CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridade Industrial

Guía Normativa de Ciberseguridade Industrial

Marzo 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

Financiado pola Unión Europea NextGenerationEU

Plan de Recuperación, Transformación e Resiliencia

incibe_

AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA

Xacobeo 2027

Índice

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

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

1 Introdución

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

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

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

--

A **Guía normativa de ciberseguridade Industrial** ten como obxectivo servir como unha referencia estruturada e práctica para as organizacións públicas e privadas de Galicia que operan en entornos industriais, especialmente aquelas que dispoñen de sistemas ou procesos baseados en **Tecnoloxía Operacional (OT)**. O seu propósito principal é **identificar e interpretar a normativa aplicable**, así como ofrecer **pautas claras para o seu cumprimento e mellora continua**.

O informe está pensado para **facilitar a comprensión do complexo marco normativo vixente**, promovendo non só o cumprimento legal, senón tamén unha evolución progresiva cara a **modelos de excelencia e madurez en seguridade** dos activos e procesos industriais fronte ás ameazas dixitais.

Vai dirixido tanto a **administracións públicas galegas** —sobre todo aquelas que xestionan infraestruturas críticas ou servizos esenciais— como a **empresas privadas industriais**, con especial atención ás **pequenas e medianas empresas (PEMEs)** que operan en sectores estratéxicos ou críticos para Galicia. Estas organizacións, a miúdo

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

cunha capacidade máis limitada para abordar o crecemento regulatorio, atoparán nesta guía unha axuda clara e aplicable.

Cómpre salientar que **a variedade normativa segundo o sector industrial pode ser moi ampla**, afectando de maneira desigual a cada subsector produtivo. Por este motivo, o enfoque do informe céntrase en **aspectos normativos troncais e boas prácticas comúns**, que serán de interese ou aplicabilidade para a **práctica totalidade da audiencia destinataria, independentemente do sector de actividade**.

Na súa elaboración empregouse unha metodoloxía baseada na análise documental da lexislación nacional e europea (**ENS**, **NIS2**, **CER**, **RGPD**, etc.), a revisión de estándares internacionais recoñecidos (**NIST CSF**, **ISO/IEC 27001**, **IEC 62443**, **CIS Controls**, entre outros), e a consulta de publicacións técnicas de organismos como **ENISA**, **INCIBE**, **CCN-CERT**, **CISA** ou o **Centro de Ciberseguridade Industrial (CCI)**.

O contido estrutúrase en torno a un **enfoque dual**: por unha banda, preséntase unha **descrición a alto nivel de diferentes normas e obrigas asociadas** que deben cumprir as organizacións industriais para adherirse a marcos de referencia nacionais, europeos e internacionais; e por outra, proporciónase unha **guía de implantación práctica para a da adopción de esas boas prácticas e estándares recoñecidos**.

Ambas perspectivas complétanse para ofrecer unha **guía comprensiva, aplicable e útil**, pensada para reforzar a **resiliencia do tecido industrial galego** nun contexto normativo e tecnolóxico en constante evolución.

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

2 Panorama xeral da ciberseguridade industrial

A ciberseguridade industrial presenta características distintivas fronte á seguridade da información tradicional (IT), tanto dende unha perspectiva técnica como organizativa.

- Mentres que en entornos **IT** a prioridade principal adoita ser a **confidencialidade dos datos**, os sistemas **OT (Tecnoloxía Operacional)** poñen o foco na **dispoñibilidade e continuidade da operación**, xa que calquera interrupción pode ter **impactos directos sobre procesos industriais, seguridade física ou servizos críticos para a cidadanía**.
- As diferenzas técnicas maniféstanse en múltiples capas. **Os dispositivos OT (como PLCs, sensores industriais ou SCADA) non foron deseñados inicialmente con criterios de ciberseguridade**, senón para funcionar de forma estable, en tempo real e durante décadas. As comunicacións baséanse en protocolos industriais como **Modbus, DNP3 ou Profinet**, moitos deles sen cifrado nin autenticación. Pola contra, os sistemas IT operan con estándares de seguridade máis consolidados (TLS, HTTPS, autenticación forte, etc.). Ademais, as redes OT tenden a estar segregadas ou compartimentadas por razóns operativas, aínda que **a súa progresiva integración con redes corporativas (converxencia IT/OT) introduce novas superficies de ataque.**
- A nivel organizativo, moitas empresas industriais galegas presentan **estruturas separadas entre os equipos de operación (OT)** e os de **tecnoloxía (IT)**. Isto tradúcese en **organigramas disxuntos, procesos de toma de decisións diferenciados, e frecuentemente, en prioridades enfrontadas**: mentres o persoal de operación prioriza a continuidade da produción, o de IT enfócase na seguridade da rede e dos datos. Esta dicotomía complica a adopción de enfoques unificados de ciberseguridade e require unha **maior cultura compartida e gobernanza transversal**.

Cómpre lembrar que moitas das instalacións industriais galegas teñen impacto directo sobre **infraestruturas críticas e servizos esenciais** (auga, enerxía, alimentación, transporte), e por tanto, calquera incidente de ciberseguridade pode ter consecuencias **económicas, sociais e mesmo para a seguridade da poboación**. Esta realidade coloca á ciberseguridade OT como un asunto estratéxico que transcende o plano tecnolóxico.

Ameazas actuais aos sistemas industriais

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

Segundo os informes do Observatorio de Ciberseguridad Industrial de **Ciberalertas** [1] e **Intelixencia de ameazas** [2], algúns dos principais vectores de risco para os sistemas industriais en Galicia e no contexto europeo son:

- **Ransomware dirixido**: con afectación a redes OT, paralización de cadeas de produción e chantaxe a operadores industriais.
- **APT (Advanced Persistent Threats)**: grupos organizados, frecuentemente vinculados a estados, que buscan persistencia e espionaxe industrial prolongada.
- **Ataques a sistemas ICS/SCADA**: mediante explotación de vulnerabilidades en compoñentes críticos de automatización industrial.
- **Accesos remotos inseguros**: o uso crecente de acceso remoto para mantemento técnico expón moitas instalacións a vulnerabilidades sen parchear.

A análise destes informes evidencia que **os ataques aos sistemas industriais non son hipotéticos, senón unha realidade crecente**, que require **capacidade de detección, resposta e mitigación adaptadas ao mundo OT**, e non simplemente trasladadas desde o ámbito IT.

Cumprimento fronte a madurez: un salto de visión

Tendo en conta o panorama anterior, ás organizacións non lles queda outra que actuar. Moitas entidades abordan a ciberseguridade como un **obxectivo de cumprimento mínimo**, orientado a pasar auditorías ou evitar sancións. Este enfoque, aínda que mal menor, resulta **insuficiente para garantir a resiliencia fronte a ameazas sofisticadas**.

Cumprir unha norma (como o **ENS** ou a **Directiva NIS2**) nunha ampla maioría de escenarios equivale a **poñer o check**, pero non implica necesariamente ter capacidade para **anticiparse, adaptarse e mellorar continuamente**. Por iso, estas guías convidan a ir un paso máis alá, incorporando en futuras edicións modelos de madurez recoñecidos internacionalmente como:

- **C2M2** (Cybersecurity Capability Maturity Model) [3]
- **CSET** (Cyber Security Evaluation Tool) [4]

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

Estes modelos permiten **avaliar o grao real de capacidade dunha organización**, identificar debilidades estruturais e deseñar unha folla de ruta realista de mellora continua baseada no ciclo **PDCA (Plan-Do-Check-Act)**.

3 Normativa nacional

O marco legal español en materia de **ciberseguridade** ten experimentado unha evolución constante nos últimos anos, co obxectivo de dar resposta aos riscos crecente derivados da dixitalización da sociedade e da industria. A lexislación nacional artéllase arredor dun conxunto de normas que afectan tanto ao **sector público** como ao **privado**, cunha especial atención ás **infraestruturas críticas**, os **servizos esenciais** e os **sistemas de información de alto impacto**.

Nesta sección revisaremos os principais textos legais e reguladores que conforman esta arquitectura normativa:

- En primeiro lugar, o **Esquema Nacional de Seguridade (ENS)**, que establece os principios básicos e os requisitos mínimos que deben cumprir as administracións públicas e os seus provedores tecnolóxicos para garantir a seguridade dos sistemas, datos e servizos. O ENS serve, ademais, como base para moitas das obrigas que posteriormente se estenden ao sector privado.

- Analizaremos tamén a **transposición da Directiva NIS** ao ordenamento xurídico español, que se materializa na **Lei 12/2018** sobre seguridade de redes e sistemas de información, e no seu desenvolvemento regulamentario a través do **Real Decreto 43/2021**. Estas disposicións afectan especialmente aos **operadores de servizos esenciais** e aos **proveedores de servizos dixitais**, e recollen medidas de prevención, xestión de riscos, notificación de incidentes e supervisión.

  ** Esta normativa segue vixente ata que se publique a nova lexislación que adapte NIS2 en España.* ***Derogará ou modificará parcialmente*** *os seus preceptos en función de como se redacte a nova norma que implemente NIS2, a cal se atopa actualmente en proceso de elaboración (a competencia é do Ministerio de Asuntos Económicos e Transformación Dixital).*

- Por último, completaremos o panorama coa referencia a outras normas nacionais relevantes para o ámbito industrial, como a **Lei de Protección de Infraestruturas Críticas (Lei PIC)**, a **Estratexia Nacional de Ciberseguridade** e a **Lei Orgánica 3/2018 (LOPD-GDD)**, especialmente no seu vínculo cos sistemas de control industrial e a protección de datos persoais que poidan coexistir nos procesos de negocio.

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

Este conxunto de normas representa o **núcleo do cumprimento legal básico en materia de ciberseguridade en España de maneira xeral**, e resulta esencial para calquera organización industrial que traballe con segundo que entidades, e/ou aspire a garantir a súa conformidade, protexer os seus activos dixitais e integrarse nun ecosistema seguro a nivel nacional e europeo.

A continuación, preséntanse os diferentes corpus normativos coas súas características principais a alto nivel, para referencia do lector.

3.1 Esquema Nacional de Seguridade

Nesta sección analizaremos con maior profundidade o **Esquema Nacional de Seguridade (ENS)**, ao tratarse da **normativa nacional de referencia** en materia de ciberseguridade, especialmente no ámbito do sector público e das entidades que colaboran con el. É certificable, con validez do mesmo por dous anos.

O ENS constitúe ademais a base sobre a que o **Centro Criptolóxico Nacional (CCN)** articula o **cumprimento da Directiva europea NIS2** en España, servindo como instrumento clave para garantir un nivel común e elevado de seguridade das redes e sistemas de información, tal e como esixe o marco normativo supranacional mencionado.

3.1.1 Introdución

O **Esquema Nacional de Seguridade (ENS)** foi creado ao abeiro da Lei 11/2007 e regulado inicialmente polo **RD 3/2010** [5], posteriormente modificado polo **RD 951/2015**, e finalmente substituído polo **RD 311/2022** [6], que actualiza o marco ás novas necesidades tecnolóxicas e normativas.

O seu obxectivo principal é **garantir a confianza no uso dos medios electrónicos** mediante políticas e medidas que aseguren a **seguridade da información, sistemas, comunicacións e servizos electrónicos**, facilitando así o exercicio de dereitos e deberes da cidadanía e das administracións.

Abrangue tanto **controles técnicos como organizativos**, e aínda que é compatible coa norma **ISO/IEC 27001** que se verá posteriormente na sección de marcos e estándares internacionais, difire no seu **ámbito de aplicación e enfoque**. As entidades certificadas en ISO 27001 terán facilitado o proceso de adaptación ao ENS.

O Esquema baséase en seis **principios fundamentais** que orientan a súa implantación en calquera organización:

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

1. **Seguridade como proceso integral**: a seguridade debe abranguer todos os elementos da organización (persoas, tecnoloxía, procesos, estrutura). Exclúese calquera enfoque puntual ou parcial.
2. **Xestión baseada en riscos**: a análise e tratamento de riscos debe ser continuo, actualizado e proporcional á natureza da información e os servizos que se protexen.
3. **Prevención, detección, resposta e conservación**: é imprescindible anticiparse ás ameazas, detectalas a tempo, responder eficazmente ante incidentes e garantir a conservación da información e a continuidade dos servizos.
4. **Defensa en profundidade**: os sistemas deben contar con múltiples capas de seguridade (organizativas, físicas e lóxicas) para minimizar o impacto de calquera fallo ou incidente.
5. **Vixilancia continua e revisión periódica**: é preciso supervisar continuamente a seguridade, detectar anomalías e actualizar as medidas ante novos riscos ou vulnerabilidades.
6. **Diferenciación de responsabilidades**: deben estar claramente definidos os roles de responsabilidade sobre a información, os servizos, a seguridade e os sistemas, sen solapamentos e con mecanismos de coordinación.

Estes principios conforman a base estrutural dun sistema de seguridade robusto, orientado á mellora continua e adaptado ás necesidades de cada organización.

Para determinar o impacto dun incidente de seguridade e establecer a **categoría do sistema**, o ENS ten en conta cinco **dimensións de seguridade** clave:

- **Dispoñibilidade (D)**: garantir que os activos estean accesibles cando os necesiten as entidades autorizadas.
- **Autenticidade (A)**: asegurar que unha entidade é quen di ser ou que a orixe dos datos é fiable.
- **Integridade (I)**: verificar que a información non foi modificada de forma non autorizada.
- **Confidencialidade (C)**: impedir que a información sexa accesible ou divulgada a persoas ou sistemas non autorizados.

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

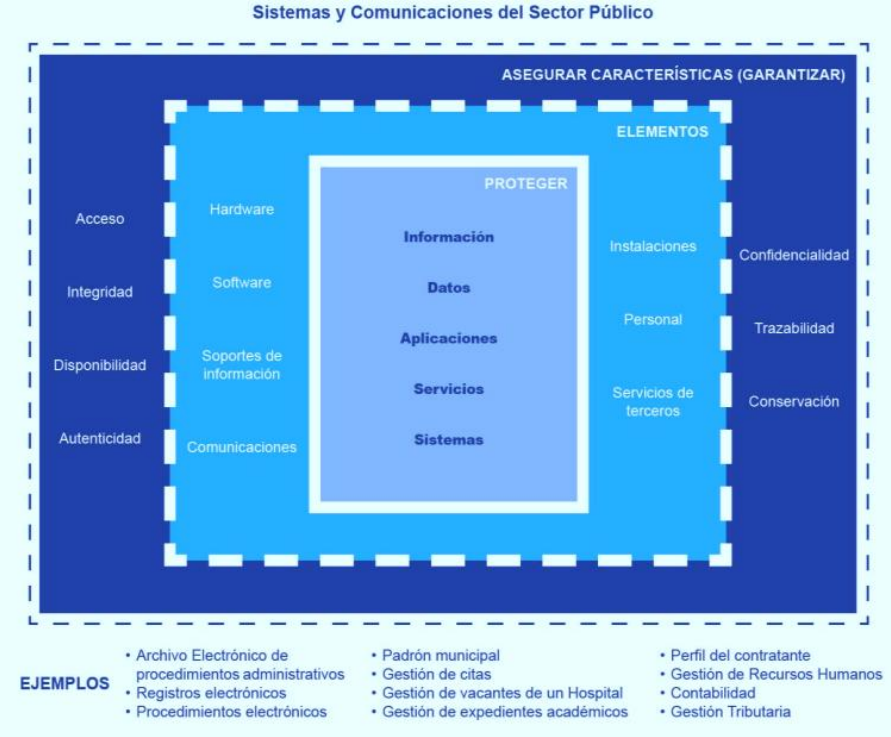
- **Trazabilidade (T)**: permitir atribuír as accións realizadas a unha entidade concreta.

Estas dimensións son a base para **avaliar e categorizar os sistemas e activos** segundo o seu nivel de sensibilidade e os requisitos de seguridade que deben cumprir.

3.1.2 Categorización de activos e sistemas

Segundo o ENS, os **activos de alto nivel** clasifícanse en tres grandes bloques: **información, servizos e sistemas de información**.

- A **información** representa os datos con significado que sustentan os procesos administrativos. As dimensións clave para avaliar este activo son a **confidencialidade** e a **integridade**.
- Os **servizos** permiten o tratamento da información e a súa dimensión prioritaria é a **dispoñibilidade**.
- Os **sistemas de información** son o conxunto de aplicacións e infraestruturas que ofrecen capacidades para xestionar tanto información como servizos.



Activos e sistemas a protexer na administración pública. Fonte: CCN (2022)

A cada un destes elementos asígnaselle un **nivel de seguridade** (baixo, medio ou alto), en función do grao de impacto que podería ter un incidente que afecte a algunha das

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

dimensións de seguridade (D, A, I, C, T). O **nivel máis alto asignado a unha dimensión determinará a categoría final do sistema**.

As categorías dos sistemas poden ser:

- **Básica**, se o nivel máis alto das dimensións é baixo.
- **Media**, se o nivel máis alto é medio.
- **Alta**, se algunha dimensión alcanza o nivel alto.

Os criterios de impacto considéranse en termos de:

- Cumprimento de obxectivos.
- Protección de activos.
- Prestación de servizos.
- Cumprimento legal.
- Protección dos dereitos das persoas.

Cada categoría implica diferentes niveis de esixencia nos controis de seguridade. As organizacións poden optar voluntariamente por **aplicar unha categoría superior** á que lle correspondería segundo a súa análise de riscos e impacto. Esta categorización condiciona os **requisitos mínimos e as medidas de seguridade obrigatorias** segundo o ENS.

3.1.3 Requisitos de seguridade

O **Esquema Nacional de Seguridade (ENS)** establece un conxunto de requisitos mínimos que deben cumprir as organizacións para garantir a seguridade dos seus sistemas de información. Estes requisitos derivan dos principios básicos do ENS e desenvólvense en medidas concretas, organizadas alfabeticamente da seguinte forma:

a) Organización e implantación do proceso de seguridade: Define os roles e responsabilidades, incluíndo os responsables de información, servizo, seguridade e sistema. É obrigatorio evitar relacións xerárquicas entre o responsable de seguridade e o do sistema. Nos servizos externalizados, debe designarse un **POC (Punto de Contacto)** de seguridade.

b) Análise e xestión de riscos: A xestión do risco debe ser continua, baseada en metodoloxías recoñecidas e xustificada en función da categoría do sistema e da natureza dos servizos e datos tratados.

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

c) Xestión de persoal: O persoal (interno e externo) debe ser formado, informado e supervisado no uso seguro dos sistemas, aplicando normas e procedementos aprobados.

d) Profesionalidade: A seguridade debe ser xestionada por profesionais cualificados ao longo de todo o ciclo de vida do sistema. Os provedores deben demostrar madurez e cualificación técnica.

e) Autorización e control de accesos: O acceso aos sistemas debe estar limitado a entidades autorizadas, con funcións e permisos definidos.

f) Protección das instalacións: Os sistemas e a súa infraestrutura deben situarse en áreas controladas e contar con medidas físicas de protección acordes aos riscos.

g) Adquisición de produtos e contratación de servizos de seguridade: Só deben empregarse produtos e servizos con funcionalidades de seguridade certificadas, axeitadas á categoría do sistema.

h) Mínimo privilexio: Os sistemas deben ser configurados para que os usuarios dispoñan só dos permisos imprescindibles, desactivando funcións innecesarias.

i) Integridade e actualización do sistema: Todo cambio ou incorporación debe estar autorizado. A seguridade debe axustarse mediante avaliación e monitorización constantes.

j) Protección da información almacenada e en tránsito: A información, especialmente en dispositivos móbiles ou medios extraíbles, debe estar protexida. Deben aplicarse procedementos de conservación e recuperación de datos.

k) Prevención ante outros sistemas interconectados: Debe protexerse o perímetro dos sistemas conectados a redes públicas ou outros entornos, minimizando riscos derivados da interconexión.

l) Rexistro de actividade e detección de código daniño: É obrigatorio rexistrar as accións dos usuarios, detectar comportamentos anómalos e previr ataques mediante análise de tráfico e contido.

m) Xestión de incidentes de seguridade: As organizacións deben contar con procedementos para detectar, clasificar, analizar, comunicar e resolver incidentes, rexistrando actuacións para mellora continua.

