determinados controis técnicos, sempre que existan procedementos claros, trazables e asumidos polos equipos implicados.

5.4 Defensa perimetral e segmentación

A separación adecuada de redes, funcións e zonas de confianza segue sendo un dos principios máis eficaces para reducir exposición e limitar a propagación lateral dun incidente. Esta subsección agrupa **controis destinados a reforzar o perímetro, ordenar os fluxos de comunicación e establecer barreiras lóxicas entre dominios IT e OT, favorecendo unha arquitectura máis resistente**, controlable e compatible coa operación industrial.

5.4.1 Firewall

Categoría: Defensa perimetral e segmentación

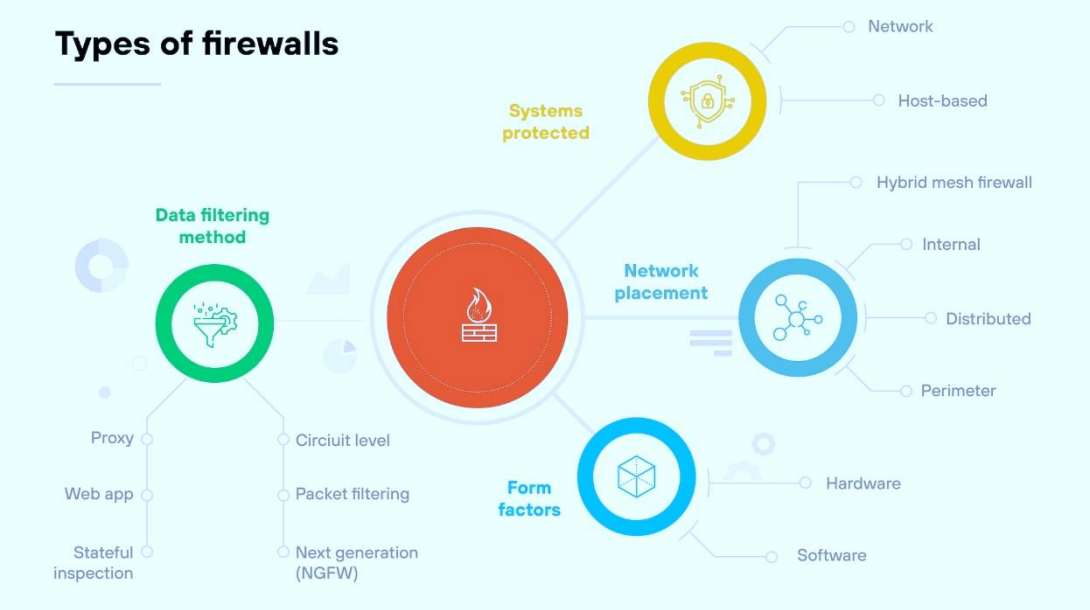
Tipoloxía: Técnico

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: O firewall é un control de seguridade destinado a regular, filtrar e supervisar as comunicacións entre redes, zonas, sistemas ou activos, de acordo cun conxunto definido de regras. A súa función principal consiste en permitir unicamente o tráfico necesario e bloquear ou restrinxir aquelas conexións non autorizadas, innecesarias ou potencialmente perigosas, aínda que existen diversas tipoloxías con funcións 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. Fonte: Palo Alto Networks (n.d.)

En contornos industriais, o seu papel vai máis alá da protección perimetral tradicional, xa que constitúe unha peza fundamental para a separación entre dominios IT e OT, para a segmentación interna da rede operativa e para o control dos fluxos entre activos con distintos niveis de criticidade.

Obxectivo: Reducir a superficie de exposición do entorno, limitar as comunicacións ao estritamente necesario e dificultar o acceso non autorizado, o movemento lateral e a propagación de incidentes entre zonas ou sistemas. No ámbito industrial, o firewall contribúe tamén a reforzar a compartimentación da arquitectura e a protexer activos sensibles fronte a comunicacións improcedentes ou non controladas.

Como funciona / como se implanta: A súa implantación baséase na definición de regras de filtrado que determinan que tráfico pode circular entre dúas redes, equipos ou segmentos, e baixo que condicións. Estas regras poden basearse en direccións IP, portos, protocolos, aplicacións, estados de conexión ou outros criterios segundo a tecnoloxía empregada. En contornos industriais, a súa configuración debe partir dun coñecemento detallado dos fluxos necesarios para a operación, da criticidade dos activos, dos protocolos utilizados, das necesidades de mantemento e dos puntos de interconexión coa infraestrutura corporativa ou con terceiros. A súa eficacia aumenta cando se integra nun deseño de zonas e condutos, con revisión periódica de regras, trazabilidade, monitorización e coordinación cos cambios na arquitectura.

Vantaxes:

- Limita as comunicacións non autorizadas entre redes, sistemas e zonas.

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

- Reduce a superficie de exposición e dificulta o movemento lateral.
- Achega control e trazabilidade sobre os fluxos permitidos e bloqueados.
- Constitúe unha base fundamental para a segmentación IT/OT e a compartimentación interna.
- Pode actuar como medida compensatoria fronte a activos vulnerables ou con soporte limitado.

Limitacións e consideracións:

- A súa eficacia depende da calidade do deseño das regras e do coñecemento real dos fluxos necesarios.
- Unha configuración incorrecta pode interromper comunicacións lexítimas ou, pola contra, deixar exposición excesiva.
- En contornos industriais, non todos os protocolos ou patróns de tráfico responden ben a enfoques de filtrado tradicionais.
- Non substitúe outros controis como segmentación lóxica completa, xestión de accesos, monitorización ou hardening.
- Require mantemento continuo, revisión de excepcións e adaptación a cambios de arquitectura, operación ou terceiros.

Relación con outros controis: Relaciónase coa segmentación de rede e separación IT/OT, coa DMZ industrial, co NGFW/UTM, co NAC, co acceso remoto seguro, coa monitorización e detección, coa revisión de arquitectura, coa xestión de vulnerabilidades e coas medidas compensatorias. Constitúe un dos controis estruturais máis relevantes dentro da defensa perimetral e da compartimentación do entorno.

Casos habituais de uso: Emprégase para separar a rede corporativa da rede OT, protexer celas ou zonas industriais, controlar accesos dende terceiros, limitar tráfico entre servidores e activos de supervisión, reforzar enlaces con sedes remotas, illar sistemas legados e establecer barreiras de control entre distintos niveis da arquitectura.

Observacións / medidas compensatorias asociadas: En contornos industriais, o firewall é unha das medidas compensatorias máis utilizadas cando non resulta viable parchear de inmediato certos activos ou substituír compoñentes vulnerables. Neses casos, pode empregarse para restrinxir protocolos, limitar orixes e destinos autorizados, reducir a exposición de servizos e introducir unha capa adicional de control mentres non se acomete unha remediación definitiva.

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

5.4.2 NGFW / UTM

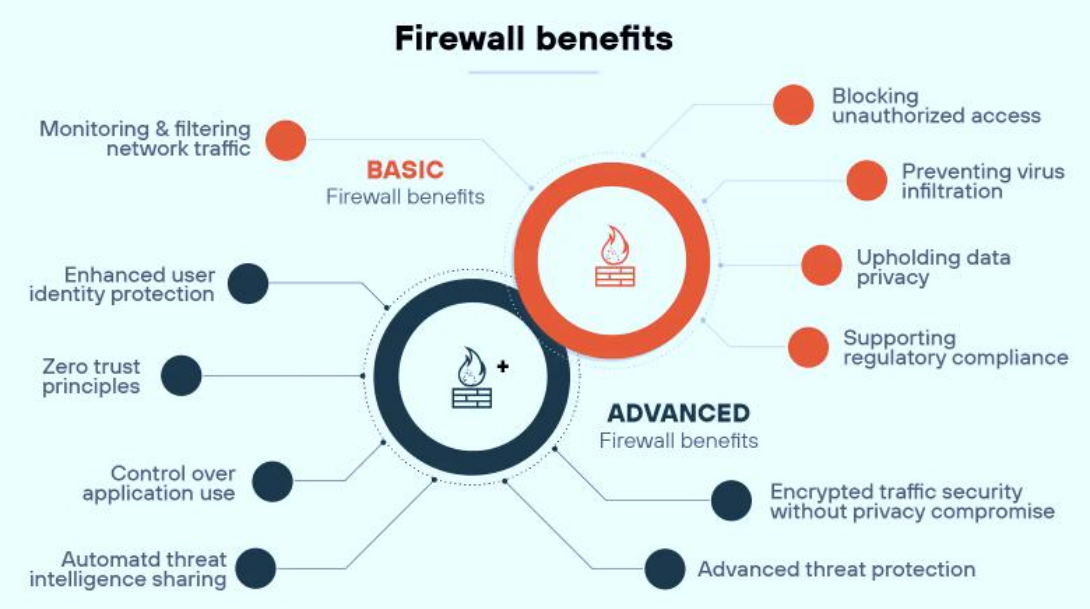
Categoría: Defensa perimetral e segmentación

Tipoloxía: Técnico

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: Os NGFW (*Next-Generation Firewall*) e as solucións UTM (*Unified Threat Management*) son plataformas de seguridade que amplían as capacidades do firewall tradicional incorporando funcións adicionais de inspección, control e detección. Ademais do filtrado básico de tráfico, poden incluír identificación de aplicacións, inspección profunda de paquetes, prevención de intrusións, control de contido, filtrado web, descifrado de tráfico cifrado, integración con intelixencia de ameazas e capacidades de rexistro e análise máis avanzadas. En contornos industriais, estas solucións poden desempeñar un papel relevante cando existe interconexión con contornos corporativos, servizos externos, acceso remoto ou necesidades de control reforzado sobre fluxos complexos, sempre que a súa implantación sexa compatible cos requisitos de estabilidade e continuidade do entorno operativo.



Beneficios dun firewall tradicional fronte a un NGFW/UTM. Fonte: Palo Alto Networks (n.d.)

Obxectivo: Incrementar o control sobre o tráfico e os servizos que atravesan os límites entre redes, zonas ou dominios, combinando filtrado, visibilidade e capacidade de detección fronte a comunicacións non autorizadas, aplicacións non previstas ou patróns de tráfico potencialmente maliciosos. No ámbito industrial, o seu obxectivo é reforzar a

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

protección perimetral e interzonal cando o nivel de exposición ou interdependencia require algo máis que un filtrado clásico baseado só en IP, portos e protocolos.

Como funciona / como se implanta: A súa implantación baséase na colocación destes dispositivos en puntos estratéxicos da arquitectura, como enlaces entre a rede corporativa e a DMZ, entre a DMZ e a rede OT, en saídas a Internet ou en accesos de terceiros. A partir desa posición, as políticas de seguridade poden construírse non só sobre regras de tráfico básicas, senón tamén sobre identificación de aplicacións, categorías de servizo, perfís de usuario, mecanismos de detección e correlación con ameazas coñecidas. En contornos industriais, a súa configuración debe realizarse con especial cautela, xa que determinadas funcións —como a inspección profunda, o descifrado ou certas formas de prevención activa— poden non ser compatibles con protocolos industriais, co rendemento da rede ou co comportamento esperado de sistemas sensibles. Por iso, a súa implantación require coñecer ben os fluxos autorizados, os protocolos presentes, a criticidade das comunicacións e o impacto potencial das funcións avanzadas sobre a operación.

Vantaxes:

- Engaden visibilidade e capacidade de control máis aló do filtrado tradicional.
- Permiten identificar aplicacións, patróns de tráfico e comportamentos non previstos.
- Poden integrar capacidades de prevención, detección e rexistro máis avanzadas.
- Resultan útiles en contornos con acceso remoto, servizos externos ou elevada interconexión.
- Reforzan a seguridade perimetral e a compartimentación cando se deseñan e configuran correctamente.

Limitacións e consideracións:

- Non todas as funcións avanzadas son adecuadas para contornos OT ou protocolos industriais.
- Unha inspección excesivamente intrusiva pode afectar á latencia, á dispoñibilidade ou á estabilidade da comunicación.
- Requiren configuración, mantemento e revisión máis complexos que un firewall básico.

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

- Non substitúen a segmentación arquitectónica, a xestión de accesos nin a monitorización específica de activos OT.
- Deben implantarse con criterio de proporcionalidade, evitando activar capacidades que non achegan valor real ao entorno protexido.

Relación con outros controis: Relaciónanse co firewall tradicional, coa segmentación de rede e separación IT/OT, coa DMZ industrial, co acceso remoto seguro, co IDS/IPS, co NDR, coa monitorización e detección, coa revisión de arquitectura e coas medidas compensatorias asociadas á limitación de exposición e control de fluxos.

Casos habituais de uso: Empréganse para reforzar a fronteira entre rede corporativa e OT, protexer DMZ industriais, controlar accesos de terceiros, inspeccionar comunicacións saíntes a servizos externos, mellorar o control sobre fluxos interzonais e complementar a protección perimetral en organizacións con elevada conectividade ou dependencia de servizos dixitais e remotos.

Observacións / medidas compensatorias asociadas: En contornos industriais, estas solucións poden ser útiles como medida compensatoria cando se precisa engadir unha capa adicional de control sobre aplicacións, servizos ou fluxos expostos e non resulta viable acometer cambios estruturais inmediatos na arquitectura. Con todo, o seu despregue debe facerse sempre tras validar a compatibilidade co entorno, os protocolos presentes e os requisitos de continuidade e seguridade funcional.

5.4.3 Segmentación de rede e separación IT/OT

Categoría: Defensa perimetral e segmentación

Tipoloxía: Técnico / mixto

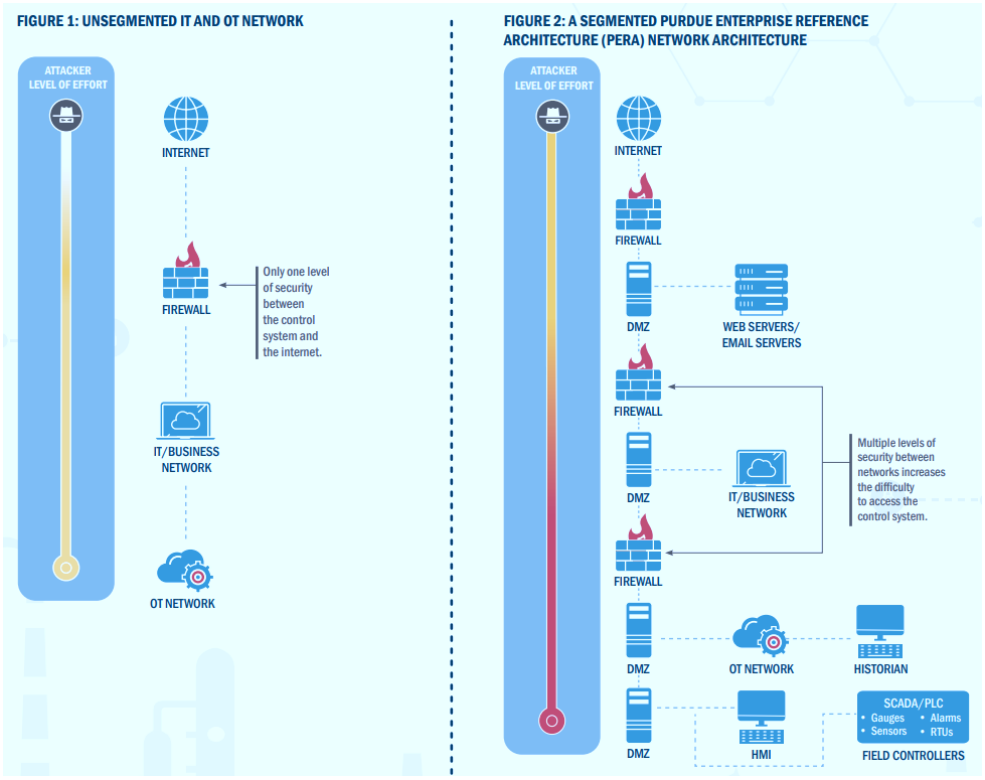
Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: A segmentación de rede e a separación IT/OT consisten na organización da arquitectura en zonas, dominios ou segmentos diferenciados, establecendo límites claros entre eles e controlando de forma explícita as comunicacións permitidas (ver IEC 62443 en [25]). O seu propósito é evitar que todos os sistemas compartan o mesmo plano de exposición, reducindo a probabilidade de propagación lateral, acceso indebido e impacto sistémico ante un incidente. En contornos industriais, este control resulta especialmente crítico porque a converxencia entre redes corporativas e operativas incrementa a eficiencia e a visibilidade, pero tamén multiplica os puntos de contacto a

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

través dos cales unha incidencia en IT pode chegar a afectar activos OT ou procesos físicos.



Redes non segmentadas fronte a IT-OT segmentado. Fonte: CISA (2022)

Obxectivo: Reducir a superficie de exposición do entorno, limitar as comunicacións ao estritamente necesario e conter de forma máis eficaz un posible compromiso, evitando que unha incidencia localizada se propague entre dominios con distinta criticidade. No ámbito industrial, o seu obxectivo inclúe tamén protexer a rede OT fronte a dependencias innecesarias da rede corporativa e establecer niveis de separación compatibles coa continuidade e coa seguridade do proceso.

Como funciona / como se implanta: A súa implantación baséase na identificación dos activos, dos fluxos de comunicación necesarios e da criticidade relativa de cada sistema, para despois estruturar a arquitectura en zonas e condutos ou segmentos con regras de interconexión ben definidas. Isto pode materializarse mediante VLAN, ACL, firewalls, DMZ industriais, servidores de salto, proxys, condutos controlados ou outros mecanismos equivalentes, sempre en función da arquitectura existente. En contornos industriais, esta segmentación debe considerar non só a separación entre rede corporativa e rede OT, senón tamén a compartimentación interna entre niveis de supervisión, operación, enxeñaría, mantemento, activos legados, acceso remoto e comunicación con terceiros. A súa eficacia depende do coñecemento real dos fluxos

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

necesarios, da revisión periódica das regras e da capacidade de adaptar a arquitectura aos cambios do proceso.

Vantaxes:

- Reduce a exposición global e limita o movemento lateral entre dominios.
- Mellora a capacidade de contención ante un incidente.
- Facilita o control e a trazabilidade das comunicacións entre zonas.
- Reforza a protección de activos críticos e compoñentes legados.
- Serve de base para a implantación doutros controis como DMZ, firewalls, NAC ou acceso remoto seguro.

Limitacións e consideracións:

- A súa implantación perde eficacia se non existe un coñecemento suficiente dos fluxos reais do entorno.
- Un deseño incorrecto pode introducir bloqueos, excepcións continuas ou dependencia excesiva de regras ad hoc.
- En contornos industriais, a segmentación debe ter en conta latencia, dispoñibilidade, seguridade funcional e necesidades de mantemento.
- Non substitúe a xestión de accesos, a monitorización, o bastionado nin a xestión de vulnerabilidades.
- Require mantemento continuo, revisión de cambios e coordinación entre sistemas, operación, enxeñaría e seguridade.

Relación con outros controis: Relaciónase co firewall, co NGFW/UTM, coa DMZ industrial, co NAC, co acceso remoto seguro, coa monitorización e detección, coa revisión de arquitectura, coa xestión de vulnerabilidades e coas medidas compensatorias. Constitúe un dos piares centrais da defensa en profundidade en contornos industriais.

Casos habituais de uso: Emprégase para separar a rede corporativa da rede OT, compartimentar redes de supervisión e control, illar activos legados, limitar comunicacións entre liñas ou celas, protexer contornos de enxeñaría, controlar accesos de terceiros e reducir a exposición de sistemas con alta criticidade operativa.

Observacións / medidas compensatorias asociadas: En contornos industriais, a segmentación é simultáneamente un control e unha das medidas compensatorias máis

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

relevantes cando non é viable actualizar, substituír ou endurecer de inmediato determinados activos. A través dela pode restrinxirse a exposición de compoñentes vulnerables, limitar canles de comunicación, reducir dependencias innecesarias e reforzar a contención mentres non se acomete unha remediación estrutural máis profunda.

5.4.4 DMZ industrial

Categoría: Defensa perimetral e segmentación

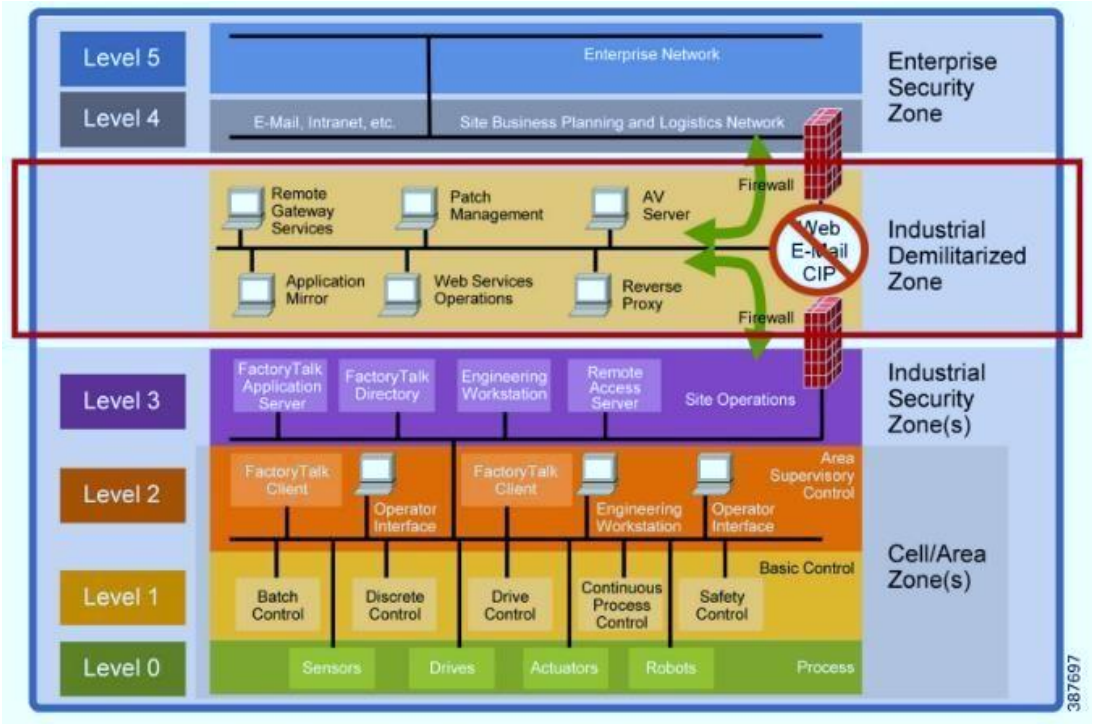
Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: A DMZ industrial é unha zona intermedia de comunicación situada entre a rede corporativa e a rede OT, deseñada para controlar, limitar e supervisar os intercambios de información entre ambos os dous dominios. A súa función principal é evitar conexións directas innecesarias entre contornos con niveis de exposición e criticidade distintos, introducindo unha capa adicional de separación, mediación e control. En contornos industriais, esta arquitectura resulta especialmente útil para canalizar servizos compartidos, acceso remoto, intercambio de ficheiros, recollida de rexistros, integración con sistemas corporativos, actualizacións ou servizos de supervisión sen expoñer directamente os activos operativos máis sensibles.

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



Exemplo de DMZ industrial. Fonte: Dale Peterson (2019)

Obxectivo: Reducir o risco derivado da interconexión entre a rede corporativa e a rede operativa, evitando accesos directos, limitando os fluxos aos estritamente necesarios e proporcionando un punto controlado para a inspección, rexistro e mediación das comunicacións. No ámbito industrial, o seu obxectivo inclúe tamén protexer a rede OT fronte a compromisos procedentes de IT e reforzar a separación entre servizos de apoio e sistemas de control.

Como funciona / como se implanta: A súa implantación baséase na creación dun segmento específico da arquitectura no que se sitúan servizos que precisan comunicarse con ambos os dous lados, pero que non deben residir nin no núcleo da rede corporativa nin no núcleo da rede OT. Nesa zona poden situarse, por exemplo, servidores de intercambio, proxies, servidores de salto, solucións de acceso remoto, colectores de logs, réplicas de datos, servidores historiadores ou mecanismos de transferencia controlada. As comunicacións dende e cara á DMZ deben regularse mediante firewalls, regras explícitas, mecanismos de autenticación e supervisión continua. En contornos industriais, o seu deseño debe partir dun coñecemento preciso dos fluxos necesarios, dos protocolos utilizados, da criticidade dos servizos aloxados e das dependencias operativas, evitando que a DMZ se converta nun simple espazo de tránsito sen gobernanza nin control real.

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

Vantaxes:

- Introduce unha capa adicional de separación entre IT e OT.
- Limita as conexións directas e reduce a superficie de exposición da rede operativa.
- Facilita o control, rexistro e supervisión dos intercambios entre dominios.
- Permite albergar servizos compartidos nunha zona con políticas específicas de seguridade.
- Resulta especialmente útil para acceso remoto, intercambio de datos, rexistro centralizado e integración con terceiros.

Limitacións e consideracións:

- A súa eficacia depende do deseño correcto dos fluxos e das regras de interconexión.
- Pode perder valor se se converte nun espazo demasiado amplo, mal segmentado ou con servizos non xustificados.
- En contornos industriais, a presenza dunha DMZ non elimina a necesidade de segmentación interna nin doutros controis de acceso e monitorización.
- Require mantemento continuo, revisión de excepcións e gobernanza clara sobre os servizos aloxados.
- Debe evitarse que a DMZ actúe como ponte implícita ou zona de confianza excesiva entre IT e OT.

Relación con outros controis: Relaciónase co firewall, co NGFW/UTM, coa segmentación de rede e separación IT/OT, co acceso remoto seguro, cos servidores de salto, coa monitorización e detección, coa xestión de identidades e accesos, coa revisión de arquitectura e coas medidas compensatorias orientadas a limitar exposición de activos OT.

Casos habituais de uso: Emprégase para canalizar acceso remoto de terceiros, intercambio seguro de ficheiros, publicación controlada de datos operativos cara a sistemas corporativos, recollida centralizada de rexistros, aloxamento de historiadores ou réplicas de información, servizos de supervisión e integración segura entre redes de distinta criticidade.

Observacións / medidas compensatorias asociadas: En contornos industriais, a DMZ industrial é unha das medidas compensatorias máis relevantes cando se precisa manter

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

interconexión con contornos corporativos, servizos externos ou terceiros sen expoñer directamente a rede OT. A súa utilidade é especialmente alta cando se combina con segmentación adicional, control de acceso robusto, trazabilidade e monitorización continua dos fluxos que a atravesan.

5.4.5 VPN e comunicacións seguras

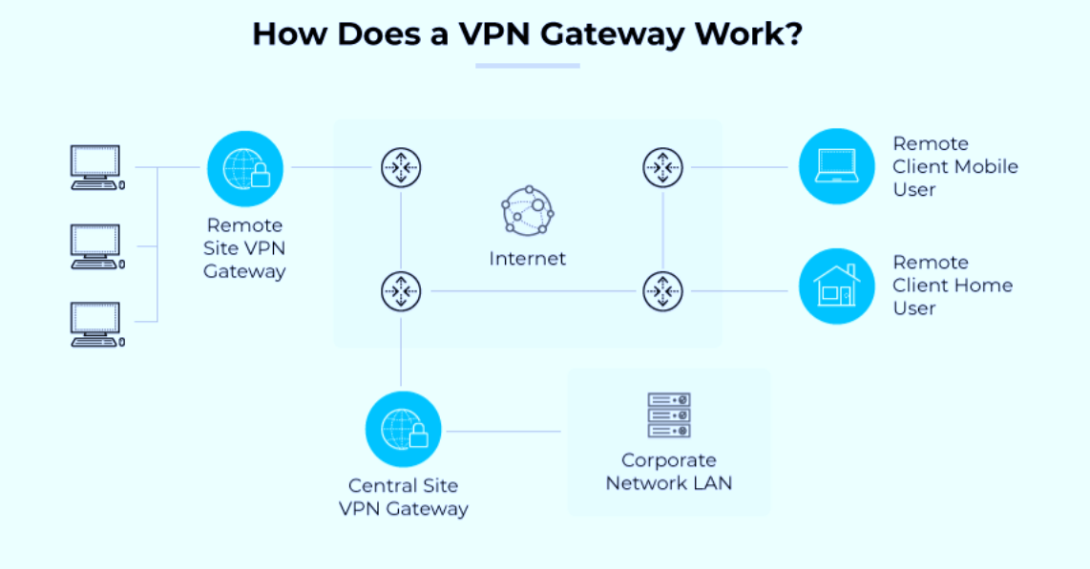
Categoría: Defensa perimetral e segmentación

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: As VPN e outras comunicacións seguras son mecanismos destinados a protexer a confidencialidade, integridade e autenticidade das conexións entre usuarios, sedes, sistemas ou redes que precisan intercambiar información a través de infraestruturas potencialmente expostas ou non confiables. A súa función principal é establecer canles de comunicación cifradas e controladas, reducindo o risco de interceptación, manipulación ou acceso indebido durante a transmisión. En contornos industriais, este control resulta especialmente relevante para o acceso remoto de persoal interno e de terceiros, para a conexión entre instalacións, para a integración de servizos distribuídos e para o intercambio seguro de información entre dominios con distinta criticidade.



Tipoloxías de VPN. Fonte: Palo Alto Networks (n.d.)

Obxectivo: Garantir que as comunicacións entre puntos autorizados se realicen mediante canles protexidas, reducindo a exposición a escoita, alteración de tráfico,

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

roubo de credenciais ou uso indebido de accesos remotos. No ámbito industrial, o seu obxectivo inclúe tamén habilitar conectividade necesaria para operación, soporte e mantemento sen comprometer a separación entre redes nin a seguridade dos sistemas OT.

Como funciona / como se implanta: A súa implantación baséase na creación de túneles cifrados ou canles seguras entre extremos autorizados, combinando mecanismos de autenticación, cifrado, control de sesión, rexistro de actividade e, cando procede, restrición por perfil, orixe, horario ou destino. Isto pode aplicarse tanto a conexións de usuario remoto como a enlaces entre sedes, servizos ou infraestruturas. En contornos industriais, a súa configuración debe partir dun criterio de mínimo privilexio, limitando o acceso ao estritamente necesario, evitando exposición innecesaria de redes completas e integrándose con segmentación, servidores de salto, MFA, trazabilidade e revisión de sesións. A súa eficacia depende non só da fortaleza criptográfica da canle, senón tamén da forma en que se gobernan os accesos, os permisos e os fluxos autorizados.

Vantaxes:

- Protexen as comunicacións fronte a interceptación, manipulación ou uso indebido.
- Permiten habilitar acceso remoto e interconexión entre sedes de forma controlada.
- Reforzan a seguridade das conexións de soporte, mantemento e operación distribuída.
- Achegan trazabilidade e control cando se integran con autenticación forte e rexistro de sesións.
- Resultan útiles para limitar a exposición de servizos que non deben publicarse directamente.

Limitacións e consideracións:

- Unha VPN segura non garante por si soa un acceso remoto seguro se os permisos son excesivos ou a segmentación é insuficiente.
- En contornos industriais, a apertura de túneles amplos ou mal gobernados pode converterse nun vector de acceso de alto risco.
- Requírese control estrito de usuarios, credenciais, horarios, destinos e actividades permitidas.

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

- Non substitúe mecanismos como MFA, servidores de salto, PAM, segmentación nin monitorización de sesións.
- Debe evitarse que a necesidade operativa de acceso remoto xustifique excepcións permanentes sen trazabilidade nin revisión periódica.

Relación con outros controis: Relaciónase co acceso remoto seguro, co firewall, co NGFW/UTM, coa DMZ industrial, coa segmentación de rede e separación IT/OT, coa xestión de identidades e accesos, co PAM, coa monitorización e coas medidas compensatorias orientadas a limitar exposición e acceso de terceiros.

Casos habituais de uso: Emprégase para conexión entre sedes industriais, acceso remoto de persoal técnico ou corporativo, soporte de provedores, mantemento programado, acceso a sistemas intermedios en DMZ, comunicacións seguras con centros de supervisión, conexión con servizos corporativos distribuídos ou intercambio controlado de información entre instalacións.

Observacións / medidas compensatorias asociadas: En contornos industriais, as VPN e comunicacións seguras deben concibirse como unha capa de protección das conexións, non como un permiso amplo de acceso á rede OT. A súa utilidade aumenta cando se combinan con segmentación, MFA, servidores de salto, control de sesións e permisos limitados. Tamén poden actuar como medida compensatoria cando é necesario manter acceso remoto por razóns operativas, sempre que a exposición quede acoutada e gobernada de forma estrita.

5.4.6 Proxy

Categoría: Defensa perimetral e segmentación

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: O proxy é un mecanismo intermediario que xestiona, filtra, media ou encapsula as comunicacións entre un cliente e un servizo de destino, evitando que ámbalas dúas partes se conecten de forma directa. A súa función pode orientarse á navegación web, ao acceso a determinados servizos, á publicación controlada de aplicacións, á transferencia de contidos ou á inspección e rexistro de tráfico. En contornos industriais, o seu papel adoita estar asociado á canalización segura de determinados fluxos entre dominios, ao control de acceso a servizos compartidos, á

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

limitación de exposición de sistemas internos e á mediación en intercambios que non deben realizarse de maneira directa entre a rede corporativa, a DMZ e a rede OT.

Obxectivo: Reducir a exposición directa entre sistemas ou redes, introducir un punto intermedio de control sobre as comunicacións e reforzar a capacidade de filtrado, rexistro e mediación do tráfico. No ámbito industrial, o seu obxectivo inclúe tamén canalizar determinados fluxos necesarios para a operación ou integración sen abrir conexións directas innecesarias cara a activos sensibles.

Como funciona / como se implanta: A súa implantación consiste en situar un servizo intermediario entre o orixe e o destino dunha comunicación, de maneira que o acceso real ao recurso se realice a través do proxy e baixo condicións definidas. Segundo o caso, o proxy pode actuar como mecanismo de saída controlada cara a servizos externos, como intermediario para acceso a aplicacións internas, como compoñente de publicación en DMZ ou como elemento de control sobre certos protocolos e contidos. En contornos industriais, a súa configuración debe responder a necesidades concretas e xustificadas, por exemplo para canalizar acceso a servizos compartidos, centralizar saídas controladas, limitar a exposición de aplicacións ou introducir trazabilidade adicional sobre determinados fluxos. A súa utilidade depende do deseño arquitectónico no que se insira, das regras de acceso definidas e da súa integración con outros controis perimetrais e de identidade.

Vantaxes:

- Evita conexións directas innecesarias entre sistemas ou dominios.
- Introduce un punto adicional de control, filtrado e rexistro.
- Pode limitar a exposición de aplicacións e servizos internos.
- Resulta útil para canalizar acceso a recursos compartidos ou saídas controladas.
- Reforza a trazabilidade de certas comunicacións cando se integra con políticas e autenticación adecuadas.

Limitacións e consideracións:

- O seu valor depende de que o fluxo intermediado estea realmente xustificado e ben gobernado.
- Non substitúe a segmentación, os firewalls nin a xestión de accesos.
- En contornos industriais, non todos os protocolos ou patróns de comunicación son compatibles cun esquema proxy convencional.

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

- Pode introducir complexidade adicional de operación, mantemento e resolución de incidencias.
- Debe evitarse que se converta nunha excepción permanente que acabe ampliando a exposición do entorno en lugar de reducila.

Relación con outros controis: Relaciónase coa DMZ industrial, co firewall, co NGFW/UTM, coa segmentación de rede e separación IT/OT, co acceso remoto seguro, coa xestión de identidades e accesos, coa monitorización e coas medidas compensatorias orientadas a limitar a exposición directa de servizos e aplicacións.

Casos habituais de uso: Emprégase para canalizar saídas controladas cara a servizos externos, limitar a exposición de aplicacións internas, mediar no acceso a servizos compartidos entre dominios, introducir control adicional sobre navegación ou transferencia de contidos, e como parte dunha arquitectura máis ampla de interconexión segura entre contornos con distinta criticidade.

Observacións / medidas compensatorias asociadas: En contornos industriais, o proxy pode resultar útil como medida compensatoria cando é necesario manter determinados intercambios entre redes ou servizos, pero non é aceptable unha conexión directa entre os sistemas implicados. Neses casos, a súa utilidade aumenta cando se combina con DMZ, autenticación forte, rexistro detallado e políticas restritivas de acceso e uso.

5.4.7 WAF

Categoría: Defensa perimetral e segmentación

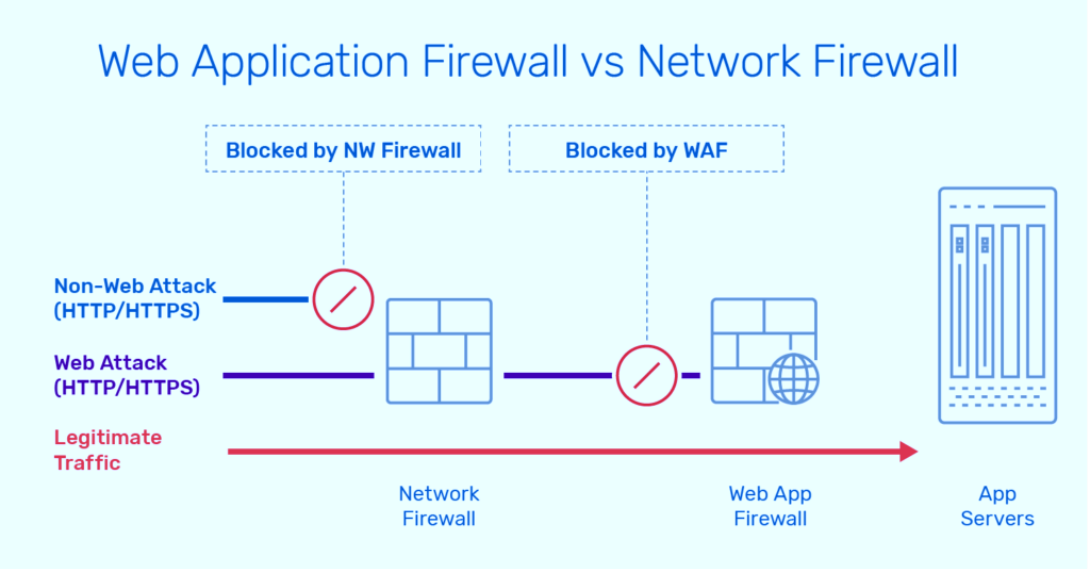
Tipoloxía: Técnico

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: O WAF (*Web Application Firewall*) é un control de seguridade deseñado para protexer aplicacións e servizos web fronte a peticións maliciosas, explotación de vulnerabilidades comúns e usos non autorizados da capa de aplicación. A diferenza do firewall tradicional, que actúa principalmente sobre IP, portos e protocolos, o WAF analiza o tráfico HTTP/HTTPS e aplica regras específicas sobre o comportamento esperado das aplicacións, os parámetros intercambiados e os patróns de ataque coñecidos. En contornos industriais, a súa relevancia aparece cando existen portais web, aplicacións de xestión, APIs, servizos de acceso remoto vía web, paneis de supervisión publicados ou compoñentes de integración accesibles mediante tecnoloxías web.

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



Función do WAF fronte ó firewall clásico. Fonte: A10 Networks (n.d.)

Obxectivo: Reducir o risco de explotación de vulnerabilidades en aplicacións e servizos web, limitando peticións maliciosas, usos indebidos e patróns de ataque orientados á capa de aplicación. No ámbito industrial, o seu obxectivo inclúe tamén protexer servizos web vinculados á operación, á supervisión, á integración de datos ou á interacción con terceiros, evitando que unha exposición web se converta nun vector de acceso cara a sistemas máis sensibles.

Como funciona / como se implanta: A súa implantación consiste en situar o WAF diante da aplicación ou servizo web que se desexa protexer, de maneira que todo o tráfico pase por el antes de chegar ao destino final. A partir desa posición, o WAF pode aplicar políticas de filtrado, detección de patróns de ataque, validación de solicitudes, limitación de certos comportamentos e rexistro de eventos. En contornos industriais, a súa configuración debe partir dun coñecemento claro dos servizos publicados, dos fluxos lexítimos, dos usuarios autorizados e das integracións necesarias, evitando bloqueos indebidos sobre funcionalidades críticas. O seu valor é maior cando forma parte dunha arquitectura segura de publicación de servizos, integrada con segmentación, DMZ, autenticación forte, rexistro e revisión periódica de regras.

Vantaxes:

- Engade unha capa específica de protección sobre aplicacións e servizos web.
- Axuda a limitar explotacións comúns da capa de aplicación.
- Mellora a visibilidade e o rexistro sobre interaccións con servizos publicados.

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

- Resulta útil para reducir a exposición de portais, APIs e compoñentes web con acceso externo ou interdominio.
- Pode complementar outros controis perimetrais cando existen servizos publicados necesarios para a operación ou a xestión.

Limitacións e consideracións:

- Só resulta aplicable cando existen aplicacións ou servizos baseados en tecnoloxías web.
- Non substitúe a seguridade no desenvolvemento, a revisión de código nin a corrección das vulnerabilidades da aplicación.
- Unha configuración insuficiente ou demasiado xenérica pode reducir a súa eficacia real.
- En contornos industriais, debe evitarse publicar servizos web sen unha revisión previa da súa necesidade, criticidade e arquitectura de protección.
- Require mantemento de políticas, análise de eventos e adaptación a cambios funcionais da aplicación protexida.

Relación con outros controis: Relaciónase co firewall, co NGFW/UTM, coa DMZ industrial, coa segmentación de rede, co acceso remoto seguro, coa xestión de identidades e accesos, co DevSecOps, co DAST, co RASP, coa monitorización e coas medidas compensatorias orientadas a limitar exposición de aplicacións publicadas.

Casos habituais de uso: Emprégase para protexer portais de xestión, aplicacións corporativas accesibles dende rede externa, servizos web publicados en DMZ, APIs de integración, interfaces web de supervisión ou mantemento e outros compoñentes expostos a través de HTTP/HTTPS que, sen seren necesariamente nucleares na operación, poden funcionar como punto de entrada cara a dominios máis sensibles.

Observacións / medidas compensatorias asociadas: En contornos industriais, o WAF pode actuar como medida compensatoria útil cando existe un servizo web que debe permanecer accesible incluso públicamente, pero non é viable corrixir de inmediato todas as súas debilidades ou redeseñar a súa arquitectura. A súa utilidade aumenta cando se combina con publicación en DMZ, autenticación reforzada, segmentación, rexistro detallado e revisión continua da superficie de exposición da aplicación.

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

5.4.8 ZTNA

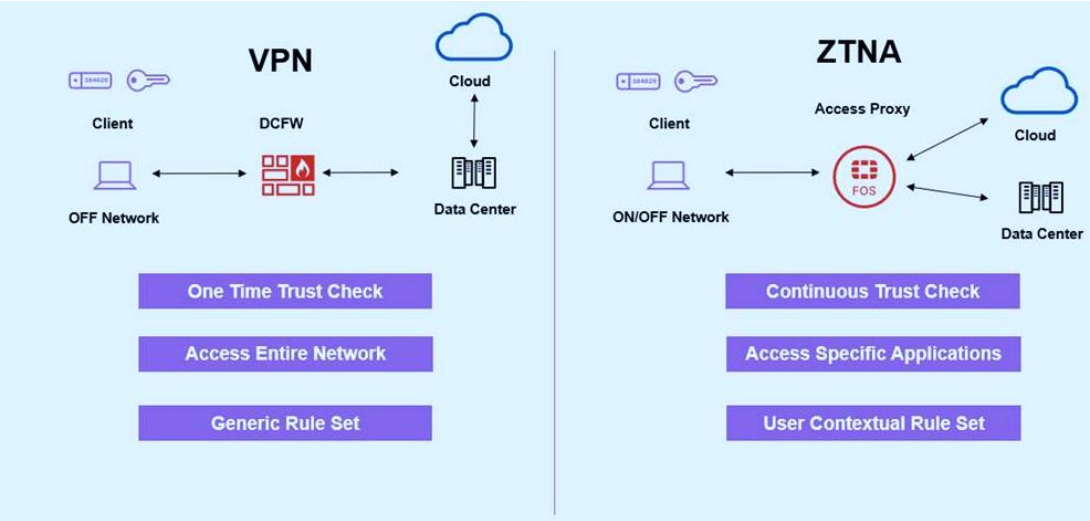
Categoría: Defensa perimetral e segmentación

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: O ZTNA (*Zero Trust Network Access*) é un modelo de acceso que substitúe a confianza implícita nas conexións pola verificación continua da identidade, do contexto (aplicación e dispositivo) e dos permisos antes de permitir a interacción cun recurso concreto. A súa lóxica non se basea en conceder acceso amplo a unha rede por estar "dentro" dela ou por conectarse a través dun túnel seguro, senón en habilitar un acceso granular, condicionado e limitado ao servizo ou activo especificamente autorizado. En contornos industriais, este enfoque resulta especialmente relevante cando existen accesos remotos, interacción con terceiros, mantemento distribuído, integración de servizos ou necesidade de limitar de forma máis estrita o alcance das conexións cara a sistemas sensibles.



Diferencias de VPN tradicional fronte a enfoque ZTNA. Fonte: Fortinet (2022)

Obxectivo: Reducir a exposición derivada do acceso remoto ou interdominio, evitando permisos excesivos e limitando cada conexión ao recurso concreto, ao contexto autorizado e ao perfil correspondente. No ámbito industrial, o seu obxectivo inclúe tamén minimizar o risco de que un acceso lexítimo se converta nunha vía de movemento lateral, exploración de rede ou compromiso de activos OT de alta criticidade.

Como funciona / como se implanta: A súa implantación baséase en validar de maneira explícita a identidade do usuario ou sistema, o dispositivo dende o que se conecta, o

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

contexto da sesión, os factores adicionais de autenticación e os permisos concretos que lle corresponden. A partir desa validación, o acceso concédese só ao recurso autorizado, sen expoñer a totalidade da rede nin habilitar visibilidade innecesaria sobre outros sistemas. En contornos industriais, o ZTNA adoita aplicarse a acceso remoto de persoal técnico, integradores, mantemento, provedores ou usuarios que precisan chegar a servizos concretos de forma puntual e controlada. A súa eficacia aumenta cando se integra con MFA, PAM, servidores de salto, segmentación, rexistro de sesións, revisión de accesos e políticas de mínimo privilexio. O seu despregue require coñecer con claridade que recursos deben ser accesibles, por quen, en que condicións e durante canto tempo.

Vantaxes:

- Reduce a confianza implícita e limita o acceso ao estritamente necesario.
- Evita expoñer segmentos completos da rede a usuarios ou terceiros que só precisan un recurso concreto.
- Dificulta o movemento lateral e a exploración innecesaria do entorno.
- Mellora o control contextual do acceso remoto e interdominio.
- Complementa de maneira eficaz a segmentación, o PAM e a trazabilidade de sesións.

Limitacións e consideracións:

- Require unha definición precisa de identidades, recursos, fluxos autorizados e políticas de acceso.
- Pode resultar complexo en contornos con arquitectura pouco documentada ou con moitas excepcións históricas.
- En contornos industriais, a súa implantación debe respectar a dispoñibilidade, os requisitos de mantemento e a compatibilidade cos procedementos operativos reais.
- Non substitúe a segmentación da rede nin a protección dos activos unha vez concedido o acceso.
- O seu valor diminúe se se configura con permisos excesivos, regras amplas ou excepcións permanentes mal gobernadas.

Relación con outros controis: Relaciónase co acceso remoto seguro, co firewall, co NGFW/UTM, coa segmentación de rede e separación IT/OT, coa DMZ industrial, coa

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

xestión de identidades e accesos, co PAM, cos servidores de salto, coa monitorización e coas medidas compensatorias destinadas a limitar o alcance do acceso de terceiros e usuarios con privilexios.

Casos habituais de uso: Emprégase para acceso remoto de mantemento, intervención de terceiros, conexión puntual a servidores ou aplicacións concretas, protección de servizos publicados a usuarios internos ou externos, control de acceso a contornos intermedios en DMZ e substitución progresiva de esquemas tradicionais de acceso remoto baseados en VPN amplas ou excesivamente permisivas.

Observacións / medidas compensatorias asociadas: En contornos industriais, o ZTNA pode actuar como medida compensatoria moi útil cando existe a necesidade de manter acceso remoto a determinados sistemas, pero non resulta aceptable abrir conectividade ampla cara á rede OT. A súa utilidade aumenta cando se combina con MFA, PAM, segmentación, rexistro de sesións e revisión periódica de permisos, reducindo o alcance efectivo de cada acceso ao mínimo imprescindible.

5.4.9 NAC

Categoría: Defensa perimetral e segmentación

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

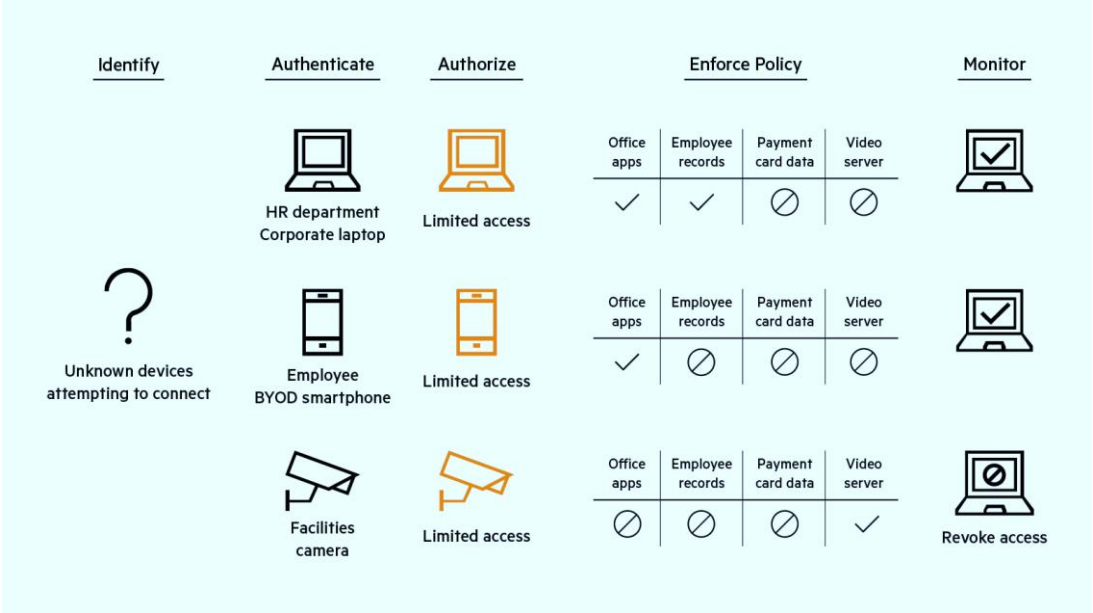
Descrición: O NAC (*Network Access Control*) é un conxunto de mecanismos destinados a identificar, autenticar, avaliar e controlar os dispositivos que pretenden conectarse a unha rede, aplicando políticas de acceso en función da súa identidade, estado, localización, tipo ou nivel de confianza. A súa función principal consiste en evitar que equipos non autorizados, mal configurados ou insuficientemente gobernados poidan incorporarse libremente ao entorno tecnolóxico. En contornos industriais, este control resulta especialmente relevante porque a incorporación de portátiles de mantemento, equipos de terceiros, dispositivos móbiles, compoñentes IIoT ou activos non inventariados pode converterse nun vector de acceso ou propagación con impacto operativo considerable.

Obxectivo: Reducir o risco de conexión non autorizada á rede, limitando o acceso de dispositivos a aqueles recursos, segmentos ou servizos que lles correspondan segundo a súa función e nivel de confianza. No ámbito industrial, o seu obxectivo inclúe tamén impedir que un equipo alleo, comprometido ou non validado poida acceder a zonas

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

operativas sensibles ou establecer conectividade directa con activos OT sen control previo.

Como funciona / como se implanta: A súa implantación baséase na definición de políticas que condicionan o acceso á rede á identificación do dispositivo, do usuario asociado, do punto de conexión, do perfil permitido e, cando procede, do estado de cumprimento de certos requisitos mínimos.



Exemplos de aplicación de NAC. Fonte: HPE (2025)

Segundo a arquitectura, o NAC pode actuar en portos de acceso, redes inalámbricas, segmentos corporativos, contornos mixtos ou puntos de conexión de terceiros. En contornos industriais, a súa implantación debe realizarse con especial cautela, xa que non todos os dispositivos OT admiten os mesmos métodos de autenticación ou comprobación de postura que un endpoint corporativo. Por iso, adoita ser máis eficaz cando se orienta a controlar os puntos de entrada de equipos externos, portátiles de mantemento, dispositivos non xestionados e zonas de converxencia IT/OT, combinándose con inventario de activos, segmentación, listas de autorización e procedementos de validación previa.

Vantaxes:

- Limita a incorporación non controlada de dispositivos á rede.
- Mellora a visibilidade sobre que equipos se conectan, dende onde e en que condicións.
- Axuda a reforzar a segmentación e a aplicación de políticas de acceso á rede.