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

n) Continuidade da actividade: Deben disporse copias de seguridade e plans de continuidade operativa ante fallos ou interrupcións.

o) Mellora continua do proceso de seguridade: O sistema de seguridade debe actualizarse e perfeccionarse de forma periódica, baseándose en estándares recoñecidos.

p) Cumprimento de requisitos mínimos: As medidas adoptadas deben axustarse á categoría do sistema e á análise de riscos. A súa implementación reflíctese na **Declaración de Aplicabilidade**, podendo incluír medidas adicionais ou compensatorias.

q) Infraestruturas e servizos comúns: O uso de servizos compartidos entre administracións facilita o cumprimento dos requisitos do ENS.

r) Perfiles de cumprimento específicos e acreditación de entidades: Permite adaptar o ENS a sectores concretos mediante perfís definidos polo CCN e esquemas de validación de entidades e produtos.

Estas medidas constitúen o núcleo operativo do ENS e deben ser aplicadas de forma proporcional á categoría dos sistemas (básica, media ou alta) e á sensibilidade da información tratada.

3.1.4 Novidades ENS 2022

A actualización do RD do ENS en 2022 busca aliñar o marco normativo español cos estándares europeos vixentes e reforzar a súa eficacia fronte ás novas ameazas en ciberseguridade. Entre os textos europeos de referencia figuran:

- Regulamento (UE) 2019/881 sobre ciberseguridade e ENISA [7]
- Directiva (UE) 2016/1148 – Directiva NIS [8]

A revisión do ENS forma parte do marco estratéxico nacional definido pola **Estratexia de Seguridade Nacional de 2017** [9], a Estratexia Nacional de Ciberseguridade 2019 [10], e o **Plan Nacional de Ciberseguridade** [11] aprobado en marzo de 2022, que prevé preto de 150 actuacións.

A reforma persegue tres grandes obxectivos:

1. **Aliñación normativa e clarificación do ámbito de aplicación**, adaptando o ENS ao marco legal vixente e simplificando os seus mandatos.

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

2. **Flexibilización mediante a figura do perfil de cumprimento específico**, que permite aplicar con eficiencia os requisitos do ENS segundo a natureza ou sector da organización. Definido no Anexo IV do RD, este perfil é un conxunto de medidas de seguridade —incluídas ou non no Anexo II— determinadas tras un análise de riscos e validadas polo CCN.
3. **Adaptación ás tendencias de ciberseguridade**, con reforzo da vixilancia continua, revisión dos principios, requisitos mínimos e medidas.

Entre as principais **novidades técnicas e organizativas** destacan:

- Inclusión expresa dos **sistemas de información clasificada** no ámbito de aplicación.
- Obrigatoriedade de **vixilancia continua mediante sistemas de detección de ameazas**.
- Ampliación das políticas de seguridade para abordar o **risco no tratamento de datos persoais**.
- Designación dun **punto de contacto (POC)** como responsable de seguridade da organización.
- Regulación detallada da **xestión de incidentes**, incluíndo a **notificación obrigatoria ao CCN-CERT**, tamén para entidades privadas que traballen coa Administración.
- **Revisión anual obrigatoria** da categoría dos sistemas.
- Novo sistema de **codificación dos requisitos de seguridade**, baseado en requisitos base e reforzos.

Os recursos máis relevantes para profundizar nestes cambios son:

- Infografías xerais sobre o ENS [12].
- Resumo gráfico das novidades do ENS 2022 [13].
- Comparativa ENS 2010 vs ENS 2022 [14].
- Proceso de adecuación ao ENS no portal da administración electrónica [15].

Adicionalmente, na web de Gobernanza da Ciberseguridade Nacional do CCN-CERT hai un magnífico recurso **chamado ENS navegable, que de maneira cómoda e visual**

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

permite revisar polo miúdo cada unha das medidas de seguridade de aplicación do Real Decreto [16]**.**

Todos os controis de seguridade evaluables, atópanse recollidos na guía **CCN-STIC-804** [17], de implantación do ENS. En total, son **74 medidas de seguridade** (organizativas, operacionais e de protección). En xeral, cabe destacar que as **guías da serie 800 do CCN** amplían o contido do Real Decreto con información complementaria de utilidade para levar á práctica a implementación do ENS.

3.2 RD 12/2018 (Directiva NIS)

A **Directiva (UE) 2016/1148** [18] do Parlamento Europeo e do Consello, do 6 de xullo de 2016, coñecida como **NIS**, relativa a medidas para garantir un **nivel elevado común de seguridade en redes e sistemas de información**, traspúxose ao ordenamento xurídico español mediante o **Real Decreto-lei 12/2018, do 7 de setembro** [19], sobre seguridade das redes e sistemas de información.

Aínda que a directiva mencionada foi derogada en detrimento da NIS2 que se verá no apartado seguinte de Normativa europea, traémola a colación pola súa relevancia e impacto, dado que moitas das medidas que se propoñen na segunda versión, estaban presentes xa na regulación orixinal.

Finalidade:

Esta Directiva establecía medidas co obxectivo de **acadar un nivel elevado común de seguridade** nas redes e sistemas de información da Unión Europea, co fin de **mellorar o funcionamento do mercado interior**. Para iso, obrigaba aos Estados membros a:

- **adoptar unha estratexia nacional de seguridade** das redes e sistemas de información;
- crear un **Grupo de Cooperación** para apoiar e facilitar a cooperación estratéxica e o intercambio de información;
- establecer unha **rede de CSIRT** (equipos de resposta a incidentes de seguridade informática);
- impoñer **requisitos de seguridade e notificación** tanto para **operadores de servizos esenciais** como para **provedores de servizos dixitais**;
- e obrigar a que cada Estado membro **designe autoridades nacionais competentes**, **puntos de contacto únicos** e **CSIRT** con funcións específicas neste ámbito.

O **RD 12/2018** establece un **dobre obxectivo**:

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

a.- **Regular a seguridade das redes e sistemas de información** que soportan servizos esenciais e servizos dixitais,

b.- **Establecer un sistema de notificación de incidentes**, e un marco institucional de coordinación entre autoridades competentes e cos órganos europeos correspondentes.

En canto aos **CSIRT de referencia en España,** son equipos de resposta a incidentes de seguridade informática, asignados segundo a tipoloxía de entidade:

- O **CCN-CERT**, do Centro Criptolóxico Nacional, para entidades do sector público conforme á Lei 40/2015.
- O **INCIBE-CERT**, para entidades privadas non incluídas na anterior, operado conxuntamente co **CNPIC** en casos que afecten a operadores críticos.
- O **ESPDEF-CERT**, do Ministerio de Defensa, que coopera cos anteriores especialmente cando os incidentes afectan á defensa nacional.

O **INCIBE-CERT** tamén actúa como equipo de referencia para a cidadanía e outras entidades privadas non incluídas nos casos anteriores.

Estes CSIRT coordinaranse entre si e cos demais equipos nacionais e internacionais. En casos de especial gravidade, o **CCN-CERT** asumirá a **coordinación nacional da resposta técnica**. Ademais, o CCN exercerá como **punto de enlace para a cooperación transfronteiriza** dos CSIRT das Administracións Públicas.

Principais novidades introducidas pola Directiva NIS:

- Necesidade dunha **estratexia nacional de seguridade** das redes e sistemas de información.
- Designación dunha ou varias **autoridades competentes** e dun **punto único de contacto** para garantir a cooperación transfronteiriza.
- Designación de **CSIRT en rede** con recursos e infraestrutura axeitada.
- Creación dun **Grupo de cooperación** formado por representantes dos Estados membros, Comisión Europea e ENISA.
- Establecemento de requisitos e medidas en materia de seguridade e notificación para **operadores de servizos esenciais** e **provedores de servizos dixitais**.
- Introdución dun **réxime sancionador efectivo e disuasorio**.

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

En relación cos **operadores de servizos esenciais**, deberán aplicar medidas técnicas e organizativas adecuadas e proporcionadas para xestionar riscos, garantir a continuidade do servizo e notificar incidentes significativos ás autoridades competentes ou ao CSIRT. Estas autoridades poderán esixir documentación, realizar auditorías ou solicitar probas da implantación das políticas de seguridade, e impartir **instrucións vinculantes** para corrixir deficiencias. Así mesmo, colaborarán coas autoridades de protección de datos nos casos de violación de datos persoais.

En canto aos **provedores de servizos dixitais**, deberán aplicar medidas técnicas e organizativas para garantir a seguridade das redes e sistemas que empregan para prestar servizos na UE. Terán que notificar os incidentes que teñan un **impacto significativo**, tendo en conta parámetros como o número de usuarios afectados, a duración do incidente, a súa extensión xeográfica, a perturbación no funcionamento do servizo e o impacto económico e social. Esta obrigación non será de aplicación a **microempresas e pequenas empresas**, segundo a Recomendación 2003/361/CE.

As autoridades competentes poderán supervisar o cumprimento mediante actividades a posteriori e esixir información ou medidas correctoras. En caso de que o provedor de servizos dixitais estea establecido fóra da UE, deberá designar un **representante legal** nun Estado membro onde preste servizos. A xurisdición aplicarase en función da localización deste representante.

Este marco, desenvolvido a través do RD 12/2018, constitúe a primeira transposición da Directiva NIS, que será posteriormente substituída pola **Directiva NIS2** e o seu regulamento correspondente. O decreto segue **formalmente vixente**, pero atópase en **proceso de revisión e substitución** para adaptarse aos requisitos da nova **Directiva (UE) 2022/2555 (NIS2)**.

3.3 Lei de Protección de Infraestruturas Críticas

A **Lei 8/2011, de protección de infraestruturas críticas** [20], xunto co **Real Decreto 704/2011** [21] e outras disposicións posteriores, establece o marco normativo polo que se regulan as **obrigas especiais** que deben asumir tanto as **administracións públicas** como os **operadores de infraestruturas críticas (IICC)**.

Considérase **infraestrutura crítica** aquela *"infraestrutura estratéxica cuxo funcionamento é indispensable e non permite solucións alternativas, polo que a súa perturbación ou destrución tería un grave impacto sobre os servizos esenciais"*.

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

Defínese **servizo esencial** como aquel *"servizo necesario para o mantemento das funcións sociais básicas, a saúde, a seguridade, o benestar social e económico da cidadanía, ou o funcionamento eficaz das institucións do Estado e das administracións públicas"*.

A información sobre a totalidade das infraestruturas críticas está clasificada como secreta, debido á alta sensibilidade que representa para a **seguridade nacional**. **España estímase que conta con máis de 3.500 infraestruturas críticas recoñecidas**.

Os sectores nos que se engloban entidades pertencentes a sectores críticos de actividade, son os seguintes [22]:

Lista de áreas estratéxicas con infraestruturas críticas. Fonte: Lisa Institute (n.d.)

A continuación, relación de entidades afectadas de xeito máis exhaustivo, seguindo a orde do gráfico anterior:

- **Financeiro**: Mercados regulados, pago e compensación.
- **Administración**: Altas Institucións do Estado, Defensa, Interior, Partidos Políticos, Servizos de Emerxencia.
- **Auga**: Depósitos, encoros, tratamento e distribución.
- **Alimentación**: Centros de almacenamento e distribución.

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

- **Enerxía**: Eléctrico, hidrocarburos, gas.
- **Espazo**: Centros de control e telecomunicacións.
- **Nuclear**: Produción e almacenamento radiolóxico.
- **Químico**: Substancias químicas, armas e explosivos.
- **Investigación**: Laboratorios e almacenamentos.
- **Saúde**: Biolóxico, asistencia hospitalaria, vacinas e laboratorios.
- **TIC (Tecnoloxías da Información e Comunicación)**: Telefonía, radio, televisión.
- **Transporte**: Aeroportos, portos, ferrocarril e estradas.

A normativa esixe **elaborar e manter actualizados**, os seguintes documentos:

- **Plan Nacional de Protección de Infraestruturas Críticas (PNPIC)**: Elaborado polo Parlamento e o Goberno, este plan é o marco estratéxico superior da protección das IICC en España. Define a política nacional neste ámbito e serve de base para o desenvolvemento normativo posterior, como a Lei 8/2011 (LPIC) e o Real Decreto 704/2011 (RDPIC).
- **Plans Sectoriais**: Son responsabilidade do Grupo de Traballo de Protección de Infraestruturas Críticas (GTPIC), que debe elaborar unha lista de operadores críticos por sector. O prazo establecido para a súa elaboración é de 12 meses desde a entrada en vigor do Real Decreto. Inclúen un análise sectorial de riscos.
- **Plans de Seguridade do Operador (PSO)**: Cada operador crítico designado debe identificar as súas infraestruturas críticas e redactar este plan estratéxico. O PSO define as políticas xerais de seguridade aplicables ao conxunto de instalacións ou sistemas xestionados polo operador. O prazo para a súa presentación é de 6 meses desde a súa designación oficial.
- **Plans de Protección Específicos (PPE)**: Por cada infraestrutura crítica identificada, o operador debe desenvolver un PPE que detalle as medidas concretas —tanto físicas como lóxicas— para garantir a súa seguridade integral. Estes plans deben elaborarse nun prazo de 4 meses tras a aprobación do correspondente PSO.
- **Plans de Apoio Operativo**: Son elaborados polas Forzas e Corpos de Seguridade do Estado (FCS) ou polas Delegacións do Goberno. Establecen a

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

resposta operativa ante posibles incidentes que afecten infraestruturas críticas. Deben estar listos nun prazo de 4 meses tras a aprobación do PPE correspondente.

Este modelo piramidal de planificación garante unha cobertura progresiva e coordinada da seguridade das infraestruturas críticas, combinando responsabilidades do sector público e privado. Todo plan debe estar coordinados coas autoridades competentes e contribúen a garantir a **resiliencia e continuidade dos servizos esenciais**, reforzando a seguridade tanto no eido físico como no dixital.

3.4 Estratexia e Plans Nacionais

A crecente dependencia dixital da sociedade e a economía converteu a ciberseguridade nunha prioridade estratéxica. En España, este compromiso artéllase a través dunha **Estratexia Nacional de Ciberseguridade (ENC)** que, desde 2019, serve de guía para protexer os intereses nacionais no ciberespazo.

3.4.1 Estratexia Nacional de Ciberseguridade 2019

A **ENC 2019** foi aprobada polo Consello de Seguridade Nacional o 12 de abril de 2019 e publicada por Orde PCI/487/2019, de 26 de abril. Actualiza a versión de 2013, e establece un **marco integral de actuación** para afrontar os riscos e ameazas no ciberespazo, tanto no sector público coma no privado. O seu propósito é reforzar a resiliencia do país fronte aos riscos emerxentes, fomentar a confianza dixital e asegurar a protección dos dereitos e liberdades da cidadanía [23][24].

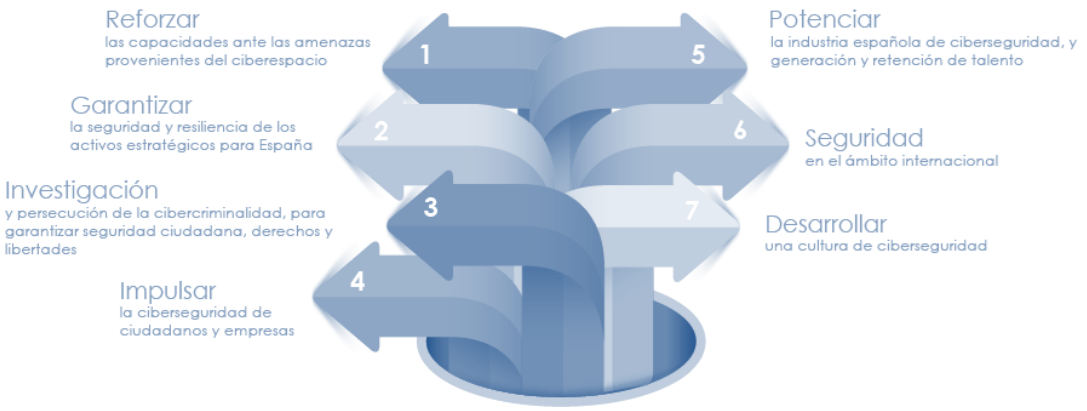
Ameazas con fins maliciosos no ciberespazo. Fonte: Departamento de Seguridade Nacional (2019)

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

A Estratexia estrutúrase arredor dun **obxectivo xeral**, cinco **obxectivos específicos** e sete **liñas de acción**, que se traducen en **65 medidas concretas**:

- **Obxectivo xeral:** Garantir a seguridade e resiliencia do ciberespazo nacional como parte esencial da seguridade nacional.
- **Obxectivos específicos:**
    1. Fortalecer a seguridade e resiliencia das redes e sistemas do sector público e dos servizos esenciais.
    2. Uso seguro e fiable do ciberespazo fronte a usos ilícitos ou maliciosos.
    3. Fomentar a ciberseguridade da cidadanía e do tecido empresarial.
    4. Promover a cultura da ciberseguridade e a formación de profesionais, potenciando capacidades humanas e tecnolóxicas.
    5. Reforzar a ciberseguridade no ámbito internacional e a participación activa en foros multilaterais.

As **sete liñas de actuación da ENC 2019**, recóllense na seguinte gráfica:



Liñas de actuación da ENC. Fonte: Foro Nacional de Ciberseguridade (2019)

3.4.2 Plan Nacional de Ciberseguridade

Para desenvolver e aplicar a Estratexia, o **Consello de Ministros aprobou o 29 de marzo de 2022 o Plan Nacional de Ciberseguridade (PNC)**. Este plan traduce os principios estratéxicos da ENC nun **conxunto de actuacións concretas**, con horizonte a tres anos, e está coordinado polo Departamento de Seguridade Nacional da Presidencia do Goberno [25].

O Plan contempla **147 actuacións estruturadas en cinco eixos estratéxicos**:

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

1. Desenvolvemento normativo e reforzo institucional.
2. Protección das capacidades tecnolóxicas nacionais.
3. Resposta eficaz ante ciberincidentes.
4. Impulso á ciberseguridade para a cidadanía, PEMEs e sectores estratéxicos.
5. Coordinación internacional e cooperación.

Inclúe ademais a creación do **Foro Nacional de Ciberseguridade** (derivada da cuarta liña de actuación da ENC), que promove o diálogo entre administracións, sector privado, academia e sociedade civil, e fomenta a implementación das medidas do Plan.

Medidas adicionais ao Plan Nacional de Ciberseguridade

Ao abeiro da **Orde Ministerial PJC/448/2025, de 6 de maio de 2025**, aprobouse unha ampliación das actuacións recollidas no PNC [26], co obxectivo de **adaptar a resposta do Estado aos novos riscos e ameazas no ciberespazo**. A motivación principal desta ampliación radica nunha serie de factores:

- **Incremento dos ciberataques** impulsados tanto por Estados como por grupos de ciberdelincuentes, con obxectivos como o roubo de datos, sabotaxes, espionaxe e disrupción de servizos críticos.
- **Transformación do escenario dixital**, que dilúe as fronteiras entre o ámbito civil e militar, e aumenta a superficie de exposición a ataques.
- **Emerxencia de tecnoloxías disruptivas** como a intelixencia artificial e a computación cuántica, que elevan o nivel de sofisticación dos ataques e obrigan a anticipar a transición a **criptografía postcuántica**.
- **Evolución do contexto xeopolítico**, con maior tensión en materia de defensa e seguridade do ciberespazo.
- **Obrigas normativas recentes**, tanto nacionais (ENS, ENS 5G, RD 7/2022 sobre redes 5G) como europeas (Directiva NIS 2, Regulamentos de Ciberresiliencia e Cibersolidariedade).

Estas actuacións buscan mellorar as capacidades nacionais en todo o ciclo de ciberseguridade e ciberdefensa: **conciencia situacional, prevención, detección, protección, resposta, recuperación e disuasión**, cun enfoque coordinado e sostido no tempo.

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

As medidas están aliñadas co **Plan de Recuperación, Transformación e Resiliencia**, especialmente coa súa Compoñente 11 (Modernización da Administración Xeral do Estado), e estarán sometidas ao marco do Real Decreto-lei 36/2020 relacionado.

3.5 Protección de datos persoais

3.5.1 Introdución

Nos procesos industriais, **cando se manexan datos persoais de empregados, clientes ou provedores**, resulta esencial ter en conta a lexislación vixente sobre protección de datos. Esta normativa garante dereitos fundamentais e impón obrigas específicas ás organización.

A continuación, analízanse os aspectos máis relevantes da lexislación española e europea en materia de **protección de datos persoais**.

A protección das persoas físicas en relación co tratamento de datos persoais é un **dereito fundamental**, recoñecido no **artigo 18.4 da Constitución Española**, no **artigo 8.1 da Carta dos Dereitos Fundamentais da Unión Europea** e no **artigo 16.1 do Tratado de Funcionamento da Unión Europea**.

Este dereito xurdiu a partir das **directrices da OCDE nos anos 80** e constitúe un dereito **independente do dereito á intimidade**, tanto persoal como familiar. En conxunto co dereito á privacidade e á inviolabilidade das comunicacións, a protección de datos proporciona á cidadanía **defensa fronte ao uso non autorizado da súa información persoal por terceiros**.

- ***Datos persoais*** *(definición da Comisión Europea no marco do* ***Regulamento Xeral de Protección de Datos – GDPR*** *[27]): Considérase dato persoal* ***calquera información relativa a unha persoa física viva identificada ou identificable****. Incluso informacións diversas que, combinadas, poidan levar á identificación dunha persoa concreta, tamén se consideran datos persoais.*

Os datos persoais que foron **anonimizados, cifrados ou seudonimizados**, pero que poidan utilizarse para **volver identificar a persoa**, seguen estando protexidos polo GDPR. Só cando a **anonimización sexa irreversible**, a información deixa de ser considerada dato persoal.

O **regulamento** é **tecnoloxicamente neutro**: protexe os datos con independencia da tecnoloxía utilizada, xa sexa tratamento automatizado ou manual, sempre que se

organicen segundo criterios predeterminados (por exemplo, alfabéticamente). **Tampouco importa o soporte**, se os datos están nun sistema informático, nunha gravación de videovixiancia ou en papel, seguirán sometidos aos requisitos.

A normativa legal non só prevén o uso indebido por parte de terceiros, senón que **outorga ao titular dos datos (interesado) o control sobre os mesmos**, a través de mecanismos como:

- A **necesidade de consentimento expreso** para o tratamento.
- O **deber de información** sobre o uso e destino dos datos.
- O exercicio dos **dereitos ARCOPOL**: acceso, rectificación, cancelación (supresión), oposición, portabilidade, esquecemento e limitación do tratamento.

A lexislación **europea é moito máis proteccionista** que a doutras rexións, como os **Estados Unidos**, onde non existe un marco normativo común senón leis sectoriais, sen autoridade de control nin esixencia de consentimento previo.

As normativas de referencia en España neste eido son:

- A **Constitución Española**
- A **Lei Orgánica 3/2018**, do 5 de decembro, de Protección de Datos Persoais e garantía dos dereitos dixitais (**LOPD-GDD**) [28]
- As **instrucións da AEPD** (Axencia Española de Protección de Datos) [29]

E a nivel europeo (de aplicación directa en España):

- O **Regulamento (UE) 2016/679**, coñecido como **Regulamento Xeral de Protección de Datos (RXPD)** ou **GDPR** nas súas siglas en inglés, **en vigor desde abril de 2016 e de aplicación obrigatoria desde maio de 2018**. Substitúe á antiga **Directiva 95/46/CE**, xa derrogada [30]. O seu obxectivo é **eliminar as asimetrías normativas** entre países membros e **armonizar os dereitos e obrigas en materia de protección de datos persoais**.

É relevante destacar o carácter disuasorio do réxime sancionador do GPDR para garantir o cumprimento efectivo da normativa, promovendo unha cultura de responsabilidade proactiva nas entidades que tratan datos persoais. Establécense sancións que poden acadar **ata 20 millóns de euros ou o 4 % da facturación anual global da entidade para incidentes moi graves**, prevalecendo o importe máis elevado.

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

3.5.2 Licitude do tratamento de datos persoais

O **interesado** é aquela **persoa física cuxa identidade pode derivarse directa ou indirectamente de datos que van ser obxecto de tratamento** (é dicir, **datos persoais**).

Segundo o **Regulamento Xeral de Protección de Datos (RXPD) e en consecuencia a LOPD-GDD**, só existen determinados escenarios nos que o **tratamento de datos persoais de interesados é lícito**:

1. **Seudonimización dos datos persoais**: cando os datos foron procesados de tal maneira que **non son atribuíbles directamente á persoa**, senón que requiren información adicional, protexida por medidas técnicas e organizativas adecuadas.

2. **Consentimento do interesado**: a **manifestación de vontade libre, específica, informada e inequívoca** por parte do interesado, expresada mediante unha declaración ou unha acción afirmativa clara, que indique a súa aceptación do tratamento de datos persoais para **un ou varios fins concretos**.

3. **Necesidade contractual**: cando o tratamento resulta necesario para a **execución dun contrato** no que o interesado é parte, ou para aplicar medidas precontractuais solicitadas por este.

4. **Obrigación legal**: cando o tratamento é necesario para **o cumprimento dunha obrigación legal aplicable ao responsable do tratamento**.

5. **Intereses vitais**: cando o tratamento é necesario para **protexer intereses vitais do interesado ou doutra persoa física**.

6. **Interese público ou función pública**: cando o tratamento é necesario para o **cumprimento dunha misión realizada en interese público** ou no exercicio de **poderes públicos conferidos ao responsable do tratamento**.

7. **Interese lexítimo**: cando o tratamento é necesario para **a satisfacción de intereses lexítimos do responsable do tratamento ou dun terceiro**, sempre que **non prevalezan os intereses ou dereitos fundamentais do interesado**, especialmente cando este sexa un neno. **Esta base legal non será aplicable ao tratamento realizado por autoridades públicas no exercicio das súas funcións.**

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

En relación coa **oferta directa a menores de servizos da sociedade da información**, establécese que:

- O tratamento de datos persoais dun neno será lícito cando este **teña polo menos 16 anos**.
- Se o neno **é menor de 16 anos**, o tratamento **só será lícito se o consentimento é outorgado ou autorizado polos titulares da patria potestade ou tutela**, e só na medida en que se outorgue dito consentimento.

Os Estados membros poden establecer por lei unha idade inferior, **sen que esta poida ser inferior aos 13 anos**. No caso de España, a **Lei Orgánica 3/2018 establece a idade mínima en 14 anos**.

3.5.3 Dereitos dos interesados

A continuación, resúmense a moi alto nivel os **dereitos ARCOPOL** (Acceso, Rectificación, Cancelación -supresión-, Oposición, Portabilidade, e Limitación do tratamento) segundo o Regulamento Xeral de Protección de Datos (GDPR) e a Lei Orgánica 3/2018 (LOPD-GDD):

- **Dereito de acceso**: permite ao interesado saber se os seus datos están a ser tratados, con que finalidade, por canto tempo, quen os recibe, de onde proceden, se existen decisións automatizadas e obter unha copia deles. Pode facilitarse mediante acceso remoto e directo. Pode limitarse por abusos (por exemplo, reiteración inxustificada en menos de 6 meses).
- **Dereito de rectificación**: dá dereito a corrixir datos inexactos ou incompletos. O interesado debe indicar cales son e achegar documentación xustificativa, se é o caso.
- **Dereito de supresión** ("dereito ao esquecemento"): permite eliminar datos cando xa non son necesarios, se retira o consentimento, o tratamento é ilícito, ou existen obrigas legais que así o requiran. Tamén se aplica a datos publicados, obrigando o responsable a solicitar a súa eliminación a terceiros. Non aplica cando prevalecen dereitos fundamentais, interese público, ou obrigas legais. En certos casos, establécese o deber de bloqueo previo á destrución definitiva.
- **Dereito de oposición**: o interesado pode opoñerse ao tratamento dos seus datos por razóns particulares, ou en calquera momento se se trata de mercadotecnia directa. Tamén pode opoñerse a elaboración de perfís, salvo

excepcións. O responsable debe deixar de tratar os datos salvo causa lexítima prevalente.

- **Dereito de portabilidade**: permite ao interesado recibir os seus datos persoais en formato estruturado e transmisible a outro responsable, cando o tratamento se basee no consentimento ou nun contrato, e se realice por medios automatizados.
- **Dereito de limitación do tratamento**: permite ao interesado solicitar a suspensión temporal do tratamento dos seus datos en certas condicións (por exemplo, cando impugna a súa exactitude, se opón á supresión ou mentres se avalía unha oposición). Os datos só poderán conservarse ou tratarse co consentimento ou para reclamacións.

Unha das novidades máis salientables da Lei 3/2018 é a **inclusión explícita do recoñecemento dos Dereitos Dixitais da cidadanía**, converténdose España no primeiro país europeo en facelo. Estes dereitos constitúen un conxunto de liberdades aplicables ao ámbito de Internet, co obxectivo de recoñecer e garantir un catálogo de dereitos dixitais conforme ao mandato establecido na Constitución.

A continuación resúmense os **17 dereitos dixitais recoñecidos pola LOPD-GDD**, agrupados segundo a súa natureza xeral ou específica do ámbito laboral:

Dereitos dixitais xerais

1. **Dereito á neutralidade de Internet**: acceso libre e non discriminatorio á rede por parte dos provedores de servizos.
2. **Dereito de acceso universal a Internet**: garantía de acceso a Internet para toda a poboación, sen discriminación e con atención á fenda de xénero, xeracional ou discapacidade.
3. **Dereito á seguridade dixital**: protección das comunicacións transmitidas e recibidas en liña.
4. **Dereito á educación dixital**: integración da competencia dixital no currículo, formación do profesorado e seguridade no uso das TIC.
5. **Protección dos menores en Internet**: uso equilibrado e seguro dos dispositivos e redes sociais, con intervención do Ministerio Fiscal se hai vulneracións.

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

6. **Dereito de rectificación en Internet**: posibilidade de corrixir información inexacta en redes e medios dixitais.
7. **Dereito á actualización de informacións**: solicitar a inclusión dun aviso visible que actualice datos publicados que xa non reflictan a realidade.
8. **Protección de datos dos menores**: esixencia de consentimento para a publicación de datos de menores en redes ou plataformas dixitais.
9. **Dereito ao esquecemento en buscadores**: eliminación de ligazóns nos resultados de buscas baseadas no nome, cando a información sexa inadecuada ou obsoleta.
10. **Dereito ao esquecemento en redes sociais**: supresión de datos publicados polos propios usuarios ou terceiros, especialmente se foron achegados durante a minoría de idade.
11. **Dereito á portabilidade en redes sociais**: posibilidade de transferir contidos facilitados a outro provedor designado.
12. **Dereito ao testamento dixital**: acceso e xestión dos contidos dixitais de persoas falecidas por parte de herdeiros ou persoas designadas.

Dereitos no ámbito laboral

13. **Dereito á desconexión dixital**: respecto ao tempo de descanso e conciliación, con políticas internas que regulen o uso razoable das tecnoloxías.
14. **Dereito á intimidade no uso de dispositivos dixitais**: protección da privacidade nos dispositivos facilitados polo empregador, con criterios claros de uso.
15. **Dereito á intimidade ante videovixiancia e gravación de son**: limitación do uso destes sistemas e prohibición en espazos de descanso ou íntimos.
16. **Dereito á intimidade ante sistemas de xeolocalización**: uso lexítimo condicionado á información previa sobre o sistema e os dereitos asociados.
17. **Dereitos dixitais na negociación colectiva**: os convenios colectivos poderán incluír garantías adicionais en materia de protección de datos e dereitos dixitais.

Estes dereitos supoñen un avance na protección dos cidadáns no entorno dixital, recoñecendo novas dimensións da intimidade, liberdade e seguridade na sociedade da información.

3.5.4 Obrigas para as entidades

As organizacións que tratan datos persoais, como son moitas do ámbito industrial como se mencionaba anteriormente, deben cumprir unha serie de obrigas legais establecidas tanto no **Regulamento Xeral de Protección de Datos (GDPR)** como na **Lei Orgánica 3/2018 (LOPD-GDD)**. A continuación, indícanse as máis relevantes.

1. Deber de información

As entidades deben informar ás persoas interesadas, no momento da recollida dos datos ou, se proceden doutros orixes, nun prazo razoable ou coa primeira comunicación, sobre a identidade e datos de contacto do responsable do tratamento, así como do delegado de protección de datos, se o houber.

Deben indicar tamén os fins do tratamento e a súa base legal, os destinatarios previstos dos datos e, no seu caso, a intención de transferilos a terceiros países, así como o prazo de conservación previsto. Tamén deberán informar sobre os dereitos que asisten ao interesado (acceso, rectificación, supresión, oposición, portabilidade, etc.), a posibilidade de retirar o consentimento en calquera momento e a existencia de elaboración de perfís ou decisións automatizadas, se é o caso.

A LOPD-GDD permite que esta información se proporcione por capas: unha **información básica inicial** e o resto mediante un medio accesible, como unha ligazón web.

2. Rexistro das actividades de tratamento

Tanto os responsables como os encargados do tratamento están obrigados a manter un rexistro documental que recolla os fins do tratamento, as categorías de interesados e de datos persoais, os destinatarios previstos (incluíndo transferencias internacionais, se as houber), os prazos de conservación e as medidas técnicas e organizativas implantadas.

Esta obriga non se aplica ás entidades con menos de 250 empregados, agás que o tratamento non sexa ocasional, implique riscos ou se manexen datos sensibles (categoría especial).

3. Cooperación coa autoridade de control

As entidades deben colaborar coa **Axencia Española de Protección de Datos (AEPD)** ou co organismo autonómico competente (non é o caso en Galicia) cando este lles solicite información ou actuacións no exercicio das súas funcións.

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

4. Protección de datos desde o deseño e por defecto

O responsable do tratamento debe aplicar medidas técnicas e organizativas axeitadas xa desde a concepción dos sistemas ou servizos, para integrar a protección de datos de forma efectiva e garantir que só se traten os datos persoais necesarios para cada finalidade específica. Por defecto, os datos non deben ser accesibles a persoas non autorizadas.

5. Avaliación de impacto e consulta previa

Nos casos nos que un tratamento poida supoñer un alto risco para os dereitos e liberdades das persoas, como a elaboración de perfís automatizados, tratamentos a gran escala de datos sensibles ou vixilancia sistemática en espazos públicos, é obrigatorio realizar unha **avaliación de impacto en protección de datos (AIPD, ou DPIA en inglés)**.

Se persisten os riscos tras esta avaliación, deberá realizarse unha consulta previa á autoridade de control (AEPD en Galicia), para verificar se é procedente o tratamento en cuestión.

Dada a importancia de esta obriga para as organización, dedicáselle un epígrafe específico a continuación.

6. Seguridade do tratamento

Deberanse aplicar medidas técnicas e organizativas para garantir a seguridade dos datos, tendo en conta os riscos potenciais. Estas medidas incluirán, entre outras, a seudonimización ou cifrado, a capacidade de garantir a confidencialidade, integridade e dispoñibilidade permanente dos sistemas, a posibilidade de restaurar datos tras incidentes e outras, así como a revisión periódica da eficacia destas medidas.

7. Xestión de brechas de seguridade

Unha **brecha de seguridade** defínese, segundo o Regulamento, como **calquera violación da seguridade que ocasione a destrución, perda ou alteración accidental ou ilícita de datos persoais transmitidos, conservados ou tratados doutra forma, ou a comunicación ou acceso non autorizados a tales datos.**

En caso de violación:

- **Notificación á autoridade de control** (AEPD ou autonómica correspondente):
    - En menos de 72 horas desde que se teña constancia.

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

- Incluíndo detalles da natureza da brecha, consecuencias e medidas correctoras.

- **Comunicación ás persoas afectadas**:
  - Sen dilación indebida se existe alto risco para os seus dereitos.
  - Agás se os datos estaban cifrados ou se adoptaron medidas suficientes para neutralizar o risco.

O responsable deberá documentar todas as brechas de seguridade, aínda que non sexa necesario notificar ás persoas afectadas.

3.5.5 AIPD

Nos **artigos 35 e 36 do RGPD** establécese a necesidade de conducir unha AIPD **(Avaliación de Impacto de Protección de Datos)** en certos supostos, antes de poder levar a cabo o tratamento de datos persoais. A continuación, inclúese unha pequena guía sobre como realizala.

O **Regulamento (UE) 2016/679** como dicíamos, incorpora unha nova obrigación para os responsables de tratamento: **avaliar o impacto das operacións de tratamento na protección dos datos persoais**, cando sexa probable que o tratamento supoña un **risco significativo para os dereitos e as liberdades das persoas**.

Podemos clasificar os riscos asociados a un tratamento en dous tipos: **os riscos inherentes ao tratamento** (como foi deseñado) e **os riscos asociados á seguridade dos datos**. O enfoque no risco que propón o Regulamento esixe **analizar os riscos** e, se son demasiado altos, **reducilos**.

O tratamento dos riscos pode levarse a cabo mediante diferentes metodoloxías, como a **ISO 31000** [31] ou **MAGERIT** [32]. A **APDCAT** (Axencia de Protección de datos catalana) propón unha metodoloxía alternativa para organizacións pequenas, que pode ser de interese pola súa simplicidade [33], aínda que lóxicamente a AEPD, ten as súas propias recomendacións [34].

Definición

A **AIPD** é un procedemento que busca **identificar e controlar os riscos** para os dereitos e as liberdades das persoas, asociados a un tratamento de datos.

Non nos limitamos aos dereitos recoñecidos polo Regulamento, senón a **calquera efecto que o tratamento poida ter sobre os dereitos e as liberdades fundamentais**

das persoas: dereito á liberdade de expresión, á liberdade de pensamento, á prohibición de sufrir discriminación, á liberdade de conciencia, á liberdade de relixión, etc.

Ao **identificar os riscos**, debemos considerar calquera **impacto** que o tratamento poida ter sobre as persoas (físico, económico, emocional, etc.). Algúns **impactos potenciais** son:

- Imposibilidade de acceder a servizos ou outras oportunidades
- Discriminación
- Roubo da identidade e outras fraudes
- Perdas económicas
- Danos á reputación
- Danos físicos
- Perda da confidencialidade
- Imposibilidade de exercer algún dereito

Os impactos poden materializarse por dúas razóns:

- **Mal deseño do tratamento de datos**. Para mitigar este risco, debemos establecer os controis para asegurar que o tratamento se realiza conforme ao RGPD.
- **Mala seguridade dos datos**. Para mitigalo, debe facerse unha análise do risco para a súa identificación, valoración, e o establecemento dos oportunos controis de seguridade.

Escenarios de aplicación

O RGPD, salvo tres supostos concretos indicados no artigo 35.3, limítase a indicar que debe levarse a cabo a AIPD cando o tratamento **poida conlevar un risco alto** para os dereitos e liberdades das persoas.