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

- Resulta especialmente útil para controlar equipos de terceiros, portátiles de mantemento e dispositivos non xestionados.
- Reduce a probabilidade de que un acceso físico ou local se traduza automaticamente en conectividade lóxica ampla.

Limitacións e consideracións:

- A súa implantación pode ser complexa en contornos con activos legados, equipos propietarios ou infraestrutura pouco documentada.
- Non todos os dispositivos industriais soportan mecanismos estándar de autenticación ou avaliación de postura.
- Debe evitarse que a política de control de acceso interfira con comunicacións críticas ou co funcionamento normal da operación.
- Non substitúe a segmentación, o control de identidades, a monitorización nin a revisión de dispositivos externos.
- Requírese unha gobernanza clara das excepcións, dos perfís autorizados e dos procedementos de conexión temporal ou de emerxencia.

Relación con outros controis: Relaciónase coa segmentación de rede e separación IT/OT, co firewall, co acceso remoto seguro, coa xestión de identidades e accesos, coa protección de endpoints industriais, coa conexión segura de dispositivos externos, coa monitorización de activos e comunicacións OT e coas medidas compensatorias destinadas a limitar exposición de puntos de acceso físicos ou lóxicos.

Casos habituais de uso: Emprégase para controlar a conexión de portátiles de mantemento, equipos de integradores, dispositivos móbiles, puntos de acceso inalámbricos, compoñentes IIoT, redes de apoio en planta, zonas de converxencia entre IT e OT e contornos nos que se necesita evitar que a simple conexión física a un porto ou rede implique acceso amplo ao entorno.

Observacións / medidas compensatorias asociadas: En contornos industriais, o NAC resulta especialmente útil como medida compensatoria cando existe risco elevado de conexión de dispositivos externos ou non inventariados e non é viable actuar de inmediato sobre toda a arquitectura. A súa utilidade aumenta cando se combina con segmentación, listas de autorización, procedementos de validación previa, trazabilidade de conexións e control reforzado sobre equipos de terceiros e portátiles de mantemento.

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

5.4.10 CASB / SASE

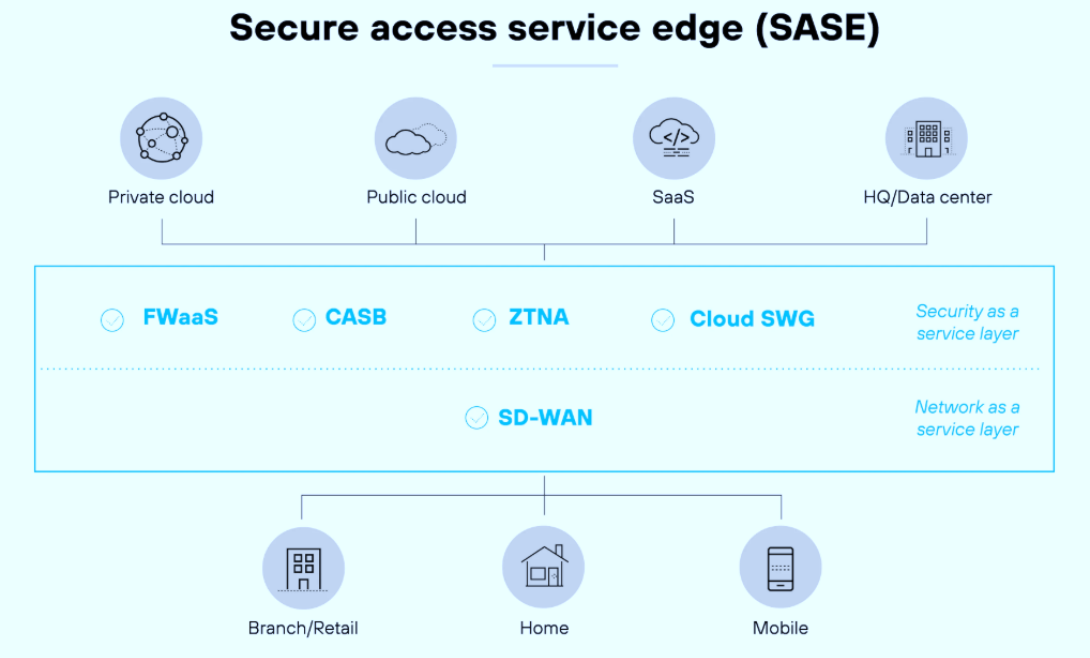
Categoría: Defensa perimetral e segmentación

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: O CASB (*Cloud Access Security Broker*) e o SASE (*Secure Access Service Edge*) son enfoques e capacidades orientados a controlar, protexer e supervisar o acceso a servizos, aplicacións e recursos distribuídos, especialmente cando estes se atopan fóra do perímetro clásico da organización ou combinan compoñentes locais, cloud e acceso remoto. O CASB céntrase principalmente na visibilidade, control e protección do uso de aplicacións e servizos cloud, mentres que o SASE integra nun modelo máis amplo capacidades de conectividade e seguridade como acceso seguro, filtrado, inspección, políticas contextuais e segmentación de acceso. En contornos industriais, estas capacidades cobran relevancia cando existen plataformas cloud de xestión, supervisión remota, analítica, colaboración, servizos distribuídos ou interacción frecuente entre usuarios, dispositivos e recursos situados en contornos mixtos.



Compoñentes da solución SASE. Fonte: Palo Alto Networks (n.d.)

Obxectivo: Reducir o risco asociado ao uso de servizos cloud, accesos distribuídos e modelos de conectividade máis descentralizados, garantindo que o acceso a recursos e aplicacións se realice baixo políticas de seguridade coherentes, con visibilidade suficiente e con control sobre usuarios, dispositivos, datos e sesións. No ámbito

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

industrial, o seu obxectivo inclúe tamén evitar que a adopción de servizos externos ou modelos híbridos introduza exposicións non gobernadas cara a sistemas ou información con impacto operativo.

Como funciona / como se implanta: A súa implantación parte da identificación dos servizos e fluxos que se desexa controlar: aplicacións cloud autorizadas, acceso remoto a recursos corporativos ou operativos, transferencia de datos, interacción entre usuarios distribuídos, publicación de servizos e conexión entre sedes ou dispositivos. A partir desa base, defínense políticas de acceso, inspección, rexistro, autenticación, avaliación contextual e protección de datos que se aplican sobre esas interaccións. En contornos industriais, estas capacidades adoitan ter sentido cando existe integración con plataformas cloud, servizos de soporte remoto, analítica centralizada, xestión distribuída ou modelos nos que a simple protección perimetral xa non resulta suficiente. A súa utilidade depende de que se implanten sobre fluxos reais e xustificados, e de que se integren con identidade, segmentación, MFA, trazabilidade e revisión continua do alcance permitido.

Vantaxes:

- Melloran a visibilidade sobre o uso de servizos cloud e accesos distribuídos.
- Permiten aplicar políticas de seguridade máis coherentes en contornos híbridos.
- Reforzan o control contextual de usuarios, dispositivos, sesións e datos.
- Resultan útiles cando a organización depende de servizos externos, acceso remoto ou conectividade máis descentralizada.
- Complementan a evolución dende o perímetro clásico cara a modelos de acceso máis segmentados e verificables.

Limitacións e consideracións:

- A súa utilidade é reducida se a organización non fai uso relevante de servizos cloud ou conectividade distribuída.
- En contornos industriais, deben implantarse con cautela para evitar dependencias excesivas de modelos non compatibles coa operación crítica.
- Non substitúen a segmentación OT, a DMZ industrial nin o control directo sobre activos de planta.
- Poden introducir complexidade adicional de integración, gobernanza e análise de políticas.

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

- Deben evitarse despregues motivados só por tendencia tecnolóxica, sen unha necesidade real e ben delimitada no contexto da organización.

Relación con outros controis: Relaciónanse co firewall, co NGFW/UTM, co proxy, co ZTNA, co acceso remoto seguro, coa xestión de identidades e accesos, co PAM, coa segmentación, coa protección de aplicacións SaaS, coa monitorización e coas medidas compensatorias orientadas a controlar fluxos externos e acceso a servizos distribuídos.

Casos habituais de uso: Empréganse en organizacións con uso significativo de aplicacións cloud, servizos de analítica ou xestión distribuída, acceso remoto frecuente a recursos corporativos, colaboración con terceiros mediante plataformas externas, publicación controlada de servizos e escenarios nos que a seguridade debe acompañar un modelo de conectividade menos centrado no perímetro clásico.

Observacións / medidas compensatorias asociadas: En contornos industriais, CASB e SASE deben interpretarse como capacidades complementarias para gobernar mellor contornos híbridos e servizos distribuídos, e non como substitutos das medidas básicas de separación e protección da rede OT. A súa utilidade aumenta cando a organización xa ten unha dependencia real de cloud, acceso remoto ou servizos externos, e cando se combinan con identidade forte, segmentación, control de sesións e limitación explícita do acceso a recursos sensibles.

5.5 Detección de ameazas e protección activa

Nun contexto no que a prevención absoluta non existe, as organizacións precisan capacidades que lles permitan identificar actividade anómala, detectar comportamentos hostís e actuar antes de que o impacto escale. Este bloque reúne **tecnoloxías e servizos orientados á detección temperá, á resposta automatizada ou asistida e á protección activa fronte a ameazas que afectan tanto aos activos corporativos como aos compoñentes propios dos contornos industriais**.

5.5.1 IDS / IPS

Categoría: Detección de ameazas e protección activa

Tipoloxía: Técnico / mixto

Función defensiva predominante: Detectivo

Función no NIST CSF: Detect, Respond

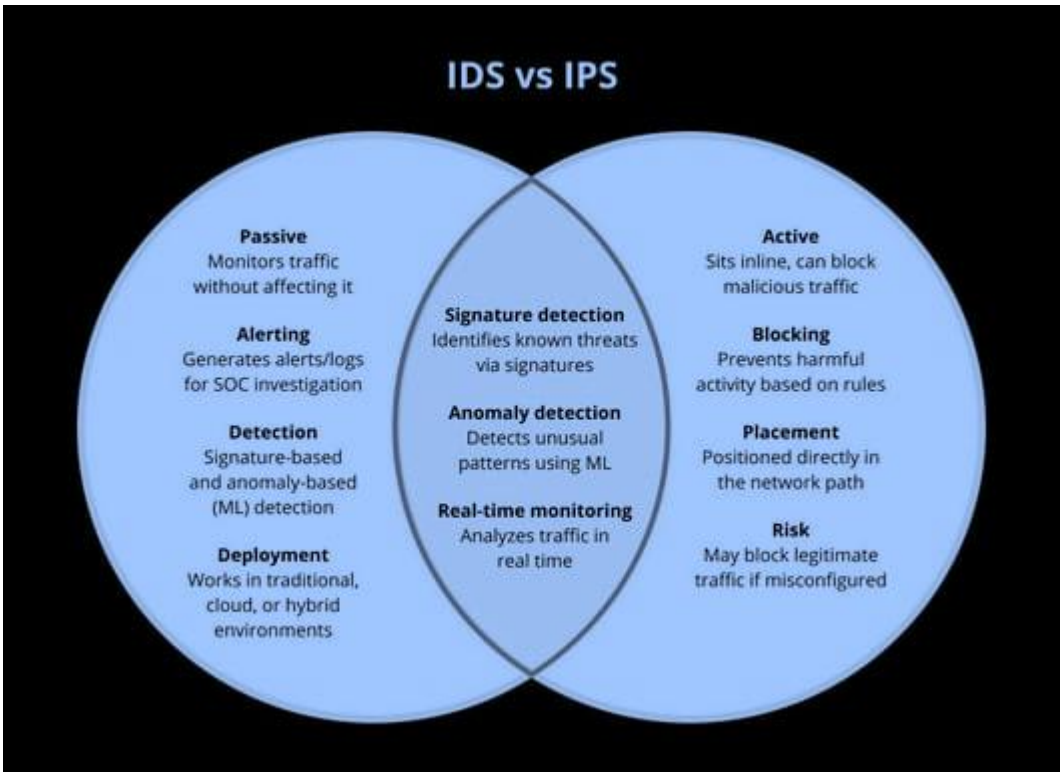
Descrición: Os sistemas IDS (*Intrusion Detection System*) e IPS (*Intrusion Prevention System*) son mecanismos orientados á identificación —e, no caso do IPS, tamén ao

bloqueo ou contención— de tráficos, patróns ou comportamentos que poden indicar intentos de intrusión, explotación de vulnerabilidades, movemento lateral ou uso indebido da rede. A súa lóxica baséase na análise do tráfico e dos eventos que circulan por determinados puntos da infraestrutura, contrastándoos con regras, firmas, patróns de comportamento ou indicadores coñecidos. En contornos industriais, este tipo de control resulta especialmente útil para mellorar a visibilidade sobre a actividade de rede e detectar comunicacións anómalas, accesos non previstos ou interaccións improcedentes entre activos con distinta criticidade.

Obxectivo: Incrementar a capacidade da organización para identificar sinais de compromiso, actividades maliciosas ou comportamentos anómalos na rede, e en determinados casos bloquear ou limitar a súa progresión. No ámbito industrial, o seu obxectivo inclúe tamén detectar interaccións indebidas sobre protocolos, servizos ou activos OT sen introducir un impacto operativo incompatible coa continuidade e estabilidade do proceso.

Como funciona / como se implanta: A súa implantación consiste en situar sensores ou compoñentes de inspección en puntos relevantes da arquitectura, como perímetros, segmentos internos, enlaces entre zonas, contornos de DMZ ou puntos de acceso remoto. Un IDS observa e analiza o tráfico sen intervir directamente sobre el, mentres que un IPS engade capacidade de resposta automática, bloqueando ou rexeitando determinadas comunicacións segundo as políticas configuradas. En contornos industriais, a elección entre un enfoque de detección pasiva ou un enfoque con capacidade preventiva activa debe facerse con especial prudencia, xa que un bloqueo inadecuado pode afectar á operación. Por iso, adoita ser recomendable comezar con configuracións de detección e alerta (fora de liña), validar o comportamento do sistema sobre os protocolos presentes e reservar as medidas de prevención automática para contornos nos que exista seguridade suficiente sobre o impacto de cada regra. A súa utilidade depende tamén da afinación das firmas, do coñecemento dos fluxos lexítimos e da integración cos procesos de análise e resposta.

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



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

Vantaxes:

- Melloran a visibilidade sobre a actividade da rede e os patróns de tráfico.
- Permiten identificar sinais de intrusión, explotación ou comportamento anómalo.
- Axudan a detectar interaccións non previstas entre zonas, servizos ou activos.
- Poden complementar a segmentación, o firewall e a monitorización de activos OT.
- Nun enfoque ben validado, os IPS poden contribuír a bloquear certos tráficos non autorizados ou maliciosos.

Limitacións e consideracións:

- A súa eficacia depende da calidade das regras, da afinación e do coñecemento do entorno.
- En contornos industriais, un IPS mal configurado pode introducir risco operativo por bloqueo indebido de comunicacións lexítimas.
- Non todos os protocolos industriais ou patróns de comunicación se interpretan ben con enfoques xenéricos baseados en sinaturas.

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

- Non substitúen a segmentación, o control de accesos, a xestión de vulnerabilidades nin a revisión da arquitectura.
- Poden xerar volume elevado de alertas se non existen procesos de análise, contextualización e resposta suficientes.

Relación con outros controis: Relaciónanse co firewall, co NGFW/UTM, coa segmentación de rede e separación IT/OT, coa DMZ industrial, co NDR, coa monitorización e operación de seguridade, coa visibilidade de activos e comunicacións OT, coa resposta ante incidentes e coas medidas compensatorias orientadas a reforzar a detección en activos con risco elevado.

Casos habituais de uso: Empréganse na supervisión de perímetros, enlaces entre IT e OT, zonas industriais internas, accesos remotos, servizos publicados, contornos con activos legados, redes con elevada criticidade ou escenarios nos que se necesita detectar interaccións indebidas, movemento lateral, escaneos, explotación de vulnerabilidades ou uso anómalo de protocolos e servizos.

Observacións / medidas compensatorias asociadas: En contornos industriais, os IDS resultan especialmente útiles como medida compensatoria cando non é viable modificar de inmediato a arquitectura, parchear determinados activos ou reducir toda a exposición existente. Os IPS, pola súa banda, poden achegar valor en segmentos concretos e ben coñecidos, sempre que a prevención automática estea validada e non comprometa a continuidade do proceso. En ambos os dous casos, a súa utilidade aumenta cando se integran con segmentación, visibilidade OT, correlación de eventos e procedementos claros de análise e resposta.

5.5.2 NDR

Categoría: Detección de ameazas e protección activa

Tipoloxía: Técnico / mixto

Función defensiva predominante: Detectivo

Función no NIST CSF: Detect

Descrición: O NDR (*Network Detection and Response*) é un conxunto de capacidades orientadas á observación, análise e contextualización do tráfico de rede co obxectivo de identificar comportamentos anómalos, indicios de compromiso, movemento lateral, uso indebido de protocolos, comunicacións non previstas ou interaccións sospeitosas entre activos. A diferenza doutros mecanismos máis baseados en sinaturas ou regras estáticas, o NDR adoita combinar visibilidade continua, análise de patróns, contextualización dos

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

fluxos e capacidade de investigación para ofrecer unha lectura máis rica da actividade real do entorno. En contornos industriais, este control resulta especialmente valioso porque permite mellorar a visibilidade sobre comunicacións IT/OT, protocolos industriais, activos de alta criticidade e relacións entre sistemas que non sempre están ben documentadas nin son facilmente observables por outros mecanismos.

Obxectivo: Incrementar a capacidade da organización para detectar sinais de compromiso, desviacións respecto do comportamento esperado e interaccións sospeitosas dentro da rede, reducindo o tempo necesario para identificar incidentes e mellorando a comprensión do seu alcance. No ámbito industrial, o seu obxectivo inclúe tamén detectar alteracións de comunicación, exploración de activos, movemento lateral e usos improcedentes de protocolos ou servizos que poidan afectar á operación ou aos sistemas OT.

Compoñentes dun NDR. Fonte: Trend Micro (n.d.)

Como funciona / como se implanta: A súa implantación baséase na recollida pasiva de tráfico ou metadatos en puntos relevantes da arquitectura, como perímetros, enlaces entre zonas, segmentos internos, contornos de DMZ ou zonas de converxencia IT/OT. A partir desa observación, o NDR analiza patróns de comunicación, relacións entre activos, frecuencia de fluxos, protocolos empregados, comportamentos habituais e desviacións respecto da normalidade esperada. En contornos industriais, a súa eficacia aumenta cando se adapta aos protocolos e patróns propios da rede OT, cando se integra cun inventario de activos e cando permite contextualizar alertas segundo a criticidade do sistema afectado e a función operativa implicada. O seu valor non reside só na xeración

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

de alertas, senón tamén na posibilidade de apoiar investigacións, validar hipóteses de incidente e achegar evidencia útil para resposta e contención.

Vantaxes:

- Mellora de forma significativa a visibilidade sobre a actividade real da rede.
- Permite detectar anomalías, movemento lateral e interaccións non previstas entre activos.
- Resulta especialmente útil en contornos con baixa visibilidade previa ou alta complexidade de fluxos.
- Achega contexto adicional sobre protocolos, relacións entre sistemas e comportamento habitual da rede.
- Complementa moi ben a segmentación, o firewall, os IDS/IPS e a monitorización OT.

Limitacións e consideracións:

- A súa eficacia depende da calidade da captura, da contextualización dos activos e da afinación do entorno.
- Pode xerar alertas pouco accionables se non existe coñecemento suficiente da arquitectura e dos fluxos lexítimos.
- En contornos industriais, o valor da análise diminúe se non se teñen en conta protocolos específicos, dependencias operativas e patróns propios do proceso.
- Non substitúe a segmentación, a xestión de accesos, a xestión de vulnerabilidades nin a resposta ante incidentes.
- Require integración con procesos de análise e investigación para converter a visibilidade en capacidade real de detección e resposta.

Relación con outros controis: Relaciónase cos IDS/IPS, co firewall, co NGFW/UTM, coa segmentación de rede e separación IT/OT, coa DMZ industrial, coa monitorización e operación de seguridade, coa visibilidade de activos e comunicacións OT, coa resposta ante incidentes e coas medidas compensatorias orientadas a reforzar detección e contextualización do risco.

Casos habituais de uso: Emprégase para supervisar enlaces entre IT e OT, detectar movemento lateral en redes industriais, observar protocolos e fluxos entre activos críticos, reforzar a visibilidade en contornos con activos legados, apoiar investigacións

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

tras alertas ou incidentes e mellorar a detección temperá de comportamentos non habituais en redes complexas ou pouco documentadas.

Observacións / medidas compensatorias asociadas: En contornos industriais, o NDR é especialmente útil como medida compensatoria cando non é viable reducir de inmediato toda a exposición arquitectónica, parchear activos sensibles ou modificar a segmentación existente. Neses casos, permite engadir unha capa de visibilidade e detección que axuda a identificar comportamentos anómalos, priorizar investigacións e mellorar a capacidade de resposta mentres non se acometen medidas estruturais máis profundas.

5.5.3 EDR

Categoría: Detección de ameazas e protección activa

Tipoloxía: Técnico / mixto

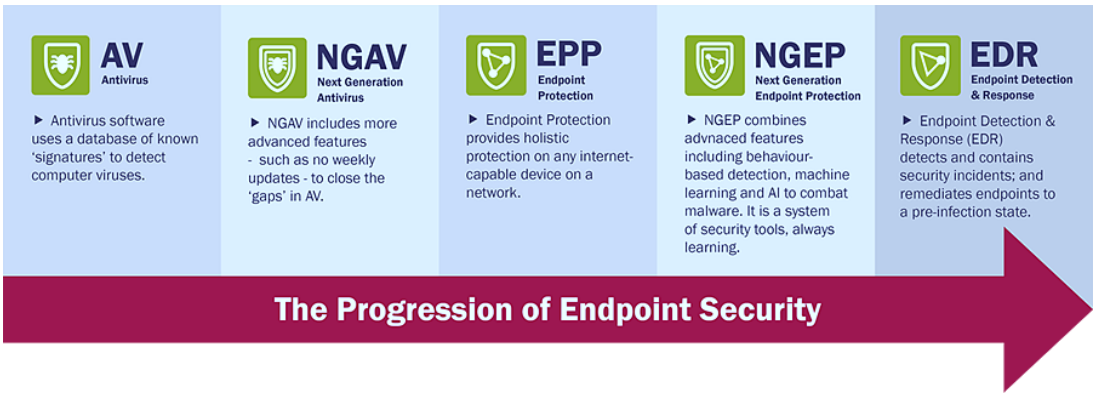
Función defensiva predominante: Detectivo

Función no NIST CSF: Detect, Respond

Descrición: O EDR (*Endpoint Detection and Response*) é un conxunto de capacidades orientadas á supervisión continua, detección, investigación e resposta sobre a actividade dos equipos finais, co obxectivo de identificar indicios de compromiso, comportamentos anómalos, execución de código malicioso, movemento lateral, abuso de credenciais ou manipulación de procesos e ficheiros. A diferenza dos mecanismos máis clásicos de protección de endpoint baseados principalmente en sinaturas, o EDR achega unha capa máis avanzada de telemetría, contexto e análise sobre o comportamento real dos dispositivos. En contornos industriais, a súa aplicabilidade depende do tipo de activo: pode resultar moi útil en estacións de traballo, portátiles de mantemento, servidores de apoio, HMI ou determinados sistemas Windows/Linux compatibles, aínda que non sempre será viable ou recomendable en controladores, sistemas moi sensibles ou activos legados con restricións estritas.

Obxectivo: Incrementar a capacidade da organización para detectar e investigar actividade maliciosa ou anómala nos equipos finais, mellorando a visibilidade sobre o comportamento dos endpoints e permitindo unha resposta máis rápida e contextualizada. No ámbito industrial, o seu obxectivo inclúe tamén reforzar a detección en activos con interacción directa ou indirecta co entorno OT, sen comprometer a dispoñibilidade nin a estabilidade dos sistemas máis sensibles.

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



Avance histórico das solucións de protección de endpoint. Fonte: cyberone.security (n.d.)

Como funciona / como se implanta: A súa implantación baséase normalmente na instalación dun axente no endpoint, capaz de recoller telemetría sobre procesos, execución, ficheiros, conexións, rexistro, actividade do usuario e outros eventos relevantes. Esa información analízase localmente ou nunha plataforma centralizada para detectar patróns maliciosos, correlacionar eventos e apoiar tarefas de investigación e resposta. En contornos industriais, a implantación debe partir dunha avaliación previa de compatibilidade e impacto, diferenciando con claridade entre activos nos que o uso dun axente é viable e beneficioso, e aqueles nos que pode introducir riscos de rendemento, estabilidade, soporte ou certificación. A súa utilidade aumenta cando se desprega en portátiles de mantemento, estacións de enxeñaría, HMI compatibles, servidores intermedios e outros sistemas con capacidade de execución xeralista, integrándose con procedementos de análise, revisión de alertas e contención.

Vantaxes:

- Mellora a visibilidade sobre o comportamento real dos equipos finais.
- Permite detectar execucións sospeitosas, abuso de procesos, persistencia e movemento lateral.
- Achega contexto útil para investigación, resposta e aprendizaxe tras incidentes.
- Resulta especialmente valioso en portátiles, estacións de traballo e servidores con maior exposición.
- Complementa outros controis de rede ao achegar detección dende o propio endpoint.

Limitacións e consideracións:

- Non todos os activos industriais admiten a instalación de axentes sen risco operativo.

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

- En contornos OT, a compatibilidade co software de fabricante, o rendemento e a estabilidade deben validarse previamente.
- Pode xerar volume elevado de telemetría e alertas se non existe capacidade suficiente de análise.
- Non substitúe o bastionado, a segmentación, a xestión de accesos nin a xestión de vulnerabilidades.
- Debe evitarse un despregue indiscriminado en activos críticos sen revisión previa de impacto e soporte.

Relación con outros controis: Relaciónase coa protección do posto de traballo, coa protección de endpoints industriais, co IDS/IPS, co NDR, coa monitorización e operación de seguridade, coa xestión de identidades e accesos, co hardening, coa conexión segura de dispositivos externos e coa resposta ante incidentes. Funciona como capa de detección e investigación especialmente útil en activos con sistema operativo xeralista e capacidade de execución avanzada.

Casos habituais de uso: Emprégase en portátiles de mantemento, estacións de enxeñaría, HMI compatibles, servidores de apoio á operación, servidores de salto, equipos corporativos con acceso a contornos OT, terminais con acceso remoto e activos nos que se precisa reforzar a detección de comportamento malicioso sen depender exclusivamente da rede.

Observacións / medidas compensatorias asociadas: En contornos industriais, o EDR pode actuar como medida compensatoria útil cando non é viable modificar de inmediato a arquitectura, reducir toda a exposición existente ou aplicar certas actualizacións, sempre que o activo sexa compatible e o impacto estea validado. A súa utilidade é especialmente alta en portátiles e estacións de enxeñaría, onde un compromiso pode servir como ponte entre dominios corporativos, terceiros e sistemas OT. Con todo, en activos críticos ou moi restrinxidos, poden ser preferibles enfoques complementarios de segmentación, monitorización pasiva e bastionado antes que un despregue directo do axente.

5.5.4 CPS PP

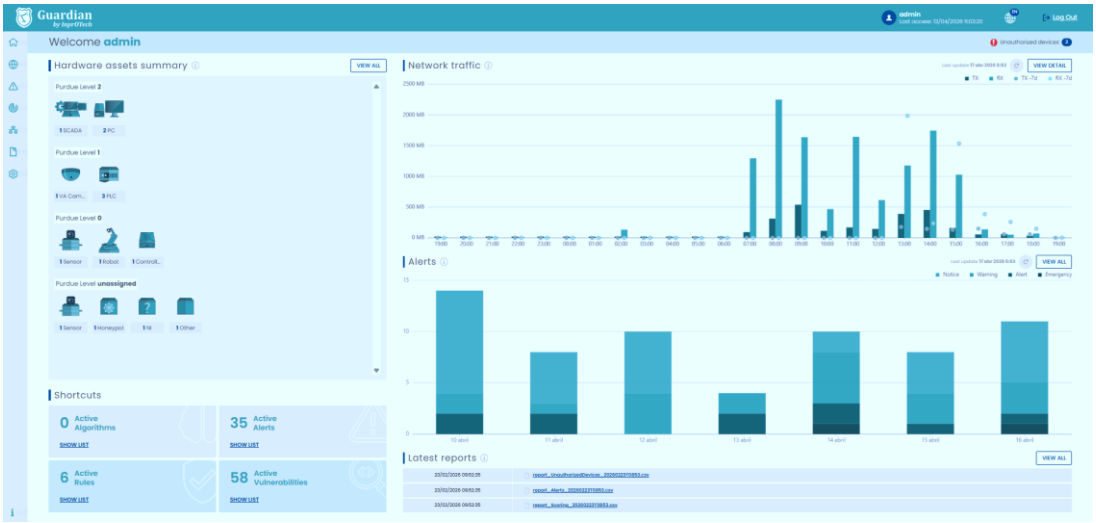
Categoría: Detección de ameazas e protección activa

Tipoloxía: Técnico / mixto

Función defensiva predominante: Detectivo

Función no NIST CSF: Identify, Detect, Protect, Respond

Descrición: As plataformas de protección de sistemas ciberfísicos (CPS PP, *Cyber-Physical Systems Protection Platform* segundo o termo acuñado por Gartner) son solucións orientadas a observar, correlacionar e contextualizar información procedente tanto da capa dixital como do comportamento físico do proceso, co fin de identificar desviacións, condicións anómalas ou sinais de compromiso que poderían non ser visibles dende unha monitorización puramente IT ou puramente OT. A súa lóxica consiste en combinar datos de rede, activos, protocolos, sinais de proceso, estados operativos, telemetría industrial e regras de comportamento esperado para ofrecer unha visión máis ampla do risco real sobre sistemas ciberfísicos. En contornos industriais, este control resulta especialmente valioso cando a detección debe ir máis aló da comunicación de rede e incorporar tamén o contexto funcional do proceso.



Exemplo de solución CPS PP. Fonte: InprOTech.es (2026)

Obxectivo: Incrementar a capacidade da organización para ganar visibilidade (inventario) detectar alteracións ou amenazas (anomalías ou vulnerabilidades) que poidan afectar á operación física, á integridade do proceso ou á seguridade dos sistemas ciberfísicos, combinando sinais técnicos e operativos nunha mesma capa de análise, ou incluso aportando capacidades de resposta. No ámbito industrial, o seu obxectivo inclúe tamén reducir o risco de que unha actividade aparentemente lexítima dende o punto de vista dixital pase inadvertida a pesar de estar producindo efectos anómalos sobre o proceso, os equipos ou as condicións de operación.

Como funciona / como se implanta: A súa implantación adoita basearse na recollida e correlación de datos procedentes de múltiples fontes: tráfico de rede, inventario de activos, protocolos industriais, estados de control, variables de proceso, eventos de sistemas, telemetría de sensores, sinais de supervisión e, cando procede, integración con plataformas de operación ou xestión. A partir desa información, a plataforma constrúe

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

unha visión do inventario, mapa de rede, comportamento esperado e detecta desviacións, inconsistencias, vulnerabilidaes, e condicións anómalas ou patróns sospeitosos que poden apuntar a un fallo, a un uso indebido ou a un incidente de seguridade. En contornos industriais, a súa utilidade depende de que se coñeza ben o proceso, de que a plataforma estea adaptada aos protocolos e activos presentes e de que exista capacidade para interpretar correctamente a diferenza entre unha anomalía técnica, unha variación operativa lexítima e un incidente potencialmente malicioso.

Vantaxes:

- Mellora a detección integrando contexto dixital e comportamento físico do proceso.
- Permite identificar dispositivos, vulnerabilidades, mapa de rede, problemas de segmentación, e desviacións que poden non ser visibles con controis baseados só en rede ou endpoint.
- Achega maior contexto para investigar incidentes con impacto operativo.
- Resulta especialmente útil en contornos críticos con forte dependencia do comportamento físico do proceso.
- Complementa outras capacidades de detección achegando unha visión máis próxima ao risco real sobre a operación, e ocasionalmente ofrecendo mecanismos de engano (honeypots).
- En ocasións, permiten resposta activa automática (bloqueo de tráfico malicioso).

Limitacións e consideracións:

- A súa eficacia depende da calidade e cobertura das fontes de datos integradas.
- Pode requirir coñecemento avanzado do proceso para interpretar correctamente alertas e desviacións.
- En contornos industriais, unha mala contextualización pode xerar falsos positivos ou lectura incorrecta de variacións operativas normais.
- Non substitúe a segmentación, a xestión de accesos, nin a protección básica da arquitectura.
- Require integración coas áreas de operación, mantemento e seguridade para converter a detección en resposta útil.

Relación con outros controis: Relaciónase co IDS/IPS, co NDR, coa monitorización ciberfísica / MES, coa visibilidade de activos e comunicacións OT, coa monitorización e

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

operación de seguridade, coa resposta ante incidentes e coas medidas compensatorias orientadas a reforzar detección e contextualización do risco sobre sistemas críticos.

Casos habituais de uso: Emprégase en contornos industriais que requiren controis esixidos por normativa, gañar visibilidade ou dotarse de detección de anomalías e correlación da actividade de rede co comportamento do proceso, detectar desviacións en sinais ou estados operativos, supervisar sistemas ciberfísicos críticos, apoiar investigacións sobre incidentes con impacto potencial na operación e reforzar a detección en instalacións con alta criticidade, automatización avanzada ou forte dependencia de variables físicas.

Observacións / medidas compensatorias asociadas: En contornos industriais, as plataformas CPS PP poden actuar como medida compensatoria especialmente útil cando non é viable reducir de inmediato toda a exposición da arquitectura ou actualizar determinados activos, xa que achegan unha capa adicional de observación centrada no comportamento real do sistema ciberfísico. A súa utilidade aumenta cando se combinan con segmentación, visibilidade OT, procedementos de resposta e coñecemento operativo suficiente para interpretar correctamente as anomalías detectadas.

5.5.5 Detección de integridade de ficheiros

Categoría: Detección de ameazas e protección activa

Tipoloxía: Técnico / mixto

Función defensiva predominante: Detectivo

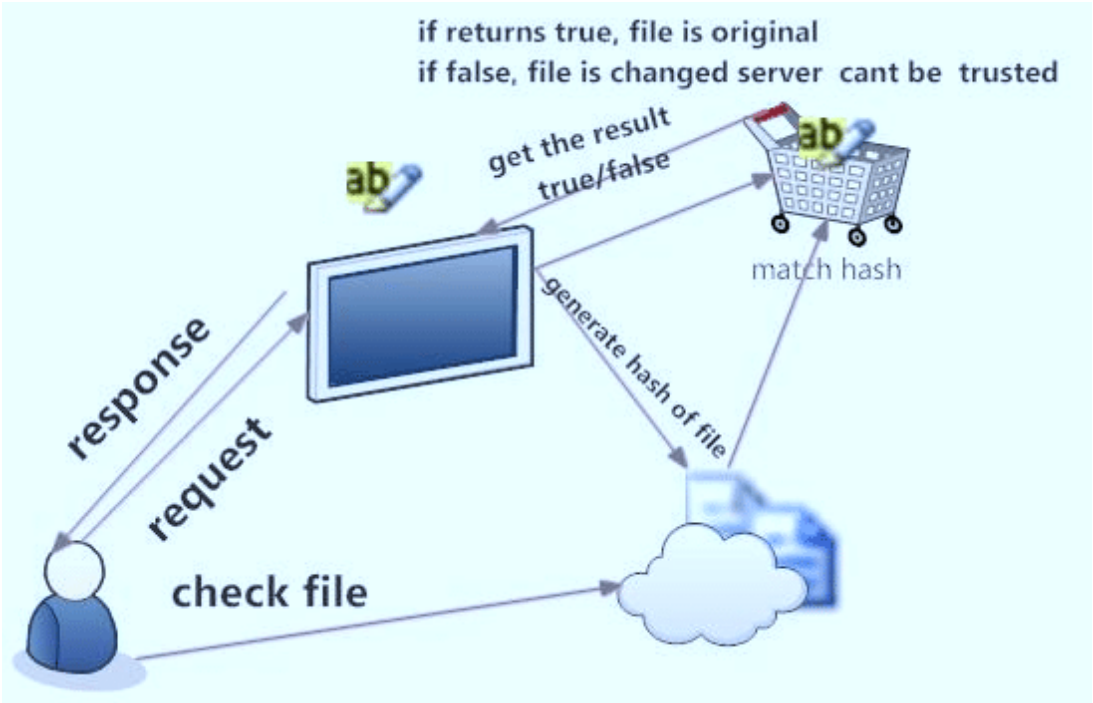
Función no NIST CSF: Detect, Respond

Descrición: A detección de integridade de ficheiros é un control orientado a identificar cambios non autorizados, inesperados ou anómalos en ficheiros, configuracións, executables, librarías, rexistros ou compoñentes críticos dun sistema. A súa lóxica baséase en establecer unha referencia coñecida do estado esperado de determinados elementos e supervisar posteriormente calquera modificación que poida indicar manipulación, persistencia maliciosa, erro operativo, instalación non controlada de software ou alteración indebida de parámetros. En contornos industriais, este control resulta especialmente útil en sistemas nos que a estabilidade e a previsibilidade son fundamentais, como HMI, estacións de enxeñaría, servidores de apoio, sistemas de supervisión ou outros activos con compoñentes críticos cuxo cambio debería estar estritamente controlado.

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

Obxectivo: Detectar modificacións non autorizadas en compoñentes clave do entorno tecnolóxico, mellorando a capacidade da organización para identificar manipulacións, compromisos, cambios non aprobados ou desviacións respecto do estado esperado dos sistemas. No ámbito industrial, o seu obxectivo inclúe tamén protexer configuracións, proxectos, ficheiros de operación e compoñentes software cuxo cambio pode ter impacto directo sobre a dispoñibilidade, a integridade do proceso ou a fiabilidade da operación.

Como funciona / como se implanta: A súa implantación adoita partir da identificación dos ficheiros, cartafoles, configuracións ou compoñentes que deben considerarse sensibles ou críticos. Unha vez definida esa base, establécese un estado de referencia mediante sumas de verificación, rexistros de versión, políticas de cambio ou outros mecanismos equivalentes. A partir dese momento, o sistema supervisa modificacións e xera alertas cando detecta cambios non previstos ou discrepancias respecto do estado autorizado. En contornos industriais, a súa aplicación debe centrarse especialmente en activos nos que o comportamento sexa relativamente estable e os cambios deban estar documentados, como estacións de enxeñaría, HMI, servidores de supervisión, repositorios de configuración, proxectos de automatización ou sistemas de apoio á operación. A súa utilidade aumenta cando se integra con procedementos formais de cambio, hardening, rexistro de intervencións e análise de alertas.



Mecanismo de verificación de integridade de ficheiros. Fonte: Sharma, Rajani & Kumar, Rajender (2014)

Vantaxes:

- Permite detectar manipulacións ou cambios non autorizados en compoñentes críticos.
- Mellora a trazabilidade sobre modificacións en sistemas estables ou sensibles.
- Resulta útil para identificar persistencia maliciosa, alteracións de configuración ou erros de operación.
- Reforza o control sobre activos nos que os cambios deben ser escasos e ben documentados.
- Complementa a monitorización de rede e de endpoint cunha visión centrada no estado interno dos sistemas.

Limitacións e consideracións:

- A súa eficacia depende da correcta definición do estado de referencia (e o almacenamento seguro do mesmo) e dos elementos a supervisar.
- Pode xerar ruído se se aplica a sistemas con cambios frecuentes ou pouco gobernados.
- En contornos industriais, debe coordinarse cos procedementos de mantemento e actualización para evitar falsos positivos constantes.
- Non substitúe o bastionado, o control de accesos nin a xestión formal de cambios.
- Requírese capacidade de análise para diferenciar entre modificacións autorizadas, erros operativos e incidentes reais.

Relación con outros controis: Relaciónase co EDR, co bastionado de HMI e sistemas de enxeñaría, coa xestión de cambios, coa monitorización e operación de seguridade, coa resposta ante incidentes, coas copias de seguridade e restauración e coas medidas compensatorias orientadas a reforzar o control sobre activos sensibles ou con soporte limitado.

Casos habituais de uso: Emprégase para supervisar HMI, estacións de enxeñaría, servidores de supervisión, proxectos de automatización, configuracións críticas, executables de aplicacións industriais, ficheiros de sistema, repositorios de receitas e outros compoñentes nos que calquera cambio non autorizado poida ter impacto relevante sobre a operación ou a seguridade.

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

Observacións / medidas compensatorias asociadas: En contornos industriais, a detección de integridade de ficheiros resulta especialmente útil como medida compensatoria cando non é viable actualizar de inmediato determinados sistemas ou reducir a exposición de certos activos, xa que permite engadir unha capa adicional de vixilancia sobre compoñentes críticos. A súa utilidade aumenta cando se combina con procedementos de cambio estritos, bastionado, rexistro de intervencións, copias de seguridade validadas e análise rápida das alertas xeradas.

5.5.6 DLP

Categoría: Detección de ameazas e protección activa

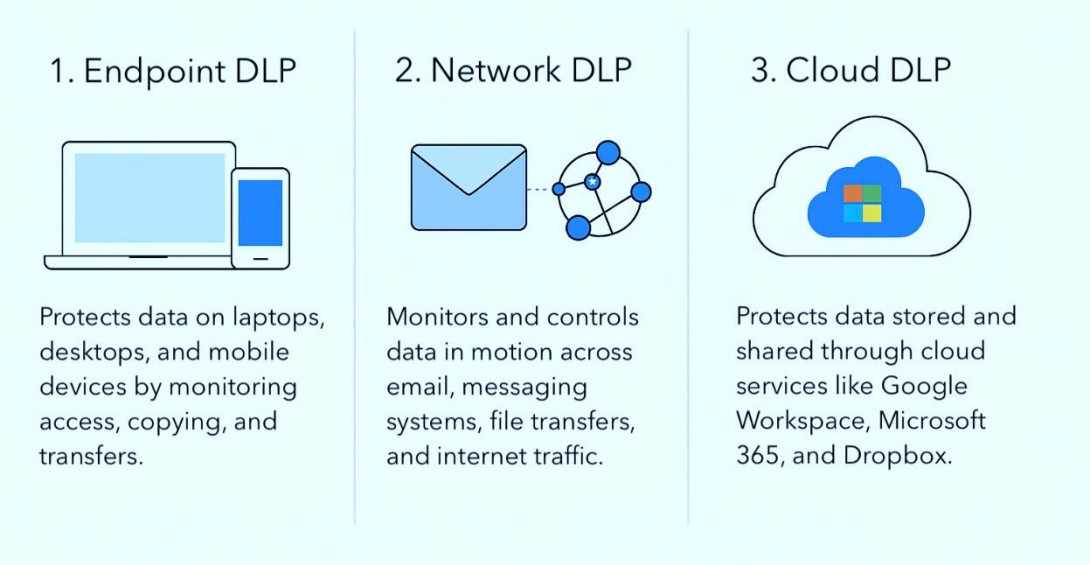
Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: O DLP (*Data Loss Prevention* ou prevención da fuga de datos) é un conxunto de capacidades orientadas a identificar, supervisar e limitar a saída, copia, transferencia ou uso non autorizado de información sensible. A súa finalidade é evitar que datos críticos abandonen a organización por canles non previstas, sen control suficiente ou en contextos de risco. En contornos industriais, este control non se limita á protección de información corporativa convencional, senón que pode abranguer tamén proxectos de automatización, configuracións de sistemas, receitas, parámetros de proceso, documentación técnica, credenciais, rexistros operativos e outro coñecemento sensible con impacto sobre a continuidade, a propiedade intelectual ou a seguridade da operación.

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



Tipos de DLP. Fonte: Lakera (2025)

Obxectivo: Reducir o risco de exfiltración, copia indebida, transferencia non autorizada ou exposición accidental de información sensible, reforzando o control sobre as canles de saída e os usos permitidos dos datos. No ámbito industrial, o seu obxectivo inclúe tamén protexer información técnica e operativa que, aínda sen ser sempre visible dende unha perspectiva puramente corporativa, pode resultar crítica para a continuidade do negocio, a competitividade ou a seguridade do proceso.

Como funciona / como se implanta: A súa implantación parte da identificación dos tipos de información que deben considerarse sensibles, das canles polas que poden circular e dos escenarios nos que existe maior risco de perda, exfiltración ou uso indebido. A partir desa base, poden aplicarse políticas de supervisión, clasificación, bloqueo, alerta ou restrición sobre correo electrónico, navegación, servizos cloud, impresión, copia a dispositivos externos, movemento de ficheiros, transferencia entre sistemas ou acceso dende determinados perfís. En contornos industriais, o DLP debe configurarse con especial criterio, evitando un enfoque excesivamente xenérico e centrando a protección na información que realmente ten valor operativo ou técnico: proxectos de enxeñaría, configuracións de control, receitas, documentación de fabricante, credenciais, exportación de datos históricos ou ficheiros empregados en mantemento e integración. A súa utilidade aumenta cando se integra con xestión de identidades, clasificación da información, protección de endpoints e procedementos operativos claros sobre uso e transferencia de datos.

Vantaxes:

- Axuda a limitar a fuga ou transferencia non autorizada de información sensible.

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

- Mellora a visibilidade sobre as canles de saída e os patróns de uso dos datos.
- Resulta útil para protexer propiedade intelectual, documentación técnica e información operativa crítica.
- Complementa outros controis de acceso, monitorización e protección de endpoint.
- Pode reforzar a trazabilidade e o control sobre soportes externos, correo, cloud e movemento de ficheiros.

Limitacións e consideracións:

- A súa eficacia depende de identificar correctamente que información debe protexerse e por que canles pode saír.
- Pode xerar ruído ou fricción operativa se as políticas son demasiado amplas ou pouco contextualizadas.
- En contornos industriais, unha mala definición do alcance pode deixar fóra información técnica crítica ou, ao contrario, bloquear fluxos necesarios para operación e mantemento.
- Non substitúe a clasificación da información, a xestión de accesos nin os procedementos de uso seguro dos datos.
- Require revisión periódica para adaptarse a cambios en procesos, aplicacións, servizos cloud, terceiras partes e necesidades de intercambio de información.

Relación con outros controis: Relaciónase coa seguridade no email, coa protección do posto de traballo, coa protección de endpoints industriais, coa conexión segura de dispositivos externos, coa xestión de identidades e accesos, co CASB / SASE, coa monitorización e operación de seguridade e cos procedementos operativos orientados a uso seguro da información sensible.

Casos habituais de uso: Emprégase para controlar a saída de documentación técnica, proxectos de automatización, receitas, exportación de datos históricos, envío de ficheiros por correo, copia a dispositivos USB, uso de servizos cloud, transferencia de información a terceiros e escenarios nos que existe risco de fuga de coñecemento técnico ou operativo con valor crítico para a organización.

Observacións / medidas compensatorias asociadas: En contornos industriais, o DLP resulta especialmente útil cando a organización manexa información técnica sensible con forte impacto sobre operación, propiedade intelectual ou seguridade do proceso.

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

Tamén pode actuar como medida compensatoria parcial cando non é viable restrinxir de inmediato todas as canles de intercambio con terceiros, sempre que se combine con clasificación da información, control de accesos, revisión de excepcións e procedementos claros sobre uso e transferencia de datos.

5.5.7 Honeypots

Categoría: Detección de ameazas e protección activa

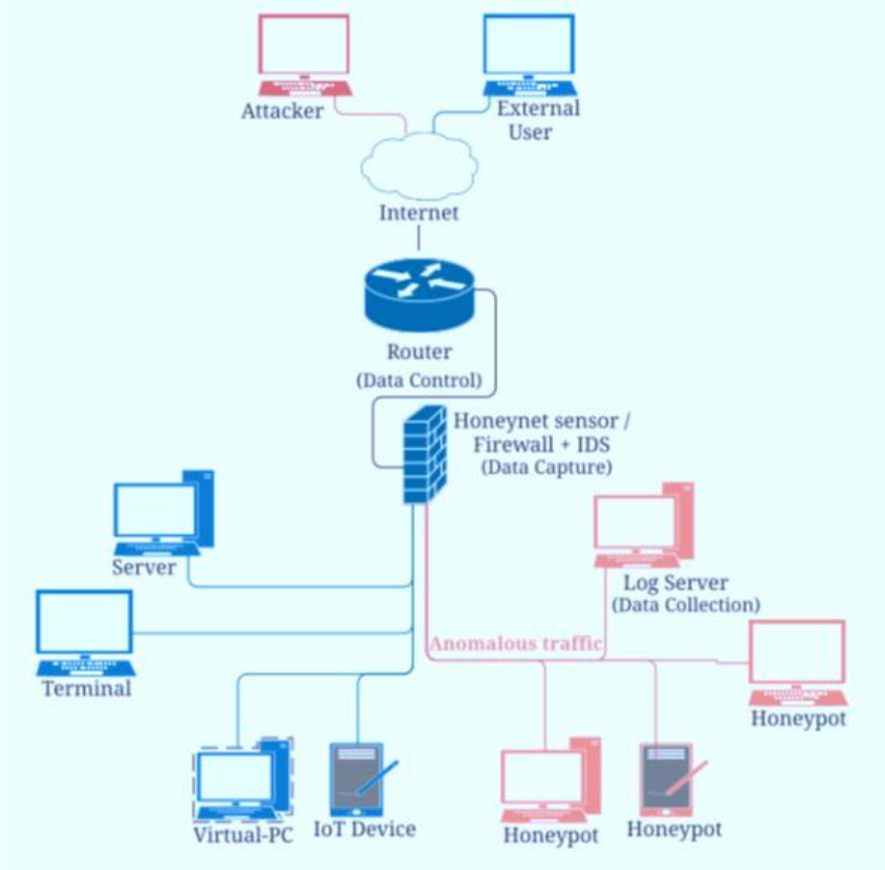
Tipoloxía: Técnico / mixto

Función defensiva predominante: Detectivo

Función no NIST CSF: Detect

Descrición: Os honeypots son sistemas, servizos ou compoñentes deliberadamente preparados para simular activos atractivos para un atacante, co obxectivo de observar, detectar e analizar interaccións maliciosas ou non autorizadas. A súa lóxica consiste en crear puntos controlados de cebo para cibercriminais que non deberían recibir actividade lexítima, polo que calquera conexión, intento de autenticación, exploración, execución de comandos ou manipulación pode interpretarse como indicio de comportamento sospeitoso. En contornos industriais, os honeypots poden deseñarse para representar activos, protocolos ou servizos próximos á realidade OT, permitindo identificar exploración de rede, actividade automatizada, movemento lateral, uso indebido de protocolos industriais ou tentativas de acceso non previstas.

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



Exemplo de ubicación de honeypot nunha rede OT. Fonte: InprOTech (2025)

Obxectivo: Mellorar a capacidade de detección temperá de actividade maliciosa, obtendo sinais de alerta de alta relevancia e información útil para análise, investigación e mellora da protección. No ámbito industrial, o seu obxectivo inclúe tamén captar interaccións anómalas dirixidas a contornos OT ou a servizos ciberfísicos, reforzando a visibilidade sobre ameazas que poderían pasar desapercibidas noutras capas de monitorización.

Como funciona / como se implanta: A súa implantación baséase na colocación de sistemas cebo en puntos seleccionados da arquitectura, configurados para aparentar ser activos ou servizos de interese sen formar parte da operación real. Estes compoñentes poden simular dende servizos sinxelos de rede ata protocolos industriais, interfaces de control, dispositivos aparentes ou contornos máis elaborados segundo o nivel de realismo buscado. En contornos industriais, a súa eficacia depende de que estean ben situados, de que resulten cribles no contexto da rede e de que a súa presenza non interfira co proceso nin xere confusión operativa. O valor do honeypot aumenta cando a información recollida se integra cos procesos de análise, co SOC, coa intelixencia de ameazas e cos mecanismos de resposta, permitindo contextualizar mellor os intentos detectados.

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

Vantaxes:

- Achegan sinais de alerta de alta calidade, xa que non deberían recibir tráfico lexítimo.
- Resultan útiles para detectar exploración, movemento lateral e actividade automatizada.
- Permiten obter información valiosa sobre patróns de ataque e comportamento adversario.
- Complementan a monitorización tradicional con puntos de observación específicos.
- Poden ser especialmente útiles en contornos OT para captar interaccións indebidas sobre protocolos ou servizos aparentes.

Limitacións e consideracións:

- O seu valor depende do deseño, da localización e do realismo do cebo.
- Non substitúen a segmentación, a xestión de accesos, a monitorización xeral nin a resposta ante incidentes.
- En contornos industriais, deben despregarse con coidado para evitar calquera interferencia coa operación real.
- Un honeypot mal integrado pode xerar pouco valor ou quedar illado do proceso de análise e resposta.
- Requiren mantemento, revisión e unha interpretación adecuada dos eventos rexistrados.