Segundo o **GT29** (grupo de traballo a este respecto a nivel comunitario), aínda que idealmente se realice sempre a AIPD, debería executarse cando se dean polo menos un dos seguintes supostos (en certos casos), ou **dous ou máis** (nese caso, habería que realizar a EIPD sempre):

- **Avaliación ou puntuación**, incluídas a elaboración de perfís e predicións
- **Toma de decisións automatizada** con efectos xurídicos ou que afecta de maneira similar e significativa á persoa física
- **Observación sistemática dunha área de acceso público**
- **Datos sensibles** (categorías especiais do artigo 9 do RXPD)
- **Tratamento de datos a gran escala**
- **Conxuntos de datos que se enlazaron ou combinaron**
- **Datos relacionados con persoas vulnerables**
- **Uso innovador de tecnoloxías**
- **Tratamento que en si mesmo impide o exercicio dun dereito ou o uso dun servizo ou contrato**

Observacións:

- Aínda que o artigo 35.4 do RXPD indica que a **AEPD** publicará unha lista de tratamentos para os que se debe realizar AIPD, a tendencia xeral é adoptar a proposta anterior.
- A **transferencia internacional de datos** era un suposto para realización da AIPD, que foi suprimido.
- Se **non aplica o RXPD**, ou ben a natureza, o alcance, o contexto e as finalidades do tratamento son moi similares a outro tratamento para o que xa se fixo unha AIPD, ou ben o tratamento ten unha **base xurídica** no dereito da UE ou dun estado membro, e xa se fixo unha EIPD no momento de adoptar esa base xurídica: nestes supostos, a AIPD **non é necesaria**.
- **Non levar a cabo a AIPD en casos de obrigación é unha conduta sancionable.**

Cando e quen a elabora

A **AIPD** hai que facela sempre **en canto sexa posible**. No caso de novos tratamentos de datos, deberá realizarse **sempre previamente** aos mesmos.

Para tratamentos xa en curso, debe realizarse en canto se teña constancia da existencia dun **risco grave** para os dereitos e liberdades das persoas. Tendo en conta que ao igual

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

que a seguridade é un proceso continuo, os **análises de riscos tamén o son**, polo que hai que reavaliar os tratamentos e as AIPD cando se produza un **cambio de contexto organizativo ou social**.

A **responsabilidade da execución** da Avaliación de Impacto é plenamente do **responsable do tratamento**, coa axuda do encargado se aplica, e o asesoramento do **Delegado de Protección de Datos**.

O responsable deberá **documentar** se solicitou a opinión dos interesados, e **xustificar** por que non o fixo, se corresponde. De calquera forma, o tratamento debe ter **base legal**, independentemente da opinión dos afectados.

Tamén pode recollerse a opinión de **axentes externos ou internos á entidade**, expertos independentes ou responsables de seguridade.

Contidos obrigatorios

A EIPD non é máis que un **informe**, que recolle uns **contidos mínimos segundo o RGPD**, que son:

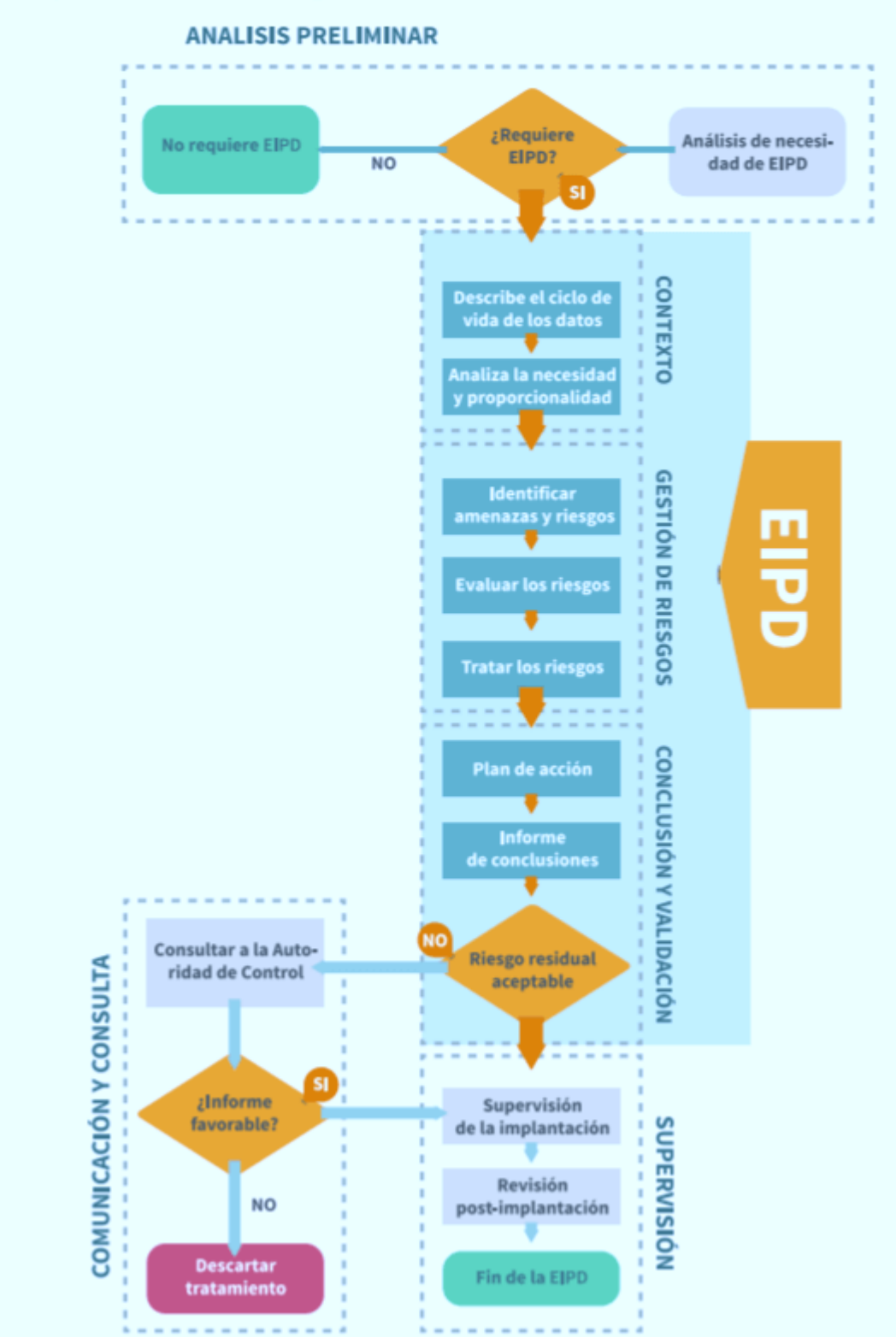
- **Descrición das operacións de tratamento de datos.**
- **Avaliación da necesidade e a proporcionalidade do tratamento.**
- **Avaliación do risco para os dereitos e liberdades das persoas.**
- **Medidas adoptadas para mitigar os riscos.**

Execución da AIPD

A elaboración práctica dunha AIPD excede o ámbito deste informe. Non é complexa, pois en esencia trátase de realizar una análise de riscos asociada ao tratamento de datos persoais. En calquera caso, aconséllase contar con asesoramento experto na materia.

O fluxo de actividades para a execución da AIPD, pode verse a continuación:

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



Etapas de elaboración da AIPD. Fonte: Axencia de Protección de datos de Cataluña (2022)

Hai que destacar que a **AEPD ten dispoñible no seu sitio web varios recursos en formas de guías e ferramentas de interese**, que facilitan tanto avaliacións de impacto, como comunicacións de brechas de datos, así como outros asuntos relativos a cifrado de información persoal, etc. [37][38].

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

4 Normativa europea

4.1 NIS2

A **Directiva (UE) 2022/2555**, coñecida como **NIS2** [39], é a nova normativa marco de ciberseguridade da Unión Europea, que substitúe e amplía o alcance da Directiva NIS orixinal. O seu obxectivo principal é **garantir un nivel elevado e común de seguridade das redes e sistemas de información** en toda a UE, respondendo á crecente sofisticación e frecuencia das ciberameazas e eliminando as disparidades entre Estados na aplicación da anterior directiva.

A NIS2 foi publicada no Diario Oficial da UE o *27 de decembro de 2022*, entrando en vigor o *16 de xaneiro de 2023* [40]. Os Estados membros dispoñían ata o *17 de outubro de 2024* para transpoñer a directiva ao seu ordenamento xurídico, data a partir da cal as medidas serán de aplicación obrigatoria. A data de elaboración de este informe, a directiva todavía non foi trasposta ao noso ordeamento xurídico (ver última subsección).

4.1.1 Alcance da directiva

A Directiva NIS2 **amplía notablemente o seu ámbito de aplicación** respecto da NIS1, abarcando un abano moito máis amplo de sectores e servizos críticos para a sociedade e a economía.

Inclúe tanto entidades *públicas* como *privadas* de sectores considerados de alta criticidade (no anexo I) e doutros sectores críticos (no anexo II), reflectindo a crecente dixitalización en todos os ámbitos. Deste modo, sectores como a **enerxía, transporte, banca, infraestruturas dos mercados financeiros, saúde, a subministración de auga potable,** entre outros, seguen estando cubertos como esenciais, e incorpóranse novos sectores e actividades non contemplados na normativa anterior: por exemplo, inclúense as **infraestruturas dixitais** (provedores de servizos de nube, DNS, redes de comunicación electrónicas, etc.), os **servizos de redes sociais**, as **administracións públicas** (central e rexional) ou a **xestión de residuos**, a **industria química** e a **alimentaria**, o sector espacial e a **investigación**, por mencionar algúns. Tamén se engaden os *provedores de servizos dixitais* que antes estaban limitados a tres categorías (mercados en liña, buscadores e cloud) incorporando agora, por exemplo, as plataformas de redes sociais como novo tipo de servizo cuberto. En consecuencia, a NIS2 **elimina a distinción previa entre "operadores de servizos esenciais" e**

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

"provedores de servizos dixitais" que establecía a NIS1, unificando todos estes axentes baixo o mesmo marco e requisitos de ciberseguridade.

Outro aspecto clave do alcance é que, con carácter xeral, a directiva **aplícase a todas as organizacións medianas e grandes** que operen nos sectores indicados (xa sexan públicas ou privadas). Isto significa que calquera empresa con máis de 50 empregados ou cuxo volume de negocio anual supere os 10 millóns de euros, pertencente a algún dos sectores críticos listados, debe considerarse dentro do ámbito de NIS2. Pola contra, as pequenas empresas e microempresas quedan exentas por defecto.

Porén, **existen excepcións importantes**: a directiva permite incluír tamén organizacións de menor tamaño cando desempeñen un papel crave para a sociedade ou a economía ou para certos servizos. En particular, independentemente do tamaño, poderían estar afectadas pequenas entidades que sexan as únicas provedoras dun servizo esencial nun Estado, aquelas cuxa interrupción poida ter un impacto significativo na *seguridade pública, orde público ou saúde pública*, ou que poidan xerar *riscos sistémicos* noutros sectores ou rexións [41].

Ademais, cada Estado membro ten a facultade de designar como *esencial* ou *importante* calquera outra entidade non incluída explicitamente nos anexos se considera que a súa interrupción tería consecuencias críticas a nivel nacional ou rexional. Deste xeito asegúrase que ningunha organización vital quede fóra da protección da directiva por mera cuestión de tamaño.

4.1.2 Entidades afectadas e categorización

A NIS2 establece dúas categorías de entidades afectadas, en función da criticidade do sector e do servizo que proporcionan, así como do seu tamaño e impacto potencial dun incidente:

- **Entidades esenciais**: Son aquelas pertencentes aos sectores de **alta criticidade** (anexo I da directiva). Inclúense aquí, por exemplo, as administracións públicas centrais e rexionais, e empresas de sectores como enerxía, transporte, finanzas (banca e infraestruturas de mercados financeiros), sanidade, subministración de auga potable, xestión de residuais, infraestruturas dixitais, espazo, etc. Pola súa relevancia, estas entidades considéranse vitais para o mantemento de actividades socioeconómicas críticas.
- **Entidades importantes**: Corresponden aos **outros sectores críticos** enumerados no anexo II. Son entidades de sectores non tan sensibles como os

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

anteriores, pero igualmente relevantes, e que superan tamén o limiar de mediana empresa. Exemplos deste grupo son os provedores de **servizos postais e de mensaxería**, empresas de **xestión de residuos**, certos fabricantes industriais (por exemplo, do sector químico, alimentario ou de produtos sanitarios e farmacéuticos), así como moitos **provedores de servizos TIC** (*IT managed services*, computación na nube, etc.) e incluso operadores do sector da **investigación** ou tecnolóxico [42].

Resumo entidades esenciais e importantes segundo a directiva NIS2. Fonte: Wallix (2025)

En termos prácticos, a directiva impón os *mesmos deberes de ciberseguridade* a entidades esenciais e importantes, diferenciándose ambos grupos principalmente no réxime de supervisión e nas consecuencias ante incumprimentos. As **entidades esenciais** estarán suxeitas a unha supervisión máis estrita e periódica por parte das autoridades competentes (enfoque *proactivo* e *reactivo*), mentres que as **entidades importantes** estarán sometidas a unha supervisión *reactiva*, é dicir, só se intervirá sobre elas a posteriori, cando a autoridade teña coñecemento ou evidencias dun posible incumprimento. Noutras palabras, as autoridades poderán inspeccionar proactivamente ás entidades esenciais para verificar que cumpren cos requisitos, mentres que nas importantes actuarán fundamentalmente **despois dun incidente grave ou denuncia**, pero non con control continuo. Esta distinción implica tamén que as sancións máis severas (como a inhabilitación de directivos, explicada máis adiante)

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

unicamente aplicarán ás entidades esenciais, reforzando a protección nos sectores de maior criticidade.

Cómpre salientar que, a diferenza da directiva precedente, agora son as propias organizacións quen deben **autoavaliar se entran no ámbito de NIS2 e, por tanto, identificarse como esenciais ou importantes** de acordo cos criterios establecidos. Xa non é preciso agardar a unha designación formal por parte da Administración, algo que baixo NIS1 xerara demoras e desigualdades na aplicación. Esta autoidentificación obrigatoria contribúe a unha implantación máis homoxénea e inmediata da normativa en toda a UE, reducindo a fragmentación que existía previamente.

4.1.3 Obrigas en materia de ciberseguridade

A Directiva NIS2 establece unha serie de **obrigas concretas de xestión de seguridade e reporte de incidentes** para todas as entidades que entren no seu ámbito, co fin último de reforzar a súa *ciber-resiliencia*. En liñas xerais, tódalas entidades esenciais e importantes deberán levar a cabo:

- **Xestión de riscos e medidas de seguridade:** Adoptar medidas técnicas, operativas e organizativas axeitadas e proporcionais para xestionar os riscos de ciberseguridade nas súas operacións. A directiva detalla unha listaxe mínima de controles que deben implementarse (descritos no capítulo IV da norma, artigo 21), que inclúen [43]:

  a) as **políticas de seguridade dos sistemas de información** e a **análise de riscos**;

  b) a **xestión de incidentes**;

  c) a **continuidade das actividades**, como a **xestión de copias de seguridade**, a **recuperación en caso de catástrofe** e a **xestión de crises**;

  d) a **seguridade da cadea de subministración**, incluídos os aspectos de seguridade relativos ás relacións entre cada entidade e os seus **provedores ou prestadores de servizos directos**;

  e) a **seguridade na adquisición, desenvolvemento e mantemento de sistemas de redes e de información**, incluída a **xestión e divulgación das vulnerabilidades**;

  f) as **políticas e procedementos para avaliar a eficacia** das medidas para a **xestión de riscos de ciberseguridade**;

g) as **prácticas básicas de ciberhixiene** e a **formación en ciberseguridade**;

h) as **políticas e procedementos relativos ao uso da criptografía** e, de ser o caso, do **cifrado**;

i) a **seguridade dos recursos humanos**, as **políticas de control de acceso** e a **xestión de activos**;

j) o uso de **solucións de autenticación multifactor ou de autenticación continua**, **comunicacións seguras** (voz, vídeo e texto), e **sistemas seguros de comunicacións de emerxencia** na entidade, cando proceda.

Todas estas medidas deben aplicarse seguindo un enfoque baseado no risco (é dicir, proporcionais á magnitude dos riscos identificados, ao tamaño da organización e ao potencial impacto dos incidentes) e tendo en conta o *estado da arte* tecnolóxico e as normas europeas/internacionais aplicables. En definitiva, búscase que as entidades integren a ciberseguridade nas súas prácticas corporativas de forma continua e preventiva, co compromiso explícito da alta dirección.

- **Notificación de incidentes:** Establecer procedementos para **notificar á autoridade competente ou ao CSIRT** correspondente aqueles incidentes de seguridade que teñan un impacto significativo na prestación dos seus servizos. A NIS2 fixa *prazos estritos* e un **procedemento escalonado de reporte**: a entidade debe emitir unha **alerta inicial** ou *alerta temperá* nun prazo máximo de **24 horas** desde que teña constancia do incidente, para informar de que ocorreu ou está ocorrendo un incidente grave. Posteriormente, nun período non superior a **72 horas**, deberá enviar unha **notificación complementaria** na que actualice a información con unha avaliación inicial máis detallada da gravidade e impacto do incidente. Finalmente, nun prazo máximo de **1 mes**, a entidade deberá remitir un **informe final** no que se inclúan todos os detalles sobre a incidencia, a súa causa raíz, o alcance dos danos causados e as medidas correctivas adoptadas. Este proceso en tres fases garante que as autoridades reciban información inmediata para reaccionar axiña, así como datos máis completos unha vez a entidade investigou en profundidade o sucedido.

  Cabe destacar que o incumprimento destes prazos de notificación, ou a ocultación deliberada de incidentes significativos, poderá levar aparelladas sancións importantes. Así mesmo, a directiva prevé que se informe ao público cando un incidente poida ter gran transcendencia (por exemplo, por afectar

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

usuarios ou cidadáns); neste sentido, as autoridades ou CSIRT poderán facer público o incidente, ou requirir á propia entidade que o comunique, se consideran que é de interese xeral.

- **Gobernanza e recursos:** Implicar activamente aos **órganos de goberno e dirección** da entidade na xestión da ciberseguridade. A alta dirección ten agora unha responsabilidade expresa de aprobar as políticas de xestión de riscos e supervisar a súa implantación efectiva. A Directiva NIS2 subliña que a ciberseguridade debe ser asumida como unha cuestión estratéxica, polo que os membros do órgano de administración deben ter un coñecemento adecuado nesta materia (por exemplo, recibindo formación específica) e garantindo que a organización destina os recursos necesarios para cumprir cos seus deberes de seguridade. De feito, a norma establece que os directivos poderán ser considerados **responsables persoalmente** no caso de incumprimentos graves das obrigas de ciberseguridade pola súa organización. Esta responsabilidade dos xestores tradúcese, entre outras medidas, na posibilidade de sancións específicas para eles (por exemplo, a *inhabilitación temporal* para exerceren cargos directivos nunha entidade esencial, en caso de infraccións moi graves).

  Por este motivo, moitas organizacións están a crear ou reforzar a figura do **Chief Information Security Officer (CISO)** ou responsable de seguridade da información, que asesore á dirección e lidere a implementación destas medidas, asegurando o cumprimento normativo.

- **Colaboración e reporte entre Estados:** A directiva tamén reforza a cooperación a nivel nacional e europeo en materia de ciberseguridade. As entidades deberán colaborar cos organismos competentes do seu Estado e, cando sexa pertinente, intercambiar información sobre ameazas e incidentes con outras partes interesadas. Estabelécense mecanismos para a **divulgación coordinada de vulnerabilidades** (vulnerability disclosure) entre as organizacións afectadas e os seus provedores ou clientes, de forma que os fallos de seguridade se comuniquen responsablemente e se corrixan canto antes.

  No plano supranacional, créase a **Rede europea de organizacións de xestión de crises cibernéticas (EU-CyCLONe)** para apoiar a coordinación da resposta a incidentes ou crises de ciberseguridade a gran escala que afecten múltiples países. Tamén se fortalece o papel do **Grupo de Cooperación NIS** da UE, que facilitará a toma de decisións conxuntas e o intercambio de información entre

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

Estados membros, por exemplo compartindo alertas temperás ou boas prácticas. En cada país, segue esixíndose ter unha estratexia nacional de ciberseguridade, un ou varios **autoridades competentes NIS** encargadas de supervisar o cumprimento nas entidades, puntos de contacto únicos de enlace internacional, e **equipos de resposta a incidentes CSIRT** nacionais que xestionen as notificacións e asistencia ás entidades. Con esta estrutura, preténdese unha resposta máis coordinada e efectiva ante ciberataques transfronteirizos ou de gran impacto, evitando a resposta illada de cada país.

En síntese, as obrigas da NIS2 abarcan desde a **prevención e preparación** (medidas de seguridade obrigatorias, avaliación de riscos, plans de continuidade, formación...) ata a **reacción e reporte** ante incidentes (notificación rápida e xestión coordinada), así como unha gobernanza clara da seguridade da información dentro das organizacións. O cumprimento destes requisitos será esixible legalmente unha vez se transpoña a directiva, e estará respaldado por un importante réxime sancionador en caso de incumprimento (algo que tamén acontece coa normativa de protección de datos, LOPD-GDD / GDPR).

4.1.4 Réxime de sancións e control do cumprimento

A Directiva NIS2 introduce un réxime de **supervisión e sancións** moito máis estrito que o da súa predecesora, co obxectivo de garantir que as entidades cumpran efectivamente as obrigas mencionadas. Cada Estado membro deberá designar autoridades competentes con facultades de inspección, auditoría e imposición de sancións administrativas. Estas autoridades poderán realizar controis de forma proactiva no caso das entidades esenciais, e investigarán posibles incumprimentos (por denuncia, incidentes notificados, etc.) no caso das importantes.

A directiva establece unha lista de poderes mínimos destas autoridades, que inclúe a posibilidade de emitir **apercibimentos e instrucións vinculantes** ás entidades para emendar deficiencias, ordear a adopción de medidas de seguridade ou a notificación de incidentes nun prazo determinado, requirir información e evidencias sobre o estado de seguridade, ou incluso **suspender temporalmente actividades** ou certificacións se se detectan incumprimentos graves. En casos extremos, e só para entidades esenciais, poderán imporse sancións como a mencionada prohibición temporal para determinados directivos responsables.

En canto ás multas económicas, a NIS2 esixe establecer **sancións administrativas proporcionadas e disuasorias**. Especificamente, fixa uns *umbrales mínimos*

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

harmonizados para as multas máximas que cada lexislación nacional debe contemplar: no caso das **entidades esenciais**, pódense impor multas de ata **10 millóns de euros ou o 2 % do volume de negocio anual mundial** da empresa (a cantidade que sexa maior); para as **entidades importantes**, as multas máximas serán de ata **7 millóns de euros ou o 1,4 % do volume de negocio anual**, escollendo igualmente a cifra de maior contía en cada caso.

Estas cifras representan os mínimos que os Estados deben aplicar, podendo cada país establecelas en valores superiores se así o decide ao transpoñer a directiva. Ademais das multas, poderán imponerse outras medidas sancionadoras como a publicación das infraccións (para dano reputacional), requirimentos de corrección auditados por terceiros, ou incluso a paralización temporal dalgunha actividade até que se resolvan as deficiencias de seguridade.

Este endurecemento das sancións vén acompañado dun claro chamamento á responsabilidade dos directivos, tal e como se indicou. A normativa deixa explícito que a **alta dirección responde en última instancia** do (incumprimento do) deber de ciberseguridade na súa organización. Así, se unha empresa incumpre gravemente as obrigas de xestión de riscos ou de notificación, os supervisores poderán aplicar sancións que afecten non só á entidade senón tamén aos seus xestores (por exemplo, multas persoais ou inhabilitacións). Todo isto pretende incitar ás empresas a que doten de medios suficientes á seguridade e fomenten unha cultura de cumprimento, sabendo que as consecuencias legais de non facelo poden ser severas.

4.1.5 Axudas ao cumprimento: guía CCN-STIC 892 (PCE-NIS2)

Para facilitar ás organizacións españolas a adaptación aos novos requisitos de NIS2, especialmente aquelas suxeitas ao Esquema Nacional de Seguridade (ENS), o Centro Criptolóxico Nacional publicará unha guía específica de axuda ao cumprimento. Trátase da guía **CCN-STIC 892**, que define o Perfil de Cumprimento Específico NIS2 (PCE-NIS2) para entidades no ámbito de aplicación da directiva [44]. Este perfil de cumprimento ofrecerá un **mapeo detallado entre os requisitos da NIS2 e os do ENS**, proporcionando directrices claras para a implementación das medidas da directiva no contexto do marco español de seguridade. Incluirá a correspondencia entre os controis de seguridade do ENS e as obrigas específicas de NIS2, axudando así ás entidades (sobre todo públicas, obrigadas a ENS) a establecer un só sistema de xestión de seguridade que satisfaga ambas normativas. Ademais, o CCN-CERT ofrece con esta guía un marco común de certificación ou auditoría de cumprimento, de forma que as organizacións poidan

demostrar que están aliñadas cos requerimentos europeos de ciberseguridade. A versión nova da guía CCN-STIC 892, substituirá a versión previa (que quedou obsoleta coa entrada de NIS2) e será de facto unha referencia práctica esencial para encarar o proceso de adecuación antes da entrada en vigor da nova lei en España.

4.1.6 Transposición da NIS2 en España

Dado que unha directiva europea non é de aplicación directa, cada país debe transpoñer NIS2 á súa lexislación interna. En España, este proceso de transposición está en marcha e materializarase nunha nova lei de ciberseguridade. O Goberno español aprobou a elaboración do **Anteproxecto de Lei de Coordinación e Gobernanza da Ciberseguridade** o 16 de xaneiro de 2025, co propósito de incorporar os requisitos da NIS2 ao marco xurídico nacional [45].

O texto do anteproxecto foi sometido a audiencia e información pública en xaneiro-febreiro de 2025, e actualmente atópase en trámite parlamentario para a súa aprobación definitiva. Esta lei, unha vez aprobada, substituirá e actualizará a normativa anterior (Real Decreto-lei 12/2018 e RD 43/2021, que traspuñan a NIS1) e establecerá as obrigas específicas en territorio español para as entidades esenciais e importantes definidas por NIS2.

O contido do anteproxecto de Lei segue de preto as disposicións da directiva europea. En liñas xerais, contempla o reforzo da **gobernanza da ciberseguridade** – atribuíndo claramente á alta dirección das entidades a responsabilidade no cumprimento –; establece as **medidas de seguridade** que deben implantarse para a xestión dos riscos (aliñadas coas mencionadas na sección anterior); require designar un **responsable de seguridade da información** (figura equivalente ao CISO); e define os **prazos e procedementos de notificación de incidentes** conforme á NIS2. Así mesmo, a futura lei española detallará o modelo de supervisión e o catálogo de sancións aplicables en caso de incumprimento, seguindo os baremos mínimos (multas de ata 10 millóns/2% do negocio) impostos pola directiva.

É importante notar que España, ao igual que a maioría de países da UE, **non chegou a tempo de transpoñer** a NIS2 antes da data límite de outubro de 2024. Isto motivou que a Comisión Europea iniciase procedementos de infracción en 2024 contra 23 Estados membros (entre eles España) pola demora na incorporación da normativa. En resposta, estanse a acelerar os traballos lexislativos para aprobar a lei o antes posible.

En canto a transposición non se finaliza, as obrigas de NIS2 aínda **non son exixibles directamente** ás entidades españolas (a directiva por si soa carece de efecto directo, a

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

diferenza dun regulamento). Porén, recoméndase encarecidamente que as organizacións non agarden pola lei nacional e vaian **adiantando os deberes de adaptación** ás novas esixencias.

A NIS2 xa marca o estándar europeo de ciberseguridade desde xaneiro de 2023, e as empresas deben aproveitar este tempo para fortalecer as súas capacidades: **identificar se están afectadas, avaliar o seu nivel de madurez en cada control requirido, e implementar melloras nos seus plans de seguridade**. As organizacións que operan en sectores críticos deben prepararse para este novo escenario no que a ciberseguridade será non só unha obrigación legal, senón un elemento central da súa continuidade de negocio e confianza do mercado.

4.2 CRA

** Esta normativa afecta tanxencialmente aos dispositivos industriais, ó ser relativa a ciberseguridade de productos. Inclúese de maneira somera como referencia, aínda que se traballará con máis profundidade dende outro ámbito do Laboratorio de Ciberseguridade Industrial da AMTEGA.*

O **15 de setembro de 2022**, a Unión Europea publicou unha **proposta lexislativa para mellorar o nivel de ciberseguridade dos dispositivos IoT** (Internet das Cousas) e dos produtos electrónicos en xeral. A denominada **Lei de Ciberresiliencia (Cyber Resilience Act, CRA)** é un regulamento que foi finalmente **aprobado o 12 de marzo de 2024**, marcando un fito ao establecer **requisitos obrigatorios de ciberseguridade para produtos con elementos dixitais**, tanto de hardware como de software, co obxectivo de reforzar a seguridade do mercado interior europeo [46].

Segundo a presentación oficial da CRA, esta iniciativa:

- **Reforza as normas de ciberseguridade** para garantir produtos máis seguros.
- Responde á crecente exposición de produtos dixitais a ciberataques, que causaron **custos globais estimados de 5,5 billóns de euros en 2021**.

Detectáronse **dúas problemáticas principais**: por una banda, un **baixo nivel de ciberseguridade** xeral dos produtos, con vulnerabilidades comúns e ausencia ou ineficiencia das actualizacións de seguridade. Por outro, **falta de transparencia e información clara para os usuarios**, que dificulta a elección e uso seguro de produtos con propiedades de seguridade adecuadas.

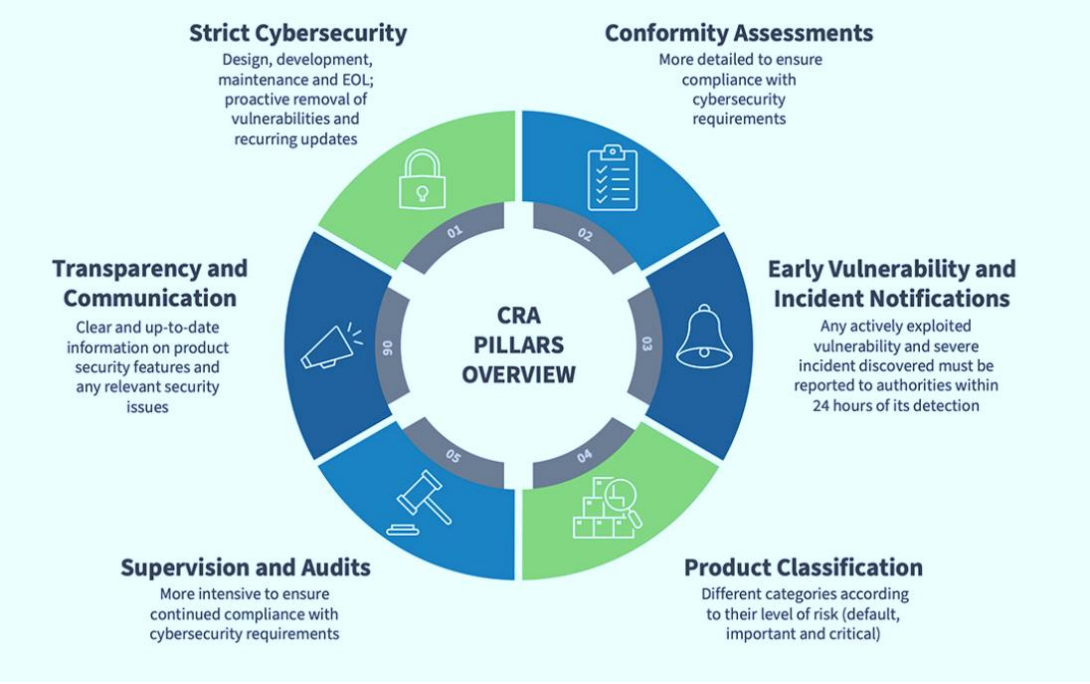
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

A maioría dos produtos con elementos dixitais non estaban cubertos por lexislación europea en materia de ciberseguridade, especialmente o **software non embebido**, pese a ser un dos obxectivos principais de ataques. Os **obxectivos principais da CRA**, son:

1. **Crear condicións para o desenvolvemento de produtos seguros**, con menos vulnerabilidades e un compromiso activo por parte dos fabricantes durante todo o ciclo de vida do produto.
2. **Permitir aos usuarios valorar a ciberseguridade** ao elixir e empregar produtos con elementos dixitais.

De xeito más específico, o que se busca co regulamento é:

1. Garantir que os fabricantes **melloran a seguridade desde o deseño e ao longo de todo o ciclo de vida** dos produtos.
2. Establecer un **marco normativo coherente** que facilite o cumprimento legal por parte de fabricantes de hardware e software.
3. **Mellorar a transparencia das propiedades de seguridade** dos produtos.
4. Permitir que **consumidores e empresas utilicen produtos dixitais con seguridade**.



Pilares do regulamento CRA de ciberseguridade. Fonte: Digi International (2025)

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

Os fabricantes estarán obrigados a **avaliar os riscos de ciberseguridade antes de poñer o produto no mercado**, mantendo **rexistros detallados da fabricación e dos compoñentes durante polo menos dez anos**. Será obrigatorio **notificar vulnerabilidades explotadas ou incidentes graves á ENISA e aos CERT nacionais nun prazo máximo de 24 horas** desde que se teña coñecemento, e deberán **designar representantes autorizados como puntos de contacto** coas autoridades.

Así mesmo, os produtos deberán contar cunha **certificación de seguridade**, que poderá ser obtida mediante mecanismos internos ou externos, dependendo do nivel de risco do servizo. Os produtos críticos ou de alta importancia estarán sometidos a procedementos de avaliación da conformidade máis esixentes que aqueles de menor risco.

A CRA introduce por primeira vez un enfoque específico para a **seguridade da cadea de subministración**, obrigando os fabricantes a considerar a ciberseguridade non só como un asunto interno, senón tamén nas relacións cos provedores de servizos e compoñentes. O cumprimento da CRA converterase así nun criterio clave á hora de establecer relacións comerciais no ecosistema dixital europeo.

Este regulamento supón un cambio de paradigma ao establecer **obrigas específicas e vinculantes** para fabricantes, importadores e distribuidores. A diferenza doutras regulacións que ofrecían directrices non obrigatorias, esta lexislación europea aplica medidas de obrigado cumprimento, orientadas á prevención, transparencia e resposta ante incidentes, consolidándose como o marco máis ambicioso ata a data en ciberseguridade de produtos.

Calendario de aplicación da CRA

Aínda que a aplicación plena da CRA non se producirá ata **decembro de 2027**, existen disposicións que entrarán en vigor **antes**, segundo o seguinte calendario:

- A partir do **11 de xuño de 2026** serán aplicables as disposicións relativas á **notificación dos organismos de avaliación da conformidade**.
- A partir do **11 de setembro de 2026** aplicaranse as **obrigas de información dos fabricantes**.
- A partir do **11 de decembro de 2027** será de **plena aplicación o conxunto do regulamento**.

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

Este calendario responde á necesidade de **conceder aos fabricantes un prazo de ata 36 meses** dende a entrada en vigor da norma para adaptar os seus produtos e procesos ao seu cumprimento.

4.3 CER

A **normativa CER** (Critical Entities Resilience) establece un novo marco legal europeo para **mellorar a protección e resiliencia das entidades críticas** fronte a calquera tipo de ameaza, sexa de natureza **física, natural, tecnolóxica, sanitaria ou híbrida**.

A base legal da CER é a **Directiva (UE) 2022/2557**, do Parlamento Europeo e do Consello, publicada o **27 de decembro de 2022** [47]. Substitúe a anterior Directiva 2008/114/CE, modernizando o enfoque para adaptarse ás novas ameazas complexas e interdependentes. É de interese visitar o sitio web con información asociada [48].

Esta directiva busca **reforzar a seguridade do mercado interior da UE** garantindo a continuidade dos servizos esenciais ante calquera interrupción grave. En España, está en tramitación o **Anteproxecto de Lei de protección e resiliencia de entidades críticas** dende o 27 de Maio de 2025 [49], que desenvolverá esta normativa a nivel estatal.

Ámbito de aplicación

A normativa CER aplícase ás entidades públicas e privadas que prestan **servizos esenciais para o mantemento de funcións sociais vitais, actividades económicas, saúde pública ou seguridade**, en sectores definidos no **Anexo da Directiva mencionada**.

Ademais, os Estados membros poden **designar entidades adicionais como críticas**, mesmo fóra destes sectores, se consideran que a súa interrupción pode ter consecuencias significativas. No caso da transposición española, **inclúese expresamente o sector da seguridade privada** como ámbito de aplicación da norma.

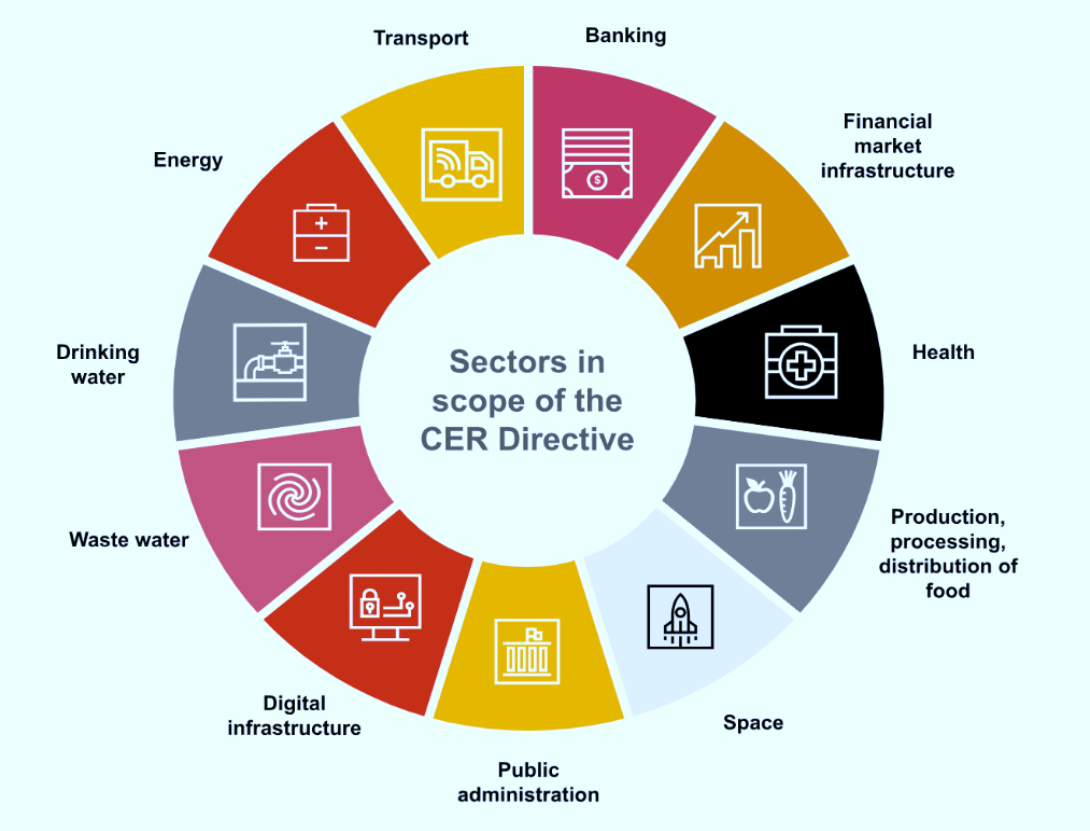
O anteproxecto de lei española especifica:

1. Esta lei é aplicable ás entidades críticas situadas no territorio nacional, vinculadas aos sectores e subsectores definidos no anexo.
2. Quedan excluídas:

a) As entidades críticas dependentes do Ministerio de Defensa, das Forzas e Corpos de Seguridade do Estado e dos corpos de policía autonómica con competencias recoñecidas para protección e orde pública.

b) As materias reguladas pola lei de transposición da Directiva (UE) 2022/2555 (NIS2), sen prexuízo do disposto na disposición adicional cuarta.

c) Non se aplicará tampouco cando outras normas sectoriais impoñan obrigas equivalentes ás previstas nesta lei, recoñecidas na normativa ou mediante resolución da Secretaría de Estado de Seguridade.