Relación con outros controis: Relaciónanse cos IDS/IPS, co NDR, co CPS PP, coa monitorización e operación de seguridade, coa intelixencia de ameazas, coa resposta ante incidentes, coa segmentación de rede e separación IT/OT e coas medidas compensatorias orientadas a reforzar a detección en contornos con exposición elevada.

Casos habituais de uso: Empréganse para detectar exploración de rede en segmentos sensibles, actividade non autorizada en contornos industriais, movemento lateral en zonas OT, interaccións indebidas con protocolos aparentes, tentativas de acceso a servizos simulados e recollida de información sobre comportamento adversario en redes con baixa visibilidade previa.

Observacións / medidas compensatorias asociadas: En contornos industriais, os honeypots poden actuar como medida compensatoria útil cando non é viable reducir de

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

inmediato toda a exposición dun segmento, actualizar certos activos ou reforzar estruturalmente a arquitectura, xa que engaden unha capa adicional de detección e observación. A súa utilidade aumenta cando se combinan con segmentación, visibilidade OT, monitorización continua e procedementos claros de análise e escalado das alertas xeradas.

5.5.8 AntiDDoS

Categoría: Detección de ameazas e protección activa

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

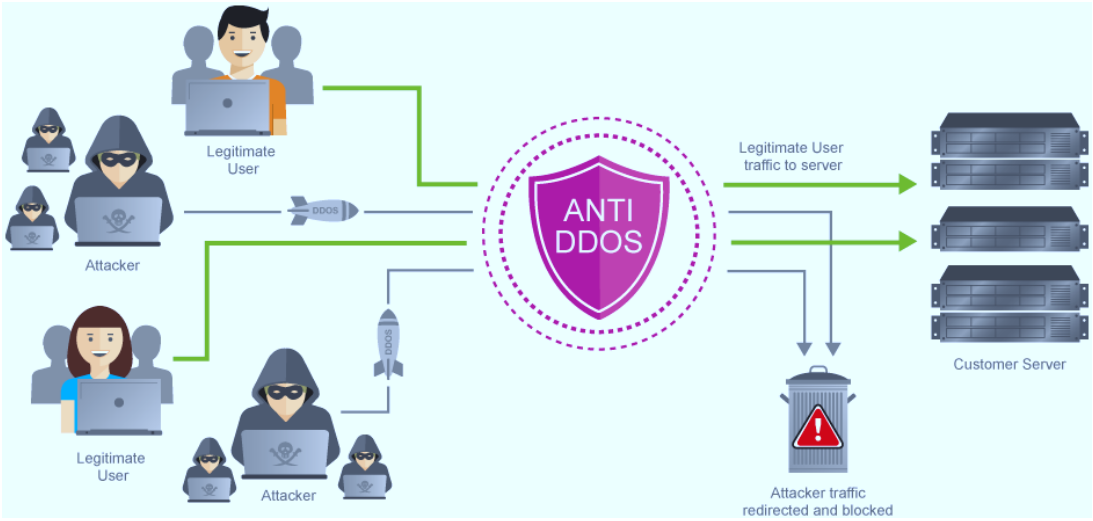
Descrición: As capacidades AntiDDoS están orientadas a detectar, absorber, filtrar ou mitigar ataques de denegación de servizo distribuída (*Distributed Denial of Service*), nos que un volume elevado de solicitudes ou tráfico malicioso tenta degradar, interromper ou saturar un servizo, unha aplicación, unha conexión ou unha infraestrutura exposta. O seu propósito é preservar a dispoñibilidade dos recursos críticos fronte a campañas que buscan esgotar capacidade de rede, procesamento ou atención de sesións. En contornos industriais, a súa relevancia adoita concentrarse en servizos publicados, portais web, accesos remotos, compoñentes en DMZ, plataformas de xestión expostas ou canles de comunicación esenciais que, sen seren necesariamente activos OT puros, poden ter impacto indirecto ou directo sobre a operación se quedan indispoñibles.

Obxectivo: Reducir o risco de interrupción ou degradación de servizos por ataques de denegación de servizo, mantendo a dispoñibilidade de recursos críticos e limitando o impacto operativo, reputacional ou funcional derivado da saturación maliciosa das comunicacións. No ámbito industrial, o seu obxectivo inclúe tamén asegurar que os servizos de acceso, supervisión, integración ou soporte que dependen de conectividade externa non se convertan nun punto único de fallo explotable por volume de tráfico.

Como funciona / como se implanta: A súa implantación pode basearse en distintos mecanismos, segundo o tipo de servizo protexido e o nivel de exposición: filtrado local, capacidade de absorción en perímetro ou na rede do provedor de comunicacións, servizos de mitigación en nube, redirección de tráfico, detección de patróns de saturación, limitación de taxa, listas de reputación ou combinación destas medidas. En contornos industriais, a súa utilidade adoita centrarse na protección de portais, aplicacións web, servizos de acceso remoto, compoñentes en DMZ ou recursos

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

publicados que dan soporte á operación ou á relación con terceiros. A súa eficacia depende da correcta identificación dos servizos críticos, da comprensión do tráfico lexítimo esperado e da integración con outros controis perimetrais e de continuidade. En contextos OT, non adoita aplicarse tanto á rede de control interna como aos puntos de exposición externa ou ás dependencias dixitais que poden afectar á operación se resultan interrompidas.



Esquema AntiDDoS na rede. Fonte: Cloud4u.com (n.d.)

Vantaxes:

- Axuda a preservar a dispoñibilidade de servizos expostos fronte á saturación maliciosa.
- Reduce o impacto de campañas de interrupción baseadas en volume ou consumo de recursos.
- Reforza a resiliencia de portais, servizos remotos e compoñentes publicados.
- Complementa outros controis perimetrais e de continuidade.
- Resulta especialmente útil en organizacións con servizos accesibles dende Internet ou con alta dependencia de conectividade externa.

Limitacións e consideracións:

- A súa utilidade é menor se a organización non dispón de servizos expostos ou dependencias externas relevantes.
- Non substitúe a necesidade de segmentación, arquitectura resiliente, balanceo nin continuidade de negocio.

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

- En contornos industriais, debe evitarse identificar AntiDDoS como control principal da rede OT cando o risco real se concentra noutros vectores.
- Pode requirir coordinación con provedores de conectividade, publicación ou mitigación externa.
- A eficacia depende de coñecer ben o patrón normal do servizo e de validar que as medidas de filtrado non afecten tráfico lexítimo crítico.

Relación con outros controis: Relaciónase co firewall, co NGFW/UTM, coa DMZ industrial, co WAF, co proxy, co acceso remoto seguro, coa continuidade de negocio e resiliencia operativa, coa monitorización e operación de seguridade e cos procedementos de resposta ante incidentes e indispoñibilidade.

Casos habituais de uso: Emprégase na protección de portais corporativos ou técnicos, servizos web publicados, interfaces de acceso remoto, compoñentes en DMZ, servizos de integración expostos, recursos accesibles dende Internet e escenarios nos que a indispoñibilidade dun servizo publicado pode afectar á xestión, á coordinación ou ao soporte da operación industrial.

Observacións / medidas compensatorias asociadas: En contornos industriais, AntiDDoS resulta especialmente útil cando existen dependencias claras de servizos publicados ou conectividade externa necesaria para operación, mantemento ou integración. Tamén pode actuar como medida compensatoria complementaria cando non é posible eliminar a exposición de determinados servizos, sempre que se combine con segmentación, DMZ, WAF, continuidade operativa e mecanismos de resposta ante interrupcións.

5.5.9 Threat hunting

Categoría: Detección de ameazas e protección activa

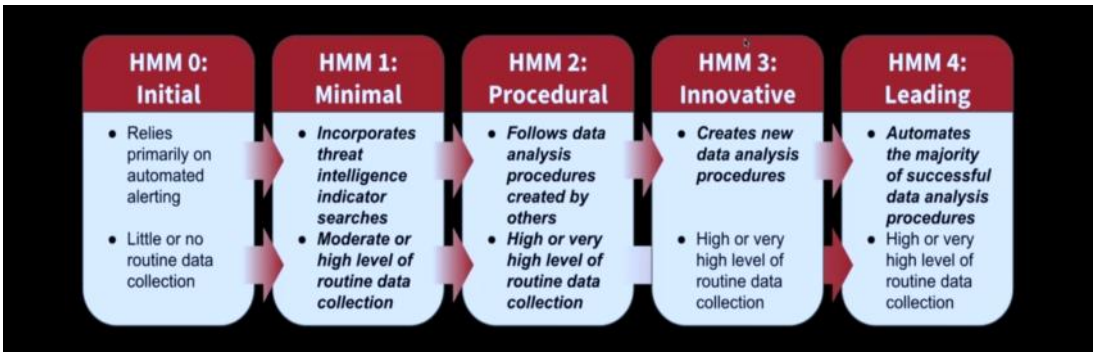
Tipoloxía: Técnico / mixto

Función defensiva predominante: Detectivo

Función no NIST CSF: Detect

Descrición: O *threat hunting* ou caza de ameazas é unha actividade proactiva de procura, análise e investigación orientada a identificar indicios de compromiso, comportamentos anómalos ou presenza adversaria que non foron detectados automaticamente polos mecanismos convencionais de seguridade. A diferenza da monitorización reactiva baseada en alertas xeradas por regras, firmas ou eventos previamente clasificados, o *threat hunting* parte de hipóteses, sinais febles, patróns

sospeitosos ou coñecemento sobre tácticas e técnicas adversarias para buscar evidencias de actividade maliciosa oculta ou insuficientemente contextualizada. En contornos industriais, esta capacidade resulta especialmente valiosa cando a organización precisa ir máis alá da detección básica e contrastar se existen movementos laterais, uso indebido de credenciais, interaccións anómalas entre activos ou comportamentos discretos con potencial impacto operativo.



Modelo de madurez da caza de ameazas. Fonte: SANS Institute (n.d.)

Obxectivo:

Incrementar a capacidade da organización para descubrir ameazas que non foron identificadas por mecanismos automáticos ou que permanecen ocultas entre o ruído operativo do entorno, reducindo o tempo de permanencia dun adversario e mellorando a comprensión do alcance real dun posible compromiso. No ámbito industrial, o seu obxectivo inclúe tamén detectar sinais precoces de actividade maliciosa en contornos nos que a dispoñibilidade e a estabilidade limitan a aplicación de medidas máis intrusivas e nos que determinados patróns poden confundirse con operación lexítima se non se contextualizan axeitadamente.

Como funciona / como se implanta:

A súa implantación require dispoñer de fontes de información suficientes sobre o entorno, como rexistros, telemetría de rede, eventos de seguridade, información de activos, contexto operativo, datos de endpoints compatibles e visibilidade sobre comunicacións IT/OT. A partir desa base, os analistas formulan hipóteses de procura —por exemplo, abuso de credenciais, movemento lateral, interaccións anómalas con protocolos industriais, uso indebido de acceso remoto ou persistencia en sistemas intermedios— e contrastan esas hipóteses mediante consultas, correlación de eventos, revisión de patróns e investigación manual ou asistida. En contornos industriais, o valor do *threat hunting* aumenta cando se integra con coñecemento do proceso, inventario de activos, NDR, IDS/IPS, visibilidade OT e procedementos de resposta, xa que moitas das

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

investigacións dependen de distinguir entre unha variación operativa lexítima e unha actividade potencialmente maliciosa.

Vantaxes:

- Permite descubrir ameazas ou comportamentos maliciosos que non xeran alertas automáticas claras.
- Reduce a dependencia exclusiva de sinaturas, regras estáticas ou detección reactiva.
- Mellora a comprensión do comportamento adversario e do alcance dun posible compromiso.
- Resulta útil para contrastar hipóteses, investigar sinais débiles e validar sospeitas en contornos complexos.
- Complementa a monitorización convencional cun enfoque máis contextual e proactivo.

Limitacións e consideracións:

- Requírese visibilidade suficiente, fontes de datos de calidade e capacidade analítica especializada.
- O seu valor é limitado se o entorno carece de rexistros, contextualización de activos ou procesos maduros de investigación.
- En contornos industriais, pode resultar difícil interpretar certos patróns sen coñecemento operativo e do proceso.
- Non substitúe a monitorización, a segmentación, a xestión de accesos nin os procedementos de resposta.
- Debe evitarse formular o *threat hunting* como actividade illada e puntual, sen integración cos procesos de operación de seguridade e mellora continua.

Relación con outros controis: Relaciónase co IDS/IPS, co NDR, co EDR, co CPS PP, coa monitorización e operación de seguridade, coa visibilidade de activos e comunicacións OT, coa intelixencia de ameazas, coa resposta ante incidentes e coas medidas compensatorias orientadas a reforzar a capacidade de detección en contornos con alta exposición ou baixa visibilidade histórica.

Casos habituais de uso: Emprégase para investigar sinais de acceso remoto sospeitoso, movemento lateral entre dominios IT/OT, uso anómalo de credenciais, exploración discreta de activos industriais, comportamento estraño en servidores intermedios,

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

persistencia en estacións de enxeñaría ou HMI compatibles, e escenarios nos que a organización sospeita da existencia de compromiso sen dispor dunha alerta concluínte.

Observacións / medidas compensatorias asociadas: En contornos industriais, o *threat hunting* resulta especialmente útil como medida complementaria cando non é viable reforzar de inmediato toda a arquitectura, reducir toda a exposición existente ou despregar controis máis intrusivos sobre certos activos. A súa utilidade aumenta cando se apoia en boa visibilidade de rede e activos, coñecemento operativo suficiente e procedementos claros para escalar, investigar e responder ás evidencias detectadas.

5.6 Monitorización, visibilidade e operación de seguridade

A visibilidade é unha condición indispensable para xestionar o risco de forma eficaz en contornos industriais complexos e interconectados. Esta subsección recolle **capacidades orientadas á recollida, correlación e análise de eventos, á supervisión continua da actividade e á operación diaria da seguridade**, co obxectivo de mellorar a capacidade de detección, investigación e toma de decisións tanto en IT como en OT.

5.6.1 SIEM

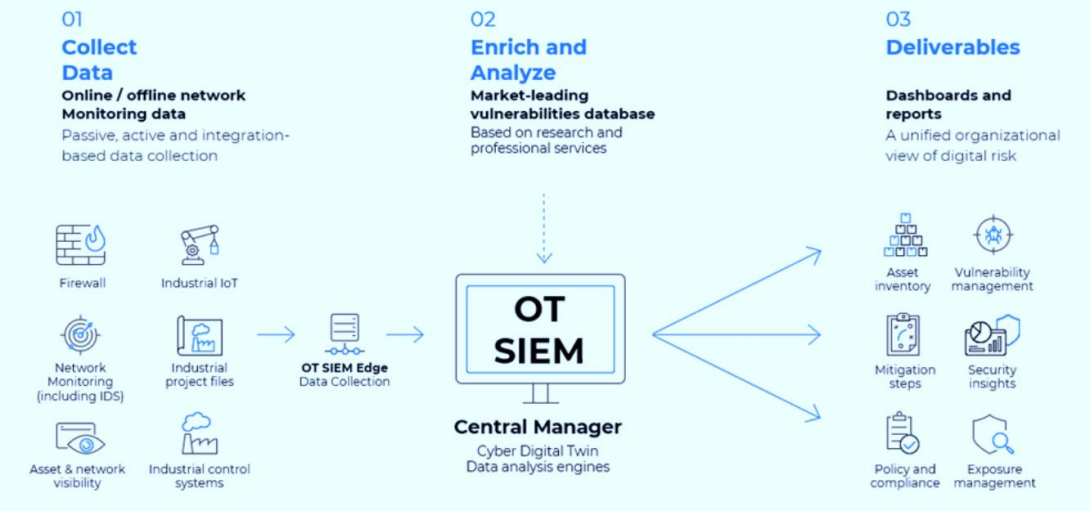
Categoría: Monitorización, visibilidade e operación de seguridade

Tipoloxía: Técnico / mixto

Función defensiva predominante: Detectivo

Función no NIST CSF: Detect

Descrición: O SIEM (*Security Information and Event Management*) é unha plataforma orientada á recollida, normalización, correlación, análise e conservación de eventos de seguridade procedentes de múltiples fontes, co obxectivo de mellorar a visibilidade global do entorno e facilitar a detección temperá de incidentes. A súa utilidade reside en unificar nun mesmo plano de observación rexistros, alertas e eventos xerados por sistemas, redes, aplicacións, dispositivos de seguridade e, cando procede, compoñentes OT, permitindo analizar relacións que non serían visibles se cada fonte se observase de maneira illada. En contornos industriais, o SIEM resulta especialmente valioso cando a organización precisa correlacionar sinais procedentes de dominios IT e OT, contextualizar alertas e apoiar a investigación de incidentes con impacto potencial sobre a operación.



Exemplo de funcionamento de SIEM OT. Fonte: Accura.io (n.d.)

Obxectivo: Incrementar a capacidade da organización para detectar, correlacionar e investigar eventos de seguridade a partir dunha visión centralizada e estruturada da telemetría dispoñible. No ámbito industrial, o seu obxectivo inclúe tamén integrar sinais procedentes de contornos corporativos e operativos para identificar patróns de risco, conexións indebidas, acceso anómalo, propagación entre dominios ou comportamentos que poidan afectar á continuidade e á seguridade do proceso.

Como funciona / como se implanta: A súa implantación baséase na conexión progresiva de fontes de eventos ao sistema: firewalls, sistemas de autenticación, servidores, endpoints, aplicacións, sistemas de correo, mecanismos de acceso remoto, compoñentes de rede, sensores de seguridade e, cando o contexto o permite, activos ou plataformas de visibilidade OT. Unha vez recibidos, os eventos normalízanse, etiquétanse e analízanse mediante regras de correlación, casos de uso, buscas, paneis e alertas. En contornos industriais, a súa eficacia depende de seleccionar ben as fontes relevantes, evitar unha integración indiscriminada sen contexto e construír casos de uso adaptados ao entorno, por exemplo sobre accesos remotos, movemento entre IT e OT, cambios non previstos, conexión de terceiros, alertas de visibilidade OT ou eventos de activos críticos. O seu valor real non reside só na acumulación de rexistros, senón na capacidade de transformar esa información en detección accionable, contexto operativo e apoio á resposta.

Vantaxes:

- Centraliza a visibilidade de eventos procedentes de múltiples fontes.
- Permite correlacionar sinais que, observados por separado, terían pouco valor.
- Mellora a detección temperá e a investigación de incidentes.

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

- Reforza a trazabilidade e a conservación de evidencias.
- Resulta especialmente útil para integrar visión IT/OT en organizacións con contornos híbridos.

Limitacións e consideracións:

- O seu valor é limitado se se concibe só como repositorio masivo de rexistros sen casos de uso nin análise.
- Pode xerar volume elevado de eventos e alertas se non existe unha selección adecuada das fontes e unha correlación ben afinada.
- En contornos industriais, a integración de sinais OT debe facerse con criterio, evitando forzar fontes pouco útiles ou mal contextualizadas.
- Non substitúe a visibilidade de activos, a detección en rede, a segmentación nin os procedementos de resposta.
- Requírese madurez operativa para manter regras, revisar alertas, investigar eventos e actualizar casos de uso segundo a evolución do risco.

Relación con outros controis: Relaciónase co SOC, co MDR, co IDS/IPS, co NDR, co EDR, coa visibilidade de activos e comunicacións OT, coa monitorización ciberfísica, coa xestión de identidades e accesos, co acceso remoto seguro, coa resposta ante incidentes e coas medidas compensatorias orientadas a reforzar a detección e a trazabilidade.

Casos habituais de uso: Emprégase para correlacionar eventos de autenticación, accesos remotos, tráfico perimetral, alertas de rede, actividade de endpoints, interaccións entre IT e OT, cambios non previstos en activos críticos, uso de contas privilexiadas, actividade de terceiros e escenarios nos que se precisa unha visión centralizada da seguridade do entorno.

Observacións / medidas compensatorias asociadas: En contornos industriais, o SIEM resulta especialmente útil como capa compensatoria cando non é viable reforzar de inmediato todos os controis preventivos ou reducir toda a exposición existente, xa que permite mellorar a capacidade de detección, correlación e investigación. A súa utilidade aumenta cando se integra con fontes OT significativas, con procedementos claros de análise e resposta, e cun deseño de casos de uso adaptado á realidade operativa da organización.

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

5.6.2 SOC

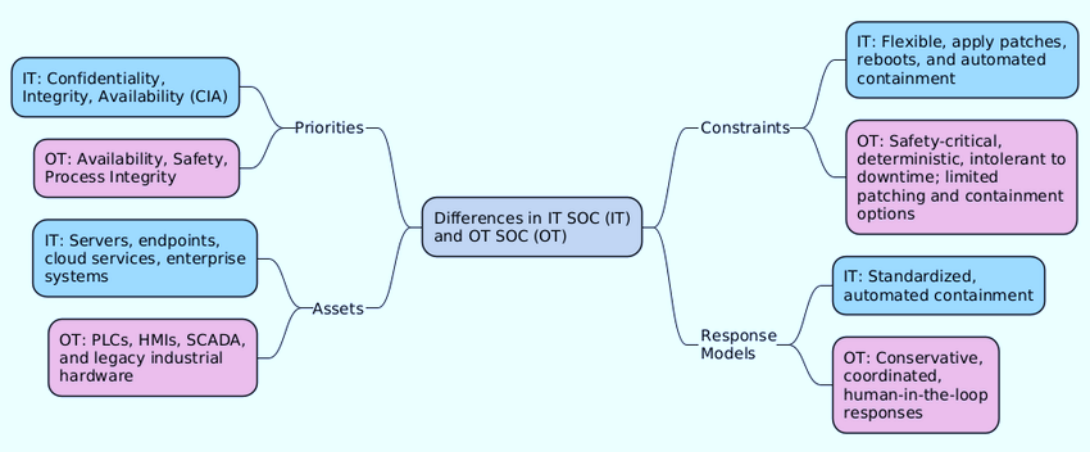
Categoría: Monitorización, visibilidade e operación de seguridade

Tipoloxía: Organizativo / técnico / mixto

Función defensiva predominante: Detectivo

Función no NIST CSF: Detect, Respond

Descrición: O SOC (*Security Operations Center* ou Centro de Operacións de Seguridade) é a capacidade organizativa e operativa encargada de supervisar de maneira continuada o entorno tecnolóxico, analizar alertas e eventos, investigar actividades sospeitosas e coordinar a resposta fronte a incidentes de seguridade. Non se limita a unha plataforma concreta nin a un espazo físico determinado, senón que representa a combinación de persoas, procedementos, ferramentas e fluxos de traballo necesarios para transformar a monitorización en capacidade real de detección e resposta. En contornos industriais, o SOC adquire especial relevancia cando a organización precisa integrar sinais procedentes de dominios IT e OT, interpretar o contexto operativo das alertas e coordinar actuacións sen comprometer a continuidade nin a seguridade do proceso.



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

Obxectivo: Dotar á organización dunha capacidade estable e estruturada para detectar, analizar, priorizar, escalar e responder fronte a incidentes de seguridade, reducindo o tempo de identificación, mellorando a calidade da análise e facilitando a coordinación entre áreas implicadas. No ámbito industrial, o seu obxectivo inclúe tamén asegurar que as alertas relacionadas con sistemas OT, acceso remoto, terceiros, protocolos industriais ou activos críticos sexan tratadas con coñecemento suficiente do seu impacto operativo.

Como funciona / como se implanta: A súa implantación require definir un modelo operativo claro: fontes de información, niveis de monitorización, roles e

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

responsabilidades, procedementos de análise, escalado, comunicación e resposta, así como ferramentas de apoio como SIEM, NDR, IDS/IPS, visibilidade OT, xestión de casos ou plataformas de intelixencia. O SOC pode ser interno, externo ou híbrido, e adaptarse á dimensión e madurez da organización. En contornos industriais, a súa eficacia depende non só das ferramentas dispoñibles, senón da capacidade para integrar coñecemento de operación, mantemento, arquitectura IT/OT, activos críticos, protocolos industriais e dependencia de terceiros. Resulta especialmente importante definir casos de uso específicos para o entorno industrial, canles de escalado cara a operación e criterios claros para actuar sobre alertas sen introducir risco innecesario sobre o proceso.

Vantaxes:

- Centraliza a supervisión e análise de eventos de seguridade.
- Mellora a capacidade de detección, priorización e resposta fronte a incidentes.
- Facilita a correlación entre sinais de múltiples fontes e dominios.
- Achega trazabilidade, continuidade operativa e procedementos estables de análise.
- Resulta especialmente útil para integrar visión IT/OT e coordinar actuacións en contornos híbridos.

Limitacións e consideracións:

- O seu valor diminúe se se concibe só como receptor de alertas sen capacidade suficiente de análise e resposta.
- Requírese madurez organizativa, procedementos claros e integración real co resto da organización.
- En contornos industriais, un SOC centrado só en TI pode interpretar mal certas alertas ou escalar accións incompatibles coa operación.
- Non substitúe a necesidade de boas fontes de telemetría, segmentación, control de accesos nin xestión de vulnerabilidades.
- A súa eficacia depende da coordinación con operación, mantemento, responsables de proceso e, cando proceda, seguridade funcional e terceiros.

Relación con outros controis: Relaciónase co SIEM, co MDR, cos IDS/IPS, co NDR, co EDR, co CPS PP, coa visibilidade de activos e comunicacións OT, coa monitorización ciberfísica, coa intelixencia de ameazas, coa resposta ante incidentes e cos

procedementos de continuidade. Funciona como capa operativa que da sentido e coordinación ao conxunto de capacidades de monitorización e detección.

Casos habituais de uso: Emprégase para supervisar alertas IT/OT, analizar accesos remotos, actividade de terceiros, movemento entre dominios, cambios non previstos, eventos procedentes de sensores de rede ou endpoint, investigación de incidentes con impacto operativo e coordinación da resposta en organizacións con exposición significativa ou necesidade de vixilancia continuada.

Observacións / medidas compensatorias asociadas: En contornos industriais, o SOC pode actuar como medida compensatoria moi relevante cando non é viable reforzar de inmediato todos os controis preventivos, xa que mellora a capacidade de detección temperá, análise e coordinación fronte a incidentes. A súa utilidade é especialmente alta cando integra coñecemento do proceso, casos de uso adaptados á realidade OT e procedementos claros para escalar de forma segura decisións que poidan afectar á operación.

5.6.3 MDR

Categoría: Monitorización, visibilidade e operación de seguridade

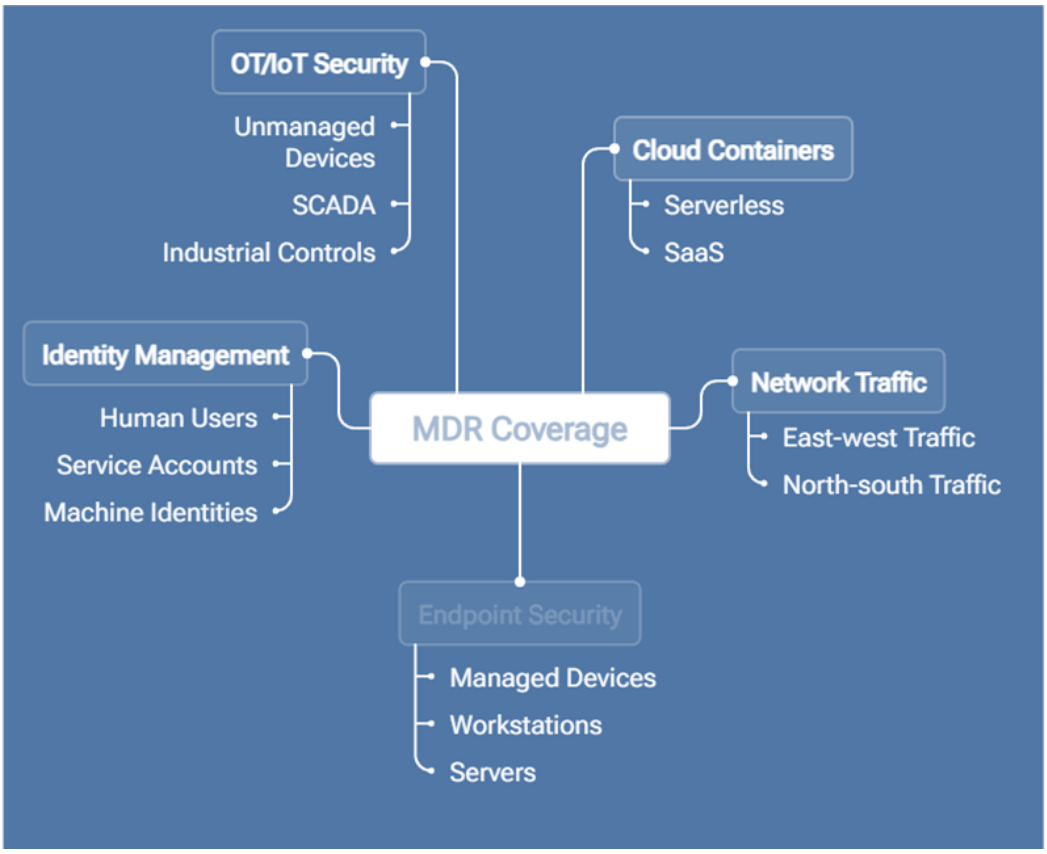
Tipoloxía: Organizativo / técnico / mixto

Función defensiva predominante: Detectivo

Función no NIST CSF: Detect, Respond

Descrición: O MDR (*Managed Detection and Response*) é un modelo de servizo mediante o cal unha organización delega, total ou parcialmente, capacidades de monitorización, detección, análise e apoio á resposta ante incidentes nun provedor especializado. A súa finalidade é complementar ou substituír capacidades internas cando non existe estrutura suficiente para operar de maneira continuada un modelo propio de supervisión avanzada. A diferenza dun servizo puramente tecnolóxico ou dunha simple xestión de alertas, o MDR combina telemetría, análise, caza de ameazas, investigación e escalado operativo, normalmente apoiándose en ferramentas como SIEM, EDR, NDR ou outras fontes de visibilidade. En contornos industriais, esta opción resulta especialmente relevante para organizacións que precisan mellorar a súa capacidade de detección e resposta sen dispoñer dun SOC propio maduro ou de recursos internos suficientes para cubrir a vixilancia continuada de contornos híbridos IT/OT.

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



Áreas de cobertura dun MDR. Fonte: Vectra.ai (n.d.)

Obxectivo: Dotar á organización dunha capacidade sostida de detección, análise e apoio á resposta ante incidentes, reducindo o tempo de identificación e mellorando a calidade do tratamento das alertas sen depender exclusivamente de medios internos. No ámbito industrial, o seu obxectivo inclúe tamén achegar coñecemento especializado e cobertura operativa fronte a eventos que afecten a accesos remotos, terceiros, activos críticos, interaccións IT/OT ou sinais de compromiso con impacto potencial sobre a operación.

Como funciona / como se implanta: A súa implantación require definir o alcance do servizo, as fontes de telemetría que serán monitorizadas, os niveis de cobertura, os criterios de escalado, os tempos de resposta esperados e a distribución de responsabilidades entre a organización e o provedor. O MDR pode operar sobre ferramentas xa existentes na organización ou incorporar parte da súa propia infraestrutura de detección e análise. En contornos industriais, a súa eficacia depende de que o servizo teña visibilidade suficiente sobre os activos e fluxos relevantes, de que exista unha correcta contextualización da arquitectura IT/OT e de que se definan procedementos claros para escalar incidentes sen comprometer a continuidade nin a seguridade do proceso. Resulta especialmente importante establecer canles fluídas entre o provedor, os equipos internos de seguridade, operación, mantemento e

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

responsables do proceso, evitando que a xestión externalizada quede desconectada da realidade operativa da planta ou da organización.

Vantaxes:

- Permite acceder a capacidades avanzadas de detección e análise sen necesidade de desenvolver internamente toda a estrutura.
- Mellora a cobertura temporal e a continuidade da supervisión.
- Achega coñecemento especializado, procedementos maduros e apoio na investigación de incidentes.
- Resulta útil para organizacións con recursos limitados ou sen SOC propio consolidado.
- Pode acelerar a detección e o escalado de incidentes en contornos híbridos IT/OT.

Limitacións e consideracións:

- O seu valor depende da calidade do servizo, da cobertura real e da integración co contexto da organización.
- En contornos industriais, un MDR alleo á realidade OT pode interpretar mal alertas ou escalar accións pouco compatibles coa operación.
- Non substitúe a necesidade de inventario, segmentación, visibilidade suficiente nin procedementos internos de coordinación.
- Requírese definir con claridade que decisións pode tomar o provedor, que accións se reservan á organización e como se xestionan incidentes con impacto operativo.
- Debe evitarse tratar o MDR como unha externalización completa da responsabilidade sobre a seguridade.

Relación con outros controis: Relaciónase co SOC, co SIEM, co EDR, co NDR, cos IDS/IPS, coa visibilidade de activos e comunicacións OT, coa monitorización ciberfísica, coa resposta ante incidentes, coa intelixencia de ameazas e cos procedementos de continuidade. Funciona como modelo operativo de apoio ou substitución parcial do centro interno de operacións de seguridade.

Casos habituais de uso: Emprégase en organizacións que precisan vixilancia continuada sen dispoñer de SOC propio, en contornos con exposición significativa a acceso remoto ou terceiros, en infraestruturas con necesidades de monitorización 24/7,

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

en escenarios de reforzo da capacidade interna de análise e resposta, e en programas de seguridade nos que se busca combinar recursos internos limitados con supervisión especializada externa.

Observacións / medidas compensatorias asociadas: En contornos industriais, o MDR pode actuar como medida compensatoria moi útil cando non é viable desenvolver de inmediato unha capacidade interna madura de operación de seguridade, sempre que exista visibilidade suficiente e unha boa integración co contexto OT. A súa utilidade aumenta cando se acompaña de procedementos claros de escalado, coñecemento dos activos críticos, coordinación con operación e limitación explícita das accións que poden afectar ao proceso sen validación previa.

5.6.4 Monitorización ciberfísica / MES

Categoría: Monitorización, visibilidade e operación de seguridade

Tipoloxía: Técnico / mixto

Función defensiva predominante: Detectivo

Función no NIST CSF: Detect

Descrición: A monitorización ciberfísica / MES comprende o conxunto de capacidades orientadas á observación continua do comportamento do proceso industrial, dos sistemas de execución e supervisión e das súas interaccións coa capa tecnolóxica, co fin de identificar desviacións, anomalías ou condicións de risco con impacto potencial sobre a operación. Este control integra, segundo o caso, a análise de variables de proceso, estados operativos, eventos de sistemas, fluxos de comunicación, sinais de produción e información procedente de plataformas MES (*Manufacturing Execution System*) ou equivalentes. O seu valor reside en achegar unha visión máis próxima ao funcionamento real da actividade industrial, permitindo detectar incidentes ou alteracións que non sempre serían visibles dende unha monitorización puramente de rede ou centrada unicamente en eventos IT.

Obxectivo: Incrementar a capacidade da organización para identificar anomalías con relevancia operativa, correlacionando información procedente do proceso, da supervisión, da execución e dos sistemas tecnolóxicos que o soportan. No ámbito industrial, o seu obxectivo inclúe tamén detectar cambios de comportamento que poidan indicar manipulación, fallo, degradación, uso indebido dos sistemas ou impacto potencial sobre a produción, a calidade, a continuidade ou a seguridade do proceso.

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

Como funciona / como se implanta: A súa implantación parte da identificación das fontes de datos máis relevantes para comprender o funcionamento do entorno: variables de proceso, estados de equipos, alarmas, eventos de supervisión, información de sistemas MES, rexistros de operación, trazas de comunicación, sinais de control e outros indicadores asociados á actividade industrial. A partir desa base, establécense mecanismos de recollida, correlación e análise que permitan distinguir entre condicións normais de operación, variacións esperadas e desviacións que requiran investigación. En contornos industriais, a súa utilidade aumenta cando se integra con coñecemento do proceso, inventario de activos, contexto de produción, monitorización de rede, visibilidade OT e procedementos de escalado cara a operación e mantemento. Non se trata só de acumular datos, senón de interpretalos á luz do comportamento esperado da planta ou do servizo industrial.

Vantaxes:

- Achega unha visión máis próxima ao comportamento real do proceso e da operación.
- Permite detectar desviacións que poden pasar inadvertidas en controis centrados só en rede ou endpoint.
- Mellora a contextualización de alertas e eventos con impacto potencial sobre a produción ou a calidade.
- Resulta especialmente útil en contornos con forte dependencia de plataformas de execución, supervisión ou integración operativa.
- Complementa a detección técnica con información directamente relacionada co estado do proceso.

Limitacións e consideracións:

- A súa eficacia depende da calidade, cobertura e contextualización das fontes de datos dispoñibles.
- Pode requirir coñecemento avanzado do proceso para diferenciar entre variacións operativas normais e sinais de risco real.
- En contornos industriais, unha mala interpretación das desviacións pode xerar falsos positivos ou escalados innecesarios.
- Non substitúe a segmentación, o control de accesos, a xestión de vulnerabilidades nin a monitorización de rede.

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

- Requírese coordinación estreita con operación, mantemento, enxeñaría e responsables de produción para que a información recollida se traduza en acción útil.

Relación con outros controis: Relaciónase co SIEM, co SOC, co MDR, co NDR, co CPS PP, coa visibilidade de activos e comunicacións OT, coa resposta ante incidentes, coa continuidade de negocio e resiliencia operativa e coas medidas compensatorias orientadas a reforzar a detección e a comprensión do risco sobre sistemas e procesos críticos.

Casos habituais de uso: Emprégase para detectar desviacións en parámetros de proceso, cambios non previstos en secuencias de operación, inconsistencias entre eventos de rede e comportamento produtivo, anomalías en plataformas MES, degradación de liñas ou servizos industriais, impacto operativo derivado de incidentes de seguridade e escenarios nos que se precisa comprender mellor a relación entre actividade tecnolóxica e estado real do proceso.

Observacións / medidas compensatorias asociadas: En contornos industriais, a monitorización ciberfísica / MES pode actuar como medida compensatoria especialmente útil cando non é viable reducir de inmediato toda a exposición arquitectónica ou actualizar determinados activos, xa que achega unha capa adicional de detección centrada no comportamento real da operación. A súa utilidade aumenta cando se combina con monitorización de rede, visibilidade OT, procedementos claros de análise e escalado, e coñecemento suficiente do proceso para interpretar correctamente as anomalías observadas.

5.6.5 Visibilidade de activos e comunicacións OT

Categoría: Monitorización, visibilidade e operación de seguridade

Tipoloxía: Técnico / mixto

Función defensiva predominante: Detectivo

Función no NIST CSF: Identify, Detect

Descrición: A visibilidade de activos e comunicacións OT consiste no conxunto de capacidades orientadas a identificar, inventariar, contextualizar e observar os dispositivos, sistemas, relacións e fluxos que conforman o entorno operativo industrial. O seu propósito é achegar unha comprensión fiable de que activos existen, como se comunican, que protocolos utilizan, que función desempeñan e que dependencias manteñen coa rede corporativa, cos sistemas de supervisión, cos provedores e co

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

proceso físico. En contornos industriais, este control resulta esencial porque unha parte significativa do risco deriva precisamente da falta de coñecemento detallado sobre activos legados, comunicacións históricas, interconexións non documentadas, dispositivos de terceiros ou cambios non suficientemente gobernados. Estas capacidades típicamente intégranse en sistemas CPS PP.

Obxectivo: Dispoñer dunha visión actualizada e contextualizada dos activos OT e das súas comunicacións, reducindo puntos cegos e mellorando a capacidade da organización para detectar exposicións, anomalías, dependencias críticas e cambios non previstos. No ámbito industrial, o seu obxectivo inclúe tamén servir de base para a segmentación, a xestión de vulnerabilidades, a resposta ante incidentes, a revisión de arquitectura e a protección dos sistemas con maior criticidade operativa.

Como funciona / como se implanta: A súa implantación adoita basearse na observación pasiva do tráfico de rede, na identificación de protocolos industriais, na correlación con inventarios existentes, na análise de configuracións e na contextualización funcional dos activos detectados. A partir desa base, constrúese unha visión máis completa do entorno: que dispositivos existen, que versións ou perfís presentan, con que sistemas se relacionan, que patróns de comunicación son habituais e que desviacións poden ser relevantes. En contornos industriais, este control debe aplicarse con criterios compatibles coa continuidade da operación, priorizando técnicas pasivas e evitando mecanismos intrusivos que poidan afectar á estabilidade do proceso. A súa utilidade aumenta cando a información recollida se integra con procesos de xestión de activos, revisión de arquitectura, monitorización de seguridade e procedementos de cambio.

Vantaxes:

- Reduce puntos cegos sobre activos, fluxos e dependencias do entorno OT.
- Mellora a base de coñecemento necesaria para segmentación, detección e resposta.
- Permite identificar activos non documentados, comunicacións non previstas e interconexións de risco.
- Resulta especialmente útil en contornos con legado tecnolóxico, terceiros ou baixa gobernanza histórica.
- Facilita a contextualización doutros controis de monitorización e protección.

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

Limitacións e consideracións:

- A súa eficacia depende da cobertura real da observación e da capacidade para contextualizar os activos detectados.
- Pode ofrecer unha visión incompleta se non se integra con coñecemento operativo e documental da organización.
- En contornos industriais, a identificación dun activo non sempre implica coñecer de inmediato a súa criticidade ou a súa dependencia funcional.
- Non substitúe a segmentación, a xestión de vulnerabilidades, o control de accesos nin a revisión formal da arquitectura.
- Requírese mantemento continuado para reflectir cambios de configuración, incorporación de terceiros, novas interconexións ou evolución do proceso.

Relación con outros controis: Relaciónase co SIEM, co SOC, co MDR, co NDR, coa monitorización ciberfísica / MES, coa segmentación de rede e separación IT/OT, coa revisión de arquitectura, coa xestión de vulnerabilidades, coa resposta ante incidentes e coas medidas compensatorias orientadas a reducir a exposición de activos críticos ou pouco coñecidos.

Casos habituais de uso: Emprégase para construír ou mellorar inventarios OT, identificar activos legados ou non documentados, analizar fluxos entre redes corporativas e operativas, revisar protocolos empregados en planta, detectar comunicacións anómalas, contextualizar alertas de seguridade, apoiar proxectos de segmentación e reforzar a comprensión do entorno antes de auditorías, cambios ou actuacións correctivas.

Observacións / medidas compensatorias asociadas: En contornos industriais, a visibilidade de activos e comunicacións OT adoita ser unha medida habilitadora e, ao mesmo tempo, compensatoria: cando non é viable acometer de inmediato cambios máis profundos, permite polo menos coñecer mellor o risco existente, reducir incerteza e priorizar actuacións sobre os activos e fluxos máis sensibles. A súa utilidade aumenta cando se combina con segmentación, monitorización, bastionado e procedementos claros de revisión e 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 compoñentes e eventos críticos

Determinados activos, canles de comunicación e soportes de operación presentan unha relevancia especial pola súa proximidade ao proceso, pola súa sensibilidade ou polo seu potencial como vector de compromiso. Este bloque agrupa **medidas de protección e monitorización focalizadas en elementos concretos —postos de operación, endpoints industriais, correo, dispositivos externos ou aplicacións conectadas— que requiren un tratamento específico** dentro da arquitectura global de seguridade.

5.7.1 Protección do posto, dos activos e dos soportes de operación

Categoría: Protección do posto, dos activos e dos soportes de operación

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: A protección do posto de traballo comprende o conxunto de medidas técnicas, configuracións, políticas e mecanismos de control destinados a asegurar os equipos de usuario que interveñen na actividade diaria da organización, reducindo a súa exposición a malware, uso indebido, configuracións inseguras, instalación de software non autorizado ou acceso non controlado. Este control abrangue tanto os postos corporativos convencionais como aqueles equipos que, sen formar parte do núcleo da rede OT, poden actuar como ponte cara a contornos operativos, servizos remotos, plataformas de xestión ou sistemas con impacto indirecto sobre a operación. En contornos industriais, o posto de traballo non debe entenderse só como un elemento de oficina, senón tamén como un compoñente que pode influír na seguridade global do entorno híbrido IT/OT.

Obxectivo: Reducir o risco de compromiso dos equipos de usuario e limitar a súa capacidade para actuar como vector de entrada, propagación ou apoio a accións maliciosas, reforzando o control sobre configuracións, software, privilexios, acceso a datos e interacción con outros sistemas. No ámbito industrial, o seu obxectivo inclúe tamén evitar que un posto aparentemente periférico se converta nun punto de apoio para acceder a servizos sensibles, credenciais, recursos compartidos ou contornos de operación.

Como funciona / como se implanta: A súa implantación baséase na aplicación de medidas de bastionado, configuración segura, xestión de privilexios, control de software

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

autorizado, protección fronte a malware, cifrado, actualización controlada, restrición de dispositivos externos, autenticación reforzada e supervisión da actividade do endpoint. En contornos industriais, este control debe aplicarse con criterio segundo o tipo de equipo e a súa relación coa operación, diferenciando entre postos corporativos xerais, equipos con acceso a servizos de supervisión, portátiles empregados en mantemento ou postos con interacción con sistemas de xestión industrial. A súa eficacia depende de que exista unha política clara de configuración, unha administración coherente dos permisos, inventario actualizado dos equipos e integración con outros controis como identidade, monitorización, protección de correo e acceso remoto.

Vantaxes:

- Reduce a superficie de exposición dun dos vectores máis habituais de compromiso.
- Mellora o control sobre configuracións, software e privilexios dos equipos de usuario.
- Dificulta a execución de código malicioso, o abuso de credenciais e a propagación dende postos comprometidos.
- Reforza a protección de equipos que poden actuar como ponte cara a servizos sensibles ou contornos industriais.
- Complementa outros controis de rede, identidade e monitorización dende a capa de endpoint.

Limitacións e consideracións:

- A súa eficacia diminúe se non existe unha administración coherente de configuracións, permisos e excepcións.
- En contornos industriais, algúns postos poden depender de software específico con restricións de actualización ou compatibilidade.
- Non substitúe a segmentación, a xestión de identidades, a protección de acceso remoto nin a formación do persoal.
- Pode xerar desviacións de seguridade se se manteñen excepcións permanentes sen trazabilidade nin revisión.
- Requírese coordinación entre sistemas, seguridade, operación e responsables das aplicacións críticas para evitar impactos non desexados.

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

Relación con outros controis: Relaciónase coa protección de endpoints industriais, co MDM, coa seguridade no email, coa conexión segura de dispositivos externos, coa xestión de identidades e accesos, co acceso remoto seguro, co EDR, coa detección de integridade de ficheiros e coas medidas compensatorias orientadas a reducir risco en equipos con exposición elevada.

Casos habituais de uso: Emprégase para reforzar postos corporativos con acceso a servizos críticos, equipos de usuario con acceso a información sensible, portátiles empregados por persoal técnico, estacións conectadas a plataformas de xestión industrial, terminais con acceso remoto e contornos nos que o posto de traballo pode actuar como punto de entrada cara a recursos de maior criticidade.

Observacións / medidas compensatorias asociadas: En contornos industriais, a protección do posto de traballo resulta especialmente útil como medida de base para limitar a exposición dos equipos máis próximos á converxencia IT/OT. A súa utilidade aumenta cando se combina con bastionado, control de privilexios, restrición de software, MFA, segmentación, monitorización e procedementos claros para a xestión de excepcións, especialmente en postos que interactúan con operación, mantemento ou terceiros.

5.7.2 Protección de endpoints industriais

Categoría: Protección do posto, dos activos e dos soportes de operación

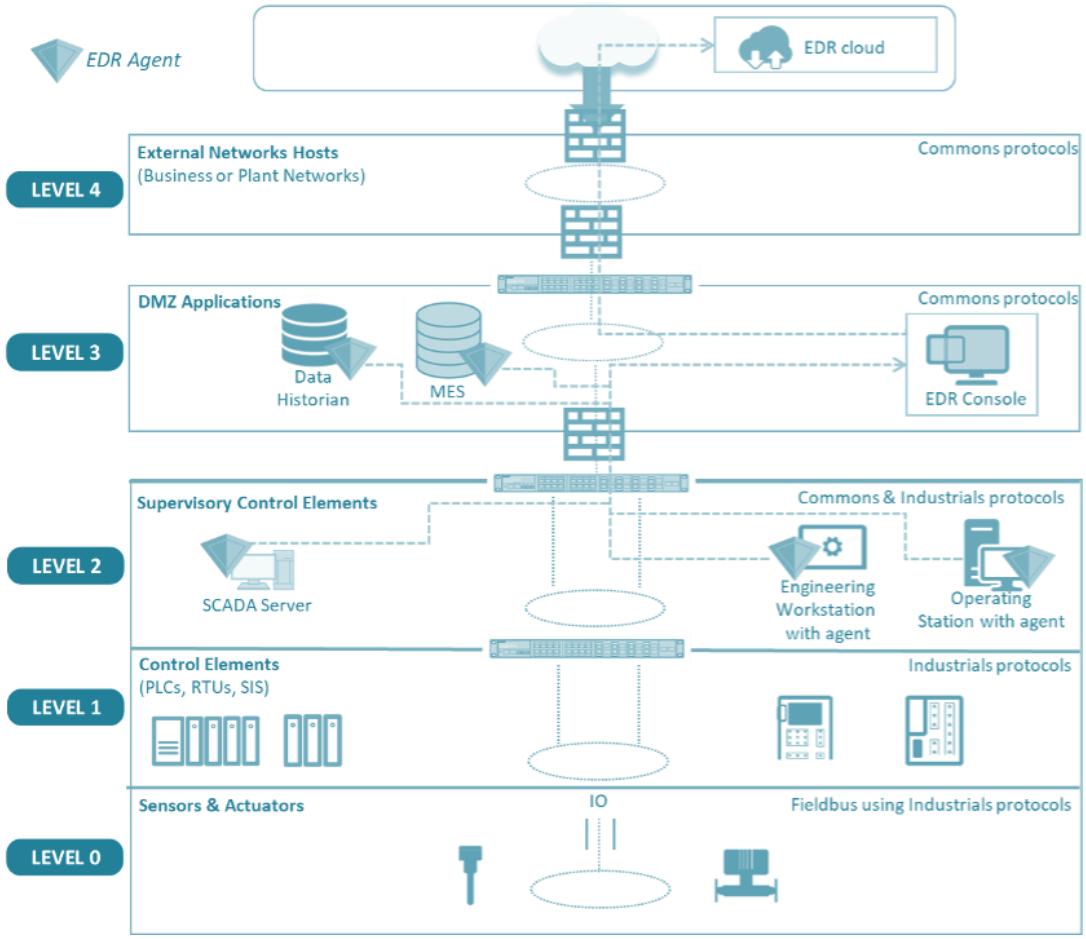
Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: A protección de endpoints industriais comprende o conxunto de medidas técnicas e procedementais destinadas a reforzar a seguridade dos equipos finais con función operativa ou relación directa cos contornos OT, como HMI, estacións de enxeñaría, servidores de supervisión, postos de mantemento, terminais asociados a aplicacións industriais e outros sistemas con capacidade de interacción co proceso ou coa infraestrutura de control. A diferenza da protección xenérica do posto de traballo, este control debe adaptarse ás restricións propias do entorno industrial, onde a dispoñibilidade, a compatibilidade co software de fabricante, a estabilidade e a continuidade da operación condicionan fortemente as medidas que poden implantarse.

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



Exemplo de despregue de EDR industrial. Fonte: Orange Cyberdefense (n.d.)

Obxectivo: Reducir o risco de compromiso, manipulación ou uso indebido dos equipos finais industriais, reforzando o control sobre configuracións, software, privilexios, acceso, execución e integridade dos sistemas que poden afectar de forma directa ou indirecta á operación. No ámbito industrial, o seu obxectivo inclúe tamén limitar a capacidade destes equipos para actuar como ponte entre terceiros, contornos corporativos e sistemas OT sensibles.

Como funciona / como se implanta: A súa implantación baséase na combinación de medidas como o bastionado específico do sistema, a restrición de software autorizado, o control de privilexios, a limitación de servizos innecesarios, a protección fronte a malware cando sexa compatible, a autenticación reforzada, a segregación de accesos, a detección de cambios non autorizados, a revisión de configuracións e a integración con mecanismos de monitorización. En contornos industriais, estas medidas deben aplicarse tras avaliar a compatibilidade co software de operación, coas ferramentas de fabricante, cos requisitos de rendemento e coa seguridade funcional. A súa eficacia depende de adaptar a protección ao papel exacto do endpoint: non é o mesmo un HMI, unha estación

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

de enxeñaría, un servidor historiador ou un portátil técnico empregado en mantemento. Por iso, a implantación require inventario claro, clasificación funcional e procedementos de cambio e validación ben definidos.