Ámbito de aplicación orixinal de directiva CER. Fonte: Price Waterhouse Cooper (2025)

Na práctica, algúns dos sectores afectados inclúen **enerxía, transporte, auga, sanidade, hidróxeno, augas residuais, sistemas urbanos de climatización e seguridade privada.**

Obrigas e medidas

A CER articúlase sobre tres eixos fundamentais:

a) Medidas estratéxicas: A nivel institucional, establece a elaboración da **Estratexia Nacional de Resiliencia**, a cargo da Secretaría de Estado de Seguridade e aprobada polo

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

Consello de Seguridade Nacional, así como unha **avaliación nacional de riscos** cada catro anos, identificando ameazas naturais, tecnolóxicas e humanas. O **CNPIC** é substituído polo novo **Centro Nacional para a Protección e Resiliencia de Entidades Críticas (CNPREC)**.

b) Medidas de resiliencia para entidades críticas: As entidades identificadas deberán **avaliar periodicamente os riscos**, incluíndo ameazas naturais, tecnolóxicas, híbridas ou de ciberseguridade, e implementar **medidas organizativas, técnicas e físicas** para mitigalos. Están obrigadas a desenvolver **Plans de Resiliencia** con medidas de prevención, resposta e recuperación no prazo de seis meses tras seren designadas. Así mesmo, deberán designar un **responsable de seguridade e resiliencia**, que actuará como interlocutor coas autoridades competentes.

Os **Plans de Resiliencia** deberán incluír:

1. Medidas para **evitar incidentes**, considerando a redución de riscos e adaptación ao cambio climático.
2. Medidas para **protexer fisicamente as infraestruturas**, como barreiras, sistemas de vixilancia e controis de acceso.
3. Procedementos para **responder e resistir aos incidentes**, con protocolos de alerta e xestión de crise.
4. Accións para **recuperar a prestación do servizo esencial**, incluíndo continuidade operativa e cadeas de subministración alternativas.
5. Medidas para **protexer o persoal**, definindo funcións esenciais, accesos, verificación de antecedentes e formación. Isto inclúe tamén persoal de provedores externos.
6. Programas de **concienciación e formación**, mediante cursos, exercicios e materiais informativos.

c) Comunicación de incidentes: As entidades críticas están obrigadas a **notificar á autoridade competente calquera incidente que poida afectar significativamente á prestación dos seus servizos** no prazo de 24 horas desde que dispoñan de indicios razoables. Ademais, deben enviar un informe máis completo tras a resolución ou contención do incidente, **como moi tarde nun prazo dun mes**.

d) Medidas de control e supervisión: Inclúese a **comprobación de antecedentes** do persoal que desempeñe funcións sensibles, mediante verificación de identidade, historial penal e datos de intelixencia.

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

Estas obrigas buscan **reforzar a preparación e capacidade de resposta** fronte a ameazas sistémicas e evitar disrupcións graves que afecten a seguridade ou o benestar da poboación.

As **sancións por incumprimento** poden alcanzar os **10 millóns de euros**, especialmente nos casos de non notificar incidentes ou non adoptar medidas esixidas pola normativa.

Período de implantación

A Directiva CER entrou en vigor o **16 de xaneiro de 2023** e os Estados membros, incluída España, debían **traspoñela ao seu ordenamento xurídico nacional antes do 17 de outubro de 2024**, coincidindo co prazo establecido para a transposición da Directiva NIS2.

Este aliñamento estratéxico entre NIS2 e CER persegue garantir unha **implementación coordinada e coherente** da resiliencia ciberfísica en Europa.

5 Marcos e estándares internacionais

Antes de abordar o contido específico de cada marco ou estándar dos que se describen a continuación, cómpre destacar que, **aínda que non todos foron deseñados exclusivamente para o ámbito industrial**, estas referencias normativas **teñen un elevado grao de aplicación e utilidade en entornos ICS/OT**, especialmente nos procesos de gobernanza, xestión do risco e seguridade técnica.

O seu carácter internacional e o seu recoñecemento no sector convérteas en **guías fundamentais para establecer prácticas robustas de ciberseguridade industrial**, adaptables segundo as necesidades e características de cada organización. Partiremos de marcos xerais, y remataremos con dous específicos de ICS/OT.

5.1 ISO/IEC 27001

5.1.1 Introdución

Un **Sistema de Xestión da Seguridade da Información (SXSI)** é un conxunto de políticas, procedementos, estruturas organizativas, procesos e recursos que unha organización establece para **protexer a confidencialidade, integridade e dispoñibilidade da súa información**.

A súa finalidade é garantir que os **datos sensibles ou críticos** se xestionan de forma segura, protexendo tanto os activos tecnolóxicos como os humanos fronte a ameazas internas ou externas. Ademais, permite demostrar **cumprimento normativo**, mellorar a confianza dos clientes e partes interesadas, e reducir o risco de incidentes de seguridade. Un SXSI adoita implantarse segundo os requisitos da norma internacional **ISO/IEC 27001**.

Trátase dun **estándar internacional para a Seguridade da Información**, posiblemente o máis coñecido, que **especifica os requisitos para definir, implantar, manter e mellorar un SXSI** (ISMS, Information Security Management System, en inglés).

É a **primeira norma da serie ISO 27000**, orixinada a partir da **ISO BS7799-2:2002**, desenvolvida pola **BSI (British Standards Institution)**. É a **norma principal da familia**, que define os **requisitos do ISMS e o seu proceso de auditoría**. Está composta por unha serie de preceptos recoñecidos internacionalmente nas prácticas de

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

seguridade da información, aplicando unha **metodoloxía de catro fases (PDCA: Plan-Do-Check-Act)**.

A **ISO 27001 é certificable**, e define o SGSI: estrutura, procesos, documentación, auditoría... A versión actual da norma **ISO/IEC 27001 é a de 2022** [50]. O resto das normas da serie, son **de apoio**.

Non é posible obter certificación da ISO 27002 [51], xa que esta se limita a recoller unha serie de **controles de seguridade como boas prácticas**, sen ser unha norma de xestión. Estes **controles son idénticos aos do anexo A da ISO 27001**, tanto en denominación como en alcance.

A **ISO 27001 está deseñada como unha aproximación concreta á creación dunha estrutura segura de xestión da información** dentro dunha organización. **Todos os controis da ISO 27002 e do anexo A deben identificarse nun documento chamado SOA (Statement of Applicability – Declaración de Aplicabilidade)**, tanto se aplican coma se non. A correcta definición e implantación destes controis **verifícase mediante auditorías**.

O modelo de implantación ten en conta os planos **tecnolóxico, organizativo, legal e humano**:

- No **aspecto humano**, considéranse factores como a **formación, os roles e responsabilidades, o control e a supervisión, e a concienciación**.
- No **ámbito técnico**: protocolos, redes, criptografía, estandarización, desenvolvemento seguro...
- En relación coa **lexislación**: cumprimento de leis, regulamentos e normativas aplicables.
- E no **plano organizativo**, establécese unha **xerarquía documental** que inclúe políticas, normas, procesos, procedementos, plans de continxencia e relacións con terceiros.

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

Clausulado da norma ISO 27001:2022. Fonte: Spectral, Check Point (2025)

O **SXSI forma parte do sistema de xestión global dunha organización**, e inclúe políticas, estrutura organizativa, procesos, recursos e obxectivos para garantir a seguridade da información. A **ISO 27001 guía na implantación, seguimento, mellora e auditoría do sistema**.

Pódese concluír que esta norma recolle os **requisitos comúns para un SXSI aplicable a calquera industria**, e pode **complementarse con outras como a ISO 22301 de Continuidade de Negocio** [52]. Constitúe un **marco estándar para desenvolver normas de seguridade sectoriais** e permite implementar un método de xestión **eficaz, auditable e certificable** dos sistemas de información.

5.1.2 Compoñentes do SXSI

A estrutura dun **SXSI** (Sistema de Xestión da Seguridade da Información) baixo a norma **ISO 27001** consta dos seguintes compoñentes:

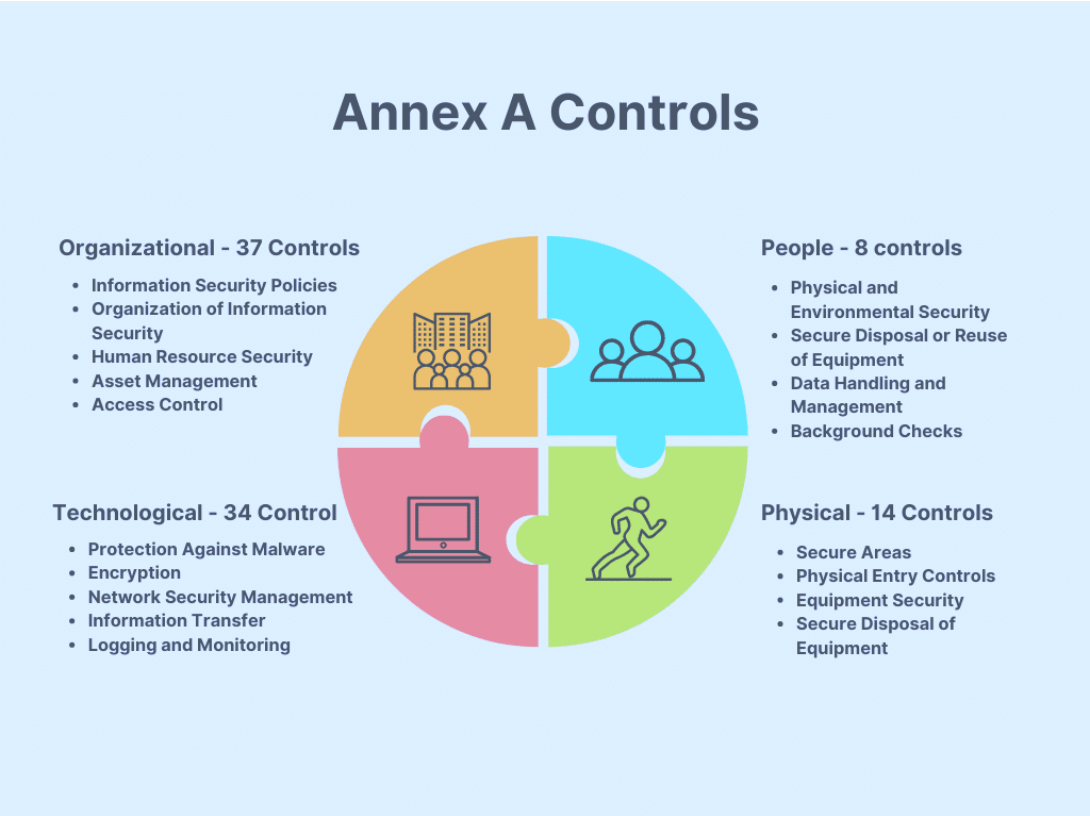
1. **Alcance:** Tal e como se indica no capítulo 4 da norma, débese definir que parte da organización quedará protexida polo SXSI, en canto a características da organización, localizacións, activos de información e sistemas, e procesos ou actividades. Isto é fundamental para delimitar o seu ámbito de aplicación. É unha decisión de xestión, e non implica necesariamente que toda a organización estea certificada.

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

2. **Organización:** Avalíanse os aspectos organizativos da seguridade da información, tanto internos como en relación con clientes e provedores. Roles clave:
    - **Dirección de seguridade:** Ten responsabilidades clave como a validación de políticas, aprobación de riscos residuais, demostración de compromiso, revisión periódica do SXSI e aprobación dos plans asociados.
    - **Responsables do SXSI:** Encárganse da xestión de usuarios e permisos, dispoñibilidade dos sistemas, definición de novos requirimentos e coordinación da seguridade.
    - **Propietario dos activos:** Define accesos, normativa aplicable, reporta incidentes e supervisa os controis implementados.
    - **Persoal:** Tanto interno como externo, debe coñecer e seguir as normas e comunicar incidentes en tempo e forma.
3. **Deseño de controis de seguridade:** Os controis son medidas para previr, deter ou mitigar ameazas. Distinguiremos entre:
    - **Controis físicos:** tornos, cámaras, portas, extintores...
    - **Controis lóxicos:** firewalls, IDS, antimalware, contrasinais...
    - **Controis organizativos**: políticas, procedementos, etc.
4. **Obxectivos de control:** Na versión 2013 da norma, agrupábanse en 14 dominios (a5 a a18). A versión 2022 presenta 4 categorías (organizacionais, de persoas, físicos e tecnolóxicos), con 93 controis. As diferencias son:
    - **11 novos controis:** intelixencia sobre ameazas, seguridade en servizos na nube, continuidade TIC, supervisión física, hardening, eliminación de datos, enmascaramento, prevención de fugas, supervisión, filtrado web, codificación segura.
    - Engádese un propósito e atributos relacionados con ciberseguridade a cada control.

    O anexo A ofrece unha guía de uso dos atributos, e o anexo B un mapeo cos controis de 2013 vs 2022.

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



Controis ISO 27001:2022. Fonte: Spectral, Check Point (2025)

5. **Declaración de aplicabilidade (SOA, *Statement of Applicability*):** Documento clave que reflicte cales controis se aplican, con estrutura tabular:
    - Nome do control
    - Aplicable (SI/NON)
    - Xustificación
    - Obxectivo
    - Descrición da implementación
    - Estado actual

    É o nexo entre avaliación, tratamento e implantación da seguridade.

6. **Corpo normativo:** A documentación de goberno estrutúrase como unha pirámide:
    - **Manual de seguridade:** Inclúe política de seguridade, alcance, avaliación de riscos (normalmente non pública), e o SOA.

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

- **Política de seguridade:** Documento estratéxico validado pola dirección, revisado periodicamente, de dominio público.
- **Procesos:** Normas internas obrigatorias que indican como actuar, clasificables como primarios, de guía ou de apoio.
- **Procedementos:** Desenvolven aspectos concretos das políticas, asociados a plataformas e sistemas.
- **Instrucións técnicas:** Guías detalladas para tarefas específicas.
- **Rexistros (logs):** Soporte para monitorización e control, recollen accións, activos, usuarios, datas, etc. e revísanse de forma periódica.

5.1.3 Documentación

A documentación que debe estar sempre dispoñible para ser auditada relativa ao SXSI de acordo coa norma ISO 27001, nunha organización cun alcance ambicioso de implantación, é:

- O **manual de seguridade** (alcance do SXSI, políticas e obxectivos de seguridade da información, metodoloxía de avaliación e tratamento de riscos, declaracións de aplicabilidade - SOA -, plan de tratamento do risco, informe de avaliación e tratamento do risco).
- **Definición de funcións e responsabilidades de seguridade**.
- **Inventario de activos** e uso aceptable dos mesmos.
- **Procedementos operativos para xestión de TI**.
- **Principios de enxeñaría para sistemas seguros**.
- **Políticas de seguridade para provedores**.
- **Procedementos de xestión de incidentes**.
- **Procedementos para a continuidade do negocio**.
- **Requirimentos legais, normativos e contractuais**.
- **Rexistros de capacitación, habilidades, experiencia e cualificacións**.
- **Resultados de supervisión e medición**.
- **Programa de auditoría interna**, resultados de auditorías internas.

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

- **Resultados de revisión por parte da Dirección**.
- **Resultados de accións correctivas**.
- **Rexistros sobre actividades de usuarios**.
- **Excepcións e eventos de seguridade**.

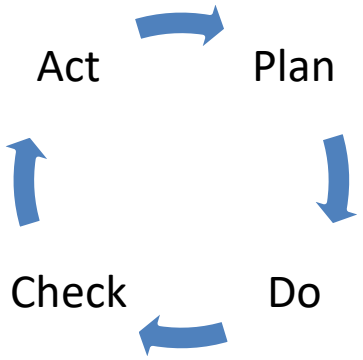
Os documentos non obrigatorios de uso habitual, poden incluír:

- Procedementos para control de documentos.
- Controis para xestión de rexistros.
- Procedementos para auditorías internas.
- Procedementos para medidas correctivas.
- Políticas **BYOD** (Bring Your Own Device).
- Políticas de **dispositivos móbiles e teletraballo**.
- Políticas de **clasificación da información**.
- Políticas de **claves criptográficas**.
- Políticas de **eliminación e destrución**.
- Procedementos de **traballo en áreas seguras**.
- Políticas de **pantalla e escritorio limpo**.
- Políticas de **xestión de cambios**.
- Política de **copias de seguridade (backups)**.
- Políticas de **transferencia de información**.
- **Análise de impacto de negocio**.
- **Plans de probas e verificación**.
- **Plans de mantemento e revisión**.

5.1.4 Certificación

A **certificación dun SXSI** é o proceso mediante o cal unha entidade de certificación externa, independente e acreditada, audita o sistema co obxectivo de determinar a súa conformidade con **ISO/IEC 27001**, o seu grao de implantación real e a súa eficacia e, no caso positivo, emite o correspondente certificado.

A norma ISO/IEC 27001 como se indicou é **certificable** e implántase nun modelo iterativo de **mellora continua** en catro fases (**Plan-Do-Check-Act, PDCA**):



Ciclo de mellora continua PDCA. Fonte: elaboración propia (2026)

- **PLAN**: Planificación, deseño inicial da primeira ou seguinte iteración do SXSI. Inclúe a xestión do risco.
- **DO**: Implantación e execución. As actividades definidas póñense en práctica.
- **CHECK**: Seguimento e revisión, avaliación da madurez do SXSI.
- **ACT**: Mellora. Co feedback da avaliación previa e o recollido dos interesados, propóñense cambios incrementais sobre o SXSI, que se inclúen na seguinte planificación dun novo ciclo PDCA.

Cada ciclo PDCA adoita desenvolverse ao longo de **6 a 12 meses**. En organizacións grandes ou entornos complexos, se o alcance da certificación abrangue toda a compañía, a implantación do SXSI conforme á norma pode **implicar varios anos de traballo**.

As **partes interesadas** achegarán as súas expectativas, necesidades en canto á seguridade da información e os requirimentos que impoñan aos sistemas da información (que deben estar aliñados cos obxectivos de negocio e o marco normativo).

Na fase de seguimento e revisión realízanse **auditorías**, se o nivel de madurez é suficiente. Estas poden ser:

- **Internas/externas**: Son obrigatorias segundo ISO 27001. Deben ser realizadas por persoal externo ou con independencia xerárquica da área auditada. O informe resultante é máis simplificado que o de certificación. Compártense cos directivos para avaliar e mellorar o sistema (fases CHECK e ACT).
- **De certificación**: Só poden ser realizadas por entidades recoñecidas conforme á **ISO 27006** (como **AENOR**, **Applus+** ou **TÜV Rheinland**). Estas acreditan que

o SXSI se axusta aos requisitos da norma. A certificación é válida por **3 anos**, con auditorías anuais:

- **Ano 1**: Avaliación completa do SXSI (xestión + todos os controis).
- **Ano 2**: Avaliación parcial (parte da xestión + parte dos controis).
- **Ano 3**: Avaliación parcial (resto da xestión + outro subconxunto de controis).
- **Ano 4**: Recertificación completa (xestión + 100% de controis).

As primeiras auditorías adoitan ser internas/externas. Contrátanse antes da certificación e, unha vez implantado o SXSI, poden asumir as revisións persoas internas para **reducir custos**.

Entre as **vantaxes asociadas á certificación**, atópanse as seguintes:

- **Mellora a reputación** da organización demostrando o compromiso coa seguridade da información ante os clientes.
- **Proba o apoio da dirección** á seguridade da información.
- **Evidencia o cumprimento de leis e regulamentos** aplicables.
- Acredita o **cumprimento de requisitos de xestión corporativa** e continuidade operativa.
- Mostra unha **xestión eficaz dos riscos** empresariais.
- Manifesta un **compromiso coa mellora continua**, a través da avaliación periódica do rendemento e implementación de melloras.

5.2 NIST CSF

O **CSF (Cybersecurity Framework)** do **NIST (Instituto Nacional de Estándares e Tecnoloxías dos Estados Unidos)** é un marco de xestión da seguridade da información, que se utiliza especialmente en entidades anglosaxonas.

O **NIST Cybersecurity Framework (CSF) 2.0** foi lanzado oficialmente o **26 de febreiro de 2024** [53][54]. Esta actualización representa un **avance moi significativo respecto da versión 1.1**, que se oficializara no ano 2018. O **NIST CSF 2.0** está deseñado para ser utilizado por **organizacións de todos os tamaños e sectores**, con independencia do seu nivel de sofisticación en materia de ciberseguridade.

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

Utiliza os **motores de negocio como guía para as actividades de ciberseguridade** dentro das compañías, considerando os **riscos asociados á tecnoloxía como parte fundamental do proceso de xestión de riscos xerais**.

Os compoñentes do modelo CSF son **tres**: o **Core**, as **capas de implementación (Tiers)**, e o **Framework Profile**.

5.2.1 Core

No **Core** deste Framework defínese un conxunto de **actividades de ciberseguridade e resultados esperados**, comúns ás organizacións de calquera sector. Indícanse unha serie de **estándares industriais e guías de boas prácticas** que permiten a execución e comunicación adecuada das actividades de ciberseguridade en toda a compañía, desde a capa executiva ata a de implementación e operacións.

O **Core define seis Funcións concurrentes e continuas** (que se descompoñen posteriormente en **Categorías** e **Subcategorías**) que, cando se consideran conxuntamente, proporcionan unha **visión estratéxica e sistemática para a xestión do ciclo de vida e das operacións de xestión de riscos de ciberseguridade** nas organizacións.

As seis funcións e as súas categorías asociadas son **moi populares** e aparecen con frecuencia na literatura técnica de ciberseguridade, especialmente nas **descricións de servizos**. Preséntanse a continuación:

Funcións NIST CSF 2.0. Fonte: NIST (2024)

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

Cómpre destacar que no Anexo A descríbense as **funcións, categorías e subcategorías do Core** do framework, así como **referencias informativas** (xa sexan do **NIST** ou doutros organismos ou estándares), para completar e ampliar a documentación ao respecto.

Función	Categoría	Identificador de Categoría
Gobernar (GV)	Contexto organizativo	GV.OC
	Estrategia de gestión de riesgos	GV.RM
	Funciones, responsabilidades y autoridades	GV.RR
	Política	GV.PO
	Supervisión	GV.OV
	Gestión de riesgos de la cadena de suministro en materia de seguridad cibernética	GV.SC
Identificar (ID)	Gestión de activos	ID.AM
	Evaluación de riesgos	ID.RA
	Mejora	ID.IM
Proteger (PR)	Gestión de identidades, autenticación y control de acceso	PR.AA
	Concienciación y capacitación	PR.AT
	Seguridad de datos	PR.DS
	Seguridad de plataformas	PR.PS
	Resistencia de la infraestructura tecnológica	PR.IR
Detectar (DE)	Monitoreo continuo	DE.CM
	Análisis de eventos adversos	DE.AE
Responder (RS)	Gestión de incidentes	RS.MA
	Análisis de incidentes	RS.AN
	Notificación y comunicación de la respuesta al incidente	RS.CO
	Mitigación de incidentes	RS.MI
Recuperar (RC)	Ejecución del Plan de Recuperación de Incidentes	RC.RP
	Comunicación de la recuperación del incidente	RC.CO

Funcións e categorías NIST CSF 2.0. Fonte: NIST (2024)

5.2.2 Niveis de Implementación

Os **niveis de implementación ou *Tiers*** defínense como se indica a continuación. **Proporcionan o contexto de como unha organización entende o risco de ciberseguridade** e os procesos establecidos para xestionar ese risco. Os niveis van dende o **parcial (nivel 1)** ata o **adaptativo (nivel 4)**.

Esta escala describe **un grao crecente de rigor e sofisticación nas prácticas de xestión de riscos de ciberseguridade**. Axuda a determinar ata que punto a xestión de riscos de ciberseguridade **se basea nas necesidades da empresa e está integrada nas prácticas xerais de xestión de riscos da organización**.

O proceso de selección de niveis ten en conta:

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

- as prácticas actuais de xestión de riscos da organización,
- o contorno de ameazas,
- os requisitos legais e regulamentarios,
- as prácticas de intercambio de información,
- os obxectivos de negocio ou misión,
- os requisitos de ciberseguridade da cadea de subministración, e
- as limitacións da organización.

As organizacións deben **determinar o nivel desexado**, asegurándose de que:

- **cumpre os obxectivos da organización**,
- é **factible de implementar**, e
- **reduce o risco de ciberseguridade** sobre os activos críticos e recursos ata niveis aceptables.

Aínda que se **anima ás organizacións identificadas como Nivel 1 (Parcial)** a considerar avanzar cara ao **Nivel 2 ou superior**, os niveis **non representan niveis de madurez**. **Están pensados para apoiar a toma de decisións organizativa sobre como xestionar o risco de ciberseguridade, así como identificar que dimensións deben priorizarse e recibir recursos adicionais.**

A progresión cara a niveis superiores recoméndase cando unha análise custo-beneficio indica unha redución viable e rendible do risco de ciberseguridade.

Como se comentaba máis arriba, existen **catro niveis**, nun esquema que lembra lixeiramente ao modelo de madurez **CMMI**:

- **Tier 1: Parcial**
- **Tier 2: Risco informado**
- **Tier 3: Repetible**
- **Tier 4: Adaptativo**

As características de cada nivel descríbense no framework en base a:

- o **grao de madurez do proceso de xestión do risco**,
- a súa **integración no programa de xestión da organización**, e

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

- o **grao de participación e implicación con stakeholders externos** na xestión do risco de ciberseguridade.

5.2.3 Perfil do Framework

O **"Perfil"** é a **aliñación das Funcións, Categorías e Subcategorías cos requisitos empresariais, a tolerancia ao risco e os recursos da organización**.

Un **Perfil permite ás organizacións establecer unha folla de ruta para reducir o risco de ciberseguridade**, aliñada cos obxectivos da organización e do sector, que teña en conta os requisitos legais/regulatorios e as mellores prácticas da industria, e reflicta as prioridades da xestión de riscos.

Dada a complexidade de moitas organizacións, estas **poden optar por ter múltiples perfís**, adaptados a **compoñentes ou unidades concretas**, recoñecendo as súas **necesidades específicas**.

Os perfís **permiten describir o estado da xestión de riscos de ciberseguridade dunha compañía nun momento dado**. A comparación entre o **perfil actual e o desexado no futuro** emprégase habitualmente para **identificar GAPs**, que serán cubertos mediante **proxectos de mellora específicos**, sempre tendo en conta **o nivel de risco e o custo/beneficio** de cada acción.

5.3 CIS Controls

O **Center for Internet Security (CIS)** é unha organización sen fins de lucro recoñecida internacionalmente polo seu labor na mellora da ciberseguridade a través de guías, recursos e boas prácticas accesibles [55]. Entre os seus principais achegues destacan os **Controis Críticos de Seguridade (CIS Controls)**, un conxunto de medidas priorizadas destinadas a **protexer as infraestruturas dixitais fronte a ameazas comúns**.

A versión 8.1 destes controis, publicada en 2024 [56], **non é certificable**, pero **a súa implementación efectiva permite elevar de maneira substancial o nivel de protección dunha organización**, sexa industrial ou non.

Aínda que orixinalmente deseñados para contornos empresariais en xeral, os CIS Controls son perfectamente **aplicables en contornos industriais OT/ICS**, contribuíndo a fortalecer a defensa das infraestruturas críticas contra ameazas cada vez máis sofisticadas e persistentes.

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

Neste caso, é clave a adaptación a estos entornos particulares, para **garantir a dispoñibilidade, integridade e continuidade dos procesos industriais**. A continuación, preséntase o listado completo de controis propostos.

1. Inventario e control de activos industriais: manter unha visibilidade completa e actualizada de todos os dispositivos OT, como PLCs, sensores, SCADA, HMIs e RTUs, resulta esencial para identificar posibles riscos. A implementación de ferramentas de descubrimento pasivo que non interfiran co funcionamento industrial, facilita a creación de mapas detallados da rede e dos seus activos.

2. Inventario e control de software de sistemas industriais: cómpre manter rexistros de firmware, sistemas operativos e software de aplicacións industriais. Este control require establecer listas de software autorizado, xestionar licenzas e validar calquera modificación mediante procesos de control de cambios. Os SCADA e sistemas DCS deben incluírse nesta revisión.

3. Protección de datos industriais sensibles: os datos operativos, como parámetros de procesos ou rexistros históricos, deben estar cifrados en tránsito e en repouso. Deben establecerse políticas claras de clasificación da información, restricións de acceso e rexistros de auditoría para garantir a súa confidencialidade e integridade.

4. Configuración segura de dispositivos industriais: empregar configuracións por defecto seguras, desactivar servizos innecesarios e aplicar políticas consistentes en todos os dispositivos OT. Estándares como os propios CIS benchmarks [57] proporcionan orientación sobre configuracións robustas para máquinas anfitrionas ou algún software de uso industrial, como bases de datos.

5. Xestión de contas e identidades OT: as contas deben ser asignadas individualmente, evitando o uso compartido. É necesario aplicar autenticación multifactor sempre que sexa posible, especialmente para accesos remotos ou privilexiados. As sesións deben rexistrarse para garantir a trazabilidade.

6. Control de accesos físicos e lóxicos: establecer políticas de acceso baseadas no principio de menor privilexio. A nivel físico, controlar o acceso a cuartos de control ou armarios de comunicación. A nivel lóxico, utilizar segmentación de redes, listas de control de acceso e proxys industriais para limitar a exposición.

7. Xestión continua de vulnerabilidades OT: realizar avaliacións de vulnerabilidades sen interromper os procesos industriais, a través de escaneos pasivos ou análise de

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

firmware. A colaboración co fabricante é esencial para aplicar parches sen afectar a estabilidade dos sistemas.

8. Rexistros e trazabilidade de eventos industriais: recoller logs de eventos de control, accesos, fallos e modificacións nos sistemas. Integrar estes rexistros nun SIEM adaptado ao contexto OT permite detectar comportamentos anómalos e responder rapidamente.

9. Protección fronte a vectores de entrada externos: limitar o uso de dispositivos USB e establecer zonas desmilitarizadas (DMZ) entre redes IT e OT. As ferramentas de control de acceso físico e os sistemas de escaneo de medios portátiles son recomendables.

10. Defensa contra malware en sistemas OT: utilizar solucións antivirus compatibles con sistemas en tempo real. Os contornos OT requiren solucións non intrusivas que non comprometan a continuidade dos procesos. É recomendable tamén illar as estacións de traballo críticas.

11. Copias de seguridade e recuperación de configuracións industriais: realizar backups periódicos dos sistemas e configuracións de dispositivos. Estes deben almacenarse de forma segura e comprobarse regularmente mediante probas de restauración.

12. Xestión segura das redes industriais: definir arquitecturas en capas, segmentar as redes por zonas e condutos segundo ISA/IEC 62443, e empregar firewalls industriais para controlar o tráfico entre segmentos.

13. Monitorización continua e detección de intrusións: integrar solucións de detección de intrusións específicas de OT (como IDS industriais) que recoñezan protocolos como Modbus, DNP3 ou OPC-UA. A resposta automática debe ser proporcional ao risco.

14. Formación e concienciación do persoal de operacións: implementar programas de formación específicos para persoal OT, sobre seguridade física, manipulación segura de dispositivos, resposta a incidentes e política de control de accesos.

15. Supervisión de provedores e integradores industriais: establecer contratos con cláusulas de seguridade, revisar os protocolos de acceso remoto dos provedores e esixir cumprimento normativo nos procesos de mantemento ou integración de novos sistemas.

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

16. Desenvolvemento e mantemento seguro de aplicacións industriais: aplicar revisións de código, validacións e probas de seguridade nas modificacións de lóxica de PLCs ou sistemas SCADA. Implantar controis de cambio rigorosos para manter a trazabilidade.

17. Preparación e resposta ante incidentes OT: definir procedementos claros de resposta, illamento e recuperación. Simular incidentes como fallos de comunicación, ransomware ou sabotaxe interna. Contar con contactos clave de fabricantes e autoridades.

18. Avaliación e test de seguridade en infraestruturas OT: realizar probas de penetración en entornos de laboratorio ou mediante revisións manuais e automáticas. Avaliar regularmente os controis aplicados e os plans de mellora continua.

É destacable o feito de que cada control CIS, dispón de un número variable de salvagardas para a súa implantación. A distribución desas salvagardas segundo os tres **grupos de implementación (*Implementation Groups*, IGs)**, é a seguinte:

- **IG1 (Grupo 1)**: salvagardas básicas, recomendadas para todas as organizacións, especialmente pequenas e medianas sen infraestrutura complexa.
- **IG2 (Grupo 2)**: salvagardas intermedias, para organizacións con máis recursos, necesidades regulatorias ou exposición ao risco.
- **IG3 (Grupo 3)**: salvagardas avanzadas, para organizacións que xestionan datos sensibles ou operan en sectores críticos como algúns do ámbito industrial, sanitario ou financeiro.

A continuación, un resumo gráfico de todo o anterior:

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

Controis CIS, salvagardas e grupos de implementación. Fonte: CIS (2024)

5.4 ISA/IEC 62443

A presente sección ten como obxectivo ofrecer unha **visión estruturada e orientativa da familia de normas IEC 62443**, que constitúen as normas transversais máis relevantes no contexto da ciberseguridade industrial. A fin é facilitar a súa comprensión, adopción progresiva e aliñamento cos marcos de cumprimento normativo vixentes.

Esta guía non substitúe, nin pretende substituír, o texto íntegro das normas IEC 62443 nin das súas correspondentes adopcións nacionais ou europeas. Para efectos de certificación, avaliación formal de conformidade, auditoría ou interpretación normativa vinculante, deberán consultarse sempre as versións íntegras e oficiais publicadas polos organismos de normalización correspondentes.

5.4.1 Introdución

A *International Society of Automation* (ISA) e a *International Electrotechnical Commission* (IEC) son dúas organizacións internacionais de referencia no ámbito da estandarización técnica e industrial [64][65].

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

A ISA é unha asociación profesional internacional especializada en automatización e sistemas de control, cun papel histórico destacado no desenvolvemento de boas prácticas e estándares orientados á seguridade e fiabilidade dos sistemas industriais. Pola súa banda, a IEC é o organismo internacional responsable da elaboración de normas globais no ámbito da tecnoloxía eléctrica, electrónica e de automatización, co obxectivo de harmonizar criterios técnicos e facilitar a interoperabilidade e a seguridade a nivel mundial.

A colaboración entre ambas organizacións permitiu trasladar o coñecemento experto da ISA ao marco normativo internacional da IEC, dando lugar a estándares amplamente aceptados como a familia IEC 62443 [66].

A familia de normas ISA/IEC 62443 constitúe o estándar internacional máis completo e específico para a protección de ciberseguridade dos sistemas de automatización e control industrial (IACS/ICS/OT).

A súa principal diferenza fronte a outros marcos de seguridade reside en que **foi concibida desde a súa orixe para entornos industriais**, onde os impactos dunha falla de seguridade non se limitan á información, senón que poden afectar directamente á seguridade das persoas, ao medio ambiente e á continuidade do proceso produtivo.

A norma **proporciona unha linguaxe común e un marco estruturado que permite aliñar a seguridade técnica, a organización e os procesos operativos**, integrando a ciberseguridade ao longo de todo o ciclo de vida dos sistemas industriais: deseño, integración, operación, mantemento e retirada.

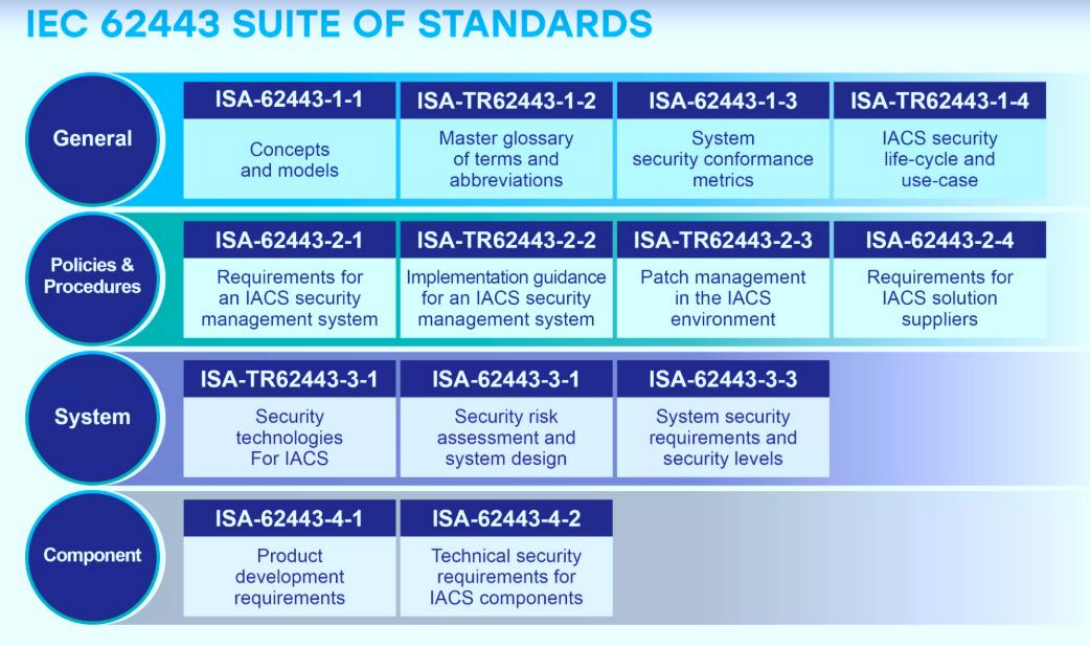
5.4.2 Estrutura da familia de normas

A familia IEC 62443 estrutúrase en catro grandes bloques que responden a unha lóxica progresiva e complementaria:

- En primeiro lugar, as normas da **Parte 1 (Xeral)** establecen a base conceptual do estándar. Nelas **defínense a terminoloxía común, os principios fundamentais e os modelos que se empregarán no resto da familia**. Estas normas non introducen requisitos técnicos nin organizativos directos, pero son imprescindibles para interpretar correctamente o estándar.
- En segundo lugar, a **Parte 2 (Políticas e procesos)** aborda a **dimensión organizativa da ciberseguridade industrial**. Este bloque céntrase en como deben estruturarse os programas de seguridade, os roles, as responsabilidades,

os procesos e as relacións entre propietarios de activos, integradores e provedores de servizos.

- A continuación, a **Parte 3 (Sistemas)** constitúe o **núcleo técnico-operativo da norma para operadores e propietarios de activos**. Nela defínense a metodoloxía de avaliación de riscos e os requisitos técnicos que deben cumprir os sistemas industriais en función do risco identificado.
- Finalmente, a **Parte 4 (Compoñentes e desenvolvemento)** está **orientada principalmente a fabricantes de produtos OT**, establecendo requisitos tanto para o desenvolvemento seguro como para as capacidades de seguridade dos compoñentes.



Estrutura de estándares ISA/IEC 62443. Fonte: Thales Cybersecurity (2024)

Esta disposición permite aplicar o estándar de maneira selectiva e proporcional, evitando enfoques indiscriminados e favorecendo unha adopción realista.