Vantaxes:

- Reduce a superficie de exposición de equipos con impacto directo ou indirecto sobre a operación.
- Mellora o control sobre configuracións, software, privilexios e servizos dos sistemas industriais finais.
- Dificulta a execución de accións non autorizadas, a persistencia maliciosa e a propagación dende endpoints sensibles.
- Reforza a protección de activos como HMI, estacións de enxeñaría e servidores de supervisión.
- Complementa a segmentación, a xestión de accesos e a monitorización do entorno OT.

Limitacións e consideracións:

- Non tódolos endpoints industriais admiten o mesmo nivel de protección sen impacto operativo.
- A compatibilidade con aplicacións de fabricante, software legado e requisitos de rendemento debe validarse previamente.
- En contornos industriais, unha medida tecnicamente adecuada pode resultar inviable se compromete a dispoñibilidade ou a estabilidade do proceso.
- Non substitúe a segmentación, o control de acceso remoto, a xestión de vulnerabilidades nin os procedementos operativos.
- Requírese coordinación entre seguridade, operación, mantemento, enxeñaría e, cando proceda, fabricantes ou integradores.

Relación con outros controis: Relaciónase coa protección do posto de traballo, co EDR, coa detección de integridade de ficheiros, co bastionado de HMI e sistemas de enxeñaría, coa conexión segura de dispositivos externos, coa xestión de identidades e accesos, co acceso remoto seguro, coa segmentación e coa monitorización de activos e comunicacións OT.

Casos habituais de uso: Emprégase para reforzar HMI, estacións de enxeñaría, servidores de supervisión, historiadores, equipos de mantemento con acceso a planta,

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

terminais asociados a aplicacións industriais e outros activos finais que, sen seren controladores puros, poden influír na operación ou actuar como vector cara a sistemas de maior criticidade.

Observacións / medidas compensatorias asociadas: En contornos industriais, a protección de endpoints industriais resulta especialmente útil como medida compensatoria cando non é viable actualizar de inmediato certos sistemas, substituír compoñentes legados ou reducir toda a exposición arquitectónica existente. A súa utilidade aumenta cando se combina con bastionado, control de cambios, segmentación, restrición de accesos, monitorización e procedementos claros de validación antes de introducir modificacións en equipos con impacto operativo.

5.7.3 MDM

Categoría: Protección do posto, dos activos e dos soportes de operación

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: O MDM (*Mobile Device Management* ou xestión de dispositivos móbiles) é o conxunto de capacidades orientadas á administración, configuración, control e supervisión centralizada de dispositivos móbiles e portátiles utilizados no ámbito da organización. A súa finalidade é garantir que estes equipos operen baixo políticas de seguridade coherentes, con configuracións coñecidas, mecanismos de autenticación adecuados, capacidade de control remoto e limitación do uso indebido. En contornos industriais, este control adquire especial relevancia cando tablets, smartphones, portátiles lixeiros ou outros dispositivos móbiles se empregan para tarefas de mantemento, supervisión, acceso a información técnica, xestión operativa ou interacción con aplicacións corporativas e industriais.

Funcións da solución MDM. Fonte: ManageEngine (n.d.)

Obxectivo: Reducir o risco asociado ao uso de dispositivos móbiles, reforzando o control sobre a súa configuración, o acceso á información, as aplicacións instaladas, os datos almacenados e a conectividade cos distintos servizos da organización. No ámbito industrial, o seu obxectivo inclúe tamén evitar que un dispositivo móbil pouco gobernado se converta nun punto de acceso, fuga de información ou ponte cara a sistemas e contornos con relevancia operativa.

Como funciona / como se implanta: A súa implantación baséase na inscrición dos dispositivos nunha plataforma central que permite aplicar políticas de seguridade, configurar parámetros, xestionar aplicacións autorizadas, esixir mecanismos de bloqueo e autenticación, cifrar datos, limitar funcións, rexistrar estado e, cando procede, executar accións remotas como illamento, borrado ou revogación de acceso. En contornos industriais, o MDM debe despregarse tendo en conta o papel real de cada dispositivo: acceso a correo e servizos corporativos, consulta de documentación técnica, uso de aplicacións de supervisión, conexión a plataformas de mantemento ou interacción con sistemas de xestión operativa. A súa eficacia depende de definir políticas proporcionais ao risco, evitar o uso indiscriminado de dispositivos persoais en tarefas sensibles e integrar o control móbil coas políticas de identidade, acceso remoto, clasificación da información e uso de redes sen fíos.

Vantaxes:

- Mellora o control centralizado sobre dispositivos móbiles e a súa configuración.

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

- Reduce o risco de perda de datos, uso indebido ou acceso non controlado dende terminais móbiles.
- Facilita a aplicación coherente de políticas de seguridade, autenticación e cifrado.
- Resulta útil para gobernar dispositivos con acceso a servizos corporativos, técnicos ou operativos.
- Complementa a xestión de identidades, o acceso remoto seguro e a protección da información sensible.

Limitacións e consideracións:

- A súa utilidade depende de que os dispositivos estean correctamente inventariados e inscritos na plataforma de xestión.
- Pode xerar fricción se as políticas son excesivamente restritivas ou non se adaptan ao uso real dos equipos.
- En contornos industriais, non todos os dispositivos móbiles teñen o mesmo nivel de exposición nin o mesmo impacto potencial sobre a operación.
- Non substitúe a segmentación, a xestión de accesos, a protección do posto de traballo nin os procedementos de uso seguro.
- Debe evitarse que a mobilidade introduza excepcións informais ou uso de dispositivos persoais sen gobernanza suficiente.

Relación con outros controis: Relaciónase coa protección do posto de traballo, coa seguridade no correo, coa xestión de identidades e accesos, co acceso remoto seguro, coas auditorías de dispositivos móbiles e endpoints, coa conexión segura de dispositivos externos, co NAC, coa monitorización e cos procedementos operativos orientados ao uso seguro de dispositivos con mobilidade.

Casos habituais de uso: Emprégase para gobernar smartphones e tablets corporativas, dispositivos móbiles usados por persoal técnico, equipos de supervisión ou mantemento con acceso a documentación ou plataformas de xestión, terminais con acceso a correo e servizos cloud e contornos nos que a mobilidade forma parte da operación ou do soporte diario.

Observacións / medidas compensatorias asociadas: En contornos industriais, o MDM resulta especialmente útil cando existe uso habitual de dispositivos móbiles para acceso a servizos corporativos, técnicos ou de mantemento, e pode actuar como medida

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

compensatoria parcial fronte á imposibilidade de eliminar completamente a mobilidade do entorno. A súa utilidade aumenta cando se combina con MFA, cifrado, control de aplicacións, segmentación das redes sen fíos e restrición clara do acceso a recursos sensibles segundo o perfil e o contexto do dispositivo.

5.7.4 Seguridade no email

Categoría: Protección do posto, dos activos e dos soportes de operación

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: A seguridade no email comprende o conxunto de medidas técnicas e organizativas destinadas a protexer o correo electrónico como canle de comunicación, acceso e intercambio de información, reducindo o risco de suplantación, entrega de malware, roubo de credenciais, fraude, fuga de datos e interacción con contidos maliciosos. A súa relevancia non se limita ao ámbito corporativo xeral, xa que en moitas organizacións industriais o correo continúa a ser unha vía habitual para a recepción de documentación técnica, coordinación con terceiros, xestión de mantemento, intercambio de instrucións operativas, envío de avisos e comunicación entre persoal interno e provedores. Por este motivo, un compromiso a través desta canle pode ter consecuencias que transcendan o plano informativo e afecten de maneira indirecta á operación.

Ameazas habituais que empregan o email como vector de ataque. Fonte: Norton (2022)

Obxectivo: Reducir a exposición da organización fronte a ameazas canalizadas por correo electrónico, limitando a recepción, execución ou interacción con mensaxes maliciosas, suplantacións e contidos non autorizados. No ámbito industrial, o seu obxectivo inclúe tamén evitar que o correo se converta nun punto de entrada cara a sistemas, contas, documentos técnicos ou procesos con impacto operativo.

Como funciona / como se implanta: A súa implantación baséase na combinación de mecanismos de filtrado, autenticación, análise de contidos, protección de ligazóns e anexos, políticas de entrega, illamento de mensaxes sospeitosas, protección fronte a suplantación de dominio e integración con procedementos de reporte e resposta. Isto inclúe medidas como validación de remitentes, control de reputación, análise antimalware, verificación de autenticidade do dominio, revisión de URLs, sandboxing de ficheiros, políticas de marcaxe ou corentena e integración con campañas de concienciación. En contornos industriais, estas medidas deben complementarse cun enfoque práctico sobre o uso real do correo: recepción de documentación de fabricante, envío de ficheiros de configuración, peticións de mantemento, mensaxes urxentes aparentando proceder de terceiros, interacción con provedores e circulación de información técnica ou operativa. A súa eficacia aumenta cando se integra con identidade, MFA, formación, DLP e procedementos claros de validación de comunicacións sensibles.

Vantaxes:

- Reduce un dos vectores máis frecuentes de acceso inicial e fraude.
- Mellora a protección fronte a suplantación, malware, ligazóns maliciosas e anexos perigosos.
- Reforza a seguridade das comunicacións con terceiros e a protección das identidades.
- Complementa a concienciación do persoal cunha capa técnica de filtrado e contención.
- Axuda a limitar a chegada de contidos que poderían comprometer postos, credenciais ou información sensible.

Limitacións e consideracións:

- A súa eficacia diminúe se se concibe como control illado e non se acompaña de formación, MFA e procedementos de validación.

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

- Os atacantes adaptan continuamente as técnicas de suplantación e enxeñaría social a este canal.
- En contornos industriais, certas mensaxes poden incluír documentación técnica ou anexos lexítimos que requiren excepcións ben gobernadas.
- Non substitúe o control de accesos, a protección do posto de traballo nin a revisión das interaccións con terceiros.
- Requírese axuste continuo das políticas para equilibrar seguridade, usabilidade e necesidades operativas reais.

Relación con outros controis: Relaciónase co phishing, vishing, smishing e técnicas afíns, coas campañas de concienciación e simulación, coa xestión de identidades e accesos, co DLP, coa protección do posto de traballo, co MDM, coa monitorización e operación de seguridade e cos procedementos de validación fronte a solicitudes sensibles ou non habituais.

Casos habituais de uso: Emprégase para protexer contas corporativas e técnicas, comunicacións con provedores e integradores, recepción de documentación ou anexos técnicos, peticións de acceso remoto, mensaxes con instrucións de mantemento, notificacións operativas e escenarios nos que o correo pode actuar como vía de entrada cara a servizos, credenciais ou información de valor para a organización.

Observacións / medidas compensatorias asociadas: En contornos industriais, a seguridade no email resulta especialmente útil cando se combina con MFA, procedementos de validación por segunda canle, restrición de privilexios e concienciación específica para persoal técnico, operación e mantemento. Tamén pode actuar como medida compensatoria parcial cando a organización mantén unha alta dependencia do correo para a coordinación con terceiros e non é viable reducir de inmediato todas as interaccións de risco asociadas a esta canle.

5.7.5 Conexión segura de dispositivos externos

Categoría: Protección do posto, dos activos e dos soportes de operación

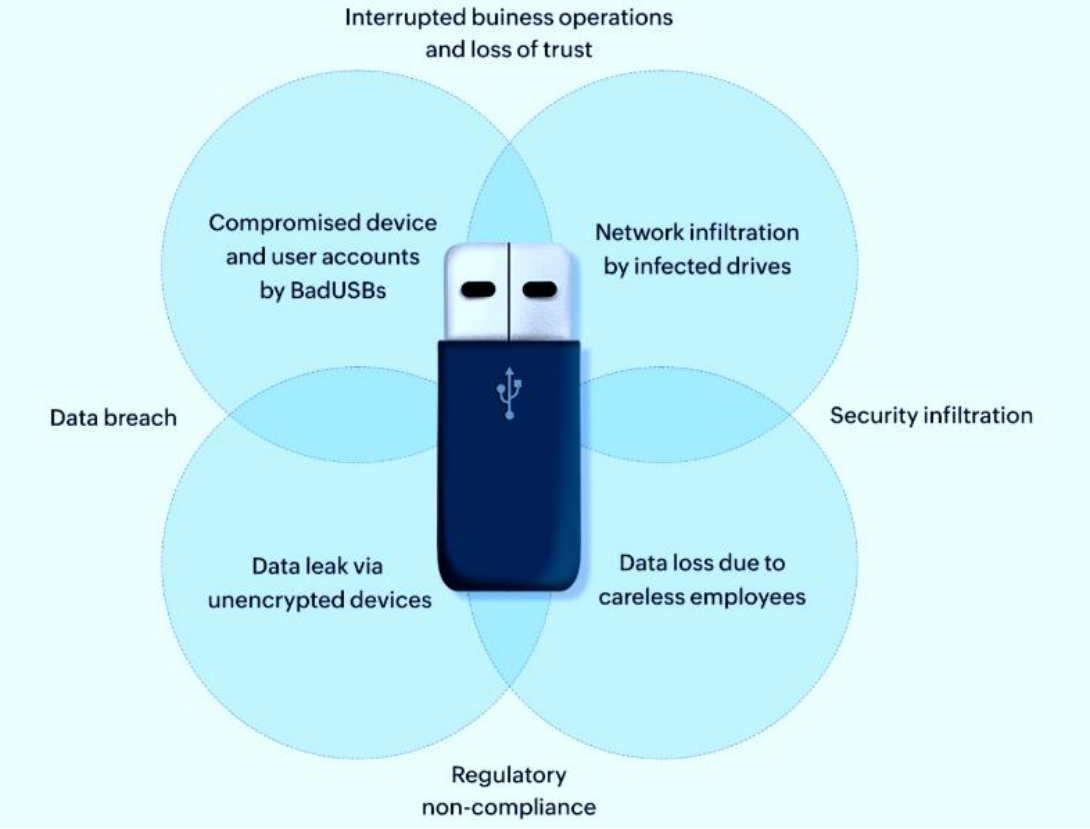
Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: A conexión segura de dispositivos externos comprende o conxunto de medidas destinadas a controlar, restrinxir, validar e supervisar a incorporación de

soportes extraíbles, portátiles de terceiros, equipos de mantemento, dispositivos USB, ferramentas de diagnóstico, medios de transferencia e outros compoñentes externos que poidan interactuar cos sistemas da organización. En contornos industriais, este control ten unha relevancia especial, xa que moitas tarefas de mantemento, actualización, configuración, soporte ou recollida de información continúan dependendo da conexión física ou lóxica de dispositivos alleos ao entorno estable da planta. Esta realidade converte os dispositivos externos nun vector recorrente de introdución de malware, alteración non autorizada, fuga de información ou acceso indebido a sistemas con impacto operativo.



Riscos de seguridade do emprego de USBs. Fonte: ManageEngine (n.d.)

Obxectivo: Reducir o risco derivado da conexión de dispositivos externos ao entorno tecnolóxico da organización, limitando a posibilidade de introducir código malicioso, copiar información sensible, executar accións non autorizadas ou establecer vías de acceso non gobernadas cara a activos corporativos ou industriais. No ámbito industrial, o seu obxectivo inclúe tamén asegurar que as tarefas lexítimas de mantemento, soporte e transferencia de información se realicen baixo condicións controladas, trazables e compatibles coa continuidade da operación.

Como funciona / como se implanta: A súa implantación baséase na definición de políticas e mecanismos que determinen que dispositivos poden conectarse, en que

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

condicións, a que equipos, por parte de quen e con que finalidade. Isto pode incluír listas de dispositivos autorizados, control de portos, validación previa de equipos de terceiros, restrición de execución automática, análise previa de soportes, uso de estacións intermedias de revisión, trazabilidade de conexións, segregación de equipos por finalidade, procedementos de autorización e control físico dos medios empregados. En contornos industriais, a súa eficacia depende de adaptar estas medidas ao uso real en planta: portátiles de mantemento, memorias USB para actualizacións ou transferencia de configuracións, equipos de fabricante, ferramentas de diagnóstico, conexións puntuais a HMI, estacións de enxeñaría ou activos de campo. A súa utilidade aumenta cando se integra con segmentación, bastionado, xestión de identidades, rexistro de intervencións e procedementos operativos claros.

Vantaxes:

- Reduce un vector frecuente de entrada de malware e acceso non controlado.
- Mellora a trazabilidade sobre que dispositivos se conectan, cando e con que finalidade.
- Axuda a protexer activos sensibles fronte a intervencións locais non gobernadas.
- Permite compatibilizar necesidades de mantemento e soporte con maior nivel de control.
- Complementa a protección do posto, o NAC, a segmentación e a xestión de privilexios.

Limitacións e consideracións:

- A súa eficacia depende de que as excepcións estean ben definidas e non se convertan nunha práctica informal permanente.
- En contornos industriais, certas tarefas de mantemento ou integración poden depender de soportes e equipos externos difíciles de substituír.
- Un control excesivamente ríxido pode xerar bloqueos operativos ou fomentar vías alternativas non gobernadas.
- Non substitúe o bastionado, a segmentación, a xestión de accesos nin a monitorización do entorno.
- Requírese coordinación con operación, mantemento, provedores e responsables técnicos para asegurar que o control sexa aplicable e sostible.

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

Relación con outros controis: Relaciónase coa protección do posto de traballo, co MDM, co NAC, coa xestión de identidades e accesos, co acceso remoto seguro, co EDR, coa detección de integridade de ficheiros, coa segmentación, coa monitorización de activos e comunicacións OT e cos procedementos operativos de mantemento e cambio.

Casos habituais de uso: Emprégase para controlar memorias USB, discos externos, portátiles de mantemento, equipos de integradores, ferramentas de diagnóstico, soportes de transferencia de configuracións, actualizacións locais, recollida de rexistros e calquera outro dispositivo alleo que precise conectarse a HMI, estacións de enxeñaría, servidores de supervisión, activos OT ou equipos corporativos con relevancia operativa.

Observacións / medidas compensatorias asociadas: En contornos industriais, a conexión segura de dispositivos externos é unha das medidas compensatorias máis relevantes cando non é viable eliminar completamente o uso de medios extraíbles ou equipos de terceiros. A súa utilidade aumenta cando se combina con procedementos formais de autorización, análise previa en estacións intermedias, control de privilexios, bastionado dos sistemas receptores, segmentación e rexistro detallado das intervencións realizadas.

5.7.6 Protección de aplicacións SaaS

Categoría: Protección do posto, dos activos e dos soportes de operación

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: A protección de aplicacións SaaS comprende o conxunto de medidas orientadas a gobernar, supervisar e asegurar o uso de servizos e aplicacións consumidos en modalidade *Software as a Service*, reducindo os riscos asociados ao acceso distribuído, á exposición de datos, á configuración insegura, ao uso indebido de identidades e á integración con outros sistemas da organización. A súa relevancia vai máis alá do ámbito estritamente corporativo, xa que moitas organizacións industriais empregan solucións SaaS para colaboración, xestión documental, ticketing, soporte remoto, monitorización, analítica, mantemento, trazabilidade, xestión de terceiros ou servizos de apoio á operación. Por este motivo, unha aplicación SaaS mal gobernada pode converterse nun punto de entrada, de fuga de información ou de dependencia insegura con impacto indirecto ou directo sobre a actividade.

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

Obxectivo: Reducir o risco derivado do uso de aplicacións SaaS, garantindo que o acceso, a configuración, a compartición de información, as integracións e os permisos asociados se xestionen de maneira controlada e coherente coas políticas de seguridade da organización. No ámbito industrial, o seu obxectivo inclúe tamén evitar que os servizos SaaS introduzan exposicións non gobernadas sobre documentación técnica, datos operativos, credenciais, fluxos de mantemento ou dependencias con terceiros.

Exemplo de problemas de seguridade en SaaS. Fonte: Intellisoft (2024)

Como funciona / como se implanta: A súa implantación parte da identificación das aplicacións SaaS autorizadas, do tipo de información que manexan, dos usuarios que acceden a elas, das integracións activas e dos riscos asociados ao seu uso. A partir desa base, establécense medidas como xestión centralizada de identidades, MFA, políticas de acceso condicional, revisión de permisos, control de compartición, configuración segura da aplicación, rexistro de actividade, protección de sesións, clasificación da información e supervisión das integracións con servizos internos ou externos. En contornos industriais, resulta especialmente importante distinguir entre aplicacións SaaS de uso xeral e aquelas que teñen relación con documentación técnica, xestión operativa, mantemento, monitorización ou servizos conectados á realidade OT, xa que o risco asociado non depende só da criticidade da aplicación, senón tamén do tipo de información ou proceso co que se vincula. A súa eficacia aumenta cando se integra con identidade, DLP, CASB/SASE, procedementos de uso seguro e revisión periódica das configuracións e permisos.

Vantaxes:

- Mellora o control sobre o uso de servizos cloud e aplicacións distribuídas.
- Reduce o risco de exposición indebida de información, permisos excesivos ou configuracións inseguras.

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

- Axuda a reforzar a protección de identidades e sesións en aplicacións de uso frecuente.
- Resulta útil para gobernar integracións con terceiros, compartición documental e servizos de apoio á operación.
- Complementa o control de accesos, o DLP e a supervisión de actividades en contornos híbridos.

Limitacións e consideracións:

- A súa eficacia depende de coñecer que aplicacións SaaS están realmente en uso e con que finalidade.
- Pode quedar limitada se existe uso informal ou non inventariado de servizos cloud por parte dos usuarios.
- En contornos industriais, o risco pode infravalorarse se se considera que unha aplicación SaaS non afecta á operación por non estar dentro da rede OT.
- Non substitúe a xestión de identidades, a clasificación da información nin os procedementos de uso seguro e compartición.
- Requírese revisión continuada de configuracións, permisos, integracións e cambios introducidos polo provedor do servizo.

Relación con outros controis: Relaciónase coa seguridade no email, co DLP, co CASB / SASE, coa xestión de identidades e accesos, co MFA, co acceso remoto seguro, co MDM, coa monitorización e operación de seguridade e cos procedementos organizativos orientados á clasificación e ao uso seguro da información.

Casos habituais de uso: Emprégase para gobernar aplicacións cloud de colaboración, xestión documental, soporte técnico, ticketing, analítica, monitorización, mantemento, relación con terceiros, intercambio de información técnica e outras plataformas SaaS que, sen formar parte da rede OT, poden influír na seguridade global da organización pola información que almacenan, procesan ou comparten.

Observacións / medidas compensatorias asociadas: En contornos industriais, a protección de aplicacións SaaS resulta especialmente útil cando a organización depende de plataformas cloud para xestión, soporte ou intercambio de información con terceiros, e pode actuar como medida compensatoria parcial fronte á imposibilidade de eliminar determinadas dependencias externas. A súa utilidade aumenta cando se combina con MFA, control de permisos, DLP, políticas de acceso condicional, revisión de integracións

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

e procedementos claros sobre o tipo de información que pode almacenarse, compartirse ou tratarse nestes servizos.

5.8 Identidade, acceso e administración segura

O control rigoroso das identidades, dos privilexios e das sesións de acceso constitúe un núcleo fundamental da ciberseguridade industrial moderna. Nesta subsección intégranse **capacidades destinadas a garantir que o acceso aos sistemas, activos e servizos se realiza de maneira autenticada, trazable, proporcionada ao risco e compatible coas necesidades de operación, mantemento e intervención de terceiros**.

5.8.1 MFA

Categoría: Identidade, acceso e administración segura

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

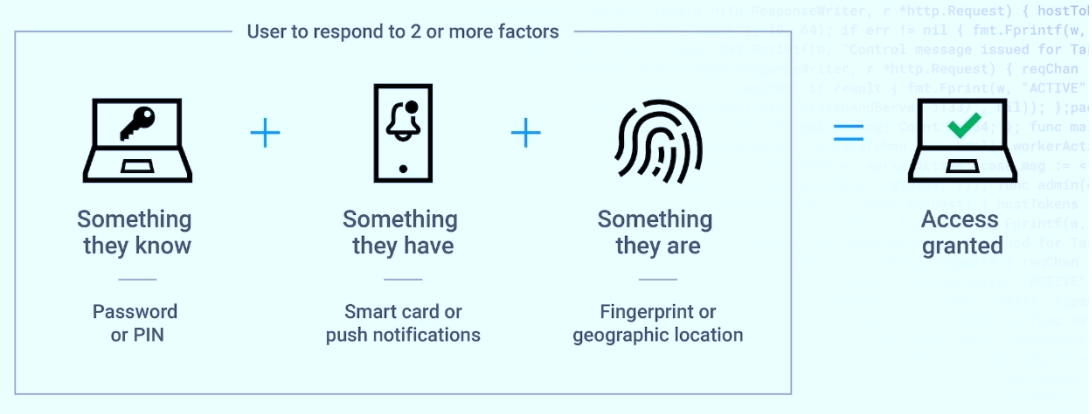
Descrición: A autenticación multifactor (MFA, *Multi-Factor Authentication*) é un mecanismo de seguridade que require a combinación de dous ou máis factores de autenticación independentes para verificar a identidade dun usuario antes de conceder acceso a un sistema, servizo ou recurso. Estes factores adoitan basearse en algo que o usuario sabe, algo que posúe ou algo que é (biometría). O seu propósito é reducir a dependencia exclusiva das credenciais tradicionais, limitando o risco de acceso indebido en caso de roubo, filtración, reutilización ou compromiso dun contrasinal. En contornos industriais, o MFA resulta especialmente relevante para accesos remotos, contas privilexiadas, portais de xestión, servizos expostos e sistemas intermedios dende os que pode acadarse a rede operativa.

Obxectivo: Reducir a probabilidade de acceso non autorizado derivado do compromiso de credenciais, reforzando a verificación de identidade e dificultando o uso indebido de contas con acceso a recursos sensibles. No ámbito industrial, o seu obxectivo inclúe tamén protexer puntos de entrada que poden servir de ponte cara a servizos de supervisión, administración, mantemento ou interacción con activos OT.

Como funciona / como se implanta: A súa implantación baséase na incorporación dun segundo factor —ou máis dun— ao proceso de autenticación habitual. Isto pode materializarse mediante aplicacións autenticadoras, tokens físicos, certificados,

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

mensaxes de verificación, claves de seguridade ou outros mecanismos equivalentes, segundo o nivel de risco e o contexto de uso. En contornos industriais, a súa aplicación debe priorizar os accesos con maior impacto potencial: administración remota, acceso de terceiros, contas privilexiadas, servizos publicados, VPN, servidores de salto, portais de soporte e outros puntos de interconexión entre IT e OT. A súa eficacia depende non só da fortaleza do segundo factor, senón tamén da correcta integración coa xestión de identidades, co control de sesións, cos procedementos operativos e coa experiencia real de uso, evitando solucións que induzan excepcións permanentes ou deterioro da operativa.



Funcionamento do MFA. Fonte: Akamai (n.d.)

Vantaxes:

- Reduce de maneira significativa o risco asociado ao roubo ou reutilización de contrasinais.
- Reforza a protección de contas privilexiadas, accesos remotos e servizos expostos.
- Mellora a seguridade de identidades con acceso a contornos sensibles ou intermedios.
- Complementa a xestión de identidades e accesos cunha capa adicional de verificación.
- Resulta especialmente útil en escenarios con terceiros, mobilidade e administración distribuída.

Limitacións e consideracións:

- A súa eficacia diminúe se se mantén como excepción o acceso sen segundo factor en contas críticas.

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

- En contornos industriais, a súa implantación pode verse condicionada por compatibilidade, dispoñibilidade ou procedementos legados.
- Non substitúe o principio de mínimo privilexio, a segmentación nin o control de sesións.
- Requírese unha boa xestión do ciclo de vida dos factores, das altas e baixas de usuarios e dos mecanismos de recuperación.
- Debe evitarse que a dificultade operativa derive en solucións informais ou compartición de credenciais e dispositivos de autenticación.

Relación con outros controis: Relaciónase coa IAM, co PAM, co acceso remoto seguro, coa xestión de sesións e trazabilidade, co control de accesos de terceiros e provedores, coa seguridade no email, co MDM e coas medidas compensatorias orientadas a reducir o risco de acceso indebido en contornos con exposición elevada.

Casos habituais de uso: Emprégase en accesos VPN, portais de administración, servidores de salto, contas privilexiadas, plataformas cloud, servizos de acceso remoto de terceiros, consolas de xestión, correo corporativo, aplicacións críticas e recursos intermedios dende os que pode acadarse información sensible ou contornos operativos.

Observacións / medidas compensatorias asociadas: En contornos industriais, o MFA é unha das medidas compensatorias máis eficaces cando non é viable reducir de inmediato toda a exposición dun servizo remoto ou eliminar certos accesos necesarios para operación e mantemento. A súa utilidade aumenta cando se combina con permisos limitados, segmentación, control de sesións, trazabilidade e revisión periódica das contas con capacidade de acceso a recursos críticos.

5.8.2 IAM

Categoría: Identidade, acceso e administración segura

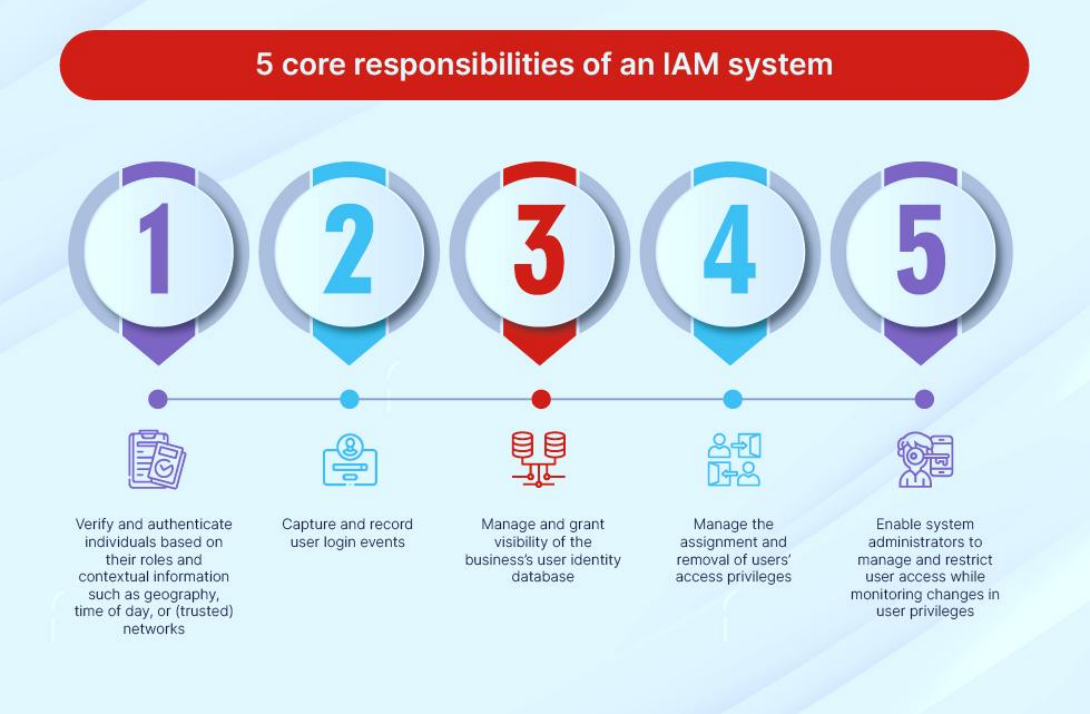
Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect, Govern

Descrición: A xestión de identidades e accesos (IAM, *Identity and Access Management*) comprende o conxunto de políticas, procesos e capacidades técnicas orientadas a definir, administrar, revisar e retirar os permisos de acceso aos sistemas, aplicacións, datos e servizos da organización. O seu propósito é asegurar que cada persoa, conta ou entidade dispoña unicamente dos accesos necesarios para desempeñar as súas funcións,

baixo criterios de trazabilidade, segregación de funcións e control continuado do ciclo de vida das identidades. En contornos industriais, a IAM resulta especialmente relevante pola coexistencia de usuarios internos, persoal de operación, mantemento, enxeñaría, terceiros, contas de servizo e accesos híbridos entre contornos IT e OT.



Funcións principais dun sistema IAM. Fonte: Fortinet (n.d.)

Obxectivo: Reducir o risco de acceso indebido, privilexios excesivos, contas non gobernadas ou permanencia innecesaria de permisos, reforzando o principio de mínimo privilexio e a coherencia do modelo de acceso da organización. No ámbito industrial, o seu obxectivo inclúe tamén limitar a exposición derivada de contas con acceso a servizos sensibles, sistemas intermedios, plataformas de supervisión, infraestruturas de mantemento e recursos dende os que poida alcanzarse o entorno operativo.

Como funciona / como se implanta: A súa implantación baséase na definición dun modelo de identidades e permisos asociado ás funcións reais da organización, aos perfís de usuario, ás responsabilidades operativas e ás necesidades de acceso a sistemas e servizos. Isto inclúe a alta, modificación e baixa de contas; a asignación de roles; a revisión periódica de permisos; o control das contas compartidas, técnicas e de servizo; a federación cando proceda; e a integración con mecanismos como MFA, políticas de acceso condicional, rexistro de actividade e procedementos de autorización. En contornos industriais, a IAM debe adaptarse a realidades específicas, como persoal de planta por quendas, acceso temporal de provedores, contas vinculadas a aplicacións de fabricante, servizos intermedios, HMI, estacións de enxeñaría ou contornos de

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

administración que conectan IT e OT. A súa eficacia depende de que o modelo de acceso reflicta a realidade operativa e non se limite a unha visión puramente corporativa.

Vantaxes:

- Reduce a acumulación de privilexios innecesarios e o acceso non gobernado.
- Mellora a coherencia entre funcións reais, permisos asignados e trazabilidade.
- Facilita a aplicación do principio de mínimo privilexio e da segregación de funcións.
- Reforza o control sobre contas internas, de terceiros, técnicas e de servizo.
- Complementa o MFA, o PAM e o control de sesións cunha base sólida de gobernanza de acceso.

Limitacións e consideracións:

- A súa utilidade diminúe se os roles e permisos non reflicten a operativa real da organización.
- En contornos industriais, poden existir contas legadas, compartidas ou dependentes de software de fabricante difíciles de gobernar a curto prazo.
- Non substitúe o PAM, o control de sesións nin a segmentación do acceso entre dominios.
- Requírese revisión continua do ciclo de vida das identidades, especialmente en contornos con terceiros, quendas e cambios frecuentes de persoal.
- Debe evitarse que a necesidade operativa xustifique de forma permanente contas xenéricas, privilexios excesivos ou excepcións sen trazabilidade.

Relación con outros controis: Relaciónase co MFA, co PAM, co acceso remoto seguro, coa xestión de sesións e trazabilidade, co control de accesos de terceiros e provedores, co MDM, coa seguridade no email e coa monitorización e operación de seguridade. Constitúe a base de gobernanza sobre a que se apoian o resto dos controis de acceso e administración segura.

Casos habituais de uso: Emprégase para definir roles de acceso a sistemas corporativos e operativos, revisar permisos de persoal interno e terceiros, retirar accesos obsoletos, controlar contas de servizo, aplicar políticas de segregación de funcións, xestionar identidades en plataformas cloud e reforzar o modelo de acceso a recursos intermedios con impacto potencial sobre IT e OT.

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

Observacións / medidas compensatorias asociadas: En contornos industriais, a IAM resulta especialmente útil como medida estrutural para reducir risco acumulado en organizacións con contas antigas, privilexios excesivos ou accesos pouco gobernados. Tamén pode actuar como medida compensatoria parcial cando non é viable modificar de inmediato a arquitectura ou reducir toda a exposición existente, xa que permite acoutar mellor quen pode acceder, a que recursos e en que condicións.

5.8.3 PAM

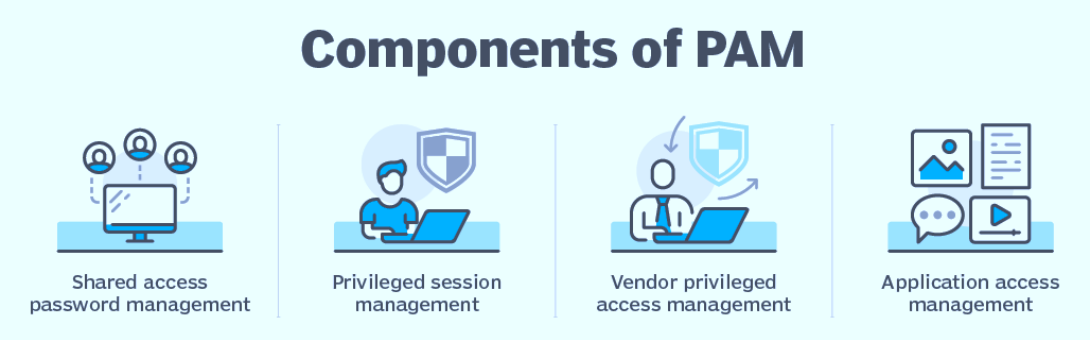
Categoría: Identidade, acceso e administración segura

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect, Govern

Descrición: A xestión de accesos privilexiados (PAM, *Privileged Access Management*) comprende o conxunto de mecanismos destinados a controlar, limitar, supervisar e protexer o uso de contas, credenciais e sesións con privilexios elevados sobre sistemas, aplicacións, infraestrutura e contornos de administración. O seu propósito é reducir o risco asociado ao abuso, compromiso ou uso indebido de accesos con capacidade de modificación, configuración, administración ou execución de accións críticas. En contornos industriais, o PAM resulta especialmente relevante porque determinadas contas privilexiadas permiten acceder a servidores de supervisión, estacións de enxeñaría, sistemas intermedios, ferramentas de mantemento, servidores de salto, servizos remotos e outros recursos dende os que pode impactarse de forma directa ou indirecta sobre a operación.



Elementos de solución PAM. Fonte: Techtarget (2025)

Obxectivo: Reducir a exposición derivada do uso de contas privilexiadas, reforzando o control sobre quen accede, en que condicións, durante canto tempo, con que permisos e con que nivel de trazabilidade. No ámbito industrial, o seu obxectivo inclúe tamén

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

limitar o risco asociado a intervencións de administración, mantemento ou soporte sobre sistemas con relevancia operativa, especialmente cando participan terceiros ou se accede a recursos de alta criticidade.

Como funciona / como se implanta: A súa implantación adoita basearse na identificación das contas privilexiadas existentes, na súa clasificación segundo criticidade e uso, e na incorporación de mecanismos como xestión segura de credenciais, rotación periódica de contrasinais, acceso xusto a tempo (JIT), autorización previa, cofres de credenciais, rexistro de sesións, restrición de uso directo de contas administrativas e control do acceso a recursos críticos a través de canles ou compoñentes específicos. En contornos industriais, o PAM debe adaptarse a realidades como accesos de mantemento, contas compartidas herdadas, intervención de fabricantes ou integradores, administración de sistemas OT, ferramentas de enxeñaría e necesidades de dispoñibilidade. A súa eficacia depende de que exista unha gobernanza clara sobre que contas son privilexiadas, quen pode utilizalas, en que condicións operativas e como se revisa a súa utilización ao longo do tempo.

Vantaxes:

- Reduce o risco asociado a contas con altos privilexios e acceso a recursos críticos.
- Mellora a trazabilidade sobre o uso de credenciais e sesións administrativas.
- Dificulta o abuso de contas compartidas, permanentes ou pouco gobernadas.
- Resulta especialmente útil para controlar intervencións de terceiros e accesos de mantemento.
- Complementa a IAM, o MFA e o control de sesións cunha capa específica sobre accesos de maior impacto.

Limitacións e consideracións:

- A súa utilidade diminúe se non se identifican correctamente todas as contas privilexiadas relevantes.
- En contornos industriais, poden existir contas herdadas, credenciais incrustadas ou dependencias de software de fabricante que dificulten a implantación completa.
- Non substitúe a segmentación, o acceso remoto seguro nin a revisión da arquitectura.

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

- Requírese coordinación estreita con operación, mantemento, seguridade e terceiros para evitar bloqueos ou excepcións permanentes.
- Debe evitarse unha implantación só formal que non modifique o uso real de contas administrativas nin reduza a dependencia de credenciais compartidas.

Relación con outros controis: Relaciónase coa IAM, co MFA, co acceso remoto seguro, coa xestión de sesións e trazabilidade, co control de accesos de terceiros e provedores, coa segmentación de rede, coa monitorización e operación de seguridade e cos procedementos de cambio e mantemento. Constitúe unha capa esencial para gobernar os accesos de maior risco dentro da administración segura.

Casos habituais de uso: Emprégase para controlar contas administrativas en servidores, HMI, estacións de enxeñaría, sistemas intermedios, infraestruturas de acceso remoto, servizos cloud, ferramentas de xestión, intervención de fabricantes ou integradores e contornos nos que o uso de credenciais privilexiadas pode ter impacto significativo sobre a seguridade ou a operación.

Observacións / medidas compensatorias asociadas: En contornos industriais, o PAM é unha das medidas máis valiosas para reducir risco cando non é viable eliminar completamente certos accesos administrativos ou dependencias de terceiros. A súa utilidade aumenta cando se combina con MFA, servidores de salto, rexistro de sesións, permisos temporais, revisión periódica de uso e segmentación do acceso a sistemas críticos.

5.8.4 Acceso remoto seguro

Categoría: Identidade, acceso e administración segura

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: O acceso remoto seguro (*Secure Remote Access*), comprende o conxunto de mecanismos, procedementos e condicións técnicas destinados a permitir a conexión a sistemas, servizos e contornos da organización dende localizacións externas sen comprometer a seguridade dos recursos accesibles nin a integridade do entorno. A súa relevancia é especialmente alta en organizacións industriais, onde o soporte remoto, o mantemento, a supervisión distribuída, a intervención de terceiros e a necesidade de continuidade operativa fan que determinadas conexións remotas sexan inevitables. O seu propósito non é simplemente permitir conectividade dende fóra, senón facelo de

forma controlada, limitada, trazable e compatible coa criticidade dos activos e coas necesidades do proceso.

Obxectivo: Reducir o risco asociado ás conexións remotas, limitando a posibilidade de acceso indebido, movemento lateral, abuso de credenciais ou exposición excesiva de servizos internos. No ámbito industrial, o seu obxectivo inclúe tamén permitir tarefas lexítimas de soporte, mantemento e administración sen abrir vías de acceso amplas ou pouco gobernadas cara a sistemas operativos, de supervisión ou de control.

Como funciona / como se implanta: A súa implantación baséase na combinación de múltiples capas de protección: autenticación reforzada, segmentación do acceso, limitación de servizos expostos, uso de servidores de salto, trazabilidade das sesións, permisos mínimos, validación previa das conexións, restrición temporal do acceso e monitorización das actividades realizadas. En contornos industriais, o acceso remoto seguro debe evitar esquemas amplos e permanentes que concedan visibilidade ou conectividade innecesaria sobre a rede OT. Pola contra, convén estruturalo arredor de recursos intermedios, autorización previa, acceso xusto no momento necesario, revisión de sesións e políticas específicas para terceiros e persoal de mantemento. A súa eficacia depende non só da tecnoloxía utilizada, senón tamén da definición clara de quen pode conectarse, a que recurso concreto, en que condicións, durante canto tempo e con que supervisión.

Vantaxes:

- Permite manter capacidades de soporte, mantemento e administración sen presenza física continua.
- Reduce o risco fronte a accesos remotos amplos, permanentes ou pouco gobernados.
- Mellora a trazabilidade sobre quen accede, cando, dende onde e con que finalidade.
- Reforza a protección de recursos intermedios e de alta criticidade fronte a terceiros ou usuarios externos.
- Resulta esencial en contornos con distribución xeográfica, servizos remotos ou dependencia de fabricantes e integradores.

Limitacións e consideracións:

- A súa utilidade diminúe se se mantén acceso amplo á rede en lugar de acceso granular a recursos concretos.

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

- En contornos industriais, as excepcións permanentes ou os accesos non revisados poden converterse nunha das principais vías de exposición.
- Non substitúe o MFA, o PAM, a segmentación nin o control de sesións, senón que depende deles para ser realmente seguro.
- Requírese coordinación entre seguridade, operación, mantemento e terceiros para definir procedementos compatibles coa continuidade.
- Debe evitarse que a urxencia operativa xustifique accesos informais, credenciais compartidas ou conexións sen trazabilidade suficiente.

Relación con outros controis: Relaciónase co MFA, coa IAM, co PAM, coa xestión de sesións e trazabilidade, co control de accesos de terceiros e provedores, coa segmentación de rede e separación IT/OT, coa DMZ industrial, cos servidores de salto, coa monitorización e operación de seguridade e cos procedementos de mantemento e cambio.

Casos habituais de uso: Emprégase para mantemento remoto, soporte técnico de terceiros, administración puntual de sistemas, acceso a recursos intermedios en DMZ, supervisión distribuída, asistencia de fabricante, intervención de integradores e operación de servizos que requiren conectividade dende localizacións externas sen expoñer directamente a rede OT.

Observacións / medidas compensatorias asociadas: En contornos industriais, o acceso remoto seguro é unha das medidas máis críticas e, ao mesmo tempo, unha das máis frecuentemente mal resoltas. Pode actuar como medida compensatoria cando non é posible eliminar a necesidade de conexión remota, sempre que se combine con MFA, PAM, servidores de salto, rexistro de sesións, permisos temporais, segmentación e revisión periódica das conexións autorizadas.

5.8.5 Xestión de sesións e trazabilidade

Categoría: Identidade, acceso e administración segura

Tipoloxía: Técnico / mixto

Función defensiva predominante: Detectivo

Función no NIST CSF: Detect

Descrición: A xestión de sesións e trazabilidade comprende o conxunto de mecanismos orientados a controlar, rexistrar, supervisar e revisar as sesións de acceso a sistemas, servizos e recursos críticos, así como a conservar evidencia suficiente sobre quen

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

accedeu, cando, dende onde, con que privilexios e que accións realizou. O seu propósito é reforzar a rendición de contas, mellorar a capacidade de análise e investigación e reducir o risco derivado de sesións non monitorizadas, mal utilizadas ou difíciles de atribuír. En contornos industriais, este control resulta especialmente relevante en accesos administrativos, intervencións de mantemento, conexións remotas, operacións realizadas por terceiros e sesións sobre sistemas con impacto operativo directo ou indirecto.

Obxectivo: Asegurar que as sesións con acceso a recursos sensibles sexan controladas e atribuíbles, reducindo o risco de actuacións non autorizadas, dificultando o abuso de contas privilexiadas e mellorando a capacidade da organización para reconstruír eventos, investigar incidentes e revisar actuacións con impacto potencial sobre o entorno. No ámbito industrial, o seu obxectivo inclúe tamén reforzar a seguridade das intervencións remotas ou administrativas sobre sistemas críticos, especialmente cando participan terceiros, persoal técnico ou contas de alto privilexio.

Como funciona / como se implanta: A súa implantación baséase na incorporación de mecanismos que permitan establecer sesións baixo condicións controladas e deixar rexistro suficiente da súa actividade. Isto pode incluír identificación unívoca do usuario, asociación da sesión co recurso e co momento temporal, rexistro de eventos relevantes, gravación ou transcrición de sesións cando proceda, conservación de evidencias, revisión posterior e integración cos procesos de análise e resposta. En contornos industriais, resulta especialmente importante aplicar estes mecanismos a accesos remotos, intervencións de mantemento, uso de servidores de salto, contas privilexiadas, sistemas de supervisión, estacións de enxeñaría e outros puntos de administración dende os que poidan executarse cambios sensibles. A súa eficacia depende de que os rexistros sexan útiles, completos, consultables e aliñados cos procedementos reais de operación e seguridade.

Vantaxes:

- Mellora a atribución das accións realizadas sobre sistemas e recursos críticos.
- Reforza a trazabilidade de accesos remotos, administrativos e privilexiados.
- Facilita a investigación de incidentes, erros operativos e usos indebidos.
- Resulta especialmente útil en intervencións de terceiros, mantemento e administración sensible.
- Complementa o MFA, o PAM e o acceso remoto seguro cunha capa de evidencia e supervisión.

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

Limitacións e consideracións:

- O seu valor diminúe se os rexistros non son completos, non se revisan ou non poden correlacionarse con outros eventos.
- En contornos industriais, a gravación ou supervisión de sesións debe compatibilizarse coas necesidades operativas e coa protección de información sensible.
- Non substitúe a segmentación, o control de identidades nin a limitación de privilexios.
- Pode xerar volume significativo de evidencia que require conservación, consulta e criterio de revisión.
- Debe evitarse que a trazabilidade se reduza a unha formalidade sen utilidade real para análise, auditoría ou resposta.

Relación con outros controis: Relaciónase co MFA, coa IAM, co PAM, co acceso remoto seguro, co control de accesos de terceiros e provedores, coa monitorización e operación de seguridade, coa resposta ante incidentes, co SIEM e cos procedementos de cambio e mantemento. Constitúe unha capa esencial para reforzar a seguridade e a auditabilidade das sesións con impacto relevante.

Casos habituais de uso: Emprégase para rexistrar intervencións remotas, sesións administrativas, accesos a servidores de salto, operacións sobre estacións de enxeñaría, actuacións de provedores, administración de sistemas críticos, revisión de cambios sensibles e investigación posterior de eventos con posible impacto sobre a operación ou a seguridade.

Observacións / medidas compensatorias asociadas: En contornos industriais, a xestión de sesións e trazabilidade resulta especialmente útil como medida compensatoria cando non é viable eliminar certos accesos administrativos ou remotos, xa que polo menos permite reforzar o control, a atribución e a revisión posterior das actuacións realizadas. A súa utilidade aumenta cando se combina con MFA, PAM, permisos temporais, servidores de salto e procedementos claros de revisión das sesións con maior criticidade.

5.8.6 Control de accesos de terceiros e provedores

Categoría: Identidade, acceso e administración segura

Tipoloxía: Organizativo / técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Govern, Protect

Descrición: O control de accesos de terceiros e provedores comprende o conxunto de medidas orientadas a regular, limitar, supervisar e revisar a conexión de entidades alleas á organización cos seus sistemas, servizos, aplicacións e contornos operativos. En contornos industriais, este control resulta especialmente relevante pola elevada dependencia de fabricantes, integradores, mantedores, provedores tecnolóxicos, servizos de soporte e empresas auxiliares que, con frecuencia, precisan acceder de forma puntual ou recorrente a recursos con impacto directo ou indirecto sobre a operación. O seu propósito é asegurar que estas interaccións se produzan baixo criterios de necesidade, mínimo privilexio, autorización formal, trazabilidade e compatibilidade coa continuidade e coa seguridade do proceso.

Obxectivo: Reducir o risco derivado do acceso de terceiros a recursos da organización, limitando a exposición, evitando permisos excesivos e asegurando que toda conexión externa se produza en condicións controladas, temporais e auditables. No ámbito industrial, o seu obxectivo inclúe tamén minimizar o risco de que provedores ou persoal externo se convertan nun vector de acceso, propagación, erro operativo ou alteración non autorizada sobre sistemas críticos.

Exemplo de riscos da cadea de subministro. Fonte: ssl2buy (n.d.)

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

Como funciona / como se implanta: A súa implantación baséase na definición de políticas específicas para terceiros, diferenciando tipos de provedor, alcance funcional do acceso, duración, recursos autorizados, canles de conexión, requisitos de autenticación e mecanismos de supervisión. Isto inclúe procesos de alta e baixa, autorización previa, revisión periódica de permisos, uso de contas nominativas, acceso xusto a tempo cando proceda, restrición de conexión a través de recursos intermedios, rexistro de sesións, limitación por horario ou finalidade e integración con procedementos de mantemento e cambio. En contornos industriais, este control debe adaptarse a escenarios habituais como soporte remoto de fabricante, intervencións de integradores, mantemento correctivo ou preventivo, actualizacións, supervisión de servizos e acceso puntual a estacións de enxeñaría, servidores de supervisión ou compoñentes intermedios. A súa eficacia depende de que os terceiros non se integren na organización mediante contas xenéricas, canles informais ou accesos permanentes sen revisión.

Vantaxes:

- Reduce a exposición derivada da conexión de entidades externas con acceso a recursos sensibles.
- Mellora a trazabilidade e a gobernanza sobre intervencións de terceiros.
- Facilita a aplicación de mínimo privilexio, temporalidade e control de alcance.
- Resulta especialmente útil en contornos con forte dependencia de fabricantes, integradores ou soporte remoto.
- Complementa o MFA, o PAM, o acceso remoto seguro e a xestión de sesións con criterios específicos para accesos externos.

Limitacións e consideracións:

- A súa eficacia diminúe se a organización mantén accesos permanentes, contas compartidas ou excepcións non revisadas para terceiros.
- En contornos industriais, as urxencias operativas poden levar a relaxar controis se non existen procedementos realistas e asumibles.
- Non substitúe a segmentación, o control de sesións nin a revisión técnica das actuacións executadas por terceiros.
- Requírese coordinación contractual, técnica e operativa entre a organización e os provedores implicados.

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

- Debe evitarse que a dependencia de terceiros derive nunha perda de gobernanza efectiva sobre os accesos críticos.

Relación con outros controis: Relaciónase co MFA, coa IAM, co PAM, co acceso remoto seguro, coa xestión de sesións e trazabilidade, cos servidores de salto, coa segmentación de rede e separación IT/OT, coa monitorización e operación de seguridade e cos procedementos de mantemento e cambio. Constitúe unha capa de control esencial en organizacións industriais con alta interacción con entidades externas.

Casos habituais de uso: Emprégase para acceso remoto de fabricantes, mantemento por parte de integradores, soporte técnico de terceiros, actualizacións puntuais sobre sistemas industriais, intervencións sobre HMI ou estacións de enxeñaría, análise de incidencias por provedores e conexión temporal a recursos intermedios ou plataformas de soporte con impacto potencial sobre a operación.

Observacións / medidas compensatorias asociadas: En contornos industriais, o control de accesos de terceiros e provedores é unha das medidas máis importantes para reducir exposición acumulada en organizacións con forte dependencia de soporte externo. Tamén pode actuar como medida compensatoria cando non é viable eliminar certos accesos necesarios para mantemento ou continuidade, sempre que se combine con MFA, PAM, permisos temporais, servidores de salto, rexistro de sesións e revisión periódica das autorizacións concedidas.

5.8.7 Programa de xestión de vulnerabilidades

Categoría: Identidade, acceso e administración segura

Tipoloxía: Organizativo / técnico / mixto

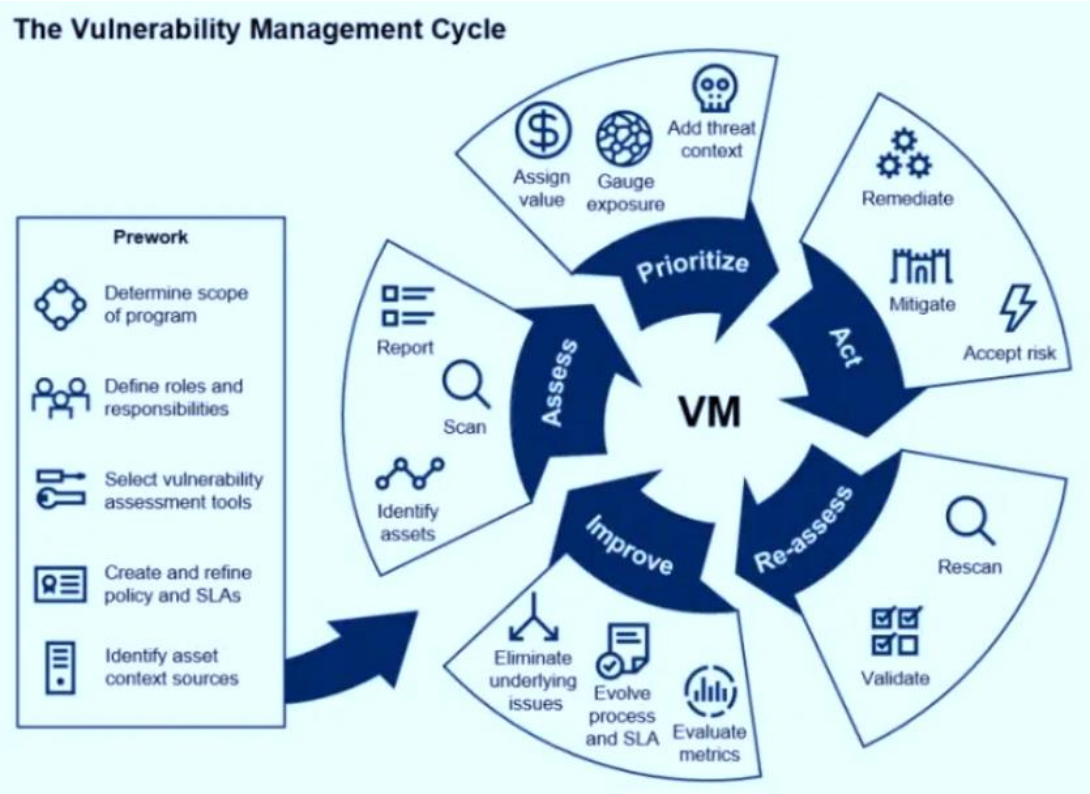
Función defensiva predominante: Preventivo

Función no NIST CSF: Identify, Govern

Descrición: O programa de xestión de vulnerabilidades é o conxunto estruturado de políticas, procesos, responsabilidades e capacidades técnicas destinadas a identificar, avaliar, priorizar, tratar e revisar as vulnerabilidades que afectan aos activos, sistemas, aplicacións e servizos da organización. A súa finalidade non é só detectar debilidades illadas, senón establecer unha disciplina continuada para comprender a exposición real do entorno e decidir de maneira proporcionada como reducila ao longo do tempo. En contornos industriais, este control resulta especialmente crítico porque a presenza de activos legados, software de fabricante, restricións de mantemento e dependencia da

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

continuidade operativa fai que a xestión da vulnerabilidade non poida limitarse a un enfoque estándar baseado unicamente en severidade técnica.



Ciclo de xestión de vulnerabilidades. Fonte: Gartner (n.d.)

Obxectivo: Dotar á organización dun modelo continuo para gobernar a exposición a vulnerabilidades, reducindo o risco de explotación mediante procesos de identificación, priorización e tratamento aliñados coa criticidade dos activos e co impacto potencial sobre a operación. No ámbito industrial, o seu obxectivo inclúe tamén asegurar que a decisión sobre como tratar cada vulnerabilidade teña en conta a dispoñibilidade, a seguridade funcional, a dependencia de terceiros e a viabilidade real das medidas correctivas ou compensatorias.

Como funciona / como se implanta: A súa implantación parte da definición dun marco de gobernanza: alcance, roles, fontes de información, activos incluídos, criterios de criticidade, metodoloxía de avaliación, tempos obxectivo de tratamento e mecanismos de revisión. Sobre esa base, intégranse actividades como recepción de avisos de seguridade, análise de vulnerabilidades, correlación con inventarios de activos, avaliación do impacto potencial, priorización segundo risco, definición de medidas de tratamento e seguimento do estado de remediación. En contornos industriais, o programa debe incorporar elementos específicos como clasificación de activos OT, dependencia de fabricantes, validación previa de cambios, bastionado, segmentación,

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

medidas compensatorias, coordinación con mantemento e revisión do risco residual cando a remediación directa non sexa viable. A súa eficacia depende de que a organización trate a vulnerabilidade como un proceso continuo de gobernanza e non como unha actividade puntual ou puramente técnica.

Vantaxes:

- Permite gobernar a exposición a vulnerabilidades de forma continuada e estruturada.
- Mellora a priorización das actuacións segundo risco real e criticidade do activo.
- Facilita a coordinación entre seguridade, sistemas, operación, mantemento e terceiros.
- Axuda a combinar remediación, bastionado e medidas compensatorias de maneira coherente.
- Reforza a trazabilidade das decisións adoptadas e o seguimento do risco residual.

Limitacións e consideracións:

- A súa utilidade diminúe se non existe un inventario fiable de activos e unha boa contextualización da súa criticidade.
- En contornos industriais, a severidade técnica dunha vulnerabilidade non sempre reflicte a prioridade real de tratamento.
- Non substitúe a análise de riscos, a segmentación, o parcheado nin o bastionado, senón que debe coordinalos.
- Requírese implicación de múltiples áreas e capacidade real para revisar, decidir e facer seguimento das medidas.
- Debe evitarse que o programa derive nun rexistro estático de vulnerabilidades sen decisións operativas nin revisión do estado real da exposición.

Relación con outros controis: Relaciónase coa análise de vulnerabilidades, coa análise de riscos tecnolóxicos, coa revisión de arquitectura, coa segmentación, co bastionado de sistemas e servizos, coa xestión de parcheado, coas validacións previas e xanela de mantemento, coa visibilidade de activos e comunicacións OT e coas medidas compensatorias. Constitúe o marco de gobernanza dende o que se ordenan e priorizan boa parte das actuacións técnicas do catálogo.

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

Casos habituais de uso: Emprégase para xestionar vulnerabilidades detectadas en activos IT e OT, analizar avisos de fabricantes, priorizar actuacións en sistemas críticos, coordinar medidas entre áreas técnicas e operativas, revisar exposición acumulada en activos legados, xustificar excepcións temporais e dar seguimento a plans de tratamento e mitigación.

Observacións / medidas compensatorias asociadas: En contornos industriais, o programa de xestión de vulnerabilidades é especialmente útil para fundamentar decisións proporcionadas cando non é viable aplicar de inmediato unha corrección directa. Neses casos, permite documentar a exposición, priorizar activos, definir medidas compensatorias —como segmentación, bastionado, limitación de acceso ou reforzo da monitorización— e revisar periodicamente se o risco residual continúa sendo asumible.

5.8.8 Xestión de parcheado

Categoría: Identidade, acceso e administración segura

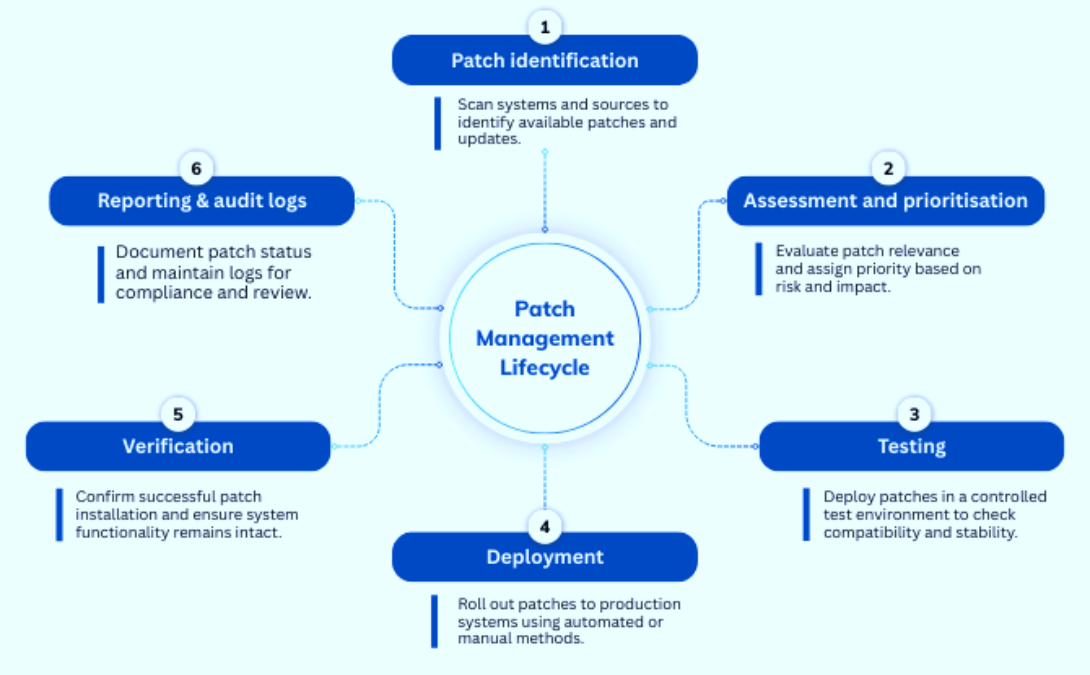
Tipoloxía: Organizativo / técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect, Govern

Descrición: A xestión de parcheado comprende o conxunto de políticas, procesos e medidas orientadas a planificar, avaliar, priorizar, aplicar e verificar actualizacións de seguridade, correccións e cambios asociados a software, firmware, sistemas operativos, aplicacións e compoñentes tecnolóxicos. A súa finalidade é reducir a exposición derivada de vulnerabilidades coñecidas mediante a incorporación controlada de correccións que melloren a protección dos activos sen comprometer a estabilidade do entorno. En contornos industriais, este control resulta especialmente delicado, xa que o parcheado non pode tratarse como unha actividade automática ou indiscriminada: debe compatibilizarse coa continuidade da operación, coa seguridade funcional, co soporte de fabricante e coa dispoñibilidade de xanelas de intervención aceptables.

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



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

Obxectivo: Reducir o risco asociado a vulnerabilidades coñecidas mediante a aplicación controlada de actualizacións e correccións, asegurando que o parcheado se realice con criterio, priorización e verificación suficientes. No ámbito industrial, o seu obxectivo inclúe tamén minimizar o risco de que unha actualización introduza inestabilidade, incompatibilidades ou alteracións non desexadas sobre sistemas críticos para a operación.

Como funciona / como se implanta: A súa implantación parte da identificación dos activos parcheables, da recepción e análise de avisos de seguridade, da avaliación de relevancia das actualizacións e da definición de criterios para decidir cando, como e sobre que sistemas aplicar cada corrección. Isto inclúe priorización (preséntanse estratexias para isto en [2]) segundo criticidade, compatibilidade, exposición e risco, así como procedementos de validación, autorización, planificación e verificación posterior. En contornos industriais, a xestión de parcheado debe estar estreitamente ligada ao inventario de activos, á dependencia de fabricantes, ás recomendacións do provedor, á dispoñibilidade de contornos de proba, ás xanelas de mantemento e ás medidas compensatorias aplicables cando a actualización non sexa viable a curto prazo. A súa eficacia depende de tratar o parcheado como un proceso gobernado, coordinado e revisable, e non como unha simple tarefa técnica de aplicación de actualizacións.

Vantaxes:

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

- Reduce a exposición a vulnerabilidades coñecidas cando as actualizacións son viables e adecuadas.
- Mellora a disciplina de mantemento e a trazabilidade sobre o estado de actualización dos activos.
- Facilita a coordinación entre seguridade, sistemas, operación, mantemento e terceiros.
- Permite integrar criterios de risco, compatibilidade e criticidade na decisión de actualización.
- Complementa o programa de xestión de vulnerabilidades cunha vía estruturada de remediación directa.

Limitacións e consideracións:

- En contornos industriais, non tódalas actualizacións poden aplicarse inmediatamente nin con seguridade.
- A compatibilidade co software de fabricante, a estabilidade e a dispoñibilidade deben validarse previamente.
- Non substitúe a segmentación, o bastionado nin outras medidas compensatorias cando o parcheado non é viable.
- Requírese coordinación estreita con mantemento, operación e provedores para evitar impactos non desexados sobre o proceso.
- Debe evitarse unha visión simplista baseada só na dispoñibilidade do parche, sen avaliar o contexto real do activo e o risco de cambio.

Relación con outros controis: Relaciónase co programa de xestión de vulnerabilidades, coa análise de vulnerabilidades, co bastionado de sistemas e servizos, coas validacións previas e xanela de mantemento, coa segmentación, coa visibilidade de activos e comunicacións OT, coa monitorización e coas medidas compensatorias orientadas a reducir exposición cando non é posible actualizar.

Casos habituais de uso: Emprégase para planificar a actualización de servidores, estacións de traballo, HMI, compoñentes software, firmware, sistemas operativos, aplicacións industriais e equipos de soporte cando existen parches dispoñibles, avaliando a súa relevancia segundo a criticidade do activo, a exposición e o impacto operativo esperado.

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

Observacións / medidas compensatorias asociadas: En contornos industriais, a xestión de parcheado é especialmente útil cando se integra cun proceso formal de decisión que permita diferenciar entre actualización inmediata, actualización diferida e tratamento compensatorio. Neses casos, se o parche non pode aplicarse, a organización debe recorrer a medidas como segmentación, bastionado, limitación de acceso, reforzo da monitorización ou illamento funcional do activo afectado, mantendo trazabilidade sobre o risco residual e revisión periódica da decisión adoptada.

5.8.9 Bastionado de sistemas e servizos

Categoría: Identidade, acceso e administración segura

Tipoloxía: Organizativo / técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

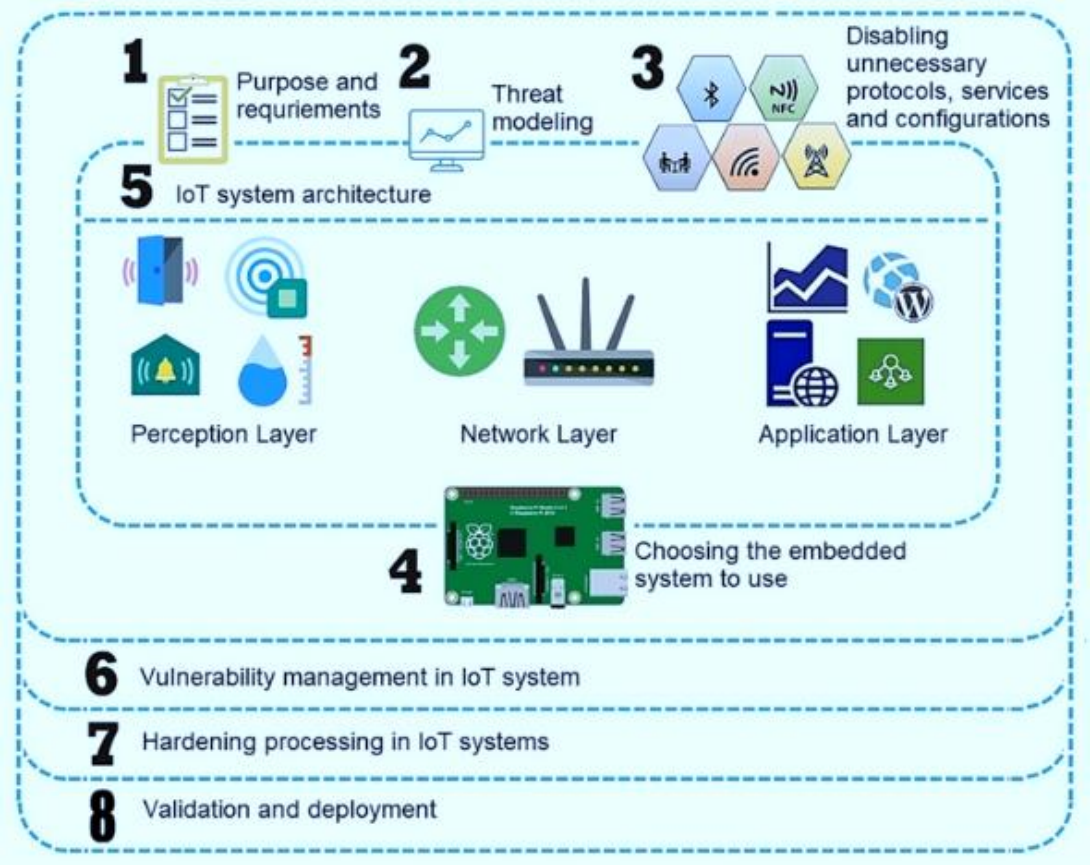
Descrición: O bastionado de sistemas e servizos comprende o conxunto de medidas orientadas a reducir a superficie de exposición dos activos mediante a configuración segura dos seus compoñentes, a desactivación de funcións innecesarias, a eliminación de servizos non requiridos, o endurecemento de parámetros de seguridade e a limitación das posibilidades de abuso ou explotación. A súa finalidade é que os sistemas operen cunha configuración máis controlada, previsible e resistente fronte a erros, usos indebidos, compromiso de credenciais, execución non autorizada ou explotación de vulnerabilidades coñecidas. En contornos industriais, este control resulta especialmente importante porque moitos activos non poden actualizarse con frecuencia, dependen de software de fabricante ou permanecen longos períodos en servizo, polo que a redución da exposición mediante configuración segura adquire un valor central.

Obxectivo: Reducir o risco asociado á configuración insegura dos sistemas e servizos, limitando a superficie de ataque e dificultando a explotación de debilidades existentes. No ámbito industrial, o seu obxectivo inclúe tamén reforzar a protección de activos con soporte limitado, sistemas legados, compoñentes de operación e servizos intermedios cuxo nivel de exposición non pode reducirse unicamente mediante parcheado ou renovación tecnolóxica.

Como funciona / como se implanta: A súa implantación baséase na revisión e axuste das configuracións dos sistemas para asegurar que só permanezan activos os compoñentes, servizos, protocolos, portos, permisos e funcionalidades estritamente

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

necesarios para a súa finalidade. Isto inclúe, entre outras medidas, desactivar servizos non utilizados, reforzar políticas de autenticación, limitar privilexios, configurar rexistro e auditoría, protexer ficheiros e directorios sensibles, eliminar software innecesario, aplicar configuracións seguras por defecto e revisar parámetros que poidan incrementar a exposición do sistema. En contornos industriais, o bastionado debe aplicarse con especial prudencia, xa que certos cambios poden afectar á compatibilidade con aplicacións de fabricante, protocolos específicos, ferramentas de mantemento ou necesidades do proceso. A súa eficacia depende de coñecer ben a función do activo, de validar previamente os cambios e de diferenciar entre activos nos que se pode aplicar un bastionado máis intenso e aqueles nos que só son viables medidas máis graduais.



Proposta de modelo de bastionado en IoT. Fonte: Echeverría, Ceballos et al. (2021)

Vantaxes:

- Reduce a superficie de exposición dos sistemas e dificulta a explotación de debilidades.
- Mellora a previsibilidade e control das configuracións dos activos.
- Resulta especialmente útil en sistemas legados ou con limitacións de actualización.

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

- Complementa o parcheado e a segmentación con medidas directas sobre o propio activo.
- Axuda a limitar software innecesario, servizos expostos e permisos excesivos.

Limitacións e consideracións:

- A súa aplicación pode verse limitada pola compatibilidade con software de fabricante ou coas condicións de soporte.
- En contornos industriais, un cambio de configuración mal validado pode introducir inestabilidade ou impacto operativo.
- Non substitúe o parcheado, a segmentación nin a xestión de accesos, senón que debe complementarse con eles.
- Requírese coñecemento técnico detallado do activo e da súa función no proceso para evitar cambios contraproducentes.
- Debe evitarse tanto o bastionado insuficiente como a aplicación indiscriminada de guías xenéricas non adaptadas ao entorno.

Relación con outros controis: Relaciónase co programa de xestión de vulnerabilidades, coa xestión de parcheado, coas validacións previas e xanela de mantemento, coa protección do posto de traballo, coa detección de integridade de ficheiros, coa segmentación, coa monitorización e coas medidas compensatorias orientadas a reducir exposición en activos críticos ou con soporte limitado.

Casos habituais de uso: Emprégase en servidores, estacións de traballo, HMI, estacións de enxeñaría, sistemas intermedios, servizos remotos, compoñentes de supervisión e outros activos nos que se precisa reducir funcionalidade innecesaria, reforzar configuracións e limitar a exposición sen modificar substancialmente a arquitectura.

Observacións / medidas compensatorias asociadas: En contornos industriais, o bastionado é unha das medidas compensatorias máis útiles cando non resulta viable aplicar de inmediato actualizacións, substituír compoñentes ou reestruturar a arquitectura. A súa utilidade aumenta cando se combina con segmentación, limitación de acceso, monitorización reforzada, control de cambios e validación previa das modificacións antes da súa aplicación en sistemas con impacto operativo.

5.8.10 Validacións previas e xanela de mantemento

Categoría: Identidade, acceso e administración segura

Tipoloxía: Organizativo / técnico / mixto

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

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect, Govern

Descrición: As validacións previas e a xanela de mantemento comprenden o conxunto de prácticas orientadas a comprobar de maneira anticipada a compatibilidade, viabilidade e impacto dos cambios técnicos antes da súa aplicación en sistemas en produción, así como a delimitar períodos específicos nos que esas intervencións poden executarse con menor risco para a operación. O seu propósito é evitar que actualizacións, modificacións de configuración, cambios de compoñentes, tarefas de bastionado ou actuacións correctivas se realicen sen avaliación previa suficiente nin en momentos incompatibles coa continuidade do servizo. En contornos industriais, este control resulta especialmente relevante porque a introdución de cambios non validados pode afectar á dispoñibilidade, á estabilidade do proceso, á seguridade funcional ou á coordinación entre sistemas e operación.

Obxectivo: Reducir o risco asociado á aplicación de cambios en sistemas e servizos, asegurando que as intervencións técnicas se executen tras unha validación suficiente e dentro de períodos controlados que minimicen o impacto operativo. No ámbito industrial, o seu obxectivo inclúe tamén evitar que actuacións orientadas á mellora da seguridade introduzan indispoñibilidade, incompatibilidades ou alteracións non desexadas sobre activos con función crítica.

Como funciona / como se implanta: A súa implantación baséase en establecer procedementos para revisar previamente os cambios propostos, avaliar a súa compatibilidade co entorno, comprobar dependencias, identificar riscos asociados e definir condicións de execución e reversión. Isto pode incluír o uso de contornos de proba, simulacións, revisión documental, validación con fabricantes, contraste con mantemento e operación, planificación de tarefas e definición de criterios de aceptación. A xanela de mantemento, pola súa parte, delimita o período temporal no que a intervención pode realizarse con menor impacto sobre a actividade normal, contando cos recursos necesarios e cos equipos implicados preparados para supervisar, validar e, se é preciso, reverter o cambio. En contornos industriais, a súa eficacia depende de que estas prácticas non se reduzan a unha formalidade, senón que reflictan a criticidade real do activo, o momento operativo, o impacto potencial sobre o proceso e a dispoñibilidade de medios para validar o comportamento posterior do sistema.

Vantaxes:

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

- Reduce o risco de introducir cambios técnicos con impacto non previsto sobre a operación.
- Mellora a coordinación entre seguridade, sistemas, operación, mantemento e terceiros.
- Facilita a planificación ordenada de actualizacións, bastionado, correccións e intervencións técnicas.
- Reforza a capacidade de anticipar incompatibilidades e definir medidas de reversión.
- Resulta esencial en contornos industriais nos que a continuidade do proceso condiciona fortemente a aplicación de cambios.

Limitacións e consideracións:

- A súa utilidade diminúe se non existen contornos de proba, documentación suficiente ou participación real das áreas implicadas.
- En contornos industriais, non sempre é doado dispoñer de xanelas amplas ou replicar con fidelidade as condicións da produción.
- Non substitúe a análise de riscos, o programa de xestión de vulnerabilidades nin a xestión de parcheado, senón que debe coordinalos.
- Pode ralentizar a aplicación de medidas correctivas se o proceso non está ben deseñado ou resulta excesivamente burocrático.
- Debe evitarse que a presión operativa leve a omitir validacións necesarias ou a executar cambios fóra dos períodos previstos sen control suficiente.

Relación con outros controis: Relaciónase co programa de xestión de vulnerabilidades, coa xestión de parcheado, co bastionado de sistemas e servizos, coa análise de riscos tecnolóxicos, coa revisión de arquitectura, coa continuidade de negocio e resiliencia operativa, coa resposta ante incidentes e cos procedementos de cambio e mantemento. Constitúe unha capa de gobernanza esencial para aplicar medidas técnicas de forma compatible coa operación.

Casos habituais de uso: Emprégase antes de aplicar parches, cambios de configuración, modificacións en HMI ou estacións de enxeñaría, actualizacións de software de fabricante, intervencións sobre sistemas de supervisión, tarefas de bastionado, cambios de conectividade, actuacións correctivas sobre activos críticos e calquera outra modificación con potencial impacto sobre a continuidade ou a seguridade do proceso.

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

Observacións / medidas compensatorias asociadas: En contornos industriais, as validacións previas e a xanela de mantemento son especialmente útiles para reducir o risco de que medidas de seguridade ben intencionadas xeren efectos adversos sobre a operación. Tamén poden actuar como soporte esencial das medidas compensatorias, permitindo decidir cando un cambio pode executarse con seguridade e cando, pola contra, debe diferirse e acompañarse temporalmente de segmentación, bastionado, reforzo de monitorización ou limitación adicional do acceso.

5.9 Resposta, recuperación e continuidade

A resiliencia dunha organización non se mide só pola súa capacidade de evitar incidentes, senón tamén pola rapidez e eficacia coa que pode conter, investigar, restaurar e recuperar a operación. Este bloque recolle **controis e servizos orientados á resposta ante incidentes, á análise forense, á restauración de sistemas e datos e á continuidade operativa**, reforzando a capacidade da entidade para resistir e superar eventos adversos.

5.9.1 Soporte á resposta ante incidentes

Categoría: Resposta, recuperación e continuidade

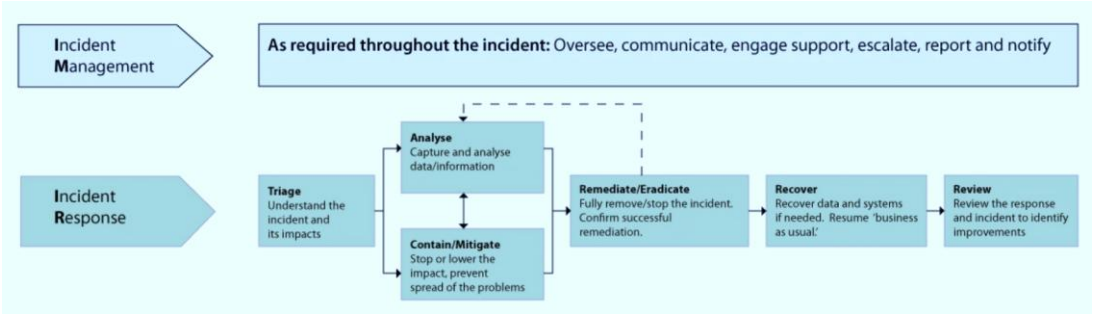
Tipoloxía: Organizativo / técnico / mixto

Función defensiva predominante: Correctivo / de recuperación

Función no NIST CSF: Respond, Recover

Descrición: O soporte á resposta ante incidentes comprende o conxunto de capacidades, procedementos, roles e medios técnicos destinados a preparar, coordinar e executar actuacións fronte a eventos de seguridade que poidan afectar aos sistemas, servizos, activos ou procesos da organización. A súa finalidade é asegurar que, unha vez detectado un incidente, existan mecanismos claros para analizar a situación, conter o seu impacto, escalar decisións, coordinar aos equipos implicados e recuperar o control do entorno afectado. En contornos industriais, este control resulta especialmente relevante porque a resposta non pode formularse só dende a óptica tecnolóxica, senón que debe considerar tamén a continuidade da operación, a seguridade do proceso, a dependencia de terceiros, a seguridade funcional e o risco de que unha actuación incorrecta agrave a situación.

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



Etapas da resposta ante incidentes. Fonte: NCSC (2019)

Obxectivo: Dotar á organización dunha capacidade estruturada para responder de forma ordenada e eficaz ante incidentes de seguridade, reducindo o tempo de reacción, limitando o impacto e mellorando a coordinación entre as áreas implicadas. No ámbito industrial, o seu obxectivo inclúe tamén asegurar que as decisións de contención, illamento, análise ou recuperación se adopten cun coñecemento suficiente do impacto potencial sobre a produción, os servizos e os sistemas ciberfísicos.

Como funciona / como se implanta: A súa implantación baséase na definición dun modelo operativo de resposta: procedementos, roles, canles de comunicación, criterios de escalado, tipoloxías de incidente, mecanismos de coordinación interna e relación con terceiros ou organismos externos cando proceda. Isto inclúe a identificación dos equipos responsables, a dispoñibilidade de medios técnicos para análise e contención, a preparación de guías de actuación, a coordinación con operación e mantemento e a realización de exercicios ou revisións periódicas. En contornos industriais, o soporte á resposta debe contemplar escenarios específicos como acceso remoto comprometido, manipulación de contas privilexiadas, propagación entre IT e OT, indispoñibilidade de sistemas de supervisión, afectación a HMI ou estacións de enxeñaría, alteración de configuracións, interacción con terceiros e incidentes con impacto sobre a continuidade do proceso. A súa eficacia depende de que o modelo estea adaptado ao entorno real e de que as decisións non se tomen illadamente dende seguridade sen coordinación coas áreas operativas.

Vantaxes:

- Mellora a capacidade de reacción fronte a incidentes e reduce o tempo de resposta.
- Facilita a coordinación entre seguridade, sistemas, operación, mantemento e dirección.
- Axuda a conter incidentes e limitar o seu impacto sobre os servizos e a operación.

- Reforza a trazabilidade e a toma de decisións baixo procedementos coñecidos.
- Resulta esencial para responder de maneira segura en contornos con impacto operativo ou ciberfísico.

Limitacións e consideracións:

- A súa utilidade diminúe se se reduce a documentación formal sen capacidade real de execución.
- En contornos industriais, unha resposta tecnicamente correcta pode resultar operativamente inadecuada se non se avalía o impacto sobre o proceso.
- Non substitúe a detección temperá, a segmentación nin a preparación previa do entorno.
- Requírese coordinación continuada, adestramento e revisión dos procedementos para que resulten realmente aplicables.
- Debe evitarse a dependencia exclusiva de persoas concretas ou coñecemento non documentado para a xestión das primeiras actuacións.

Relación con outros controis: Relaciónase co SOC, co MDR, co SIEM, co IDS/IPS, co NDR, coa monitorización ciberfísica / MES, coa visibilidade de activos e comunicacións OT, cos servizos forenses, coas copias de seguridade e restauración, coa recuperación de operación e continuidade e co plan de continuidade de negocio e resiliencia operativa.

Casos habituais de uso: Emprégase para coordinar a resposta fronte a accesos remotos comprometidos, infeccións por malware ou ransomware, propagación entre dominios IT/OT, actividade anómala en contas privilexiadas, afectación de sistemas de supervisión, intervencións non autorizadas de terceiros, alteración de configuracións e incidentes que requiren análise, contención e recuperación baixo presión operativa.

Observacións / medidas compensatorias asociadas: En contornos industriais, o soporte á resposta ante incidentes é especialmente valioso cando a organización non pode eliminar totalmente certas exposicións pero si prepararse mellor para detectalas e xestionalas con rapidez. A súa utilidade aumenta cando se combina con procedementos específicos para OT, canles de escalado claras, inventario de activos críticos, trazabilidade de accesos, medios de análise dispoñibles e coordinación previa con operación, mantemento e terceiros.

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

5.9.2 Servizos forenses

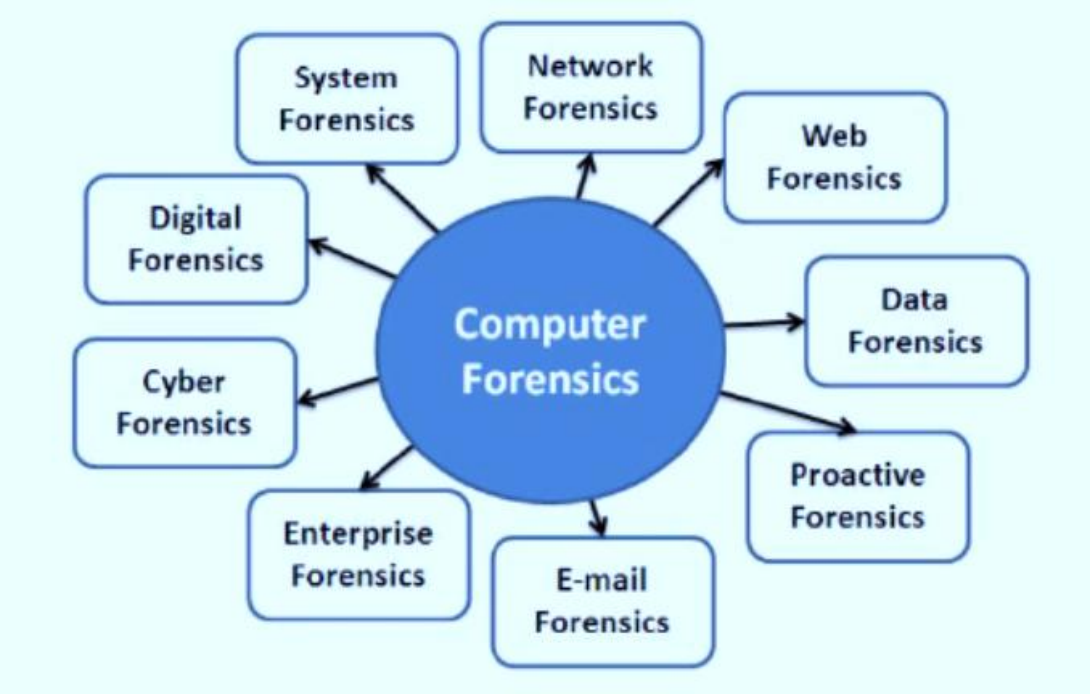
Categoría: Resposta, recuperación e continuidade

Tipoloxía: Técnico / mixto

Función defensiva predominante: Correctivo / de recuperación

Función no NIST CSF: Respond

Descrición: Os servizos forenses comprenden o conxunto de capacidades, técnicas e procedementos destinados á identificación, preservación, recollida, análise e interpretación de evidencias dixitais relacionadas cun incidente de seguridade. A súa finalidade é reconstruír o ocorrido, determinar vectores de acceso, alcance, impacto, persistencia e posibles responsabilidades, así como apoiar a toma de decisións técnicas, organizativas e, cando proceda, legais ou regulamentarias. En contornos industriais, esta capacidade resulta especialmente relevante porque os incidentes poden afectar non só a sistemas informáticos convencionais, senón tamén a compoñentes OT, estacións de enxeñería, HMI, servidores de supervisión, rexistros operativos, contas de terceiros e evidencias asociadas ao comportamento do proceso.



Actividades do ámbito forense dixital. Fonte: Sridhar N. et al. (2011)

Obxectivo: Obter e analizar evidencias fiables que permitan comprender a natureza e o alcance dun incidente, apoiar a súa contención e recuperación, e preservar información útil para aprendizaxe posterior, revisión interna ou actuacións legais e de cumprimento. No ámbito industrial, o seu obxectivo inclúe tamén identificar se existiu impacto sobre

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

sistemas con función operativa, manipulación de configuracións, alteración de parámetros, acceso indebido de terceiros ou efectos indirectos sobre a continuidade do proceso.

Como funciona / como se implanta: A súa implantación require procedementos claros para preservar evidencias, delimitar cadea de custodia, decidir cando e como intervir sobre os sistemas afectados e coordinar a análise coas necesidades de continuidade operativa. Isto pode incluír a adquisición de rexistros, imaxes de disco, memoria, eventos de rede, evidencias de endpoints, sesións administrativas, configuracións, ficheiros de proxecto, rexistros de HMI, datos de supervisión ou información de plataformas de monitorización. En contornos industriais, o enfoque forense debe adaptarse ás restricións propias do entorno: non sempre é viable illar ou apagar un sistema para capturalo, nin todos os activos OT permiten técnicas forenses estándar sen risco operativo. Por iso, adoita ser necesario combinar análise tradicional con revisión de rexistros, telemetría, trazabilidade de accesos, copia de configuracións, correlación con eventos de rede e coñecemento do proceso. A súa eficacia depende de actuar con rapidez, criterio e coordinación entre seguridade, operación, mantemento e, cando proceda, terceiros especializados.

Vantaxes:

- Permiten comprender con maior precisión o que ocorreu durante un incidente.
- Axudan a identificar vectores de entrada, persistencia, alcance e posibles movementos laterais.
- Reforzan a capacidade de mellora posterior, revisión de controis e aprendizaxe organizativa.
- Achegan evidencias útiles para auditoría, cumprimento e posibles actuacións legais.
- Resultan especialmente valiosos en incidentes con impacto operativo, terceiros implicados ou dúbidas sobre manipulación de sistemas críticos.

Limitacións e consideracións:

- A súa utilidade diminúe se a preservación de evidencias non se activa con rapidez ou se se alteran sistemas antes de analizalos.
- En contornos industriais, algunhas técnicas forenses convencionais poden ser incompatibles coa continuidade ou coa seguridade funcional.

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

- Non substitúen a resposta operativa nin a contención, aínda que deben integrarse con ambas.
- Requírese coñecemento técnico especializado e, en ocasións, apoio externo con experiencia específica en OT.
- Debe evitarse que a urxencia por restaurar a operación elimine evidencias clave sen realizar polo menos unha preservación mínima e trazable.

Relación con outros controis: Relaciónase co soporte á resposta ante incidentes, co SIEM, co SOC, co MDR, co NDR, co EDR, coa xestión de sesións e trazabilidade, coa monitorización ciberfísica / MES, coas copias de seguridade e restauración e coa recuperación de operación e continuidade. Funciona como capacidade de análise profunda para apoiar tanto a resposta inmediata como a mellora posterior.

Casos habituais de uso: Emprégase tras incidentes de malware ou ransomware, accesos remotos comprometidos, uso indebido de contas privilexiadas, sospeita de manipulación de configuracións, actividade anómala en HMI ou estacións de enxeñaría, intervencións de terceiros con resultado non previsto, exfiltración de información técnica e calquera escenario no que sexa necesario reconstruír o ocorrido con base en evidencias.

Observacións / medidas compensatorias asociadas: En contornos industriais, os servizos forenses resultan especialmente útiles cando é necesario reconstruír un incidente sen comprometer a continuidade da operación e cando as decisións posteriores dependen de coñecer con precisión o alcance real do compromiso. A súa utilidade aumenta cando existen rexistros suficientes, trazabilidade de accesos, coordinación co proceso de resposta e criterios previos para preservar evidencias mínimas antes de proceder á recuperación ou á reconfiguración dos sistemas afectados.

5.9.3 Copias de seguridade e restauración

Categoría: Resposta, recuperación e continuidade

Tipoloxía: Técnico / mixto

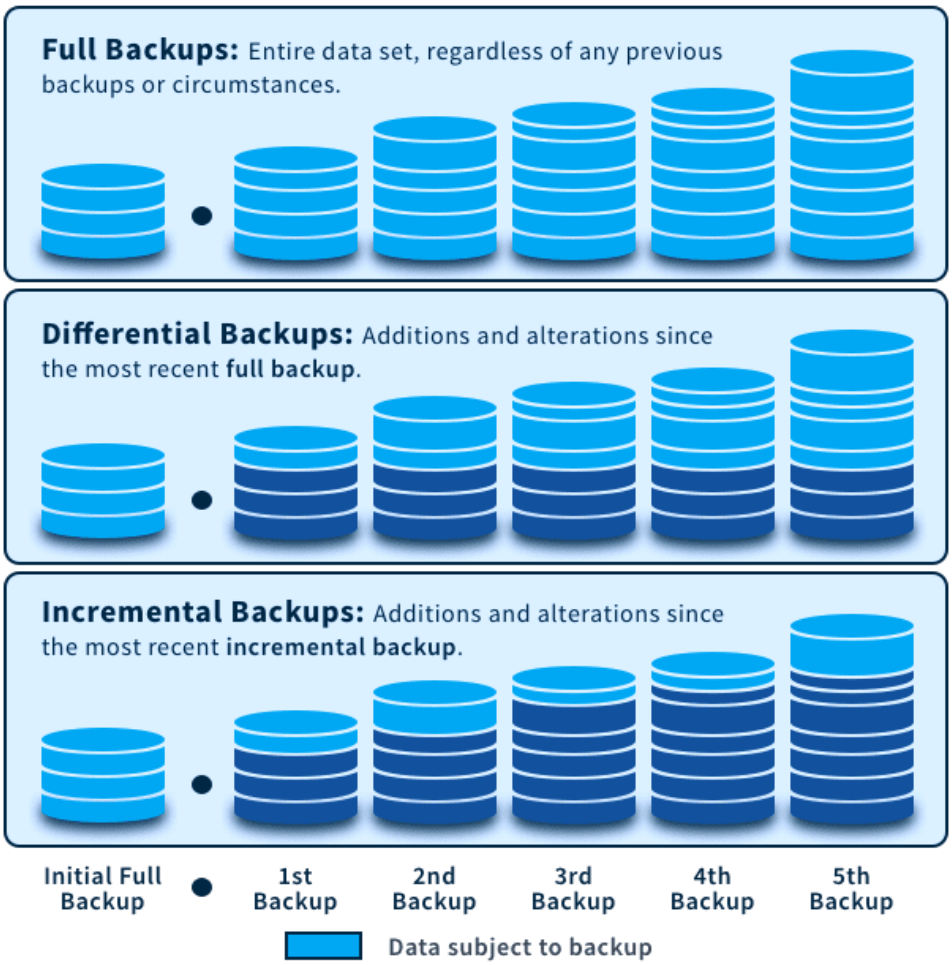
Función defensiva predominante: Correctivo / de recuperación

Función no NIST CSF: Recover

Descrición: As copias de seguridade e restauración comprenden o conxunto de medidas orientadas a preservar información, configuracións, sistemas e compoñentes críticos mediante réplicas controladas que permitan a súa recuperación tras un incidente, erro, fallo ou perda de dispoñibilidade. A súa finalidade non é unicamente conservar datos,

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

senón asegurar que a organización poida restaurar capacidades esenciais nun tempo e cun nivel de integridade compatibles coa continuidade da actividade. En contornos industriais, este control abrangue non só ficheiros corporativos ou servidores convencionais, senón tamén proxectos de enxeñaría, configuracións de HMI, receitas, bases de datos operativas, historiadores, parámetros de sistema, máquinas virtuais, rexistros relevantes e outros compoñentes cuxa perda ou corrupción podería afectar á produción, á supervisión ou á seguridade do proceso.



Tipos de copia de seguridade. Fonte: Spanning.com (2020)

Obxectivo: Garantir que a organización dispoña de copias fiables, íntegras e recuperables dos activos de información e dos compoñentes tecnolóxicos necesarios para restablecer a operación tras un incidente. No ámbito industrial, o seu obxectivo inclúe tamén asegurar que a restauración poida realizarse sen introducir configuracións incoherentes, perda de trazabilidade ou risco adicional sobre sistemas con impacto operativo.

Como funciona / como se implanta: A súa implantación parte da identificación do que debe copiarse, de que xeito e con que frecuencia, durante canto tempo debe conservarse

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

e baixo que condicións debe poder restaurarse. Isto inclúe definir alcances, prioridades, periodicidade, tipos de copia, segregación do almacenamento, protección fronte a manipulación, control de acceso ás copias e procedementos de restauración verificada. En contornos industriais, este control debe contemplar tanto datos como configuracións e compoñentes técnicos específicos: proxectos de automatización, imaxes de sistemas, configuracións de dispositivos, servidores de supervisión, parámetros de aplicacións industriais, documentación operativa e outros elementos necesarios para reconstruír o entorno de maneira coherente. A súa eficacia depende non só de facer copias, senón de comprobar periodicamente que poden restaurarse, que son utilizables e que están aliñadas coa realidade actual do proceso e da arquitectura.

Vantaxes:

- Permiten recuperar información e sistemas tras incidentes, erros ou corrupción de datos.
- Reforzan a resiliencia fronte a ransomware, fallo técnico, erro humano ou perda de dispoñibilidade.
- Axudan a reducir tempos de recuperación e impacto sobre a actividade.
- Resultan esenciais para restaurar configuracións e compoñentes críticos en contornos industriais.
- Complementan os plans de continuidade e os procedementos de resposta cunha capacidade técnica de recuperación.

Limitacións e consideracións:

- A súa utilidade diminúe se as copias non se proban, non están actualizadas ou non inclúen os compoñentes realmente críticos.
- En contornos industriais, non abonda con copiar datos: tamén deben preservarse configuracións, dependencias e elementos necesarios para a restauración funcional do entorno.
- Non substitúen a prevención, a segmentación nin a resposta temperá ante incidentes.
- Requírese protección fronte a borrado, cifrado ou manipulación das propias copias.
- Debe evitarse unha falsa sensación de seguridade baseada na existencia de copias non verificadas ou sen procedementos claros de restauración.

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

Relación con outros controis: Relaciónase co soporte á resposta ante incidentes, cos servizos forenses, coa recuperación de operación e continuidade, co plan de continuidade de negocio e resiliencia operativa, coa detección de integridade de ficheiros, co bastionado de sistemas e servizos e cos procedementos de cambio e mantemento. Constitúe unha das capacidades técnicas máis relevantes dentro da recuperación.

Casos habituais de uso: Emprégase para restaurar servidores, postos críticos, configuracións de HMI, proxectos de enxeñaría, bases de datos operativas, historiadores, documentación técnica, servizos de supervisión, contornos virtualizados e outros compoñentes afectados por ransomware, erro humano, corrupción de datos, fallo de infraestrutura ou intervención técnica fallida.

Observacións / medidas compensatorias asociadas: En contornos industriais, as copias de seguridade e restauración resultan especialmente útiles cando se integran nunha estratexia máis ampla de continuidade e recuperación, e non como mecanismo illado. A súa utilidade aumenta cando se combinan con segmentación, protección das copias fronte a manipulación, probas periódicas de restauración, validación posterior do estado do sistema e coordinación con operación e mantemento antes da posta en servizo do entorno restaurado.

5.9.4 Recuperación de operación e continuidade

Categoría: Resposta, recuperación e continuidade

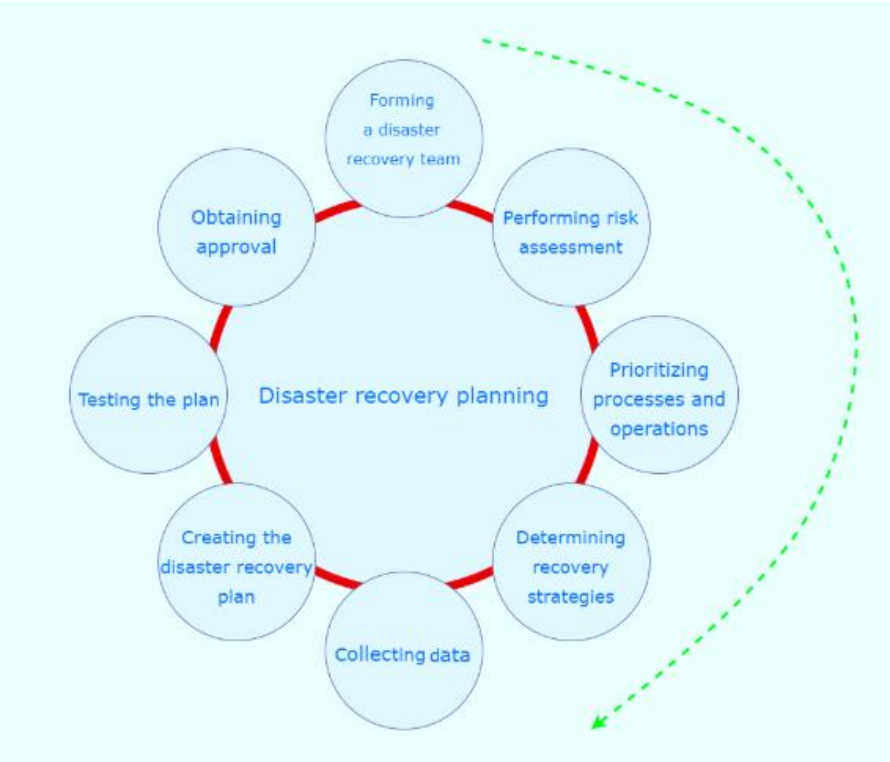
Tipoloxía: Organizativo / técnico / mixto

Función defensiva predominante: Correctivo / de recuperación

Función no NIST CSF: Recover, Govern

Descrición: A recuperación de operación e continuidade comprende o conxunto de medidas, procedementos e decisións orientadas a restablecer de maneira segura e ordenada a actividade da organización tras un incidente, fallo ou interrupción que afecte aos seus sistemas, servizos ou procesos críticos. A súa finalidade vai máis alá da mera restauración técnica de compoñentes: implica asegurar que a operación poida retomarse baixo condicións aceptables de seguridade, integridade, trazabilidade e coordinación entre áreas. En contornos industriais, este control resulta especialmente relevante porque a recuperación non debe centrarse só na dispoñibilidade dos sistemas, senón tamén na coherencia do proceso, na validación do estado dos activos, na continuidade do servizo e na protección das persoas, das instalacións e da produción.

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



Planificación de recuperación ante desastres. Fonte: Cybersecurity - Attack and Defense Strategies (2018)

Obxectivo: Restablecer a operación e os servizos esenciais da organización de forma progresiva, segura e controlada tras un incidente, minimizando o tempo de interrupción e reducindo o risco de reintroducir fallos, configuracións incoherentes ou condicións de inseguridade. No ámbito industrial, o seu obxectivo inclúe tamén asegurar que a volta á operación se produza con validación técnica e operativa suficiente, evitando recuperacións apresuradas que poidan comprometer o proceso ou xerar novos incidentes.

Como funciona / como se implanta: A súa implantación parte da identificación previa das funcións críticas, dos activos necesarios para sostelas, das prioridades de restauración e dos criterios de aceptación para considerar que a operación pode retomarse. Isto inclúe procedementos de recuperación, dependencias entre sistemas, ordes de restauración, validación do estado dos compoñentes, coordinación con copias de seguridade, revisión de configuracións, comprobación de comunicacións e definición de responsables para cada fase. En contornos industriais, este control debe contemplar tamén a verificación de HMI, estacións de enxeñaría, sistemas de supervisión, conexións de rede, parámetros de proceso, receitas, sistemas intermedios, dependencias con terceiros e condicións de seguridade funcional. A súa eficacia depende de que a recuperación estea planificada, probada e aliñada co funcionamento real da operación,

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

e de que exista coordinación entre seguridade, sistemas, operación, mantemento, produción e dirección.

Vantaxes:

- Axuda a reducir o tempo de interrupción e a restaurar servizos esenciais con maior orde e control.
- Mellora a coordinación entre áreas técnicas e operativas durante a volta á normalidade.
- Reforza a seguridade da recuperación evitando restauracións improvisadas ou incoherentes.
- Resulta especialmente útil en contornos industriais con forte dependencia de activos, secuencias e estados operativos.
- Complementa as copias de seguridade e os plans de continuidade cun enfoque orientado á posta en servizo real.

Limitacións e consideracións:

- A súa utilidade diminúe se non existen prioridades claras, procedementos definidos ou probas previas suficientes.
- En contornos industriais, a recuperación técnica dun sistema non garante por si soa a recuperación funcional do proceso.
- Non substitúe a preparación previa, a resposta ante incidentes nin a resiliencia da arquitectura.
- Requírese coordinación estreita con operación, mantemento e responsables do proceso para validar a volta ao servizo.
- Debe evitarse unha recuperación precipitada que reintroduza sistemas comprometidos, configuracións defectuosas ou estados non verificados.

Relación con outros controis: Relaciónase co soporte á resposta ante incidentes, cos servizos forenses, coas copias de seguridade e restauración, co plan de continuidade de negocio e resiliencia operativa, coa monitorización ciberfísica / MES, coa xestión de cambios e coas validacións previas e xanela de mantemento. Constitúe a capa que transforma a restauración técnica en recuperación operativa efectiva.

Casos habituais de uso: Emprégase tras incidentes de ransomware, caída de sistemas de supervisión, corrupción de configuracións, fallos en servidores ou plataformas críticas, indispoñibilidade de contornos intermedios, recuperación de liñas ou servizos

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

industriais, reactivación de operación tras illamento preventivo e escenarios nos que se precisa unha posta en servizo gradual e validada.

Observacións / medidas compensatorias asociadas: En contornos industriais, a recuperación de operación e continuidade resulta especialmente útil cando se formula como un proceso graduado, con validación técnica e operativa antes de cada paso de restitución. A súa utilidade aumenta cando se combina con copias fiables, trazabilidade das intervencións, revisión do estado do sistema, coordinación con mantemento e operación e criterios claros para decidir cando a actividade pode considerarse restablecida en condicións aceptables.

5.9.5 Ciberseguros

Categoría: Resposta, recuperación e continuidade

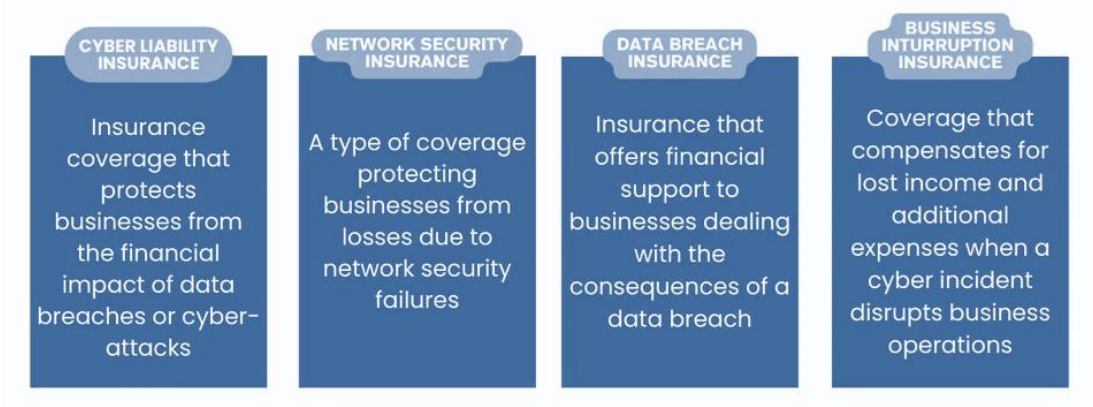
Tipoloxía: Organizativo / mixto

Función defensiva predominante: Correctivo / de recuperación

Función no NIST CSF: Recover, Govern

Descrición: Os ciberseguros son instrumentos de transferencia e mitigación financeira do risco de ciberseguridade que permiten á organización contar cunha cobertura económica e, nalgúns casos, con servizos asociados para facer fronte aos custos derivados dun incidente. A súa finalidade non é substituír os controis técnicos e organizativos de prevención, detección e resposta, senón complementar a capacidade da organización para absorber o impacto económico, operativo, legal e reputacional dun incidente grave. En contornos industriais, esta figura pode adquirir especial relevancia cando unha interrupción, un ransomware, unha afectación á produción, un incidente con terceiros ou unha degradación prolongada dos servizos ten potencial para xerar perdas significativas, custos de recuperación elevados ou responsabilidades contractuais e reguladoras adicionais.

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



Tipo de ciberseguros. Fonte: onsurity.com (2024)

Obxectivo: Reducir a exposición financeira da organización ante incidentes de ciberseguridade graves, achegando un mecanismo de cobertura e apoio que complemente a preparación técnica e organizativa fronte a eventos de alto impacto. No ámbito industrial, o seu obxectivo inclúe tamén mellorar a capacidade da entidade para afrontar custos asociados á interrupción da operación, á recuperación de sistemas, á asistencia especializada, á xestión legal e á comunicación posterior ao incidente.

Como funciona / como se implanta: A súa implantación require analizar o perfil de risco da organización, o tipo de coberturas necesarias, os límites da póliza, as exclusións aplicables, as condicións de activación e os servizos complementarios asociados, como apoio legal, resposta técnica, comunicación ou peritaxe. En contornos industriais, esta análise debe ter en conta aspectos como dependencia da produción, impacto dunha parada, uso de terceiros, exposición remota, criticidade dos sistemas, requisitos contractuais, posibles afectacións á cadea de subministración e custos derivados da recuperación de activos e servizos. A súa eficacia depende de que a póliza estea aliñada co risco real da organización e de que os equipos responsables coñezan as condicións de cobertura, os procedementos de notificación e os límites do que pode esperarse do seguro. Non se trata só de contratar unha póliza, senón de integrala dentro da gobernanza do risco e da continuidade.

Vantaxes:

- Axudan a absorber parte do impacto económico derivado dun incidente de ciberseguridade grave.
- Poden facilitar acceso a servizos especializados de apoio técnico, legal ou comunicativo.
- Reforzan a planificación financeira ante escenarios de alta severidade.

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

- Resultan útiles en organizacións con elevada dependencia da continuidade ou da prestación de servizos.
- Complementan os plans de continuidade e resposta cunha capa de cobertura económica e contractual.

Limitacións e consideracións:

- Non substitúen a necesidade de controis preventivos, detectivos e correctivos sólidos.
- A súa cobertura pode incluír exclusións, límites ou condicións que reduzan o seu valor real se non se analizan con detalle.
- En contornos industriais, os custos e impactos relevantes non sempre encaixan de maneira simple nas coberturas estándar.
- Requírese coñecemento previo da póliza e dos procesos de activación para evitar erros ou atrasos durante un incidente.
- Debe evitarse unha falsa sensación de seguridade baseada na transferencia do risco financeiro sen mellora paralela do nivel de protección real.

Relación con outros controis: Relaciónase coa análise de riscos tecnolóxicos, co plan de continuidade de negocio e resiliencia operativa, co soporte á resposta ante incidentes, cos servizos forenses, coas copias de seguridade e restauración, coa recuperación de operación e continuidade e cos procedementos de gobernanza do risco. Funciona como mecanismo complementario de absorción e xestión do impacto, non como control técnico de seguridade.

Casos habituais de uso: Emprégase para cubrir custos asociados a ransomware, interrupción da actividade, recuperación técnica, asistencia forense, asesoramento legal, notificacións, reclamacións, afectación de terceiros, perdas por indispoñibilidade de servizos ou outros incidentes con impacto económico relevante sobre a organización.

Observacións / medidas compensatorias asociadas: En contornos industriais, os ciberseguros resultan especialmente útiles cando a organización ten unha exposición significativa a interrupcións operativas, dependencia de terceiros ou impacto económico elevado ante incidentes prolongados. A súa utilidade aumenta cando se integran cunha análise de risco realista, cun coñecemento claro das condicións da póliza e cunha preparación previa que permita activar a cobertura sen interferir na resposta técnica, na continuidade nin na recuperación do proceso.

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

5.10 DevSecOps, software e contornos dixitais conectados

A crecente dixitalización da industria e a integración entre software, operación e conectividade fan necesario incorporar a seguridade ao propio ciclo de vida das aplicacións e compoñentes dixitais (desenvolvemento e operación, ou DevSecOps). Esta subsección aborda **capacidades destinadas a mellorar a seguridade do desenvolvemento, da integración e do software vinculado á operación, reducindo o risco introducido por erros de deseño, vulnerabilidades e dependencias tecnolóxicas**.

5.10.1 SAST

Categoría: DevSecOps, software e contornos dixitais conectados

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Identify

Descrición: A análise estática de seguridade do código (SAST, *Static Application Security Testing*) é unha práctica orientada á identificación temperá de debilidades e patróns inseguros no código fonte, nos compoñentes da aplicación e noutros artefactos de desenvolvemento, antes da súa posta en execución. A súa finalidade é detectar erros de programación, usos inseguros de funcións, fallos de validación, xestión incorrecta de entradas, problemas de autenticación, exposición de segredos e outras vulnerabilidades potenciais durante as fases iniciais do ciclo de vida do software. En contornos industriais, esta práctica resulta especialmente relevante cando a organización desenvolve ou adapta software propio ligado á operación, integra compoñentes de supervisión, crea aplicacións de soporte ao proceso ou mantén capas dixitais conectadas con sistemas produtivos, de monitorización ou de xestión operativa.

Obxectivo: Reducir o risco de introducir vulnerabilidades no software antes da súa implantación, mellorando a calidade do código e reforzando a seguridade dende fases temperás do desenvolvemento. No ámbito industrial, o seu obxectivo inclúe tamén limitar a incorporación de debilidades en aplicacións, integracións ou compoñentes software que poidan influír sobre a operación, a supervisión ou a exposición de información técnica e operativa sensible.

Como funciona / como se implanta: A súa implantación baséase na análise automatizada ou asistida do código fonte, das bibliotecas empregadas e doutros compoñentes do desenvolvemento para localizar patróns asociados a prácticas

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

inseguras ou a vulnerabilidades coñecidas. Esta análise pode integrarse no repositorio de código, nos fluxos de integración continua, nas revisións de cambios ou nas fases previas á posta en produción. En contornos industriais, o valor do SAST aumenta cando se aplica de maneira temperá e recorrente sobre software propio, scripts de automatización, compoñentes de integración, aplicacións de soporte á operación e ferramentas desenvolvidas internamente ou adaptadas ao contexto da organización. A súa eficacia depende de que os resultados se revisen con criterio, se prioricen segundo risco e se integren nun proceso de desenvolvemento seguro e gobernado.

Vantaxes:

- Permite detectar vulnerabilidades antes de que o software entre en produción.
- Reduce o custo de corrección ao actuar en fases iniciais do ciclo de desenvolvemento.
- Mellora a calidade do código e a disciplina de desenvolvemento seguro.
- Resulta útil para reforzar aplicacións e compoñentes software con impacto sobre a operación.
- Pode integrarse de forma continua nos fluxos DevSecOps e de revisión técnica.

Limitacións e consideracións:

- Non todas as debilidades detectadas teñen a mesma relevancia real nin o mesmo impacto no contexto da aplicación.
- Pode xerar falsos positivos ou alertas pouco accionables se non existe revisión técnica suficiente.
- En contornos industriais, o valor da análise depende de que o software examinado estea ben identificado e do coñecemento do seu papel operativo.
- Non substitúe as probas dinámicas, a revisión funcional nin a protección da aplicación unha vez despregada.
- Requírese integración cos equipos de desenvolvemento, mantemento e seguridade para que as detección se convertan en melloras reais do software.

Relación con outros controis: Relaciónase co DAST, co RASP, coas prácticas seguras de desenvolvemento e integración, coa protección de software ligado á operación, coa xestión de vulnerabilidades, co bastionado de sistemas e servizos e cos procedementos de validación previa antes da posta en produción. Constitúe unha das capas preventivas máis relevantes no desenvolvemento seguro.

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

Casos habituais de uso: Emprégase para revisar aplicacións internas, portais de xestión, compoñentes de integración, scripts de automatización, APIs, ferramentas de soporte, software desenvolvido para monitorización ou operación e outros compoñentes nos que se precisa reducir a presenza de vulnerabilidades antes da súa implantación ou actualización.

Observacións / medidas compensatorias asociadas: En contornos industriais, o SAST resulta especialmente útil cando a organización desenvolve ou adapta software con relación directa ou indirecta coa operación e precisa anticipar riscos antes de introducir cambios en produción. A súa utilidade aumenta cando se combina con revisión técnica manual, DAST, validación en contornos de proba, xestión de cambios e procedementos de liberación que teñan en conta a criticidade do entorno no que o software será executado.

5.10.2 DAST

Categoría: DevSecOps, software e contornos dixitais conectados

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Identify

Descrición: A análise dinámica de seguridade de aplicacións (DAST, *Dynamic Application Security Testing*) é unha práctica orientada á identificación de vulnerabilidades e comportamentos inseguros mediante a avaliación dunha aplicación en execución, observando como responde a peticións, interaccións e entradas maliciosas ou non previstas. A diferenza do SAST, que actúa sobre o código fonte e outros artefactos antes da execución, o DAST céntrase no comportamento efectivo da aplicación despregada en real ou en entorno de proba, permitindo detectar debilidades visibles dende o exterior, erros de validación, exposición de compoñentes, configuracións inseguras ou fallos na xestión de sesións e parámetros. En contornos industriais, esta práctica resulta especialmente relevante cando existen aplicacións web, portais de xestión, APIs, compoñentes de integración ou servizos software que, directa ou indirectamente, se conectan con sistemas de supervisión, operación, mantemento ou intercambio de información técnica.

Obxectivo: Detectar vulnerabilidades e fallos de seguridade no comportamento real dunha aplicación antes da súa posta en produción ou durante o seu ciclo de vida, reducindo o risco de explotación externa ou interna sobre servizos software accesibles.

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

No ámbito industrial, o seu obxectivo inclúe tamén identificar exposicións en aplicacións e interfaces que poidan actuar como punto de entrada cara a servizos técnicos, datos operativos ou compoñentes con impacto indirecto sobre a operación.

Como funciona / como se implanta: A súa implantación baséase na execución de probas sobre a aplicación en funcionamento, enviando peticións e interaccións deseñadas para comprobar como xestiona entradas, sesións, autenticación, autorización, erros, navegación, exposición de compoñentes e outras condicións de risco. Esta análise pode realizarse en contornos de desenvolvemento, preprodución ou, con moita cautela, sobre aplicacións xa despregadas cando exista control suficiente do alcance. En contornos industriais, o DAST debe aplicarse preferentemente sobre contornos de proba ou réplicas representativas, especialmente cando a aplicación ten relación con sistemas de mantemento, supervisión, xestión técnica ou intercambio de información operativa. A súa eficacia depende de que o alcance estea ben definido, de que as probas reflictan o comportamento real da aplicación e de que os resultados se integren nun proceso de mellora e validación previa antes da posta en servizo.

Vantaxes:

- Permite identificar vulnerabilidades observables no comportamento real da aplicación.
- Complementa o SAST ao analizar a aplicación en execución e non só o código.
- Resulta útil para detectar exposicións en sesións, entradas, erros e configuracións visibles.
- Axuda a avaliar servizos web, APIs e compoñentes de integración antes do seu despregue definitivo.
- Pode integrarse en procesos de validación e liberación de software con enfoque DevSecOps.

Limitacións e consideracións:

- Non substitúe a revisión do código nin detecta todos os problemas internos non visibles dende a aplicación en execución.
- Pode xerar resultados incompletos se o entorno de proba non reproduce adecuadamente o comportamento real.
- En contornos industriais, debe evitarse a execución indiscriminada de probas dinámicas sobre servizos en produción con impacto potencial sobre a operación.

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

- Requírese interpretación técnica dos achados para distinguir entre exposición real, erro de configuración e vulnerabilidade explotable.
- Debe complementarse con procedementos de validación, xestión de cambios e revisión funcional da aplicación.

Relación con outros controis: Relaciónase co SAST, co RASP, co WAF, coas prácticas seguras de desenvolvemento e integración, coa protección de software ligado á operación, coa xestión de vulnerabilidades e coas validacións previas antes da posta en produción. Constitúe unha capa moi útil para avaliar a seguridade observable das aplicacións despregadas.

Casos habituais de uso: Emprégase para revisar portais web, servizos de administración, APIs, compoñentes de integración, aplicacións de soporte á operación, interfaces técnicas publicadas en contornos de proba e outros servizos software nos que se precisa detectar vulnerabilidades antes do despregue ou dunha actualización relevante.

Observacións / medidas compensatorias asociadas: En contornos industriais, o DAST resulta especialmente útil cando existen aplicacións conectadas a procesos de mantemento, supervisión ou integración e se precisa validar o seu comportamento antes da súa exposición ou actualización. A súa utilidade aumenta cando se combina con SAST, revisión manual, contornos de proba representativos, WAF, xestión de cambios e procedementos de liberación adaptados á criticidade do entorno no que a aplicación vai operar.

5.10.3 RASP

Categoría: DevSecOps, software e contornos dixitais conectados

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect, Detect

Descrición: A autoprotección de aplicacións en tempo de execución (RASP, *Runtime Application Self-Protection*) é un conxunto de capacidades orientadas a supervisar e protexer o comportamento dunha aplicación mentres está en funcionamento, co fin de detectar e bloquear interaccións maliciosas, explotacións de vulnerabilidades ou usos indebidos no propio momento en que se producen. A diferenza de controis externos como o WAF, que observan o tráfico dende fóra da aplicación, o RASP opera con maior proximidade ao contexto interno da execución, o que lle permite interpretar mellor

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

certas chamadas, fluxos lóxicos, entradas e patróns de comportamento. En contornos industriais, esta capacidade pode resultar especialmente útil en aplicacións web, servizos de integración, interfaces técnicas, compoñentes software de apoio á operación e outras pezas dixitais conectadas que requiren protección adicional sen depender exclusivamente do perímetro.

Obxectivo: Reducir o risco de explotación de vulnerabilidades ou de uso indebido das aplicacións en execución, achegando unha capa adicional de protección capaz de detectar e, cando proceda, bloquear accións maliciosas en tempo real. No ámbito industrial, o seu obxectivo inclúe tamén reforzar a protección de aplicacións ligadas á xestión, á supervisión, á integración ou ao soporte técnico cando estas teñen relación con información operativa, servizos sensibles ou contornos con impacto indirecto sobre a operación.

Como funciona / como se implanta: A súa implantación baséase na integración de compoñentes de observación e protección dentro da aplicación ou no seu entorno inmediato de execución, de maneira que poidan analizar chamadas, fluxos, entradas, sesións e comportamento interno con contexto suficiente para identificar accións sospeitosas. Isto permite detectar explotacións que poden pasar desapercibidas para outros mecanismos máis externos e, en determinados casos, interromper a acción antes de que se complete. En contornos industriais, o RASP debe aplicarse principalmente a aplicacións desenvolvidas ou mantidas pola organización, ou a compoñentes software nos que exista capacidade real de integración e validación. A súa eficacia depende de compatibilidade co entorno de execución, impacto asumible sobre rendemento e mantemento, e integración cun proceso de desenvolvemento seguro no que os resultados poidan analizarse e incorporarse de maneira ordenada.

Vantaxes:

- Engade protección sobre a aplicación no propio momento da execución.
- Pode detectar e bloquear explotacións con maior contexto que outros controis externos.
- Complementa SAST, DAST e WAF cunha capa próxima á lóxica interna da aplicación.
- Resulta útil para aplicacións con exposición relevante ou función sensible.
- Pode mellorar a visibilidade sobre comportamentos 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

Limitacións e consideracións:

- A súa aplicabilidade depende do tipo de aplicación, do entorno de execución e da posibilidade real de integración.
- Pode introducir impacto en rendemento, compatibilidade ou mantemento se non se valida adecuadamente.
- En contornos industriais, non resulta igualmente axeitado para todos os compoñentes software, especialmente se son moi pechados ou dependen de provedores externos.
- Non substitúe o desenvolvemento seguro, o SAST, o DAST nin a revisión da arquitectura da aplicación.
- Requírese control do ciclo de vida da aplicación e criterio técnico suficiente para interpretar e axustar o comportamento da protección en execución.

Relación con outros controis: Relaciónase co SAST, co DAST, co WAF, coas prácticas seguras de desenvolvemento e integración, coa protección de software ligado á operación, coa xestión de vulnerabilidades e coa monitorización e operación de seguridade. Constitúe unha capa avanzada de protección orientada ao comportamento real da aplicación en execución.

Casos habituais de uso: Emprégase en aplicacións web de xestión, APIs, compoñentes de integración, portais técnicos, servizos conectados a información sensible e outras aplicacións nas que se busca engadir unha capa adicional de protección fronte a explotacións en tempo real sen depender só de controis perimetrais.

Observacións / medidas compensatorias asociadas: En contornos industriais, o RASP pode resultar especialmente útil cando unha aplicación debe permanecer accesible ou exposta e non é viable redeseñala de inmediato nin eliminar completamente determinadas debilidades. A súa utilidade aumenta cando se combina con SAST, DAST, WAF, validación en contornos de proba, xestión de cambios e revisión continua do impacto da protección sobre o comportamento funcional da aplicación.

A continuación, amósanse as diferencias e similitudes dos tres últimos controis descritos.

Característica	SAST	DAST	RASP
Método de funcionamento	Examina o código fonte sen executalo	Avalía aplicacións en execución simulando ataques	Intégrase na aplicación para detectar e defenderse contra ataques en tempo real
Fase no SDLC	Nas primeiras fases do ciclo de desenvolvemento	Despois do desenvolvemento, en preprodución	En produción / en tempo de execución
Tipo de problemas detectados	Erros de sintaxe, fallos de seguridade como desbordamentos de búfer e inxeccións SQL	Problemas en tempo de execución, erros de autenticación/autorización, problemas de xestión de sesións	Ataques en tempo real, entradas maliciosas, vulnerabilidades en execución
Integración	Integrado no proceso de desenvolvemento	Parte dunha estratexia AST máis ampla, usada en contornos de staging	Integrado dentro da aplicación; funciona nun entorno de produción
Granularidade	Examina o código a un nivel detallado	Avalía a aplicación no seu conxunto	Supervisa e protexe en tempo de execución, proporcionando información contextual
Asistencia para a corrección	Permite a detección temperá e a corrección de problemas	Identifica problemas nun estado de execución, proporcionando contexto para as vulnerabilidades en tempo de execución	Proporciona protección e mitigación inmediatas
Cobertura	Código fonte, ficheiros de configuración	Solicitudes HTTP, respostas e datos de sesión	Fluxo de datos, fluxo de control, información de conexión interna
Falsos positivos	Poden ser máis numerosos debido á falta de contexto de execución	Xeralmente menos, xa que avalía o comportamento real en execución	Baixos, xa que opera no entorno real de execución

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

Vantaxes	Detección temperá dunha ampla gama de problemas detectables	Eficaz para identificar vulnerabilidades específicas de execución	Protección inmediata e continua, defensa con coñecemento do contexto
Desvantaxes	Pode non detectar problemas específicos do tempo de execución	Require unha aplicación en execución, con posible dependencia do entorno	Sobrecarga no rendemento da aplicación e complexidade na integración

Comparativa SAST, DAST, RASP. Fonte: Somi, Vivek (2024)

5.10.4 Prácticas seguras de desenvolvemento SW e integración

Categoría: DevSecOps, software e contornos dixitais conectados

Tipoloxía: Organizativo / técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect, Govern

Descrición: As prácticas seguras de desenvolvemento e integración comprenden o conxunto de principios, procedementos, controis e rutinas orientados a incorporar a seguridade de maneira continua ao longo do ciclo de vida do software, dende a análise de requisitos ata o desenvolvemento, integración, validación, despregue e mantemento evolutivo. O seu propósito é evitar que a seguridade apareza como unha revisión tardía e illada, converténdoa nun criterio transversal de deseño, implementación e entrega. En contornos industriais, esta aproximación resulta especialmente relevante cando a organización desenvolve software propio, adapta compoñentes, integra aplicacións con sistemas de supervisión ou operación, automatiza procesos ou mantén contornos dixitais conectados con impacto potencial sobre servizos, datos técnicos ou procesos produtivos.

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

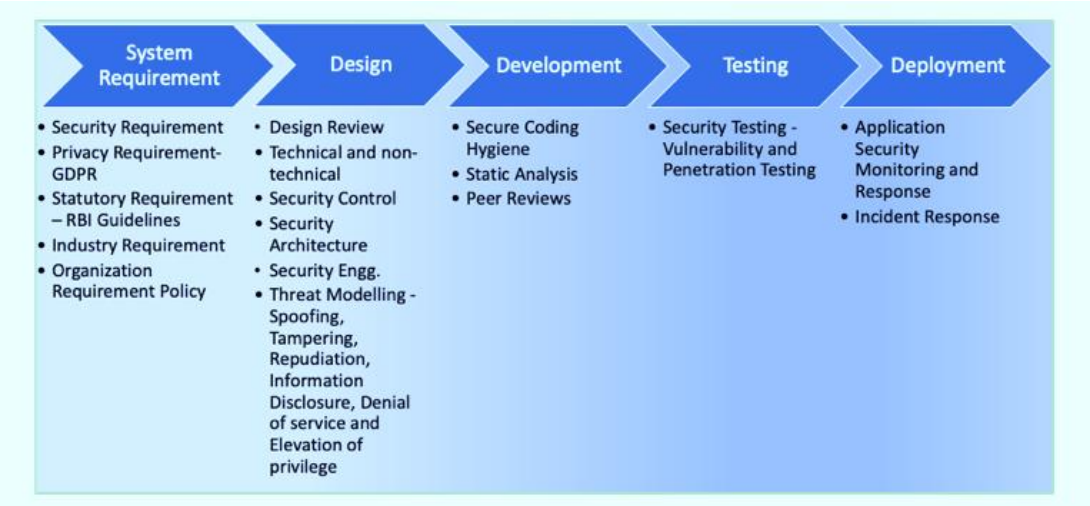


Diagrama do ciclo de vida de desenvolvemento de software seguro (S-SDLC). Fonte: Digisec360 (2020)

Obxectivo: Reducir a incorporación de riscos e vulnerabilidades ao software e ás súas integracións mediante prácticas sistemáticas de deseño seguro (S-SDLC), revisión técnica, control de cambios e validación continuada. No ámbito industrial, o seu obxectivo inclúe tamén asegurar que as integracións entre aplicacións, sistemas corporativos, compoñentes técnicos e servizos ligados á operación se realicen baixo criterios compatibles coa continuidade, a trazabilidade e a protección do entorno.

Como funciona / como se implanta: A súa implantación baséase na incorporación de controis e rutinas de seguridade ao fluxo habitual de desenvolvemento e entrega: definición de requisitos de seguridade, revisión de arquitectura, uso de boas prácticas de codificación, xestión segura de dependencias, revisión por pares, control de segredos, análise automatizada, probas de seguridade, validación previa ao despregue e gobernanza do cambio. En contornos industriais, estas prácticas deben estenderse tamén ás integracións entre software e sistemas técnicos, aos scripts de automatización, ás APIs, aos compoñentes de intercambio de datos, ás aplicacións de soporte á operación e a calquera peza dixital que poida afectar a supervisión, mantemento, produción ou xestión operativa. A súa eficacia depende de que a seguridade se integre nos procedementos reais dos equipos e de que exista coordinación entre desenvolvemento, operación, seguridade, mantemento e responsables funcionais.

Vantaxes:

- Reduce a incorporación de vulnerabilidades dende fases temperás do ciclo de vida do software.
- Mellora a calidade técnica das aplicacións e das integración e reduce custos.
- Reforza a coherencia entre desenvolvemento, cambio, validación e despregue.

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

- Resulta útil para controlar riscos en compoñentes conectados á operación ou a información sensible.
- Complementa SAST, DAST e RASP cun marco máis amplo de gobernanza e boas prácticas.

Limitacións e consideracións:

- A súa utilidade diminúe se se formula como conxunto teórico de principios sen integración real no fluxo de traballo.
- En contornos industriais, as integracións con software legado, compoñentes de fabricante ou servizos pouco documentados poden dificultar a súa aplicación completa.
- Non substitúe as probas técnicas nin a validación previa á posta en produción.
- Requírese madurez organizativa, disciplina de cambio e participación coordinada de varios perfís.
- Debe evitarse que a presión por entregar cambios rápidos relegue a seguridade a unha revisión final sen capacidade real de corrección.

Relación con outros controis: Relaciónase co SAST, co DAST, co RASP, coa protección de software ligado á operación, coa xestión de vulnerabilidades, coas validacións previas e xanela de mantemento, co bastionado de sistemas e servizos e cos procedementos de cambio e liberación. Constitúe o marco de traballo que integra a seguridade no desenvolvemento e na entrega continua de software.

Casos habituais de uso: Emprégase en equipos que desenvolven aplicacións internas, scripts de automatización, APIs, integracións con plataformas industriais, servizos de soporte técnico, compoñentes de intercambio de datos, portais de xestión e outros elementos software que necesitan control de seguridade ao longo de todo o seu ciclo de vida.

Observacións / medidas compensatorias asociadas: En contornos industriais, estas prácticas resultan especialmente útiles cando a organización mantén software propio ou integracións críticas e precisa reducir o risco antes do despregue. A súa utilidade aumenta cando se combinan con revisión técnica manual, SAST, DAST, contornos de proba representativos, xestión de cambios, validación funcional e criterios claros de liberación adaptados á criticidade do entorno no que o software vai operar.

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

5.10.5 Protección de software ligado á operación

Categoría: DevSecOps, software e contornos dixitais conectados

Tipoloxía: Técnico / mixto

Función defensiva predominante: Preventivo

Función no NIST CSF: Protect

Descrición: A protección de software ligado á operación comprende o conxunto de medidas orientadas a asegurar aplicacións, compoñentes, integracións e ferramentas software que, sen formar parte necesariamente do núcleo de control industrial, teñen unha relación directa ou indirecta co funcionamento operativo da organización. Isto inclúe software de supervisión, xestión técnica, integración de datos, apoio ao mantemento, interfaces con sistemas industriais, compoñentes de analítica, servizos intermedios, scripts de automatización e outras pezas dixitais que poden influír sobre a visibilidade, a coordinación, a trazabilidade ou a execución de tarefas críticas. En contornos industriais, este tipo de software adoita constituír unha ponte entre os dominios IT e OT, polo que a súa protección adquire un valor especial dentro da superficie de risco global.

Obxectivo: Reducir o risco de que o software vinculado á operación introduza vulnerabilidades, exposicións ou dependencias inseguras que poidan afectar á continuidade, á integridade do proceso, á xestión técnica ou ao acceso a información e servizos críticos. No ámbito industrial, o seu obxectivo inclúe tamén reforzar a protección das aplicacións e integracións que, sen seren controladores ou compoñentes OT puros, poden servir como vía de acceso, manipulación ou degradación do entorno operativo.

Como funciona / como se implanta: A súa implantación baséase na identificación dos compoñentes software que teñen relación coa operación e na aplicación sobre eles dun conxunto combinado de medidas: desenvolvemento seguro cando proceda, revisión de configuración, control de accesos, xestión de dependencias, bastionado, protección fronte a explotación, validación previa ao despregue, monitorización, trazabilidade e revisión continua do seu ciclo de vida. En contornos industriais, este control debe aplicarse con especial atención a aplicacións propias, compoñentes adaptados, integracións con MES ou sistemas de supervisión, portais técnicos, ferramentas de xestión de activos, servizos de intercambio de datos, APIs, software de apoio ao mantemento e outras pezas que conectan a operación con servizos corporativos ou externos. A súa eficacia depende de que a organización identifique este software como

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

parte do seu entorno crítico, e non como un conxunto de aplicacións auxiliares alleas á gobernanza da seguridade.

Vantaxes:

- Reduce a exposición derivada de aplicacións e compoñentes conectados coa operación.
- Mellora o control sobre pezas software que adoitan actuar como ponte entre IT e OT.
- Axuda a limitar vulnerabilidades, configuracións inseguras e dependencias pouco gobernadas.
- Resulta útil para reforzar servizos técnicos, integracións e ferramentas con impacto operativo indirecto.
- Complementa o desenvolvemento seguro e os controis de protección de aplicacións con enfoque máis orientado á operación.

Limitacións e consideracións:

- A súa eficacia diminúe se non se identifican correctamente todas as aplicacións e integracións con relevancia operativa.
- En contornos industriais, algúns compoñentes poden depender de software de fabricante ou de terceiros con pouca capacidade de modificación local.
- Non substitúe a segmentación, a xestión de accesos, a validación previa nin a protección do entorno no que ese software se executa.
- Requírese coordinación entre desenvolvemento, seguridade, operación, mantemento e responsables funcionais para contextualizar o risco real.
- Debe evitarse tratar como "auxiliar" un software que, na práctica, condiciona o acceso á información operativa ou a execución de procesos relevantes.

Relación con outros controis: Relaciónase co SAST, co DAST, co RASP, coas prácticas seguras de desenvolvemento e integración, co WAF, coa xestión de vulnerabilidades, co bastionado de sistemas e servizos, coas validacións previas e xanela de mantemento e coa monitorización e operación de seguridade. Constitúe unha capa orientada a reducir o risco específico do software conectado coa actividade operativa.

Casos habituais de uso: Emprégase en software de supervisión, portais técnicos, ferramentas de soporte ao mantemento, aplicacións de integración con sistemas industriais, servizos de intercambio de datos, compoñentes MES auxiliares, APIs

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

internas, scripts de automatización e outras solucións software que, sen controlar directamente o proceso, teñen impacto sobre a súa visibilidade, coordinación ou continuidade.

Observacións / medidas compensatorias asociadas: En contornos industriais, a protección de software ligado á operación resulta especialmente útil cando a organización depende de múltiples capas dixitais intermedias entre IT e OT e precisa reducir o risco sen agardar a unha renovación completa da arquitectura. A súa utilidade aumenta cando se combina con desenvolvemento seguro, validación en contornos de proba, bastionado, segmentación, control de acceso, monitorización e revisión periódica das dependencias e integracións que manteñen estes compoñentes.

5.11 Tendencias emerxentes e capacidades avanzadas

A evolución da industria conectada está a introducir novas tecnoloxías, novos modelos de operación e tamén novos escenarios de risco que non sempre encaixan nos esquemas tradicionais de protección. Este último bloque reúne **capacidades asociadas a ámbitos emerxentes como o IoT industrial, as comunicacións avanzadas, a intelixencia artificial ou a resiliencia ciberfísica**, coa finalidade de ofrecer unha **visión prospectiva sobre controis ou tecnoloxías que xa comezan a ser relevantes en moitos contornos industriais**. Dado este enfoque híbrido, permítese unha maior liberdade no formato da ficha descriptiva.

5.11.1 IoT industrial

Categoría: Tendencias emerxentes e capacidades avanzadas

Tipoloxía: -

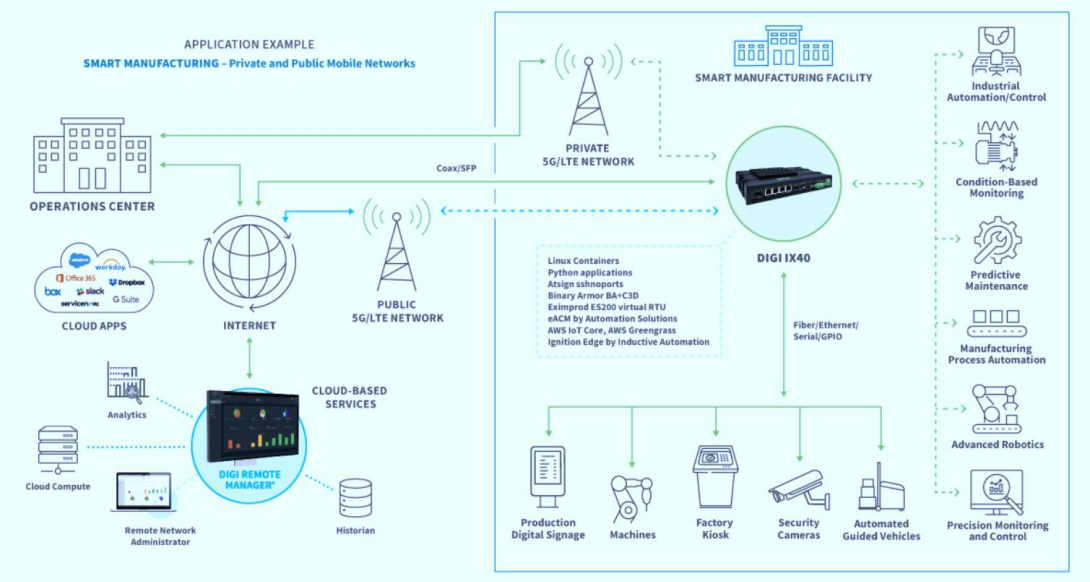
Función defensiva predominante: -

Función no NIST CSF: -

Descrición e alcance: O IoT industrial (IIoT, *Industrial Internet of Things*) refírese ao uso de sensores, actuadores, dispositivos conectados, pasarelas, módulos de comunicación e plataformas asociadas para recoller datos, intercambiar información, automatizar tarefas e mellorar a visibilidade sobre procesos, activos e condicións operativas. A súa relevancia no ámbito industrial non reside só na conectividade de novos dispositivos, senón na capacidade de incorporar capas adicionais de medición, supervisión, trazabilidade e análise sobre procesos físicos e infraestruturas que tradicionalmente funcionaban con menor nivel de observabilidade ou integración dixital.

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

Nun sentido amplo, o IoT industrial abrangue dende sensores ambientais ou de condición ata dispositivos de mantemento preditivo, compoñentes de telemetría, solucións de localización, equipos de comunicación avanzada, instrumentación conectada, pasarelas de integración ou elementos que alimentan plataformas de analítica, mantemento, trazabilidade ou xestión enerxética. Esta evolución abre oportunidades relevantes en eficiencia, coñecemento do proceso e resiliencia operativa, pero tamén introduce novos activos, máis software embebido, máis firmware, máis comunicacións e máis dependencias tecnolóxicas que deben ser gobernadas con criterios de ciberseguridade dende o inicio.



Exemplo de uso de IIoT en fabricación intelixente. Fonte: Digi (2023)

Obxectivo: Aproveitar as capacidades do IoT industrial para mellorar a visibilidade, a automatización e a toma de decisións sobre a operación, incorporando ao mesmo tempo medidas suficientes para limitar o risco derivado da proliferación de dispositivos conectados, da expansión da superficie de exposición e da aparición de novas interdependencias entre sistemas físicos e dixitais.

Como se materializa nun entorno industrial: Na práctica, o IoT industrial adoita introducirse de forma progresiva arredor de casos de uso concretos: monitorización de condición, mantemento preditivo, eficiencia enerxética, sensorización de activos, trazabilidade de operacións, supervisión remota, control ambiental, localización de elementos críticos ou integración de datos en plataformas analíticas e de decisión. A súa implantación require normalmente a combinación de dispositivos de campo, redes de comunicación, pasarelas, plataformas de xestión, mecanismos de integración e, en moitos casos, servizos cloud ou contornos híbridos.

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

Dende a perspectiva da seguridade, o valor do IIoT depende de que estes compoñentes non se traten como elementos "auxiliares" ou de baixa criticidade só porque non formen parte do núcleo tradicional do control industrial. Un sensor, unha pasarela ou unha plataforma asociada poden converterse en fonte de visibilidade moi valiosa, pero tamén nun vector de acceso, nun punto de fuga de información, nunha dependencia insegura ou nun elemento de degradación do proceso se non existe inventario, control de acceso, segmentación, actualización, bastionado e supervisión suficientes.

Principais vantaxes:

- Mellora a visibilidade sobre activos, condicións e comportamento do proceso.
- Permite ampliar capacidades de monitorización, trazabilidade e mantemento.
- Facilita a integración de datos para analítica, optimización e soporte á decisión.
- Pode contribuír á detección temperá de anomalías operativas ou técnicas.
- Favorece a evolución cara a contornos máis conectados, medibles e adaptativos.

Principais riscos e limitacións:

- Incrementa o número de activos conectados e a superficie global de exposición.
- Introduce compoñentes con firmware, software embebido e ciclos de actualización a miúdo complexos.
- Pode xerar dependencias novas con provedores, plataformas cloud ou pasarelas de integración.
- En contornos industriais, moitos dispositivos IIoT non teñen o mesmo nivel de robustez ou gobernanza que outros activos máis maduros.
- O seu valor diminúe rapidamente se a conectividade medra máis rápido que a capacidade de inventariar, segmentar, supervisar e manter o entorno.

Elementos de seguridade especialmente relevantes: Neste ámbito cobran especial importancia controis como a visibilidade de activos e comunicacións OT, a segmentación de rede, o control de accesos, o NAC cando aplique, a xestión de vulnerabilidades, o bastionado, a monitorización de rede, a seguridade no acceso remoto, a protección das pasarelas de integración, a gobernanza de dispositivos externos e a revisión de dependencias cloud ou SaaS asociadas ao caso de uso.

Casos habituais de uso: Emprégase en sensorización de activos industriais, monitorización ambiental, mantemento preditivo, eficiencia enerxética, localización de compoñentes, trazabilidade de operacións, recollida distribuída de datos, supervisión

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

de condicións de proceso e ampliación da observabilidade en infraestruturas con elevada dispersión física ou necesidade de medición fina.

Enfoque recomendado no catálogo: Dentro deste catálogo, o IoT industrial debe interpretarse menos como un "produto" e máis como unha capacidade habilitadora que transforma a arquitectura e a superficie de risco do entorno. Polo tanto, a súa valoración debe facerse sempre atendendo a tres dimensións combinadas: utilidade operativa, grao de exposición introducido e capacidade real da organización para gobernar os novos activos e fluxos. En organizacións maduras, pode actuar como acelerador de visibilidade e resiliencia; en organizacións con pouca gobernanza técnica, pode ampliar de forma significativa a complexidade e o risco.

Observacións / medidas compensatorias asociadas: En contornos industriais, o despregue de IoT industrial resulta máis seguro cando se realiza de forma gradual, con inventario previo, segmentación específica, autenticación axeitada, protección das pasarelas, limitación de accesos e monitorización continua dos fluxos introducidos. Cando non sexa viable asegurar de inmediato todos os compoñentes do ecosistema IIoT, convén reforzar medidas compensatorias como a separación de redes, o control estrito de conectividade, a revisión das integracións externas e a supervisión intensificada dos novos dispositivos e canles de comunicación.

5.11.2 Redes privadas e comunicacións avanzadas

Categoría: Tendencias emerxentes e capacidades avanzadas

Tipoloxía: -

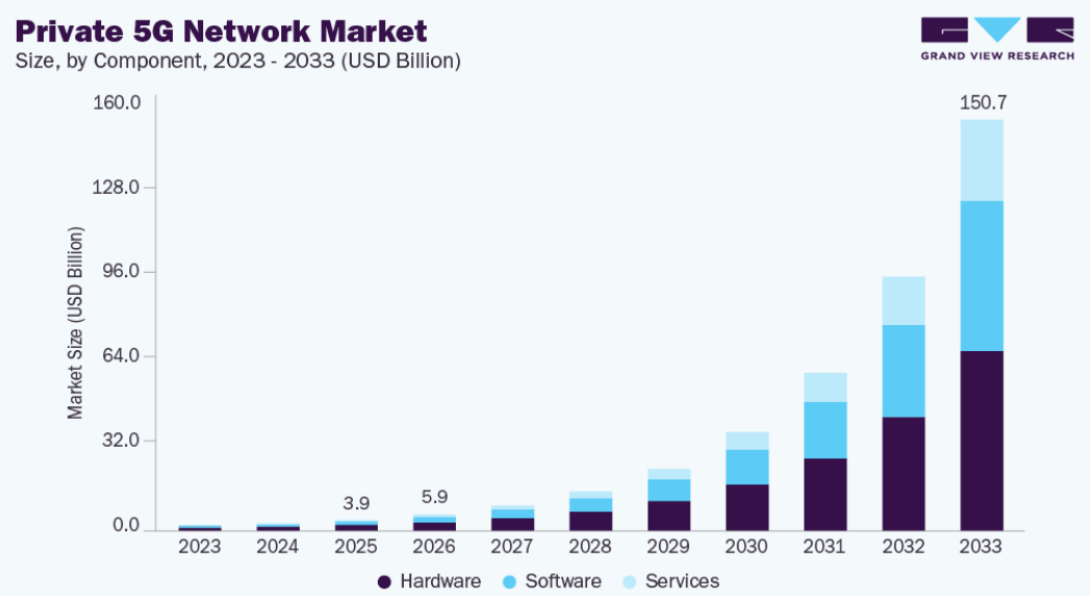
Función defensiva predominante: -

Función no NIST CSF: -

Descrición e alcance: As redes privadas e comunicacións avanzadas abranguen o conxunto de tecnoloxías e arquitecturas de conectividade orientadas a proporcionar comunicacións máis segmentadas, resilientes, de baixa latencia, con maior control operativo e con capacidade de adaptación ás necesidades específicas do entorno industrial. Nesta categoría poden incluírse redes privadas móviles (por exemplo 5G), solucións avanzadas de comunicación sen fíos, infraestruturas dedicadas para operación crítica, mecanismos de conectividade distribuída con control reforzado e, en xeral, modelos de comunicación que superan a lóxica tradicional de rede plana ou conectividade xenérica.

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

No ámbito industrial, estas capacidades resultan relevantes porque a dixitalización, a sensorización distribuída, a mobilidade operativa, a supervisión remota, a automatización flexible e o uso crecente de contornos conectados esixen comunicacións máis previsibles, máis gobernables e mellor aliñadas coas necesidades do proceso. Ao mesmo tempo, a introdución destas tecnoloxías modifica a topoloxía de conectividade, incorpora novos compoñentes de rede, novos planos de xestión e novas dependencias con provedores e servizos, polo que debe abordarse tamén dende unha perspectiva clara de ciberseguridade.



Previsións de crecemento do mercado das redes 5G privadas. Fonte: Grand View Research (2025)

Obxectivo: Mellorar a conectividade do entorno industrial mediante arquitecturas de comunicación máis robustas, adaptadas e controladas, asegurando ao mesmo tempo que a incorporación destas capacidades non amplíe de maneira desordenada a superficie de exposición nin introduza novas dependencias mal gobernadas.

Como se materializa nun entorno industrial: Na práctica, estas capacidades adoitan implantarse para soportar casos de uso como mobilidade en planta, conectividade de sensores e dispositivos distribuídos, comunicación entre áreas extensas, integración de equipos móbiles ou autónomos, supervisión remota, intercambio intensivo de datos, control máis granular da conectividade ou despregue de servizos con requisitos estritos de latencia e dispoñibilidade. Tamén poden resultar útiles para separar mellor determinados fluxos, crear dominios de comunicación con maior control e reducir a dependencia de redes compartidas ou pouco axeitadas para certas funcións críticas.

Dende a perspectiva da seguridade, o valor destas redes depende de que a organización non as interprete unicamente como unha mellora de capacidade ou rendemento, senón

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

como un cambio de arquitectura que debe ir acompañado de segmentación, gobernanza de identidades, protección do plano de xestión, visibilidade de activos, control de dispositivos conectados, revisión de integracións e mecanismos de monitorización acordes ao novo modelo de comunicación. En contornos industriais, unha comunicación máis avanzada non é necesariamente unha comunicación máis segura se non se acompaña de control técnico e procedemental suficiente.

Principais vantaxes:

- Permiten adaptar mellor a conectividade ás necesidades reais do proceso e da operación.
- Poden mellorar a resiliencia, a previsibilidade e o control da comunicación entre compoñentes distribuídos.
- Resultan útiles para contornos con mobilidade, dispersión física ou alta necesidade de observabilidade.
- Facilitan a incorporación de novos casos de uso dixital sen depender exclusivamente de redes tradicionais menos flexibles.
- Poden contribuír a unha mellor separación funcional de fluxos cando se deseñan con criterio arquitectónico.

Principais riscos e limitacións:

- Introducen novos compoñentes, planos de xestión, dependencias e superficies de exposición.
- Poden xerar unha falsa sensación de control se se prioriza a capacidade técnica sobre a gobernanza da seguridade.
- En contornos industriais, a integración con redes existentes pode aumentar a complexidade e a dificultade de supervisión.
- A dependencia de provedores, tecnoloxías especializadas ou servizos externos pode converterse nun factor crítico de risco.
- O seu valor diminúe se non existe inventario claro dos dispositivos conectados nin visibilidade suficiente dos fluxos habilitados.

Elementos de seguridade especialmente relevantes: Neste ámbito cobran especial importancia a segmentación de rede e separación IT/OT, o NAC cando aplique, a visibilidade de activos e comunicacións OT, a monitorización de rede, o control de accesos, o MFA para os planos de xestión, a seguridade no acceso remoto, o bastionado

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

dos compoñentes de comunicación, a revisión das dependencias con terceiros e a integración con capacidades como NDR, SIEM ou SOC.

Casos habituais de uso: Emprégase en plantas con alta dispersión física, contornos con mobilidade técnica ou operativa, comunicación con sensores distribuídos, integración de activos IIoT, soporte a plataformas de monitorización avanzada, conectividade de equipos autónomos ou móbiles, e escenarios nos que a arquitectura de comunicación tradicional non responde adecuadamente aos novos requisitos de dixitalización e control.

Enfoque recomendado no catálogo: Dentro deste catálogo, as redes privadas e comunicacións avanzadas deben interpretarse como unha capacidade arquitectónica habilitadora, non como unha medida de seguridade por si mesma. O seu valor dependerá da capacidade da organización para incorporalas dentro dun deseño segmentado, visible e gobernado, no que a conectividade non se expanda máis rápido que os controis necesarios para protexela. En organizacións maduras, poden reforzar a resiliencia e a flexibilidade; en organizacións con pouca gobernanza, poden aumentar a opacidade e a dificultade de control.

Observacións / medidas compensatorias asociadas: En contornos industriais, o despregue destas redes resulta máis seguro cando se acompaña dende o inicio de inventario de dispositivos, segmentación por función, protección reforzada do plano de xestión, control de accesos, monitorización dos fluxos e revisión das dependencias externas. Cando non sexa viable asegurar plenamente todos os compoñentes da nova arquitectura, convén reforzar medidas compensatorias como separación adicional de dominios, restrición de conectividade, supervisión intensificada e validación progresiva dos casos de uso antes de ampliar o despregue.

5.11.3 Contornos industriais conectados

Categoría: Tendencias emerxentes e capacidades avanzadas

Tipoloxía: -

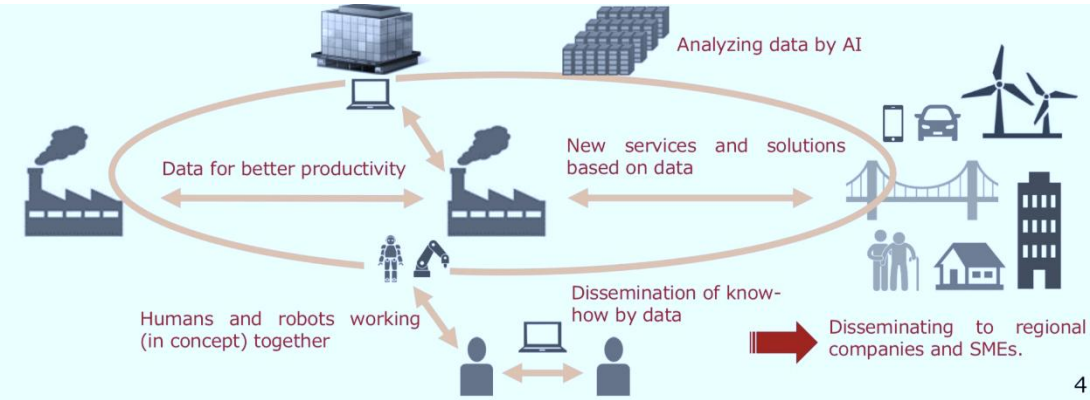
Función defensiva predominante:-

Función no NIST CSF: -

Descrición e alcance: Os contornos industriais conectados representan unha evolución da arquitectura industrial tradicional cara a modelos nos que os sistemas de operación, supervisión, análise, mantemento, xestión e soporte intercambian información de maneira máis continua, distribuída e interdependente. Esta conectividade pode

producirse entre activos de planta, sistemas corporativos, plataformas cloud, servizos de terceiros, contornos de mantemento remoto, compoñentes IIoT, solucións de analítica, ferramentas de trazabilidade ou infraestruturas de apoio á decisión. Máis que unha tecnoloxía concreta, trátase dun modelo de funcionamento no que a conectividade pasa a ser un elemento central da operación, da visibilidade e da eficiencia.

No ámbito industrial, esta evolución permite mellorar a integración de datos, a capacidade de supervisión, a coordinación entre áreas, a optimización do proceso e o soporte á toma de decisións. Porén, tamén introduce unha característica crítica desde o punto de vista da ciberseguridade: a progresiva desaparición de fronteiras ríxidas entre dominios que antes estaban máis separados. Isto fai que o risco deixe de concentrarse só no perímetro e pase a distribuírse a través de múltiples relacións, dependencias e superficies de exposición que afectan tanto á capa dixital como ao comportamento operativo.



Concepto de industria conectada. Fonte: METI "Connected Industries Tokyo Initiative" (2017)

Obxectivo: Aproveitar os beneficios da conectividade industrial —maior visibilidade, integración, eficiencia e capacidade de supervisión— asegurando ao mesmo tempo que esa conectividade se produce baixo criterios de segmentación, control, trazabilidade, resiliencia e gobernanza suficientes para non incrementar de forma desordenada a exposición do entorno.

Como se materializa nun entorno industrial: Na práctica, os contornos industriais conectados adoitan manifestarse a través da integración entre OT e sistemas corporativos, do uso de plataformas compartidas para analítica ou xestión, da conexión con servizos externos, do acceso remoto para mantemento, da incorporación de IIoT, da supervisión distribuída, do intercambio de datos en tempo real e da interrelación crecente entre operación, cadea de subministración e servizos dixitais. Esta realidade permite mellorar a observabilidade e a capacidade de resposta da organización, pero

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

tamén implica que unha incidencia nun punto periférico ou aparentemente auxiliar pode propagarse, directa ou indirectamente, cara a funcións de maior criticidade.

Dende a perspectiva da seguridade, o máis relevante non é só a presenza de máis conectividade, senón o feito de que esa conectividade transforma a arquitectura do risco. Os activos xa non poden analizarse illadamente: deben comprenderse como parte dun ecosistema de relacións no que a identidade, o acceso remoto, os fluxos de datos, os terceiros, as plataformas intermedias, a nube, os servidores de salto e as integracións pasan a ter un papel estruturante. Isto obriga a reforzar a defensa en profundidade e a pasar dunha lóxica de protección puntual a outra baseada na gobernanza continuada do entorno conectado.

Principais vantaxes:

- Melloran a integración de información entre operación, mantemento, supervisión e xestión.
- Permiten aumentar a visibilidade do proceso e a capacidade de análise.
- Facilitan novos modelos de mantemento, soporte, trazabilidade e optimización.
- Favorecen a coordinación entre dominios antes máis illados.
- Poden contribuír á eficiencia, á resiliencia e á capacidade de resposta da organización.

Principais riscos e limitacións:

- Ampliación da superficie de exposición e das vías de propagación entre dominios.
- Maior dependencia de integracións, terceiros, servizos externos e plataformas intermedias.
- Dificultade para manter unha visión clara de activos, fluxos e relacións cando a conectividade medra rapidamente.
- Incremento do impacto potencial dunha credencial comprometida, dunha integración insegura ou dun acceso remoto mal gobernado.
- Risco de asumir que a conectividade achega eficiencia sen acompañala dunha gobernanza proporcional do risco.

Elementos de seguridade especialmente relevantes: Neste ámbito cobran especial importancia a segmentación de rede e separación IT/OT, a DMZ industrial, a visibilidade de activos e comunicacións OT, o acceso remoto seguro, o MFA, a IAM, o PAM, o control

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

de accesos de terceiros, a monitorización e operación de seguridade, a protección das integracións software, a revisión das dependencias cloud e SaaS e a existencia de procedementos de cambio e continuidade adaptados á realidade conectada.

Casos habituais de uso: Emprégase para integración de datos OT con plataformas corporativas, supervisión remota de procesos, mantemento distribuído, analítica operativa, conexión con cadea de subministración, incorporación de servizos cloud, trazabilidade en tempo real, integración con plataformas MES, soporte remoto de fabricantes e arquitecturas nas que a operación depende crecentemente de servizos e relacións dixitais interconectadas.

Enfoque recomendado no catálogo: Dentro deste catálogo, os contornos industriais conectados deben interpretarse como un marco estrutural de evolución da industria, non como un control concreto. O seu valor dependerá da capacidade da organización para acompañar a conectividade con arquitectura segura, control de accesos, gobernanza das integracións, visibilidade continua e preparación para responder a incidentes que xa non afectan a compoñentes illados, senón a ecosistemas interdependentes. En organizacións maduras, poden reforzar moitas capacidades; en organizacións con gobernanza débil, poden converterse no principal multiplicador do risco.

Observacións / medidas compensatorias asociadas: En contornos industriais, a evolución cara a modelos máis conectados resulta máis segura cando se produce de maneira gradual, con inventario actualizado, segmentación explícita, control de accesos, trazabilidade das integracións e monitorización suficiente dos novos fluxos. Cando non sexa posible asegurar plenamente todos os elementos do ecosistema conectado, convén reforzar medidas compensatorias como separación adicional de dominios, limitación de conectividade entre compoñentes, validación previa de integracións, revisión periódica de permisos e supervisión intensificada das relacións entre sistemas e servizos.

5.11.4 Uso de intelixencia artificial en seguridade

Categoría: Tendencias emerxentes e capacidades avanzadas

Tipoloxía: Técnico / organizativo / mixto

Función defensiva predominante: Detectivo / preventivo

Función no NIST CSF: Detect, Respond

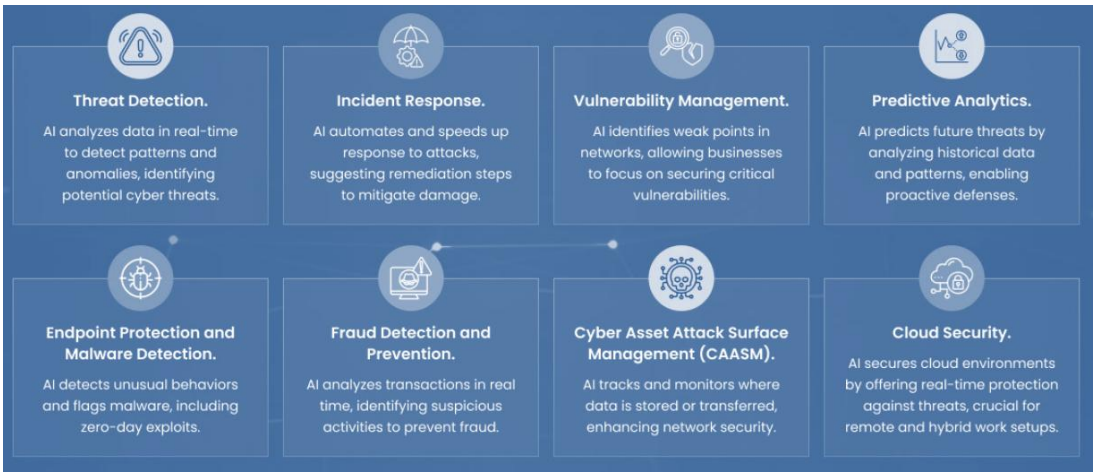
Descrición e alcance: O uso de intelixencia artificial en seguridade refírese á aplicación de técnicas de analítica avanzada, aprendizaxe automática, correlación automatizada,

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

modelos de predición, asistencia á decisión e automatización contextual para mellorar a capacidade da organización de identificar, interpretar, priorizar e responder fronte a riscos e incidentes de ciberseguridade. No ámbito industrial, esta tendencia non debe entenderse só como un fenómeno tecnolóxico emerxente, senón como unha capa potencial de amplificación das capacidades xa existentes de monitorización, análise e resiliencia, especialmente en contornos con grandes volumes de telemetría, alta complexidade operativa e necesidade de detectar patróns pouco evidentes.

A intelixencia artificial pode empregarse, entre outros fins, para detectar anomalías en tráfico e comportamento de activos, correlacionar sinais de múltiples fontes, apoiar tarefas de caza de ameazas, mellorar a análise de eventos, reducir ruído en operacións de seguridade, priorizar alertas, identificar desviacións en parámetros de proceso, reforzar o mantemento preditivo ou asistir na simulación de escenarios e na análise forense. Ao mesmo tempo, a súa incorporación introduce novos riscos: dependencia de datos de calidade, opacidade dos modelos, falsas conclusións, automatización excesiva de decisións e exposición a manipulación ou uso indebido da propia IA.

Obxectivo: Aproveitar a intelixencia artificial para aumentar a capacidade da organización de interpretar grandes volumes de información, identificar patróns relevantes e mellorar a eficacia da detección, análise e resposta fronte a riscos de seguridade, sen perder control humano nin contexto operativo sobre as decisións máis sensibles. No ámbito industrial, o seu obxectivo inclúe tamén reforzar a comprensión de relacións complexas entre actividade dixital, comportamento de rede e sinais operativos que, doutro modo, resultarían máis difíciles de analizar con rapidez e precisión.



Casos de uso de IA en ciberseguridade. Fonte: IS Partners (2024)

Como se materializa nun entorno industrial: Na práctica, o uso de IA en seguridade adoita aparecer integrado noutras capacidades xa coñecidas: plataformas NDR, SIEM,

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

SOC, monitorización ciberfísica, detección de anomalías, correlación de eventos, análise de comportamento de usuarios ou activos, priorización automática de incidentes e soporte á investigación. Tamén pode empregarse en contornos máis avanzados para apoiar simulacións, predición de fallos, análise de telemetría industrial, clasificación de riscos ou automatización parcial de respostas controladas.

En contornos industriais, o seu valor depende especialmente da calidade das fontes de datos, da correcta contextualización dos activos e do coñecemento do proceso. A IA pode resultar moi útil para sinalar desviacións, relacións anómalas ou hipóteses de risco, pero dificilmente substitúe por completo o criterio técnico e operativo humano cando están en xogo a continuidade da produción, a seguridade funcional ou a interpretación de variacións lexítimas do proceso. Por iso, o enfoque máis sólido adoita ser o da intelixencia artificial como capacidade de asistencia e reforzo, máis que como substitución automática da análise experta.

Principais vantaxes:

- Mellora a capacidade para analizar grandes volumes de eventos e telemetría.
- Pode axudar a identificar anomalías e correlacións pouco evidentes con maior rapidez.
- Resulta útil para reducir ruído e priorizar alertas en operacións de seguridade complexas.
- Pode reforzar a detección e a interpretación de sinais procedentes de múltiples dominios IT/OT.
- Favorece a evolución cara a modelos de monitorización e análise máis adaptativos.

Principais riscos e limitacións:

- A súa eficacia depende fortemente da calidade, cobertura e contexto dos datos dispoñibles.
- Pode xerar falsas conclusións, sesgos ou automatizacións inadecuadas se se aplica sen supervisión suficiente.
- En contornos industriais, o contexto operativo e as variacións lexítimas do proceso poden dificultar a interpretación correcta dos modelos.
- A opacidade dos algoritmos pode reducir a trazabilidade e a explicabilidade de certas decisións.

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

- O seu valor diminúe se se emprega como argumento comercial ou de modernización sen un caso de uso claro e ben gobernado.

Elementos de seguridade especialmente relevantes: Neste ámbito cobran especial importancia a calidade do inventario e da telemetría, a visibilidade de activos e comunicacións OT, a monitorización ciberfísica / MES, o NDR, o SIEM, o SOC, o MDR, a caza de ameazas, a gobernanza do dato, a revisión humana das decisións automatizadas e a definición clara de que tarefas poden asistirse con IA e cales requiren validación experta obrigatoria.

Casos habituais de uso: Emprégase para correlación avanzada de eventos, detección de anomalías de comportamento, priorización de alertas, apoio á investigación de incidentes, análise de telemetría industrial, mantemento preditivo con impacto en seguridade, detección temperá de desviacións operativas, apoio á caza de ameazas e análise de grandes volumes de información procedente de contornos híbridos e conectados.

Enfoque recomendado no catálogo: Dentro deste catálogo, o uso de intelixencia artificial en seguridade debe interpretarse como unha capacidade de reforzo transversal, e non como un control autónomo suficiente. O seu valor real dependerá da madurez da organización, da calidade do dato, da existencia de procesos de monitorización xa estruturados e da capacidade para integrar a IA como apoio á análise, e non como substitución acrítica do criterio humano. En organizacións maduras, pode amplificar moito a visibilidade e a detección; en organizacións pouco maduras, pode engadir complexidade, opacidade e dependencia tecnolóxica sen mellora proporcional do control.

Observacións / medidas compensatorias asociadas: En contornos industriais, o uso de IA en seguridade resulta máis robusto cando se introduce de forma gradual, ligado a casos de uso concretos e acompañado de mecanismos de supervisión humana, validación de resultados e revisión periódica do rendemento do modelo. Cando non exista madurez suficiente para automatizar decisións sensibles, convén empregar a IA como apoio á análise e á priorización, mantendo como medidas compensatorias o reforzo da monitorización convencional, a revisión experta dos eventos relevantes e a limitación das accións automáticas sobre sistemas con impacto operativo.

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

5.11.5 Monitorización avanzada e resiliencia ciberfísica

Categoría: Tendencias emerxentes e capacidades avanzadas

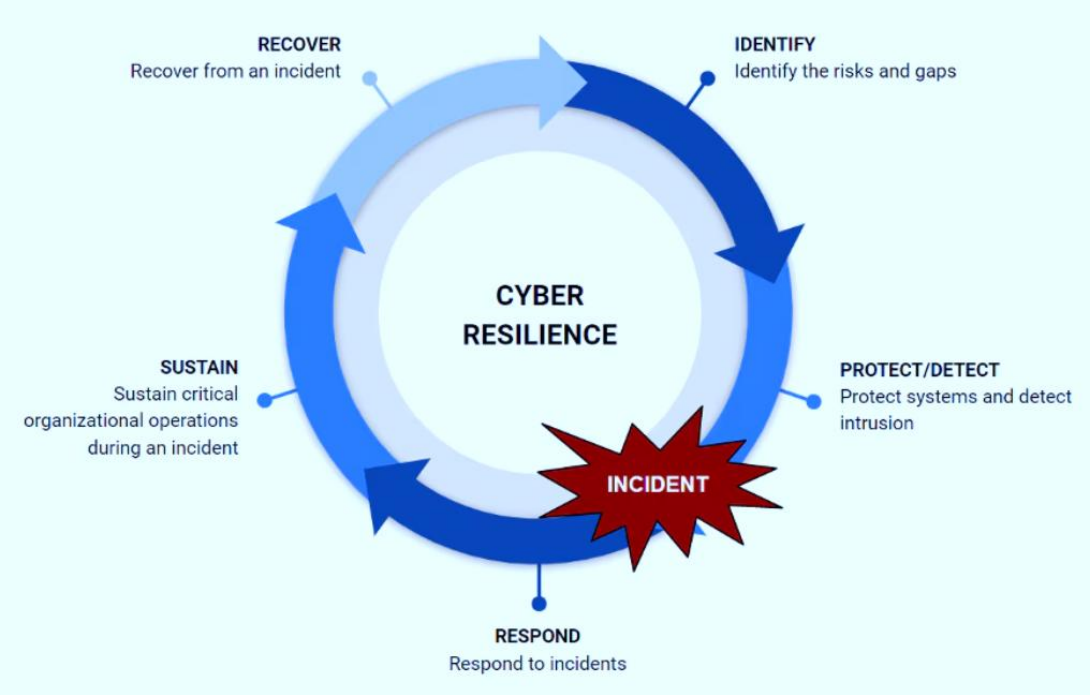
Tipoloxía: Técnico / organizativo / mixto

Función defensiva predominante: Detectivo / correctivo

Función no NIST CSF: Detect, Recover

Descrición e alcance: A monitorización avanzada e resiliencia ciberfísica comprende o conxunto de capacidades orientadas a observar, interpretar e reforzar o comportamento combinado dos sistemas dixitais, das comunicacións, dos activos físicos e do propio proceso industrial, co fin de anticipar desviacións, detectar condicións de risco, resistir mellor impactos e recuperar a operación con maior seguridade e control. Máis que un control illado, trátase dunha evolución cara a modelos nos que a protección xa non se limita a detectar eventos informáticos ou a restaurar compoñentes técnicos, senón que incorpora unha lectura máis integral do funcionamento real do sistema ciberfísico e da súa capacidade para manter condicións aceptables de operación baixo perturbación, fallo ou incidente.

Esta perspectiva combina elementos de monitorización técnica, observación de sinais de proceso, análise de comportamento operativo, correlación de eventos, coñecemento do estado dos activos e preparación para absorber degradacións sen perda inmediata de control. En contornos industriais, onde a relación entre a capa dixital e a física é directa, esta capacidade resulta especialmente valiosa porque permite pasar dunha visión fragmentada do risco a outra máis próxima á realidade do proceso, da produción e da continuidade operativa.



Etapas da resiliencia en ciberseguridade. Fonte: Foro Económico Mundial (2022)

Obxectivo: Reforzar a capacidade da organización para detectar de forma máis temperá condicións de risco con impacto ciberfísico, interpretar mellor a súa evolución e soster a operación ou recuperala baixo criterios máis seguros e resilientes. No ámbito industrial, o seu obxectivo inclúe tamén reducir o risco de que un incidente dixital, un fallo técnico ou unha alteración de comunicacións derive nunha perda abrupta de control, visibilidade ou capacidade de resposta sobre o proceso físico.

Como se materializa nun entorno industrial: Na práctica, esta capacidade adoita materializarse mediante a integración de múltiples planos de observación e preparación: telemetría de rede, estado de activos, datos de proceso, alarmas, variables industriais, eventos de sistemas, información de plataformas de supervisión, monitorización ciberfísica, análises de comportamento e procedementos de resposta e recuperación adaptados ao entorno real. O seu valor non está só na cantidade de datos dispoñibles, senón na capacidade de interpretalos de maneira conxunta para identificar degradacións, condicións anómalas, sinais febles de compromiso ou patróns que poidan afectar á estabilidade do sistema ciberfísico.

En contornos industriais maduros, esta aproximación adoita complementarse con exercicios de resiliencia, revisión de dependencias críticas, análise de modos degradados de operación, validación de capacidades de recuperación e deseño de mecanismos que permitan manter certa funcionalidade mesmo en escenarios adversos. Deste xeito, a monitorización avanzada non se limita a “ver máis”, senón que contribúe

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

tamén a responder mellor e a recuperar con maior coñecemento das condicións reais do entorno.

Principais vantaxes:

- Mellora a comprensión do estado real do sistema ciberfísico e das súas condicións de risco.
- Permite detectar anomalías con maior contexto operativo e técnico.
- Reforza a capacidade de anticipar degradacións ou evolucións perigosas do entorno.
- Axuda a planificar respostas e recuperacións máis coherentes co comportamento do proceso.
- Favorece unha visión máis integrada da continuidade, da seguridade e da resiliencia industrial.

Principais riscos e limitacións:

- Requírese unha base sólida de visibilidade, telemetría e coñecemento do proceso para que sexa realmente útil.
- Pode xerar complexidade elevada se se incorporan demasiadas fontes sen capacidade suficiente de interpretación.
- En contornos industriais, a correlación entre sinal dixital e comportamento físico non sempre é directa nin trivial.
- O seu valor diminúe se se limita a paneis de observación sen procedementos claros de actuación, escalado e recuperación.
- Pode depender de tecnoloxías avanzadas ou especializadas que exixen madurez organizativa e técnica para seren sostibles.

Elementos de seguridade especialmente relevantes: Neste ámbito cobran especial importancia a visibilidade de activos e comunicacións OT, a monitorización ciberfísica / MES, o NDR, o SIEM, o SOC, o MDR, o soporte á resposta ante incidentes, as copias de seguridade e restauración, a recuperación de operación e continuidade, o coñecemento das dependencias críticas e a coordinación entre seguridade, operación, mantemento e responsables do proceso.

Casos habituais de uso: Emprégase para reforzar a observación de procesos críticos, identificar modos degradados de operación, correlacionar sinais dixitais e físicos, mellorar a detección temperá de desviacións, apoiar a resposta ante incidentes con

impacto operativo, validar a recuperación de sistemas industriais e avanzar cara a modelos de operación máis resistentes fronte a perturbacións tecnolóxicas e ciberfísicas.

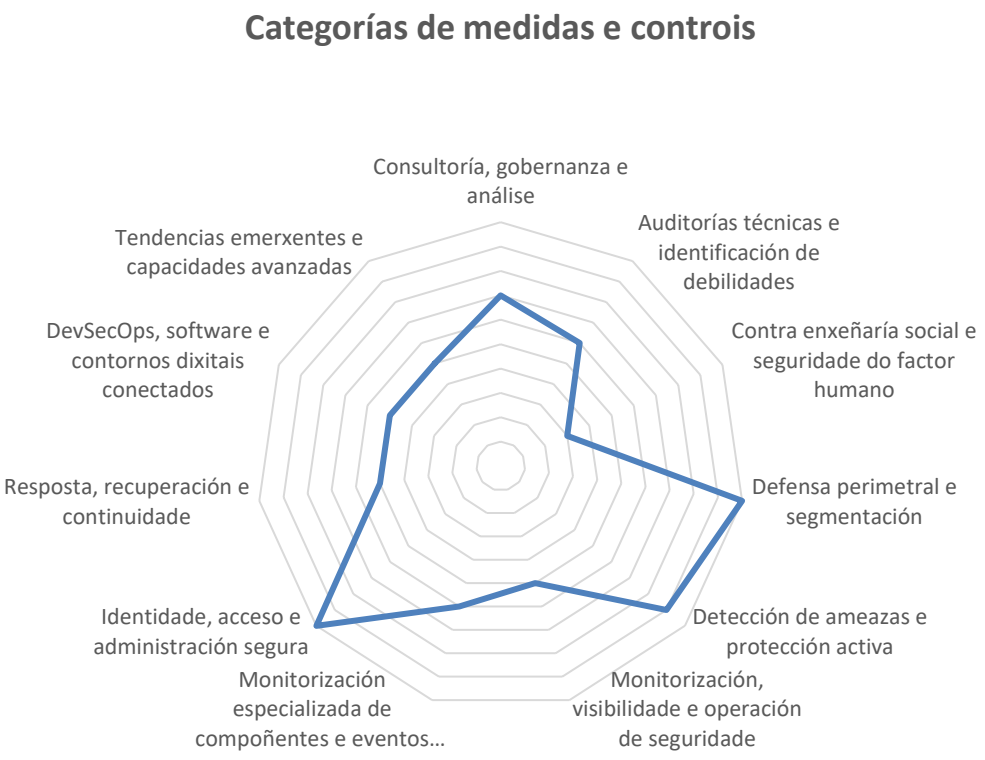
Enfoque recomendado no catálogo: Dentro deste catálogo, a monitorización avanzada e resiliencia ciberfísica debe interpretarse como unha capacidade avanzada de maduración do entorno, especialmente útil en organizacións que xa dispoñen dunha base razoable de visibilidade, segmentación, control de acceso e operación de seguridade. O seu valor non reside en substituír os controis básicos, senón en amplificalos mediante unha comprensión máis profunda do comportamento do sistema e da súa capacidade de resistir, adaptarse e recuperarse. En organizacións con baixa madurez, convén priorizar primeiro a base; en organizacións máis avanzadas, esta capacidade pode marcar unha diferenza clara en anticipación e resiliencia.

Observacións / medidas compensatorias asociadas: En contornos industriais, esta capacidade resulta máis útil cando se constrúe de maneira progresiva, partindo de fontes fiables, coñecemento operativo e procedementos claros de actuación. Cando non exista aínda madurez suficiente para unha resiliencia ciberfísica avanzada, convén reforzar como medidas compensatorias a visibilidade OT, a segmentación, a monitorización de rede, a coordinación entre operación e seguridade, as probas de recuperación e a preparación de modos degradados de funcionamento baixo control.

5.12 Resumo do catálogo

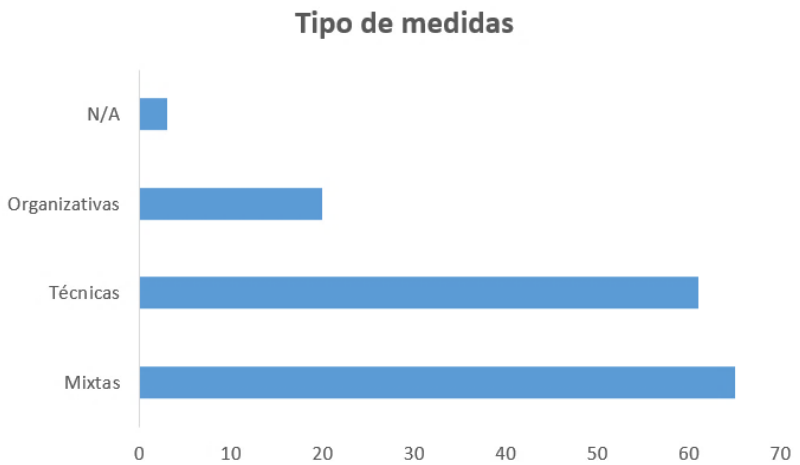
Co obxectivo de facilitar unha lectura de conxunto do catálogo e complementar a descrición individual de cada control, inclúese a continuación unha síntese gráfica da súa composición. Estas representacións permiten visualizar de maneira agregada a natureza das medidas propostas, a súa orientación funcional predominante, o seu aliñamento coas funcións do marco NIST CSF e a distribución interna do catálogo por grandes bloques temáticos.

A representación por categorías funcionais permite observar a súa distribución interna e o peso relativo de cada bloque. Destacan especialmente as áreas de **defensa perimetral e segmentación**, **identidade, acceso e administración segura** e **detección de ameazas e protección activa**, que concentran unha parte relevante das medidas propostas. Este reparto é coherente coa necesidade de reforzar, nos contornos industriais conectados, **os mecanismos de separación entre dominios, o control do acceso a activos críticos e a capacidade de identificar comportamentos anómalos ou maliciosos nunha fase temperá**.



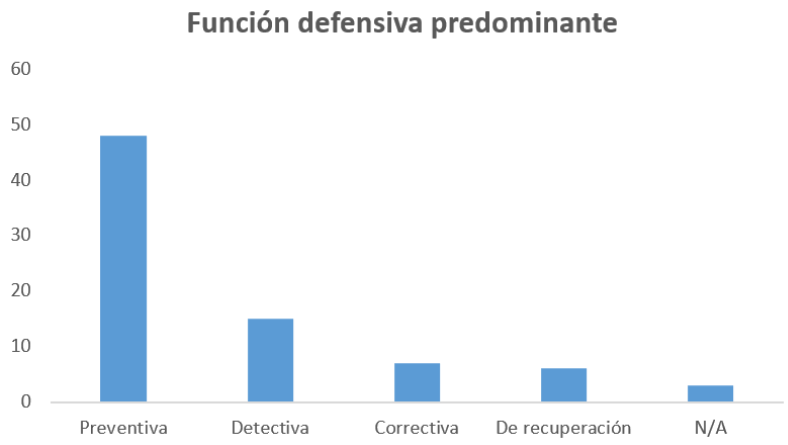
Volume de controis por categoría no catálogo. Fonte: elaboración propia (2026)

A análise por tipoloxía confirma o **claro predominio de medidas de carácter técnico e mixto**, o que resulta coherente coa natureza do ámbito ICS/OT e coa finalidade práctica deste documento. A presenza de controis organizativos, aínda que menor en termos absolutos, **segue a ser relevante**, xa que achega a capa de gobernanza, procedemento e coordinación necesaria para que as medidas técnicas poidan implantarse, sosterse e revisarse con criterios de risco e continuidade.



Tipoloxía de medidas do catálogo. Fonte: elaboración propia (2026)

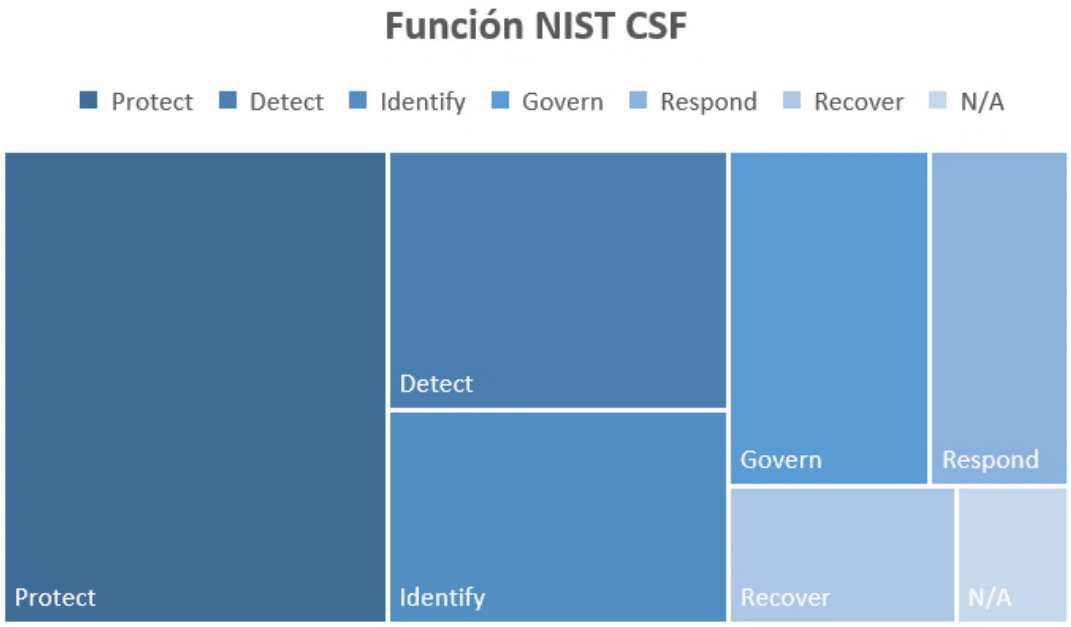
Por outra banda, a distribución segundo a función defensiva predominante mostra unha **orientación maioritariamente preventiva**. Este resultado era esperable nun catálogo concibido como instrumento de mellora progresiva da postura de seguridade, xa que unha parte moi significativa dos controis descritos persegue **reducir exposición, limitar superficies de ataque, reforzar o acceso, mellorar a segmentación e diminuír a probabilidade de compromiso**. Xunto a esta base preventiva, obsérvase tamén a presenza de capacidades detectivas e, en menor medida, de controis correctivos e de recuperación, o que reforza a idea de **defensa en profundidade e de resiliencia operativa**.



Funcións defensivas no catálogo. Fonte: elaboración propia (2026)

Por último, a lectura agregada segundo as funcións do marco NIST CSF evidencia unha concentración principal nas funcións **Protect**, **Detect** e **Identify**, acompañadas por unha representación tamén significativa de **Govern**. Isto indica que o catálogo **non se limita a propor medidas de protección illadas**, senón que incorpora tamén capacidades de visibilidade, análise, inventario, contextualización do risco e estruturación da gobernanza. Pola súa banda, as funcións **Respond** e **Recover** presentan un menor peso relativo, pero seguen estando presentes para cubrir a resposta a incidentes, a restauración de capacidades e a continuidade da operación.

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



Funcións do NIST CSF representadas no catálogo. Fonte: elaboración propia (2026)

No seu conxunto, esta información permite concluír que o catálogo presenta unha **orientación eminentemente práctica, con forte peso técnico, predominio preventivo e aliñamento claro cos piares fundamentais da protección, a detección e a gobernanza**. Ao mesmo tempo, a distribución por bloques amosa que o documento procura ofrecer unha **cobertura ampla do ciclo de defensa**, integrando medidas de análise, endurecemento, supervisión, administración segura, resposta e recuperación, aínda que con diferente densidade segundo a natureza de cada dominio funcional.

6 Estratexia de priorización e implantación

6.1 Criterios de priorización

A utilidade real dun catálogo de controis como o presente **non depende unicamente da calidade ou amplitude das medidas descritas**, senón tamén da capacidade da organización para **priorizar a súa implantación con criterios realistas, proporcionados e sostibles**. En contornos industriais, esta cuestión resulta especialmente relevante, xa que a mellora da ciberseguridade debe convivir coa continuidade da operación, coa estabilidade do proceso, coas restricións de mantemento, coa presenza de sistemas legados e coa dependencia habitual de fabricantes, integradores e provedores de servizos. Por este motivo, a selección da orde de implantación non debería responder a unha lóxica de acumulación de tecnoloxías nin a unha visión puramente normativa, senón a unha análise contextualizada do risco e da viabilidade.

Neste marco, a priorización dos controis pode apoiarse nun conxunto de criterios complementarios que permiten ordenar as actuacións segundo o seu valor real para a organización. Entre eles, destacan especialmente o **risco**, a **criticidade**, a **exposición**, o **impacto operativo**, a **facilidade de implantación** e a **dependencia de terceiros**. A combinación destes factores permite construír unha secuencia de despregue máis sólida que a que resultaría de atender exclusivamente á severidade teórica dunha vulnerabilidade, ao custo da solución ou á súa popularidade no mercado [13] [14] [15].

- O primeiro criterio, e probablemente o máis relevante, é o de **risco**. Priorizar en función do risco implica **valorar a probabilidade de que unha ameaza poida facerse efectiva sobre un activo ou proceso e o impacto que esa materialización tería sobre a organización**. Esta aproximación obriga a ter en conta non só a existencia dunha debilidade técnica, senón tamén o nivel de exposición do activo, o seu papel dentro da arquitectura, a existencia ou non de medidas compensatorias, a accesibilidade dende outros dominios e o tipo de consecuencias que poderían producirse. Nun contorno industrial, este risco non pode medirse unicamente en termos de perda de información, senón tamén de interrupción da operación, degradación da calidade, dano físico, afectación á seguridade das persoas ou incumprimento de servizos esenciais.
- Un segundo criterio clave é a **criticidade** do activo, do sistema ou do proceso afectado. **Non todos os compoñentes teñen o mesmo peso dentro da**

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

organización, nin todos os incidentes producen consecuencias equivalentes. Existen activos que, pola súa función, polos servizos que soportan ou pola súa relación co proceso industrial, deben considerarse prioritarios dende o punto de vista da protección. Isto inclúe, por exemplo, sistemas de supervisión e control, estacións de enxeñaría, servizos de acceso remoto, repositorios de configuración, sistemas de autenticación, compoñentes de comunicación entre zonas, activos ligados á seguridade funcional ou infraestruturas sen as cales non sería posible manter unha operación segura e estable. A criticidade, ademais, pode non ser visible nun inventario puramente tecnolóxico, polo que resulta esencial interpretala co apoio de operación, mantemento e responsables de proceso.

- O terceiro criterio é a **exposición**, entendida como o **grao en que un activo, servizo ou comunicación se atopa accesible, directa ou indirectamente, a interaccións non desexadas**. Un sistema altamente exposto —por exemplo, un servizo publicado, unha conexión remota ampla, un dispositivo con acceso dende a rede corporativa ou un activo situado nun segmento pouco compartimentado— tende a requirir maior prioridade que outro cunha debilidade semellante pero fortemente illado ou ben compensado. A exposición tamén debe valorarse de maneira dinámica: non depende só de se un activo está "en rede", senón de quen pode chegar a el, por que canles, con que privilexios, mediante que dependencias e baixo que grao de trazabilidade e control.
- Un cuarto criterio esencial é o **impacto operativo** da medida a implantar. **En ciberseguridade industrial non abonda con saber que un control sería desexable; tamén é necesario valorar que consecuencias pode ter a súa aplicación sobre a continuidade, o rendemento, a seguridade funcional, a dispoñibilidade ou o mantemento do proceso**. Algunhas medidas poden reducir o risco de maneira moi significativa, pero resultar inviables a curto prazo por obrigar a paradas prolongadas, introducir incerteza técnica, xerar incompatibilidades con software de fabricante ou requirir validacións que non poden executarse de inmediato. Nestes casos, a priorización debe distinguir entre o valor teórico do control e a súa implantabilidade real, articulando se é preciso secuencias graduais e medidas compensatorias intermedias.
- O quinto criterio é a **facilidade de implantación**, que permite **identificar aqueles controis que, cun esforzo asumible, poden producir unha redución de risco significativa**. Este criterio non debe confundirse cunha visión simplista

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

baseada en escoller sempre o máis fácil, pero si resulta útil para detectar actuacións de alto valor e baixa complexidade relativa. En moitas organizacións industriais, existen melloras que poden executarse sen transformacións profundas da arquitectura, como reforzar accesos remotos, mellorar copias de seguridade, limitar privilexios, inventariar activos, endurecer configuracións ou introducir maior trazabilidade en conexións de terceiros. Priorizar este tipo de medidas pode xerar un efecto tractor positivo, ao permitir gañar protección real mentres se preparan iniciativas de maior complexidade.

- O sexto criterio é a **dependencia de terceiros**, particularmente relevante no ámbito industrial. **Moitas decisións de seguridade non dependen exclusivamente da vontade ou capacidade interna da organización, senón da intervención de fabricantes, integradores, mantedores, operadores de servizos, provedores cloud ou empresas externas con acceso ao contorno**. Cando un control require coordinación contractual, actualizacións de firmware, cambios validados por fabricante, reconfiguración de sistemas mantidos por terceiros ou alteracións en servizos externalizados, a súa implantación pode verse condicionada por tempos, custos, autorizacións e restricións que cómpre incorporar explicitamente á priorización. Ignorar este factor adoita conducir a follas de ruta pouco realistas e a expectativas de execución difíciles de cumprir.

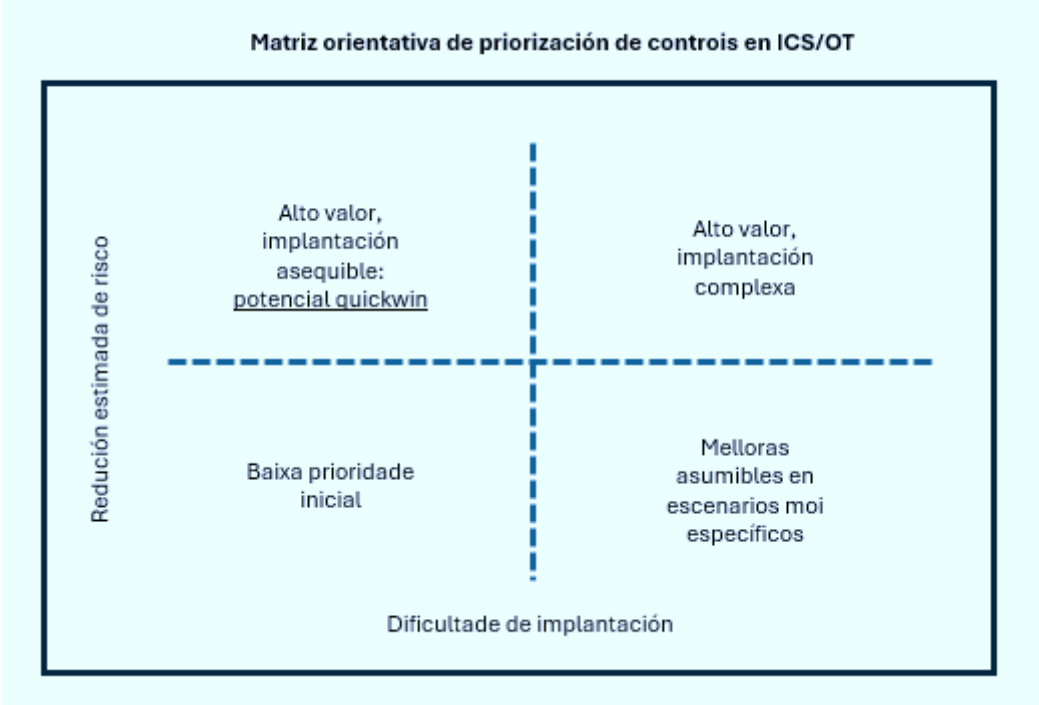
A partir destes criterios, a organización pode construír unha **matriz de priorización** na que cada control se valore segundo o risco que mitiga, a criticidade do activo asociado, o seu nivel de exposición, o impacto operativo da súa implantación, a súa facilidade de despregue e a dependencia de terceiros. O resultado non debe interpretarse como un algoritmo automático nin como unha fórmula pechada, senón como un instrumento de apoio á decisión. O máis importante non é obter unha puntuación exacta, senón facer explícita a racionalidade coa que se decide que medidas se implantan primeiro, cales se difiren, cales requiren condicións previas e cales deben acompañarse de medidas compensatorias.

Dende unha perspectiva práctica, esta priorización adoita conducir a un equilibrio entre tres tipos de actuacións.

- En primeiro lugar, medidas que aborden situacións de **alto risco e alta criticidade**, que deben tratarse con carácter preferente aínda que a súa implantación sexa máis complexa.

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

- En segundo lugar, medidas de **alto valor e baixa complexidade**, que permiten reducir exposición con rapidez e xerar melloras visibles a curto prazo.
- En terceiro lugar, medidas de **maior madurez ou sofisticación**, que poden ofrecer gran valor nun escenario máis avanzado, pero que non deberían desprazar a implantación previa dunha base mínima de control, visibilidade, segmentación, acceso seguro e capacidade de recuperación.



Matriz bidimensional de priorización de controis ICS/OT. Fonte: elaboración propia (2026)

A priorización dos controis debe entenderse como un exercicio continuo e revisable, non como unha decisión única adoptada ao inicio dun programa. A evolución da arquitectura, dos procesos, das ameazas, dos requisitos regulamentarios e das dependencias externas pode alterar a orde razoable de implantación ao longo do tempo. Por iso, convén revisar periodicamente os criterios aplicados e adaptar a folla de ruta segundo cambien o risco real, a madurez alcanzada ou a capacidade de execución da organización.

Priorizar ben significa **implantar primeiro aquilo que máis reduce o risco real nas condicións concretas da organización**, e non necesariamente aquilo que resulta máis avanzado, máis visible ou máis próximo ao ideal teórico. Este enfoque é especialmente importante en contornos industriais, onde a seguridade efectiva adoita construírse mediante decisións graduais, ben fundamentadas e compatibles coa operación.

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

6.2 Implantación por niveis de madurez

A implantación dos controis descritos neste catálogo non debería abordarse como un exercicio uniforme nin como un itinerario idéntico para todas as organizacións. A realidade industrial amosa situacións de partida moi diversas: entidades con escasa visibilidade sobre os seus activos e comunicacións conviven con organizacións que xa dispoñen de segmentación parcial, monitorización avanzada ou procedementos maduros de continuidade e resposta. Por este motivo, unha aproximación baseada en **niveis de madurez** resulta especialmente útil para orientar a adopción progresiva de medidas, establecer expectativas realistas e evitar tanto a inacción por exceso de ambición como a implantación desordenada de capacidades illadas.

A lóxica de madurez permite ordenar os controis **non só polo seu valor teórico, senón tamén pola súa relación co punto de partida da organización**. En lugar de asumir que todas as entidades deben aspirar de inmediato ás mesmas capacidades avanzadas, este enfoque propón **construír a seguridade en capas sucesivas, consolidando primeiro unha base mínima de coñecemento, control e resiliencia antes de acometer despregues de maior sofisticación técnica ou operativa**. Deste xeito, a madurez non debe entenderse como unha etiqueta estática, senón como unha guía práctica para estruturar unha folla de ruta de mellora graduada.

Con carácter orientativo, pode distinguirse entre **tres niveis principais de implantación**: **medidas básicas**, **medidas intermedias** e **medidas avanzadas**. Esta clasificación non pretende ser ríxida nin universal, xa que a mesma capacidade pode situarse nun nivel distinto segundo o sector, a arquitectura, a criticidade do proceso ou a existencia de dependencias externas. Con todo, ofrece unha base útil para interpretar o catálogo e traducilo a programas de mellora máis asumibles.

- O primeiro chanzo estaría constituído polas **medidas básicas**, isto é, aquelas capacidades que deberían considerarse prioritarias en organizacións con baixa madurez inicial ou con escasa formalización previa da súa seguridade industrial. Trátase de medidas que permiten coñecer mellor o entorno, limitar exposicións evidentes, reforzar accesos e asegurar unha capacidade mínima de continuidade e recuperación. Neste nivel adoitan situarse, entre outras, a análise de riscos tecnolóxicos, a recomendación de controis, o inventario e a visibilidade básica de activos e comunicacións, a segmentación elemental entre IT e OT, o acceso remoto seguro, o reforzo do control de identidades, o hardening básico, o control de dispositivos externos, a protección do posto e dos endpoints máis expostos, as copias de seguridade e restauración, así como determinadas medidas de

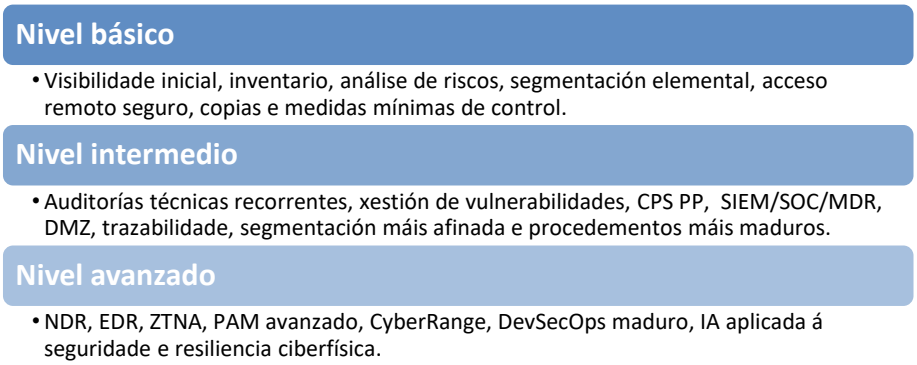
concienciación e procedementos formais de validación. Son controis que, sen requirir necesariamente unha gran sofisticación, **poden producir unha redución significativa do risco cando se implantan con criterio**.

- O segundo nivel correspondería ás **medidas intermedias**, orientadas a organizacións que xa dispoñen dunha base razoable de control e que precisan mellorar a súa capacidade de detección, trazabilidade, análise e coordinación operativa. Neste nivel adoitan incorporarse controis como auditorías técnicas máis frecuentes, revisións de arquitectura, programas de xestión de vulnerabilidades, xestión de parches estruturada, segmentación máis detallada, DMZ industriais, plataformas CPS PP, SIEM, SOC ou MDR, NAC en puntos sensibles, protección reforzada do correo electrónico, trazabilidade de sesións, control máis granular de accesos de terceiros, e mecanismos de monitorización OT máis avanzados. O seu valor principal é **consolidar a capacidade da organización para pasar dunha seguridade basicamente preventiva a un modelo no que a observación, a análise e a resposta comezan a ter un papel máis relevante**.
- O terceiro nivel agruparía as **medidas avanzadas**, propias de contornos cunha madurez xa consolidada, cunha arquitectura máis ordenada e cunha certa capacidade de operación da seguridade. Neste nivel situaríanse controis como ZTNA, PAM moi estruturado, NDR, EDR nos activos compatibles, threat hunting, integración avanzada de sinais IT/OT, validacións en CyberRange, prácticas maduras de DevSecOps, protección de software ligado á operación, uso de capacidades de IA aplicadas á análise de riscos e incidentes, e mecanismos avanzados de resiliencia ciberfísica. Estas medidas poden achegar un valor moi alto, pero **adoitan depender da existencia previa de inventario fiable, segmentación razoable, identidade gobernada, procedementos claros, telemetría útil e capacidade real de análise e resposta**. **Sen esa base, corren o risco de quedar infrautilizadas, mal configuradas ou desconectadas da realidade operativa**.

A principal vantaxe deste enfoque por niveis é que permite **adaptar a folla de ruta á situación real da organización**. Unha empresa industrial pequena ou mediana, cunha arquitectura pouco documentada e escasa capacidade interna de seguridade, obterá normalmente máis valor introducindo visibilidade, acceso remoto seguro, segmentación básica e copias validadas que incorporando de inmediato tecnoloxías avanzadas de detección sen contexto suficiente. Pola contra, unha organización xa madura, cunha base

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

preventiva consolidada, pode atopar máis beneficio relativo na mellora da correlación, da detección temperá, da resposta estruturada e da resiliencia operativa.



Resumo simplificado de controis por nivel de madurez en ICS/OT. Fonte: elaboración propia (2026)

Con todo, este modelo tamén require cautela. A clasificación por madurez **non debe empregarse para pospoñer indefinidamente medidas necesarias nin para asumir que todos os controis avanzados son sempre secundarios**. En certos contextos, un control habitualmente avanzado pode ser prioritario se responde a un risco moi exposto ou a unha obriga específica do proceso. Do mesmo xeito, unha medida básica mal implantada ou insuficientemente gobernada pode ofrecer menos valor que outra aparentemente máis sofisticada pero ben contextualizada. A madurez, polo tanto, debe lerse como **criterio de orientación, non como regra automática**.

Outra vantaxe relevante é que esta estrutura facilita a **comunicación entre áreas técnicas, operativas e directivas**. Presentar a implantación en niveis permite explicar mellor **por que determinadas capacidades se incorporan antes ca outras, que dependencias existen entre elas e que condicións previas deben consolidarse antes de avanzar cara a escenarios máis complexos**. Isto favorece a elaboración de follas de ruta comprensibles, compatibles co orzamento, coa dispoñibilidade de persoal e coas restricións operativas da organización.

Dende unha perspectiva práctica, a implantación por niveis de madurez pode empregarse de varias maneiras. En primeiro lugar, como instrumento de **autoavaliación**, permitindo á entidade identificar en que estadio se atopan as súas capacidades actuais. En segundo lugar, como base para **priorizar investimentos**, orientando os recursos cara ás medidas que máis contribúen a consolidar o seguinte chanzo razoable de madurez. En terceiro lugar, como marco para **ordenar o despregue temporal**, distinguindo entre controis que poden abordarse no curto prazo, medidas que requiren preparación previa e capacidades que só terán sentido cando a organización dispoña dunha base mínima sólida. Finalmente, tamén pode servir como

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

apoio para procesos de adecuación a marcos como NIST CSF [11], ISO 27001 [26], IEC 62443 [27] ou ENS [28], nos que a progresividade e a trazabilidade da mellora teñen un papel central. Mais detalle de cumprimento normativo en [25].

A implantación por niveis de madurez en definitiva, debe entenderse como unha **ferramenta para facer máis realista, sostible e eficaz a adopción do catálogo**. O seu valor non reside en clasificar organizacións de forma ríxida, senón en ofrecer unha estrutura que permita construír capacidades de maneira ordeada, progresiva e coherente coa realidade do risco e da operación industrial.

6.3 Quick wins en contornos industriais

Nun programa de mellora da ciberseguridade industrial, non todas as medidas teñen o mesmo tempo de maduración nin requiren o mesmo nivel de investimento, transformación arquitectónica ou coordinación interna. Xunto a actuacións de maior alcance e complexidade, existen tamén controis e decisións que, ben seleccionados, poden producir unha **redución relevante do risco nun prazo relativamente curto e cun esforzo asumible**. **A estas actuacións adoita aludirse como *quick wins***: medidas de impacto alto, implantación comparativamente viable e capacidade para mellorar de maneira visible a postura de seguridade sen depender necesariamente de proxectos longos ou de transformacións profundas da arquitectura.

En contornos industriais, este enfoque ten unha utilidade especial. A presenza de sistemas legados, a dificultade para executar cambios en produción, as restricións de mantemento, a dependencia de terceiros e a necesidade de preservar a continuidade fan que moitas organizacións perciban a mellora da ciberseguridade como un proceso complexo, custoso e lento. **Identificar *quick wins* permite romper esa inercia inicial e demostrar que é posible reducir exposición e gañar control mediante actuacións graduais, proporcionadas e moi orientadas á realidade operativa**. Ademais, estas medidas adoitan xerar un efecto tractor positivo: melloran a base de control do entorno e crean condicións máis favorables para abordar posteriormente capacidades de maior madurez.

É importante subliñar que un *quick win* non é sinónimo de medida superficial nin de acción meramente cosmética. A súa principal característica non é a simplicidade abstracta, senón a **boa relación entre esforzo de implantación e redución efectiva do risco**. Un control pode considerarse un *quick win* cando, partindo da situación real da organización, permite resolver exposicións evidentes, introducir unha capa de seguridade significativa ou reforzar de inmediato a gobernanza dun ámbito

especialmente sensible. Pola contra, unha medida técnicamente atractiva pero con pouca aplicación práctica, con escaso alcance real ou con forte dependencia de condicións previas non debería tratarse como tal.

- Entre os *quick wins* máis habituais en contornos industriais adoitan destacar, en primeiro lugar, o **inventario e a visibilidade básica de activos e comunicacións**. Non é posible protexer axeitadamente aquilo que non se coñece, e moitas organizacións seguen tendo carencias relevantes na identificación de equipos, fluxos e relacións entre sistemas IT e OT. Mellorar esta visibilidade —aínda que sexa inicialmente de maneira parcial e progresiva— adoita xerar un beneficio inmediato: permite identificar puntos cegos, reducir incerteza, apoiar a análise de riscos e fundamentar mellor a priorización doutros controis. Isto pode facerse manualmente, ou da man da integración por exemplo dunha plataforma CPS PP que adquira tráfico pasivamente sen interferir coa producción.
- Outro ámbito no que adoitan existir melloras de implantación asumible é o da **segmentación básica**. Sen necesidade de acometer de inicio unha arquitectura extremadamente sofisticada, moitas organizacións poden reducir exposición introducindo separacións mínimas entre a rede corporativa e a rede OT, limitando fluxos innecesarios, controlando mellor accesos de terceiros ou illando activos especialmente sensibles ou legados. Estas actuacións, cando se basean nun coñecemento razoable dos fluxos necesarios e se executan con criterio, adoitan proporcionar unha mellora clara na capacidade de contención e na redución do movemento lateral.
- Seguindo cos *quick win* de alto valor, outra mostra é o **acceso remoto seguro**. En moitos contornos industriais, o mantemento, a asistencia técnica e a operación distribuída dependen de conexións remotas, moitas veces con forte presenza de terceiros. Reforzar este ámbito mediante MFA, segmentación do acceso, servidores de salto, limitación de permisos, trazabilidade de sesións e procedementos formais de validación adoita ofrecer unha mellora moi significativa da seguridade sen requirir necesariamente unha transformación integral da arquitectura. Dado que o acceso remoto segue sendo un dos vectores máis relevantes de exposición, calquera avance neste ámbito adoita producir beneficios rápidos e claramente visibles.
- Tamén deben considerarse *quick wins* as **copias de seguridade e a restauración validada**, especialmente cando a organización depende de

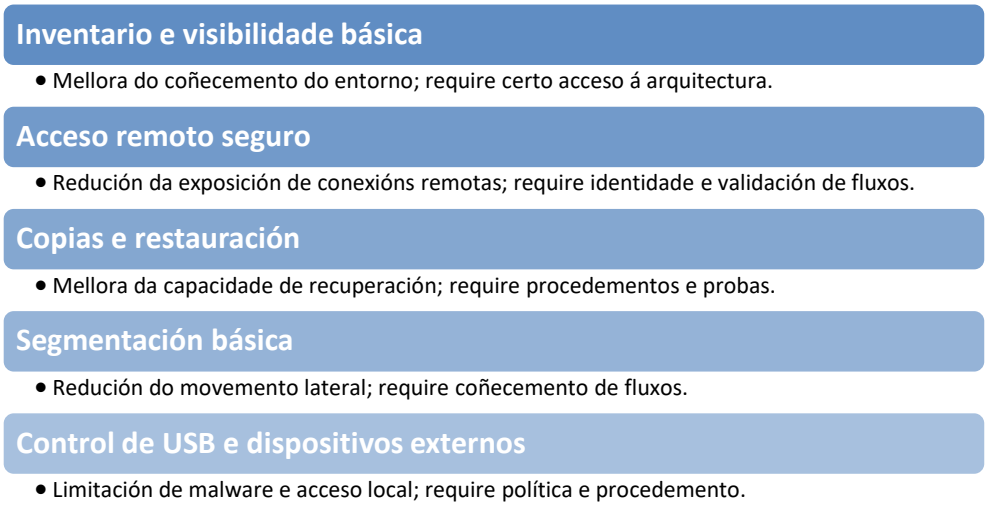
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

sistemas cuxa indispoñibilidade pode comprometer a continuidade da operación (por exemplo ante un ataque de ransomware). Dispoñer de copias non só existentes senón tamén estruturadas, actualizadas, protexidas e periodicamente verificadas é unha das medidas con mellor relación entre custo e valor práctico. En contornos industriais, este enfoque debe estenderse non só a servidores e datos corporativos, senón tamén a configuracións, proxectos, receitas, sistemas de supervisión, estacións de enxeñaría e compoñentes cuxa recuperación resulte crítica para volver a condicións operativas aceptables.

- Do mesmo xeito, o **control de USB e doutros dispositivos externos** adoita constituír un *quick win* especialmente relevante. En numerosos contornos industriais, o uso de soportes extraíbles, portátiles de mantemento e equipos de terceiros continúa sendo unha vía de interacción habitual cos sistemas. Introducir políticas de restrición, trazabilidade, escaneo previo, validación de dispositivos autorizados e procedementos de conexión controlada pode reducir de forma moi significativa o risco asociado á introdución de malware, á fuga de información ou á modificación non autorizada de compoñentes sensibles.

Ademais destas medidas, existen outros *quick wins* frecuentes segundo o contexto: reforzo de privilexios administrativos, eliminación de contas por defecto, revisión de exposición de servizos innecesarios, bastionado básico en HMI e estacións de enxeñaría, mellora da seguridade no correo electrónico, revisión dos accesos de terceiros, formalización de procedementos de cambio, endurecemento de credenciais ou introdución de mecanismos simples de monitorización e trazabilidade.

O carácter de *quick win* dependerá sempre do punto de partida da organización, pero a idea central permanece: identificar actuacións que poidan executarse con relativa rapidez e que aporten valor inmediato.



Exemplo de potenciais Quick Wins en contornos ICS/OT. Fonte: elaboración propia (2026)

A selección destes *quick wins* debe facerse con criterio. Non se trata de escoller só o máis fácil, senón o que **máis contribúe a reducir o risco real con menor fricción de implantación**. Para iso, convén combinar os criterios expostos na sección inicial do bloque: risco, criticidade, exposición, impacto operativo, facilidade de implantación e dependencia de terceiros. Un *quick win* deixa de selo se a súa execución require longos ciclos de validación, cambios profundos de arquitectura ou coordinación contractual complexa; do mesmo xeito, unha medida simple pero de valor marxinal tampouco debería ocupar o lugar de actuacións máis relevantes.

Dende unha perspectiva de xestión, os *quick wins* teñen tamén unha función pedagóxica e organizativa. Permiten demostrar resultados temperáns, mellorar a percepción interna do programa de seguridade, facilitar a implicación de áreas operativas e xustificar novas fases de investimento ou despregue. Nun entorno no que a seguridade industrial pode percibirse como un ámbito especialmente técnico ou distante da operación diaria, estas actuacións visibles e asumibles contribúen a facer máis tanxible o valor da mellora continua.

Con todo, cómpre evitar unha interpretación reducionista. Os *quick wins* son útiles para iniciar ou acelerar unha folla de ruta, pero **non substitúen a necesidade de construír capacidades estruturais e sostibles no tempo**. A súa función é reforzar a base, non esgotar a estratexia. Un programa maduro non se limita a acumular medidas rápidas, senón que utiliza esas primeiras melloras para crear as condicións que permitan abordar despois segmentación máis avanzada, operación de seguridade máis madura, detección contextualizada, resposta estruturada e resiliencia ciberfísica.

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 despregue

A implantación dun catálogo amplo de controis de ciberseguridade industrial require non só priorizar medidas segundo risco ou madurez, senón tamén establecer unha **orde lóxica de despregue** que evite dependencias mal resoltas, proxectos desconectados entre si ou investimentos prematuros en capacidades que non contan aínda cunha base suficiente. En contornos industriais IT/OT, esta necesidade é especialmente importante, xa que moitos controis só alcanzan o seu valor pleno cando se apoian sobre coñecemento previo do entorno, gobernanza mínima, acceso razoablemente ordenado e certa estabilidade arquitectónica.

Por este motivo, a implantación non debería formularse como unha simple sucesión de produtos ou iniciativas illadas, senón como unha secuencia progresiva na que cada etapa prepara as condicións para a seguinte. Isto non significa que exista unha orde universal e inmutable aplicable a todas as organizacións, pero si unha lóxica xeral que adoita resultar válida na maioría dos contornos: primeiro cómpre **coñecer e visualizar**, despois **controlar e limitar o acceso**, a continuación **segmentar e reducir exposición**, máis tarde **mellorar a detección e a contextualización do risco**, e finalmente **consolidar capacidades de xestión de vulnerabilidades, resposta e continuidade**. Esta progresión reduce o risco de despregar capacidades avanzadas nun entorno pouco coñecido ou escasamente gobernado.

1. Un primeiro chanzo da secuencia debería centrarse na **visibilidade e no coñecemento do entorno**. Sen inventario, sen comprensión dos activos e das comunicacións, e sen unha análise mínima de riscos e dependencias, a implantación do resto dos controis tende a basearse en supostos incompletos. Nesta fase resultan especialmente relevantes capacidades como a análise de riscos tecnolóxicos, a recomendación de controis, as avaliacións técnicas e revisións de arquitectura, a visibilidade de activos e comunicacións OT e, segundo o caso, auditorías de infraestrutura ou revisións de perímetro físico-lóxico. O seu propósito é crear unha base factual que permita entender que debe protexerse, con que prioridade e a través de que relacións técnicas e operativas.
2. Unha vez acadado un nivel razoable de visibilidade, a seguinte prioridade adoita ser o **control do acceso e da identidade**. En moitos incidentes industriais, o acceso remoto excesivamente amplo, as credenciais mal gobernadas, os privilexios innecesarios ou a falta de trazabilidade sobre sesións e terceiros actúan como multiplicadores do

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

risco. Por iso, nunha secuencia de despregue realista, adoita ter sentido reforzar cedo controis como MFA, IAM, PAM, acceso remoto seguro, xestión de sesións e trazabilidade e control de accesos de terceiros e provedores. O valor desta etapa reside en reducir a confianza implícita, limitar a superficie de acceso e crear condicións máis seguras para o funcionamento do resto da arquitectura.

3. O terceiro momento lóxico é o da **segmentación e separación de dominios**. Unha vez coñecido o entorno e minimizado en certa medida o risco derivado do acceso, a organización atópase en mellor posición para estruturar a arquitectura en zonas e condutos, introducir DMZ industriais, reforzar a compartimentación entre IT e OT e limitar fluxos innecesarios. Nesta fase cobran protagonismo controis como firewall, NGFW/UTM, segmentación de rede e separación IT/OT, DMZ industrial, NAC, proxy, ZTNA ou, cando proceda, mecanismos máis avanzados de control de conectividade. A segmentación non debería ser o primeiro movemento se os fluxos non están ben comprendidos, pero tampouco debería adiarse en exceso, xa que constitúe unha das bases máis eficaces para limitar movemento lateral, conter incidentes e protexer activos legados ou de alta criticidade.

4. Un cuarto bloque da secuencia debería centrarse na **detección, monitorización e contextualización da actividade**. Unha vez existen visibilidade básica, control de acceso e certa compartimentación, a organización pode extraer moito máis valor de controis orientados á observación e análise de eventos. Aquí sitúanse capacidades como IDS/IPS, NDR, SIEM, SOC, MDR, monitorización ciberfísica / MES, EDR nos activos compatibles, CPS PP, detección de integridade de ficheiros, honeypots ou threat hunting. O seu valor é moito maior cando se despregan sobre unha arquitectura xa razoablemente coñecida e estruturada, pois as alertas poden interpretarse con máis contexto e con menos ruído. Esta fase permite avanzar dende unha seguridade fundamentalmente preventiva cara a unha postura máis consciente, capaz de detectar indicios de compromiso e apoiar investigacións de maneira máis temperá.

5. A continuación, resulta recomendable consolidar de maneira máis estruturada a **xestión de vulnerabilidades, o bastionado e o control**

do cambio. Cando a organización xa dispón de mellor visibilidade, dunha arquitectura máis ordenada e dunha certa capacidade de identificación e detección, está en mellor disposición para organizar un programa sostible de xestión de vulnerabilidades, xestión de parcheado, bastionado de sistemas e servizos e validacións previas e xanela de mantemento. Este momento é especialmente importante en contornos industriais, xa que a remediación non pode basearse en decisións illadas nin en parcheado indiscriminado, senón nun proceso gobernado, compatible coa operación e apoiado en criterios de criticidade, exposición e medidas compensatorias.

6. Finalmente, a secuencia debería culminar coa consolidación das capacidades de **resposta, recuperación e continuidade**. Isto non significa que estas medidas deban pospoñerse ata o final absoluto —de feito, certos elementos como as copias de seguridade deberían abordarse cedo—, pero si que o seu desenvolvemento máis robusto require certa base previa de coñecemento, inventario, acceso gobernado, arquitectura razoablemente estruturada e visibilidade operativa. Nesta etapa sitúanse controis como soporte á resposta ante incidentes, servizos forenses, copias de seguridade e restauración, recuperación de operación e continuidade e, cando proceda, instrumentos complementarios como o ciberseguro. O seu propósito é asegurar que a organización non só poida previr e detectar mellor, senón tamén conter, restaurar e volver a condicións operativas aceptables con maior rapidez e menor impacto.

Esta secuencia xeral pode resumirse de forma simplificada, na seguinte cadea:

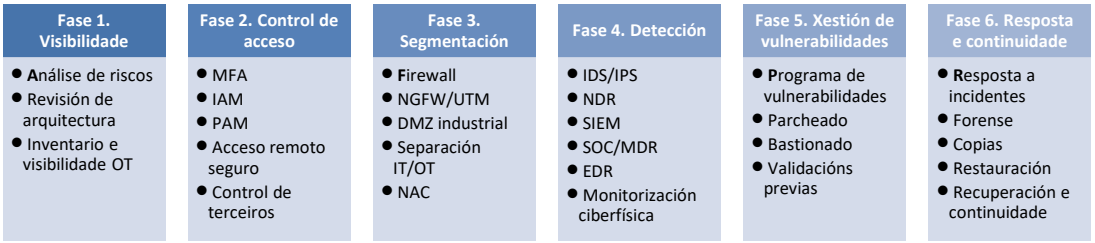
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

Proposta de priorización de controis en contornos ICS/OT. Fonte: elaboración propia (2026)

Esta formulación ten a vantaxe de ser intuitiva e útil para a elaboración de follas de ruta. Non obstante, **debe interpretarse como unha guía flexible e non como unha prescrición ríxida. Na práctica, algunhas medidas poden avanzar en paralelo e outras deberán anticiparse ou retrasarse segundo o contexto**. Por exemplo, as copias de seguridade poden merecer unha atención inmediata mesmo antes de completar a fase de detección, e certas organizacións poden precisar abordar moi cedo a protección do acceso remoto ou o control de terceiros por ter nese ámbito a súa principal exposición. A clave non está en seguir unha secuencia mecánica, senón en manter a coherencia entre dependencias, capacidade de implantación e redución efectiva do risco.

Outra cuestión importante é que esta orde de despregue **non debe confundirse coa orde de importancia absoluta dos controis**. Un control pode ser moi relevante e, con todo, necesitar condicións previas para ser implantado con sentido. Isto ocorre con frecuencia con tecnoloxías avanzadas de detección, correlación ou acceso contextualizado, que poden achegar gran valor pero requiren inventario fiable, identidade razoablemente gobernada, arquitectura segmentada e procesos operativos maduros para ofrecer resultados consistentes. Distinguir entre "control moi importante" e "control que debe implantarse primeiro" é esencial para construír unha folla 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 seguridade específicas por bloque de controis. Fonte: elaboración propia (2026)

Dende unha perspectiva de gobernanza, esta secuencia tamén facilita a coordinación entre áreas. Axuda a explicar por que determinados investimentos teñen máis sentido nun momento concreto, que dependencias deben resolverse antes de avanzar e como se relacionan os controis entre si. Isto resulta especialmente útil en contornos industriais nos que sistemas, operación, mantemento, enxeñaría, seguridade e dirección deben compartir unha visión común sobre a orde lóxica das actuacións.

En contornos industriais adoita resultar máis eficaz **despregar primeiro aquilo que permite coñecer, ordenar e limitar o entorno**, para despois **engadir observación, capacidade de resposta e mecanismos máis avanzados de mellora e resiliencia**.

6.5 Relación entre controis base e controis avanzados

Un dos erros máis habituais nos programas de mellora da ciberseguridade industrial consiste en asumir que a incorporación de controis máis sofisticados ou tecnolóxicamente avanzados permite compensar a ausencia dunha base mínima suficientemente consolidada. Na práctica, isto adoita traducirse en contornos nos que se despregan solucións de alto valor potencial —por exemplo, NDR, EDR, ZTNA, PAM avanzado, threat hunting ou capacidades de análise asistida por IA— sen dispoñer aínda de inventario fiable, segmentación suficiente, control rigoroso do acceso remoto, políticas de identidade maduras ou procedementos claros de resposta e continuidade. O resultado adoita ser unha arquitectura de seguridade desequilibrada, na que certas capacidades existen formalmente, pero non alcanzan o valor esperado ou quedan infrautilizadas pola falta de condicións previas.

Por este motivo, resulta esencial explicar a **relación de complementariedade e dependencia entre controis base e controis avanzados**. Os primeiros son aqueles que proporcionan os fundamentos mínimos para coñecer, ordenar, limitar e estabilizar o entorno; os segundos introducen capacidades de maior profundidade, contextualización, automatización ou especialización, pero adoitan necesitar esa base para funcionar de maneira eficaz. Esta relación non debe interpretarse como unha

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

oposición entre dous mundos separados, senón como unha progresión lóxica: os controis avanzados non substitúen a base, senón que a amplían, a refinan e a fan máis eficaz cando esta existe.

Os **controis base** adoitan incluír, entre outros, a análise de riscos tecnolóxicos, o inventario e a visibilidade básica de activos e comunicacións, a segmentación elemental entre IT e OT, o firewall, o acceso remoto seguro, o reforzo de identidades e autenticación, o control de terceiros, o bastionado básico, o control de dispositivos externos, as copias de seguridade e restauración e unha capacidade mínima de procedementos para xestionar cambios, incidencias e continuidade. Estas medidas non sempre resultan espectaculares nin representan o nivel máximo de sofisticación técnica, pero son as que permiten reducir exposicións evidentes, limitar o movemento lateral, coñecer o entorno e establecer un marco operativo mínimamente gobernado.

Os **controis avanzados**, pola súa parte, adoitan engadir unha capa adicional de profundidade analítica, granularidade, automatización ou contexto. Nese grupo poden situarse capacidades como ZTNA fronte a esquemas remotos máis tradicionais, PAM avanzado con control detallado de sesións privilexiadas, NDR, EDR, función avanzadas de plataformas CPS PP, threat hunting, CyberRange, prácticas maduras de DevSecOps, integración avanzada de sinais IT/OT, detección contextualizada e mecanismos máis sofisticados de resiliencia ciberfísica. O seu valor potencial é elevado, pero a súa eficacia depende moito máis de que existan condicións previas: activos coñecidos, arquitectura razoablemente segmentada, identidade gobernada, fluxos comprendidos, telemetría útil, procedementos claros e capacidade real de análise e resposta.

Un primeiro aspecto que cómpre destacar é que **un control avanzado non corrixe automaticamente as carencias dun control base ausente ou mal implantado**. Por exemplo, un NDR pode mellorar moito a visibilidade sobre comportamentos anómalos na rede, pero non substitúe a necesidade de segmentar adecuadamente nin de limitar accesos remotos amplos. Do mesmo xeito, un PAM moi sofisticado perde gran parte do seu valor se a organización non ten unha gobernanza mínima das identidades, se existen contas compartidas sen control ou se o acceso remoto segue sendo excesivamente amplo e pouco trazable. Unha plataforma CPS PP pode achegar un contexto moi valioso sobre o comportamento ciberfísico, pero non resolverá por si soa a exposición arquitectónica dun entorno escasamente compartimentado. Esta lóxica é esencial: o control avanzado mellora, refina ou amplifica a protección; non a substitúe desde cero.

Un segundo aspecto importante é que a existencia dunha base sólida **aumenta exponencialmente o valor dos controis avanzados**. Cando a organización xa dispón

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

de inventario fiable, acceso remoto gobernado, segmentación razoable, fontes de telemetría útiles e procedementos claros, entón capacidades como SIEM avanzado, NDR, EDR, ZTNA, threat hunting ou monitorización ciberfísica poden ofrecer resultados moito máis consistentes. Nese escenario, a tecnoloxía avanzada non opera no baleiro, senón sobre un entorno máis coñecido e estable, no que as alertas son máis interpretables, as decisións máis accionables e a relación entre control e risco máis visible.

Tamén é importante subliñar que a distinción entre base e avanzado **non é absoluta nin fixa**. Un mesmo control pode comportarse como capacidade avanzada nunha organización cun nivel inicial moi baixo e, pola contra, pasar a considerarse parte da base operativa nunha entidade xa madura. O relevante non é tanto a etiqueta, senón a función que cumpre dentro da arquitectura e as dependencias que arrastra. Por exemplo, un SIEM pode parecer avanzado para unha organización sen inventario nin procedementos de análise, pero converterse nun compoñente case básico nunha organización que xa opera cun SOC estruturado. O mesmo ocorre co NAC, co ZTNA ou coas capacidades de visibilidade OT: o seu lugar real na folla de ruta depende do punto de partida e do contexto.

Outra cuestión clave é que a relación entre controis base e avanzados non debe lerse só en termos tecnolóxicos. Tamén existe unha dependencia forte no plano **organizativo e procedemental**. A resposta ante incidentes, por exemplo, pode apoiarse en tecnoloxías moi avanzadas de detección e análise, pero seguirá sendo débil se non existen roles definidos, criterios de escalado, coordinación entre áreas técnicas e operativas, procedementos validados e capacidade de restauración. Do mesmo xeito, a mellor ferramenta de acceso contextualizado perderá valor se a organización non ten claros quen debe acceder, a que recursos, en que condicións e baixo que aprobación. A madurez real deriva tanto da tecnoloxía como da forma en que esta se integra con procesos, responsabilidades e práctica operativa.

Dende unha perspectiva de implantación, esta relación suxire unha regra práctica moi útil: **antes de investir nun control avanzado, convén preguntarse que condicións previas debe cumprir a organización para obter valor del**. Se esas condicións non existen, pode ser máis eficiente reforzar primeiro os controis base dos que depende. Esta pregunta axuda a evitar despregues prematuros, expectativas irreais e investimentos que terminan ofrecendo menos retorno do esperado. Tamén axuda a construír follas de ruta máis coherentes, nas que cada capacidade nova se apoia sobre unha base xa parcialmente consolidada.

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

A utilidade desta diferenciación é tamén comunicativa. Permite explicar á dirección, aos equipos técnicos e ás áreas operativas por que determinadas medidas, aínda sendo menos vistosas, deben consolidarse antes de dar o salto a tecnoloxías máis avanzadas. Axuda a ordenar o discurso: primeiro coñecer, limitar e gobernar; despois observar mellor, correlacionar, automatizar e especializar. Nun contexto no que a ciberseguridade industrial pode percibirse como unha sucesión de ferramentas ou proxectos independentes, esta visión contribúe a reforzar a idea de arquitectura de capacidades e non de acumulación de solucións.

A relación entre controis base e controis avanzados debe formularse como un principio de **acumulación coherente**. Os controis avanzados son desexables e poden ofrecer un valor moi alto, pero a súa eficacia depende de que exista previamente un nivel mínimo de control do entorno, de gobernanza da identidade, de compartimentación, de visibilidade e de capacidade de resposta. Sen esa base, a sofisticación pode converterse nunha ilusión de seguridade máis que nunha mellora real da postura defensiva.

Podemos pechar dicindo que nunha folla de ruta madura, os controis avanzados deben entenderse como mecanismos para **reforzar e expandir unha base xa construída**, non como atallos para substituír os fundamentos que aínda non existen.

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

7 Conclusións

Este informe reúne un **catálogo amplo, ordenado e conciso** para seleccionar, priorizar e implantar medidas de ciberseguridade en contornos industriais nos que conviven activos, procesos e dependencias de natureza **IT e OT**. O seu interese principal non está só na listaxe de controis, senón en ofrecer unha lectura estruturada do conxunto: **que capacidades existen, como se relacionan entre si e con que criterios ten sentido incorporalas** nun entorno marcado pola complexidade técnica, a criticidade operativa e a necesidade de preservar a continuidade.

A primeira idea que se desprende do documento é que **a ciberseguridade industrial require un tratamento específico**. Non abonda con trasladar ao entorno operativo controis pensados para sistemas corporativos convencionais. Os ciclos de vida longos, a presenza de sistemas legados, a dependencia de fabricantes e integradores, as limitacións de mantemento, os requisitos de dispoñibilidade e a crecente interdependencia entre dominios corporativos e industriais obrigan a traballar cunha lóxica distinta. Por iso, **protexer un contorno industrial esixe combinar perspectiva técnica, coñecemento operativo e criterio organizativo**, e non resolver a seguridade como unha suma de ferramentas.

A segunda conclusión é igual de relevante: **non existe unha medida única capaz de resolver por si soa o risco industrial**. A protección real depende da combinación de controis complementarios: gobernanza, segmentación, control de acceso, visibilidade, detección, resposta e recuperación. O catálogo deixa ver con claridade esa idea de fondo: cada capacidade ten sentido por separado, pero **gaña valor cando forma parte dun conxunto coherente**, ben relacionado e construído sobre unha base mínima suficiente.

Nese sentido, o informe insiste con razón en que **a visibilidade é un punto de partida imprescindible**. Inventariar activos, comprender fluxos, revisar arquitectura, identificar dependencias e contextualizar o risco non son tarefas accesorias, senón condicións necesarias para decidir con criterio. Sen ese coñecemento, as organizacións tenden a aplicar medidas xenéricas, a investir en capacidades pouco aproveitadas ou a incorporar controis sofisticados sen unha base suficientemente coñecida.

Tamén resulta significativo o peso que adquiren os **controis preventivos** e as **capacidades de protección**, acompañados por funcións de identificación, detección e gobernanza. Esta distribución encaixa coa realidade de moitas organizacións industriais, nas que segue sendo prioritario reducir exposición, ordear accesos, reforzar

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

a segmentación, controlar terceiros e mellorar a disciplina de cambio. Agora ben, o informe deixa claro que esa base preventiva **non é suficiente por si soa**. Debe completarse con capacidades de observación, correlación, investigación e resposta, porque a prevención absoluta non existe e porque, nun entorno industrial, detectar tarde pode traducirse en consecuencias moito máis graves.

Outro dos puntos fortes do documento é a maneira de abordar a **priorización**. O informe sostén que a orde de implantación dos controis debe responder ao **risco real e á viabilidade operativa**, e non só á severidade teórica dunha ameaza ou á dispoñibilidade dunha tecnoloxía. Iso significa incorporar á decisión factores como a criticidade do proceso, a exposición efectiva, o impacto operativo da medida, a facilidade de implantación e a dependencia de terceiros. Esta lectura permite pasar dunha aproximación abstracta a unha folla de ruta máis realista e sostible.

Na mesma liña, a proposta de organizar a implantación segundo **niveis de madurez** —básico, intermedio e avanzado— resulta especialmente útil. Non todas as organizacións parten do mesmo punto nin teñen as mesmas condicións para avanzar. Esta estrutura axuda a evitar dous erros frecuentes: por unha banda, a parálise que produce querer chegar de inmediato a un estado demasiado ambicioso; pola outra, a tendencia a incorporar capacidades avanzadas sen ter consolidado previamente o esencial. A mensaxe de fondo é clara: **a madurez non depende de acumular tecnoloxías, senón de construír unha base sólida e evolucionar sobre ela con sentido**.

O informe tamén acerta ao destacar o papel dos **quick wins**, entendidos como medidas cunha **boa relación entre esforzo e redución efectiva do risco**. En moitos contornos industriais, melloras como o inventario de activos, o acceso remoto seguro, as copias validadas, a segmentación básica ou o control de dispositivos externos poden xerar beneficios claros nun prazo relativamente curto. O seu valor non está só no resultado inmediato, senón en que **permiten gañar control sobre o entorno e preparar o terreo para actuacións posteriores máis esixentes**.

Moi relacionada con isto está a idea de que **a orde de implantación importa**. O documento mostra que adoita ter máis sentido avanzar dende a **visibilidade** cara ao **control de acceso**, a **segmentación**, a **detección**, a **xestión de vulnerabilidades** e, finalmente, a **resposta e continuidade**, que intentar despregar desde o primeiro momento capacidades avanzadas sen base suficiente. Non se trata dunha secuencia ríxida, pero si dunha lóxica sensata que axuda a evitar proxectos desconectados, dependencias mal resoltas e expectativas pouco realistas.

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

Outra conclusión importante é que **os controis avanzados non substitúen os controis base**. Tecnoloxías como NDR, EDR, ZTNA, PAM avanzado, threat hunting ou capacidades máis sofisticadas de resiliencia poden ser moi valiosas, pero adoitan depender dunha base previa de inventario, acceso gobernado, segmentación, telemetría útil, procedementos claros e capacidade de análise. Sen eses fundamentos, existe o risco de proxectar unha imaxe de madurez que logo non se corresponde coa capacidade real da organización para operar, interpretar e aproveitar eses controis.

O catálogo tamén destaca polo lugar que concede ás **medidas compensatorias**, algo especialmente relevante no ámbito industrial. En moitas organizacións non é viable parchear, substituír ou reconfigurar de inmediato certos activos. Neses casos, reducir o risco pasa por medidas como a segmentación, o hardening, a limitación de accesos, a monitorización reforzada, a trazabilidade ou o illamento de compoñentes. O valor do informe está en tratar esta realidade con naturalidade e sen simplificacións: **compensar non é renunciar á seguridade, senón xestionar o risco con criterio e de forma compatible coa operación**.

Dende unha perspectiva máis transversal, o documento reforza unha idea que adoita pasarse por alto: **a ciberseguridade industrial non pode sosterse só dende a área técnica**. Requírese coordinación entre gobernanza, operación, mantemento, enxeñaría, seguridade e terceiros. A claridade procedemental, a definición de responsabilidades e a existencia dunha linguaxe común son condicións tan importantes como os propios controis técnicos. Neste sentido, o catálogo tamén cumpre unha función útil como **marco compartido de lectura e decisión** entre perfís moi distintos.

Cómpre destacar, ademais, que se adopta unha visión **ampla e realista** da seguridade industrial. Non se limita aos controis máis próximos á rede OT, senón que incorpora tamén cuestións ligadas á identidade, ao acceso remoto, á seguridade do correo, á protección de aplicacións, á xestión de vulnerabilidades, ao DevSecOps, á continuidade ou á resiliencia ciberfísica. Esta elección responde a unha evidencia cada vez máis clara: **as organizacións industriais xa non operan en compartimentos estancos**, e a exposición pode proceder tanto dun PLC como dun portátil de mantemento, dun servizo SaaS mal gobernado ou dunha conexión remota excesivamente aberta.

O traballo deixa unha conclusión principal bastante nítida: **a mellora da ciberseguridade industrial depende menos de incorporar unha tecnoloxía concreta que de construír unha arquitectura de controis coherente, gradual e sostible no tempo**. Iso implica coñecer mellor o entorno, priorizar con criterio, reforzar

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

primeiro a base, empregar medidas compensatorias cando sexa necesario e avanzar cara a capacidades máis sofisticadas só cando existan condicións reais para aproveitalas.

Así, o catálogo pode funcionar como **ferramenta de referencia para a autoavaliación, a planificación e a revisión de capacidades**, tanto en organizacións que están a comezar como naquelas que precisan reorganizar ou reforzar o xa existente. O seu mérito principal está en **converter un conxunto amplo e heteroxéneo de controis nunha guía comprensible e aplicable a situacións reais**.

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 Ciberseguridade Industrial de Galicia (2026). *Informe de Ciberalertas - I*. Recuperado de https://ciberseguridadegalicia.gal/es

[2] Observatorio de Ciberseguridade Industrial de Galicia (2026). *Informe de Ciberalertas - II*. Recuperado de https://ciberseguridadegalicia.gal/es

[3] Observatorio de Ciberseguridade Industrial de Galicia (2026). *Informe de Intelixencia de Ameazas - I*. Recuperado de https://ciberseguridadegalicia.gal/es

[4] Observatorio de Ciberseguridade Industrial de Galicia (2026). *Informe de Intelixencia de Ameazas - II*. Recuperado de https://ciberseguridadegalicia.gal/es

[5] Observatorio de Ciberseguridade Industrial de Galicia (2026). *Informe de tendencias e regulamento*. 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). *Levando o regulamento á realidade OT: medidas compensatorias en OT (Parte I)*. Recuperado de https://www.cci-es.org/activities/llevando-la-regulacion-a-la-realidad-ot-medidas-compensatorias-en-ot-parte-i/

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

[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 Ciberseguridade Industrial de Galicia (2026). *Guía normativa de ciberseguridade 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 Criptolóxico Nacional (2022). *ENS Navegable – Revisión visual e interactiva das medidas de seguridade do Real Decreto 311/2022.* Recuperado de https://gobernanza.ccn-cert.cni.es/ens-navegable

Glosario

Acceso remoto seguro

Conxunto de medidas e mecanismos destinados a permitir conexións remotas a sistemas e servizos baixo condicións controladas, trazables e proporcionadas ao risco. En contornos industriais adoita apoiarse en MFA, segmentación, servidores de salto, permisos limitados e rexistro de sesións.

ACL (Access Control List / Lista de control de acceso)

Conxunto de regras que determinan que comunicacións, usuarios ou dispositivos están autorizados a acceder a un recurso, a unha interface ou a un segmento de rede. Utilízase con frecuencia como apoio á segmentación e ao control de fluxos.

Activo OT

Elemento tecnolóxico con función directa ou indirecta sobre a operación industrial, como PLC, HMI, estacións de enxeñaría, redes de control, sensores ou sistemas de supervisión. A súa protección debe ter en conta a criticidade do proceso, a dispoñibilidade e a seguridade funcional.

Análise GAP

Exercicio de comparación entre a situación real dunha organización e o nivel obxectivo definido por un marco, unha norma ou un conxunto de requisitos. Resulta útil para identificar carencias, priorizar melloras e ordear unha folla de ruta de implantación.

Análise de riscos tecnolóxicos

Proceso estruturado de identificación, avaliación e tratamento dos riscos que afectan aos activos, servizos, procesos e dependencias tecnolóxicas dunha organización. No ámbito industrial debe considerar tanto compoñentes IT como OT e os posibles impactos operativos, físicos e de continuidade.

API (Application Programming Interface / Interface de programación de aplicacións)

Mecanismo que permite a comunicación entre aplicacións, servizos ou plataformas. A súa protección é relevante cando se emprega para integracións, publicación de datos, servizos cloud ou interacción entre sistemas corporativos e operativos.

Auditoría técnica

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

Revisión sistemática dun entorno, sistema, rede ou conxunto de controis co obxectivo de identificar debilidades, exposicións, erros de configuración e carencias de protección. Pode abranguer arquitectura, infraestrutura, dispositivos finais, redes sen fíos, perímetro ou activos OT específicos.

BC/DR (Business Continuity / Disaster Recovery)

Conxunto de plans, procedementos e capacidades orientados a garantir a continuidade da actividade e a recuperación tras un incidente grave. En contornos industriais inclúe tamén a restauración de sistemas de control, comunicacións e servizos ligados á operación.

Bastionado

Proceso de reforzo da configuración dun sistema para reducir a súa superficie de ataque. Inclúe a desactivación de servizos innecesarios, a limitación de privilexios, o endurecemento de parámetros de seguridade e a eliminación de configuracións por defecto inseguras.

CASB (Cloud Access Security Broker)

Capacidade orientada a dar visibilidade e control sobre o uso de aplicacións e servizos cloud. Permite aplicar políticas de acceso, protección de datos e supervisión sobre interaccións con recursos SaaS e outros servizos externos.

CERT (Computer Emergency Response Team)

Equipo especializado na xestión de incidentes de ciberseguridade, análise de ameazas, publicación de alertas e emisión de recomendacións técnicas. Poden existir CERT nacionais, sectoriais, corporativos ou vinculados a organismos públicos.

Control compensatorio

Medida alternativa ou complementaria que permite reducir o risco cando a remediación directa ideal non é viable de forma inmediata. En OT é especialmente relevante cando non se pode parchear, substituír ou reconfigurar un activo sen afectar á operación.

CPS (Cyber-Physical Systems / Sistemas ciberfísicos)

Sistemas nos que compoñentes dixitais, comunicacións e procesos físicos interactúan de forma estreita. Os contornos OT e ICS son exemplos característicos de sistemas ciberfísicos.

CPS PP (Cyber-Physical Systems Protection Platforms)

Plataformas de seguridade orientadas a contornos ciberfísicos que combinan información de rede, activos, proceso e telemetría para detectar anomalías, mellorar a visibilidade e contextualizar riscos. Resultan especialmente útiles cando a análise debe integrar sinais dixitais e comportamento físico do sistema.

CSIRT (Computer Security Incident Response Team)

Equipo de resposta ante incidentes de seguridade informática. Adoita encargarse da análise, contención, coordinación e seguimento técnico de incidentes, de forma complementaria ou integrada cun SOC.

CVE (Common Vulnerabilities and Exposures)

Sistema de identificación normalizada de vulnerabilidades coñecidas mediante un código único. Emprégase habitualmente para referenciar debilidades técnicas en advisories, informes de seguridade e programas de xestión de vulnerabilidades.

CVSS (Common Vulnerability Scoring System)

Sistema estandarizado para valorar a severidade dunha vulnerabilidade. A súa puntuación resulta útil como referencia, pero non substitúe a análise contextual do risco real nun entorno industrial.

CyberRange

Contorno controlado de proba, simulación e adestramento no que se poden ensaiar controis, validar cambios, executar exercicios e formar equipos sen afectar á operación real. En industrial pode recrear de forma parcial ou completa arquitecturas IT/OT, activos e escenarios de incidente.

DAST (Dynamic Application Security Testing)

Técnica de análise de seguridade que avalía aplicacións en execución para identificar vulnerabilidades observables dende o seu comportamento real. Resulta útil para detectar fallos na capa de aplicación antes da posta en produción ou dunha actualización relevante.

DCS (Distributed Control System / Sistema de control distribuído)

Arquitectura de control habitual en industrias de proceso continuo, formada por múltiples controladores coordinados e supervisados dende interfaces centrais. Ten un papel relevante en sectores como enerxía, química, auga ou fabricación avanzada.

Defensa en profundidade

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

Principio segundo o cal a seguridade debe construírse mediante capas complementarias de control e non cun único mecanismo illado. En contornos industriais adoita combinar gobernanza, segmentación, control de accesos, visibilidade, detección, resposta e recuperación.

DLP (Data Loss Prevention)

Conxunto de capacidades orientadas a evitar a fuga, transferencia ou copia non autorizada de información sensible. En contornos industriais pode aplicarse tamén a proxectos de automatización, configuracións, receitas, documentación técnica e outros datos operativos críticos.

DMZ industrial

Zona de rede intermedia entre IT e OT destinada a canalizar intercambios necesarios baixo control, evitando conexións directas innecesarias entre ambos os dous dominios. Pode aloxar servizos compartidos, proxies, servidores de salto, historiadores ou mecanismos de intercambio controlado.

EDR (Endpoint Detection and Response)

Capacidade de supervisión, detección, investigación e resposta sobre a actividade de equipos finais. En contornos industriais adoita aplicarse a estacións de traballo, portátiles de mantemento, servidores intermedios e outros activos compatibles cun axente sen risco operativo excesivo.

ENS (Esquema Nacional de Seguridade)

Marco normativo español que establece principios e medidas para garantir a seguridade da información no sector público e nas entidades que prestan servizos relacionados. Pode ser unha referencia útil para estruturar controis, gobernanza e adecuación documental tamén en contornos con compoñente industrial.

FAIR (Factor Analysis of Information Risk)

Metodoloxía orientada á análise e cuantificación do risco da información. Pode empregarse como apoio para estruturar escenarios, impacto e exposición de forma máis formalizada.

Firewall

Mecanismo de filtrado que regula que comunicacións poden establecerse entre redes, sistemas ou segmentos. En contornos industriais constitúe unha peza fundamental para a separación IT/OT, a compartimentación interna e a limitación do movemento lateral.

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

Firmware

Software embebido que controla o funcionamento básico dun dispositivo, equipo ou compoñente hardware. En contornos industriais adoita ter un papel crítico en PLC, RTU, sensores, gateways, equipos de rede e outros activos específicos.

GRC (Governance, Risk and Compliance / Goberno, risco e cumprimento)

Enfoque de xestión orientado a integrar gobernanza, análise de risco e cumprimento normativo nun mesmo marco de decisión e control. Resulta útil para estruturar programas de seguridade de maneira coordinada.

Hardening

Termo empregado habitualmente como equivalente de bastionado. Refírese ao reforzo da configuración e da superficie de exposición dun sistema para facelo máis resistente fronte a usos indebidos ou explotacións.

HMI (Human-Machine Interface / Interface home-máquina)

Sistema ou pantalla a través da cal os operadores visualizan o estado do proceso e interactúan con el. A súa protección é crítica porque adoita estar ligada á supervisión, á operación e á execución de accións con impacto directo sobre o entorno OT.

IAM (Identity and Access Management)

Conxunto de procesos e ferramentas destinados a xestionar identidades, contas, roles, permisos e ciclo de vida do acceso. A súa finalidade é garantir que cada usuario ou sistema dispoña só dos privilexios necesarios e baixo condicións trazables.

ICS (Industrial Control Systems / Sistemas de control industrial)

Conxunto de sistemas utilizados para supervisar, controlar e automatizar procesos industriais. Inclúe compoñentes como PLC, DCS, SCADA, sensores, HMI, estacións de enxeñaría e redes de comunicación industrial.

IDS / IPS

Os IDS detectan patróns ou tráficos sospeitosos na rede; os IPS, ademais, poden bloquear ou limitar certas comunicacións. En contornos industriais adoitan utilizarse con prudencia, especialmente cando a prevención activa pode afectar á dispoñibilidade da operación.

IEC 62443

Familia de normas internacionais de referencia para a ciberseguridade de sistemas de automatización e control industrial. Aporta conceptos, requisitos e boas prácticas sobre

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

gobernanza, zonas e condutos, sistemas, compoñentes e relacións entre operadores, integradores e fabricantes.

IIoT (Industrial Internet of Things / IoT industrial)

Aplicación de sensorización, conectividade e intercambio de datos a activos, procesos e compoñentes do entorno industrial. Achega visibilidade e eficiencia, pero tamén amplía a superficie de exposición e as dependencias tecnolóxicas.

Inventario de activos

Relación estruturada dos activos tecnolóxicos presentes nun entorno, incluíndo identificación, función, localización, propietario, versións e relacións de dependencia. É unha base esencial para análise de riscos, segmentación, xestión de vulnerabilidades e resposta ante incidentes.

IoT industrial

Conxunto de dispositivos, sensores, actuadores e compoñentes conectados que recollen, transmiten ou procesan información relacionada coa operación. A súa seguridade require prestar atención a inventario, autenticación, segmentación, firmware e canles de comunicación.

IT (Information Technology / Tecnoloxía da información)

Conxunto de sistemas, redes, aplicacións e servizos orientados principalmente ao tratamento, almacenamento e intercambio de información. Nun entorno industrial convive cada vez máis con OT, xerando interdependencias que deben gobernarse con criterio.

MAGERIT

Metodoloxía de análise e xestión de riscos promovida no ámbito español para apoiar exercicios de avaliación, tratamento e documentación do risco. Pode empregarse como referencia en programas de seguridade e adecuación normativa.

MDR (Managed Detection and Response)

Servizo xestionado de detección e resposta que achega supervisión, análise e apoio operativo ante incidentes. Pode complementar ou substituír parcialmente capacidades internas, especialmente en organizacións sen SOC propio maduro.

MDM (Mobile Device Management)

Capacidade orientada á administración centralizada de dispositivos móbiles, incluíndo configuración, políticas, control de acceso, cifrado e, cando procede, borrado remoto.

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

Resulta útil para reforzar a seguridade de smartphones, tablets e outros dispositivos portátiles.

MES (Manufacturing Execution System)

Sistema de execución de manufactura que actúa como capa intermedia entre a planificación e a operación, coordinando información de produción, trazabilidade, ordes e control do proceso. A súa protección é relevante pola súa posición de enlace entre dominios corporativos e operativos.

MFA (Multi-Factor Authentication / Autenticación multifactor)

Mecanismo de autenticación que require máis dun factor de verificación para conceder acceso, como contrasinal, token, certificado ou biometría. É especialmente recomendable en accesos remotos, contas privilexiadas e interaccións con activos sensibles.

NAC (Network Access Control)

Conxunto de mecanismos orientados a controlar que dispositivos poden conectarse á rede e en que condicións. Resulta útil para limitar a incorporación non autorizada de portátiles, equipos de terceiros, dispositivos móbiles ou compoñentes non inventariados.

NDR (Network Detection and Response)

Capacidade orientada á observación e análise do tráfico de rede para detectar anomalías, movemento lateral, exploración ou interaccións sospeitosas. En OT é moi valiosa para gañar visibilidade sobre fluxos, protocolos e relacións entre activos.

NGFW (Next-Generation Firewall)

Firewall de nova xeración que engade ao filtrado clásico capacidades como inspección máis avanzada, identificación de aplicacións, integración con intelixencia de ameazas ou prevención de intrusións. Debe configurarse con prudencia en contornos industriais.

NIST

National Institute of Standards and Technology dos Estados Unidos. É unha das entidades de referencia internacional na publicación de marcos, guías e boas prácticas de ciberseguridade.

NIST CSF (Cybersecurity Framework)

Marco de referencia do NIST para estruturar programas de ciberseguridade arredor de funcións como Govern, Identify, Protect, Detect, Respond e Recover. Resulta útil para

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

clasificar controis, orientar follas de ruta e comunicar madurez de maneira comprensible.

OT (Operational Technology / Tecnoloxía de operación)

Conxunto de tecnoloxías empregadas para supervisar, controlar e manter procesos físicos, industriais ou operativos. Diferénciase de IT polo seu vínculo directo coa dispoñibilidade, a estabilidade do proceso e, en moitos casos, coa seguridade das persoas e das instalacións.

PAM (Privileged Access Management)

Capacidade orientada a controlar, limitar e supervisar o uso de contas e sesións privilexiadas. O seu valor é especialmente alto en contornos con acceso remoto de terceiros, administración de sistemas críticos ou operación sobre activos sensibles.

Patch management

Expresión habitual para referirse á xestión de parcheado. Inclúe planificación, validación, aplicación e seguimento das actualizacións de seguridade e correccións técnicas.

Pentesting

Exercicio controlado de simulación de ataque destinado a comprobar se determinadas debilidades poden ser explotadas e con que consecuencias. En contornos industriais debe formularse con forte prudencia, alcance delimitado e validación previa para evitar impacto na operación.

Phishing

Técnica de enxeñaría social baseada normalmente en correo electrónico para enganar a unha persoa e conseguir credenciais, datos, execución de accións ou acceso inicial. Pode combinarse con suplantación de identidade, urxencia aparente ou uso de ligazóns e anexos maliciosos.

PLC (Programmable Logic Controller / Controlador lóxico programable)

Dispositivo fundamental en moitos contornos industriais encargado de executar lóxicas de control sobre máquinas e procesos. A súa criticidade fai que a súa seguridade, configuración e exposición deban tratarse con especial prudencia.

Proxy

Servizo intermediario que media e controla comunicacións entre un cliente e un recurso de destino, evitando conexións directas innecesarias. Pode utilizarse para canalizar

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

acceso a servizos, filtrar tráfico, rexistrar actividade ou publicar aplicacións baixo control.

PRTR (Plan de Recuperación, Transformación e Resiliencia)

Marco de investimento público vinculado a fondos europeos que financia, entre outras liñas, iniciativas de modernización, dixitalización e ciberseguridade.

RASP (Runtime Application Self-Protection)

Capacidade de protección integrada na aplicación ou no seu contorno de execución, deseñada para detectar e bloquear certos usos maliciosos en tempo real. Complementa outros controis de seguridade da aplicación, especialmente cando existen servizos expostos.

RETECH (Redes Territoriais de Especialización Tecnolóxica)

Programa de apoio a proxectos de especialización tecnolóxica impulsado no ámbito estatal e autonómico. Pode aparecer como marco institucional do Observatorio e doutros entregables asociados.

Resiliencia ciberfísica

Capacidade dun sistema ou dunha organización para anticipar, resistir, absorber, responder e recuperarse de incidentes que afectan simultaneamente ás capas dixitais e físicas. En contornos industriais implica non só restaurar sistemas, senón volver a condicións operativas seguras e aceptables.

RTU (Remote Terminal Unit / Unidade terminal remota)

Dispositivo empregado para recoller datos e executar accións de control en contornos distribuídos, especialmente en infraestruturas xeograficamente dispersas. É habitual en sectores como enerxía, auga ou transporte.

SaaS (Software as a Service)

Modelo no que unha aplicación se consome como servizo a través da rede, normalmente xestionado por un provedor externo. O seu uso require controlar acceso, configuración, intercambio de datos, permisos e integracións.

SANS

Organización internacional coñecida pola publicación de estudos, boas prácticas, formación e investigación aplicada en ciberseguridade. As súas guías e enquisas adoitan utilizarse como referencia sectorial.

SASE (Secure Access Service Edge)

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

Modelo que combina conectividade e seguridade para controlar accesos distribuídos, servizos cloud e recursos híbridos baixo políticas coherentes. Pode integrar capacidades como acceso seguro, filtrado, inspección e control contextual.

SAST (Static Application Security Testing)

Técnica de análise de seguridade aplicada ao código fonte, binarios ou compoñentes antes da execución, co fin de detectar vulnerabilidades e patróns inseguros. Resulta útil en procesos de desenvolvemento e integración de software.

SCADA (Supervisory Control and Data Acquisition)

Arquitectura de supervisión e adquisición de datos empregada para controlar procesos distribuídos e recoller información de campo. É habitual en sectores como auga, enerxía, transporte e outras infraestruturas con operación remota ou descentralizada.

Segmentación IT/OT

Separación arquitectónica e lóxica entre dominios corporativos e operativos para limitar exposición, movemento lateral e propagación de incidentes. Pode complementarse con zonas e condutos, DMZ industriais, firewalls e regras de comunicación estritamente definidas.

SGSI (Sistema de Xestión da Seguridade da Información)

Estrutura organizativa, documental e operativa orientada a xestionar a seguridade da información de forma continua e sistemática, habitualmente asociada a ISO/IEC 27001.

SIEM (Security Information and Event Management)

Plataforma orientada á recollida, normalización, correlación e análise de eventos de múltiples fontes. Permite mellorar a detección e a investigación de incidentes a partir dunha visión centralizada da actividade de seguridade.

SOC (Security Operations Center)

Capacidade organizativa e operativa encargada de supervisar, analizar e coordinar a resposta fronte a incidentes de seguridade. Pode ser interno, externo ou híbrido, e en contornos industriais debe integrar tamén o contexto operativo das alertas relacionadas con OT.

SSID (Service Set Identifier)

Nome identificador dunha rede Wi-Fi. A súa configuración, visibilidade e segregación poden ter relevancia en auditorías de redes sen fíos e control de acceso inalámbrico.

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

SW (Software)

Abreviatura habitual de software. No catálogo aparece especialmente vinculada a desenvolvemento seguro, integración, análise de aplicacións e protección de software ligado á operación.

Threat hunting

Actividade proactiva de procura de indicios de compromiso ou comportamento malicioso que non foi detectado automaticamente polos mecanismos convencionais. Require visibilidade suficiente, hipótese de investigación e capacidade analítica para contextualizar sinais débiles.

UTM (Unified Threat Management)

Solución que integra nun mesmo dispositivo ou servizo varias capacidades de seguridade, como firewall, inspección, filtrado ou prevención de intrusións. En contornos industriais debe empregarse con criterio e validación previa do impacto.

Vishing

Técnica de enxeñaría social baseada en chamadas telefónicas ou comunicación de voz para enganar a unha persoa e obter información, credenciais ou accións indebidas.

VLAN (Virtual Local Area Network)

Mecanismo de segmentación lóxica que permite separar redes ou grupos de dispositivos dentro da mesma infraestrutura física. É un recurso frecuente para compartimentar tráfico e apoiar o deseño de zonas.

VPN (Virtual Private Network)

Tecnoloxía que establece canles cifradas entre usuarios, sedes ou sistemas para protexer as comunicacións sobre redes potencialmente expostas. En industrial debe empregarse con alcance limitado, autenticación forte e integración con segmentación e trazabilidade.

WAF (Web Application Firewall)

Control de seguridade orientado a protexer aplicacións e servizos web fronte a peticións maliciosas e explotacións na capa de aplicación. É útil cando existen portais, APIs ou interfaces web que deben permanecer accesibles baixo condicións de control reforzado.

Xestión de parcheado

Proceso de planificación, validación, aplicación e verificación de actualizacións e correccións de seguridade en sistemas e compoñentes tecnolóxicos. En contornos

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

industriais debe conciliarse coa dispoñibilidade, a validación previa e o uso de medidas compensatorias cando o parcheo directo non é viable.

Xestión de sesións e trazabilidade

Conxunto de mecanismos orientados a rexistrar, supervisar e, cando procede, revisar as sesións de acceso a recursos sensibles. É especialmente relevante en contas privilexiadas, mantemento remoto e accesos de terceiros.

ZTNA (Zero Trust Network Access)

Modelo de acceso baseado na verificación explícita da identidade, do dispositivo e do contexto antes de conceder acceso a un recurso concreto. Procura substituír a confianza implícita por permisos granulares e limitados ao mínimo necesario.

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

CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridade Industrial
Catálogo de boas prácticas e controis de seguridade 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