5.4.3 Conceptos fundamentais da IEC 62443

5.4.3.1 Defensa en profundidade

O principio de defensa en profundidade é un dos pilares da IEC 62443. Este concepto establece que **a seguridade non debe depender dun único mecanismo ou control, senón dunha combinación de medidas técnicas, organizativas e procedimentais distribuídas en diferentes capas.**

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

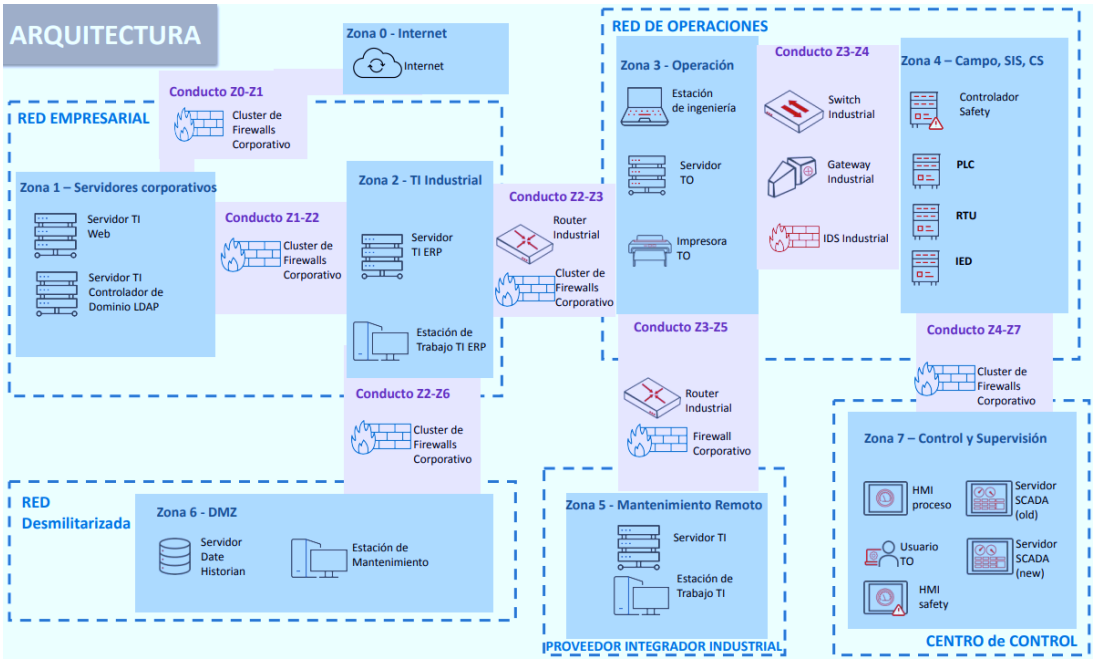
En entornos OT, isto tradúcese na combinación de segmentación de rede, control de accesos, mecanismos de autenticación, procedementos operativos seguros, monitorización e capacidades de resposta. O obxectivo non é impedir absolutamente calquera incidente, senón limitar o seu impacto e evitar a propagación dun fallo ou ataque a todo o sistema.

5.4.3.2 Zonas e condutos

O modelo de zonas e condutos é unha das achegas máis distintivas da IEC 62443. Unha **zona** defínese como un **conxunto de activos, físicos ou lóxicos, que comparten requisitos de seguridade comúns.** Os **condutos representan as canles de comunicación entre zonas e deben ser protexidos acorde aos riscos** asociados.

Este modelo permite estruturar a seguridade dun sistema industrial de forma comprensible e verificable, facilitando tanto o deseño de arquitecturas seguras como a súa avaliación posterior.

A continuación, un exemplo de arquitectura baseado en zonas e condutos:



Arquitectura de rede ICS baseada en zonas e condutos. Fonte: CCI (n.d.)

5.4.3.3 Niveis de seguridade (*Security Levels*, SL)

Os **niveis de seguridade (*Security Levels*, SL) describen o grao de protección requirido fronte a distintos perfís de ameaza**, caracterizados polo nivel de recursos, coñecementos e motivación do atacante. A IEC 62443 define cinco niveis:

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

- **SL 0**: non se require **ningún requisito específico de seguridade**. Só é aceptable en entornos illados ou sen impacto relevante.
- **SL 1**: **protección fronte a erros ou usos non intencionados**. Abarca medidas básicas como control de accesos elementais e boas prácticas operativas.
- **SL 2**: **protección fronte a ataques intencionados simples**, realizados con ferramentas comúns e coñecementos xerais. Require controis técnicos básicos de autenticación, segmentación e rexistro.
- **SL 3**: **protección fronte a ataques dirixidos con coñecementos específicos** de sistemas OT. Implica medidas avanzadas de control de acceso, monitorización, defensa en profundidade e protección da integridade.
- **SL 4**: **protección fronte a ataques altamente sofisticados e dirixidos, con amplos recursos e alta motivación**. Normalmente restrínxese a escenarios moi críticos.

Os SL non son obxectivos arbitrarios: deben derivarse dunha avaliación de riscos e aplicarse de forma diferenciada a zonas, condutos, sistemas e compoñentes.

5.4.3.4 Niveis de madurez organizativa

Ademais dos niveis de seguridade técnica, a familia IEC 62443 introduce un **modelo de madurez organizativa** que **permite avaliar ata que punto unha organización ten integrados e institucionalizados os procesos de ciberseguridade industrial**. Este modelo é especialmente relevante para provedores de servizos e fabricantes, aínda que tamén resulta útil como referencia para operadores e administracións.

Os niveis de madurez definidos son os seguintes:

- **Nivel de madurez 1 – Inicial**: a seguridade xestiónase de maneira reactiva e ad-hoc. Os procesos non están formalizados, dependen das persoas e existe pouca ou ningunha documentación. As actuacións en seguridade prodúcense habitualmente tras incidentes.
- **Nivel de madurez 2 – Xestionado**: existen procesos documentados e directrices formais. O persoal coñece os procedementos básicos e aplícanse de maneira repetible, aínda que con variabilidade entre proxectos ou áreas.
- **Nivel de madurez 3 – Definido**: os procesos de seguridade están estandarizados en toda a organización, intégranse no ciclo de vida dos sistemas e existe evidencia sistemática da súa aplicación.

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

- **Nivel de madurez 4 – Mellora continua**: a organización mide a eficacia e eficiencia dos seus procesos de seguridade, utiliza indicadores e métricas, e aplica melloras continuas baseadas en datos e revisións periódicas.

Este modelo permite avaliar non só se existen controis, senón se estes son sostibles no tempo e son xestionados de modo oportuno.

5.4.4 Certificación na IEC 62443

A familia IEC 62443 dispón dun esquema de certificación específico, xestionado por ISASecure, que permite certificar distintos obxectos:

- **Procesos**: certificación do ciclo de vida de desenvolvemento seguro (baseado en IEC 62443-4-1).
- **Produtos e compoñentes**: certificación das capacidades técnicas de seguridade (IEC 62443-4-2).
- **Sistemas**: certificación de sistemas industriais completos conforme a requisitos de sistema (IEC 62443-3-3). Posteriormente centrarémonos en este, por ser o máis relevante para as organizacións que queiran protexer o entorno operativo.

As certificacións realízanse por entidades acreditadas independentes e teñen carácter temporal, requirindo **renovación periódica**, habitualmente anual ou plurianual segundo o esquema, incluíndo revisións documentais e, cando procede, auditorías técnicas.

En contraste como vimos, certificacións como **ISO/IEC 27001** ou o **Esquema Nacional de Seguridade** teñen unha vixencia de tres e dous anos, respectivamente. Estas non avalían directamente a seguridade técnica dun sistema industrial nin dun produto concreto, senón a existencia dun marco de xestión adecuado.

5.4.5 Documentos principais da familia IEC 62443

A continuación preséntase unha descrición breve dos principais documentos da familia IEC 62443 que se consideran máis relevantes a efectos de cumprimento normativo.

5.4.5.1 IEC 62443-1-1 – Conceptos, terminoloxía e modelos fundamentais

Establece a **base conceptual da familia IEC 62443, definindo a terminoloxía común, os principios fundamentais de ciberseguridade industrial e o modelo xeral de aplicación do estándar.** Introduce conceptos clave como defensa en profundidade, zonas e condutos, niveis de seguridade e a relación entre riscos e requisitos, actuando

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

como marco interpretativo imprescindible para o resto das normas da serie. Máis detalle dalgunha destas cuestión na seguinte sección.

5.4.5.2 IEC 62443-1-5 – Perfís de seguridade

Introduce o **concepto de perfís de seguridade** como mecanismo para adaptar a IEC 62443 **a sectores, regulacións ou contextos específicos**.

5.4.5.3 IEC 62443-2-1 – Sistema de xestión da seguridade do propietario do activo

Este documento define os **requisitos para establecer e manter un sistema de xestión da seguridade OT por parte do propietario dos activos.** Proporciona o marco organizativo que conecta a avaliación de riscos, os requisitos técnicos e a operación segura.

5.4.5.4 IEC 62443-2-4 – Requisitos de seguridade para provedores de servizos IACS

Aborda a dimensión **organizativa e operativa dos integradores, empresas de mantemento e provedores de servizos OT, un dos vectores de risco máis relevantes** en entornos industriais.

5.4.5.5 IEC 62443-3-2 – Avaliación do risco de seguridade para o deseño de sistemas

Establece a **metodoloxía para realizar avaliacións de risco específicas para sistemas OT**, servindo de punto de partida para o deseño de arquitecturas seguras baseadas en zonas, condutos e niveis de seguridade.

5.4.5.6 IEC 62443-3-3 – Requisitos técnicos de seguridade para sistemas

Define os **requisitos técnicos que deben cumprir os sistemas industriais para acadar os niveis de seguridade establecidos** tras a avaliación de riscos. Fundamental para protexer e certificar unha planta produtiva. Profundizaremos nesta cuestión na seguinte sección.

5.4.5.7 IEC 62443-4-1 – Ciclo de vida de desenvolvemento seguro de produtos

Establece os r**equisitos que deben cumprir os fabricantes para integrar a seguridade no desenvolvemento de produtos OT** desde as fases iniciais.

5.4.5.8 IEC 62443-4-2 – Requisitos técnicos de seguridade para compoñentes

Define as **capacidades de seguridade que deben ofrecer os compoñentes industriais**, como PLC, HMI, dispositivos de rede ou software.

5.4.6 Aplicación da IEC 62443 a sistemas industriais

A aplicación práctica da familia de normas IEC 62443 **non debe entenderse como a implantación illada dun conxunto de controis técnicos**, senón como un **proceso estruturado e coherente**, no que cada decisión de seguridade deriva do risco e pode ser xustificada técnica e organizativamente. Este enfoque articúlase como unha **cadea lóxica de pasos**, que permite garantir proporcionalidade, trazabilidade e evidencias de cumprimento.

5.4.6.1 Avaliación do risco

O punto de partida é sempre a **avaliación do risco de ciberseguridade**, conforme á IEC 62443-3-2. Nesta fase identifícanse os activos industriais, as súas funcións críticas, as ameazas relevantes, as vulnerabilidades existentes e os impactos potenciais sobre a seguridade das persoas, a continuidade do proceso, o medio ambiente ou a calidade do servizo.

Exemplo: nunha planta de tratamento de auga, identifícase que a perda de control sobre determinados PLC pode provocar a interrupción do subministro ou a dosificación incorrecta de produtos químicos. As ameazas inclúen accesos remotos non controlados e malware introducido a través de portátiles de mantemento.

5.4.6.2 Determinación do nivel de seguridade obxectivo (SL-T)

Unha vez analizado o risco, establécese o **nivel de seguridade obxectivo (SL-T)** para cada zona e conduto. Este nivel expresa o grao de protección necesario fronte ao perfil de ameaza considerado, evitando tanto a infra-protección como a sobre-protección innecesaria.

Exemplo: a rede de supervisión pode requirir un SL-2, mentres que a zona de control de procesos críticos pode necesitar un SL-3 debido ao maior impacto operativo e á posibilidade de ataques dirixidos.

A estos efectos, **vexamos qué di a norma sobre os niveis de seguridade (SL).** No anexo A da IEC 62443-3-3, reza o seguinte:

Os niveis de seguridade supoñen un enfoque cualitativo á hora de abordar a seguridade dunha zona. Como método cualitativo, a definición do nivel de seguridade pode aplicarse para comparar e xestionar a seguridade das zonas dentro dunha organización. A medida que se dispoña de máis datos e se desenvolvan as representacións matemáticas do risco, das ameazas e dos incidentes de seguridade, este concepto pasará a ter un enfoque cuantitativo para a selección e verificación dos niveis de seguridade (SL). Poderá ser

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

aplicado tanto polas organizacións usuarias finais como polos provedores de IACS e de produtos de seguridade. Empregarase para seleccionar os dispositivos IACS e as contramedidas que se vaian utilizar nunha zona e para identificar e comparar a seguridade das zonas en distintas organizacións do sector.

Os SL clasifícanse en tres categorías: **niveis obxectivo**, **niveis acadados** e **niveis de capacidade**. Aínda que estas categorías están relacionadas entre si, fan referencia a distintos aspectos do ciclo de vida da seguridade.

- **Os niveis de seguridade obxectivo (SL-T)** son o nivel de seguridade que se desexa para un sistema determinado. Normalmente, este nivel determínase a través dunha avaliación de riscos do sistema, mediante a cal se establece que é necesario un determinado nivel de seguridade para garantir un funcionamento correcto.
- **Os niveis de seguridade acadados (SL-A)** son o nivel de seguridade real dun sistema determinado. Estes niveis mídense unha vez que se dispón dun deseño do sistema ou cando o sistema está implantado. Empréganse para determinar se un sistema de seguridade está a cumprir os obxectivos que se estableceran inicialmente nos niveis de seguridade obxectivo.
- **Os niveis de seguridade de capacidade (SL-C)** son os niveis de seguridade que poden proporcionar os compoñentes ou os sistemas cando están configurados correctamente. Estes niveis expresan que un compoñente ou sistema determinado é capaz de acadar os SL obxectivo de forma nativa, sen empregar contramedidas compensatorias adicionais, sempre que estea configurado e integrado de maneira correcta.

Os distintos tipos de niveis de seguridade (SL) aplícanse en diferentes fases do ciclo de vida da seguridade. En primeiro lugar, defínese o nivel de seguridade obxectivo (SL-T) a partir da avaliación de riscos. A continuación, deséñase o sistema de maneira iterativa para acadar ese nivel, seleccionando compoñentes e sistemas co nivel de capacidade (SL-C) axeitado ou, de ser necesario, aplicando contra medidas compensatorias. Unha vez o sistema entra en operación, mídese o nivel de seguridade acadado (SL-A) e comprárase co SL obxectivo para verificar o cumprimento dos requisitos establecidos.

5.4.6.3 Aplicación de requisitos técnicos e organizativos

A continuación, procédese á **selección e implantación dos requisitos de seguridade** axeitados para acadar o SL-T definido. Estes requisitos poden ser de natureza técnica (IEC 62443-3-3 e 4-2) ou organizativa e procedimental (IEC 62443-2-4, 4-1).

5.4.6.3.1 Requerimentos e formato vector do SL

Existe unha forma compacta de describir os niveis de seguridade. Tal e como se define na Norma **IEC 62443-1-1**, os niveis de seguridade (SL) previamente descritos baséanse en **sete requisitos fundamentais (FR)** para a seguridade:

1. **control de identificación e autenticación (IAC);**
2. **control de uso (UC);**
3. **integridade do sistema (SI);**
4. **confidencialidade dos datos (DC);**
5. **fluxo de datos restrinxido (RDF);**
6. **resposta oportuna aos eventos (TRE);** e
7. **dispoñibilidade de recursos (RA).**

En lugar de reducir os SL a un único valor numérico, **é posible empregar un vector de SL que utilice os sete FR mencionados en lugar dun único factor de protección**. Este vector de SL permite establecer separacións definibles entre os SL para os distintos FR mediante unha linguaxe específica. Esta linguaxe pode basearse en consecuencias adicionais asociadas aos sistemas de seguridade ou en distintos tipos de ataques contra os obxectivos de seguridade abordados polos FR, e pode incluír explicacións prácticas sobre como un sistema pode ser máis seguro ca outro sen necesidade de relacionar todo con consecuencias para a saúde, a seguridade e o medio ambiente (HSE).

É preferible empregar un **vector** para describir os requisitos de seguridade dunha zona, dun conduto, dun compoñente ou dun sistema, en lugar de utilizar un único número que proporciona menor detalle. Este vector pode conter un requisito específico de SL ou un valor igual a cero para cada requisito fundamental. **O formato vector do SL**, é:

SL-?([FR], dominio) = { IAC UC SI DC RDF TRE RA }

onde:

- **SL-? = (Requirido)** representa o tipo de SL. Os formatos posibles son:

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

- **SL-T** = SL obxectivo
- **SL-A** = SL acadado
- **SL-C** = SL de capacidade

- **[FR] = (Opcional)** Campo que indica o requisito fundamental ao que se aplica o valor do SL. Os FR escríbense de forma abreviada, en lugar de empregar unha notación numérica, para facilitar a comprensión.
- **dominio = (Requirido)** O dominio ao que se aplica o SL. Os dominios poden facer referencia a zonas, sistemas de control, subsistemas ou compoñentes.

  Nesta norma en particular, todos os requisitos fan referencia ao sistema de control, polo que o termo "dominio" non se utiliza como noutros documentos da serie de Normas IEC 62443.

Exemplos:

- SL-T (Zona BPCS) = { 2 2 0 1 3 1 3 }
- SL-C (Posto de traballo técnico do SIS) = { 3 3 2 3 0 0 1 }
- SL-C (RA, FS-PLC) = 4

5.4.6.3.2 Implantación da ciberseguridade

O **Anexo B da IEC 62443-3-3** describe como se constrúen os **niveis de seguridade (SL 1 a SL 4)** a partir da asignación progresiva de **requisitos do sistema (SR)** e das súas **melloras (RE)** aos **sete requisitos fundamentais (FR)** definidos no estándar, enumerados arriba.

A norma establece **100 requisitos técnicos** (descritos con detalle na norma no corpo principal da mesma), resultado da combinación de SR e RE (requisitos básicos do sistema e melloras), que permiten materializar os distintos niveis de seguridade para cada FR. **A progresión dos SL é acumulativa: para cumprir un nivel superior é necesario cumprir todos os requisitos dos niveis inferiores máis os adicionais definidos para ese nivel.**

A táboa B.1 indica, para cada FR e para cada SL, que requisitos deben aplicarse para que un sistema poida considerarse conforme a ese nivel. Deste xeito, os SL deixan de ser un concepto abstracto e convértense nun conxunto de **capacidades técnicas verificables**.

Este enfoque permite avaliar de forma obxectiva o SL acadado (SL-A) dun sistema, comparar sistemas ou zonas con distintos perfís de seguridade, e garantir

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

coherencia entre o risco identificado, o nivel de seguridade esixido e as medidas técnicas implantadas.

Vexamos a continuación un exemplo:

SR y RE		SL 1	SL 2	SL 3	SL 4
FR 1 – Control de identificación y autenticación (IAC)					
SR 1.1 – Identificación y autenticación de usuarios humanos	5.3	✓	✓	✓	✓
SR 1.1 RE 1 – Identificación y autenticación únicas	5.3.3.1		✓	✓	✓
SR 1.1 RE 2 – Autenticación multifactor para redes que no son de confianza	5.3.3.2			✓	✓
SR 1.1 RE 3 – Autenticación multifactor para todas las redes	5.3.3.3				✓

Mostra de asignación de SR e RE a os RF dos niveis de seguridade. Fonte: ISA 62443-3-3 (2020)

Como se pode apreciar no exemplo, para cumprir co Requisito do Sistema (SR) 1.1 do Requisito Fundamental 1 (Control de identificación e autenticación, IAC), en caso de precisar un Nivel de Seguridade dado no sistema:

- De SL1: bastaría con implementar o requisito SR 1.1.
- De SL2: precisaríase ademais do anterior, a mellora SR 1.1. RE 1.
- De SL3: ao anterior, sumaríamos a mellora SR 1.1 RE 2.
- De SL4: necesitaríamos aplicar todo, tanto o requisito de sistema, como as tres melloras definidas.

Así, para definir as necesidades de seguridade do noso sistema, debemos en base á análise de riscos determinar os SL-T asociados ás diferentes zonas e condutos, e implementalas mediante as medidas correspondentes na ISA 62443-3-3.

En conxunto, o Anexo B proporciona a ponte entre os niveis de seguridade definidos conceptualmente e a súa **implementación técnica concreta** en sistemas industriais.

No seguinte recurso, pode verse un exemplo ilustrativo dun escenario real de implantación da norma IEC 62443 no sector enerxético, en colaboración co CCI (Centro de Ciberseguridade Industrial) [67].

5.4.6.4 Certificación e verificación

A última peza da cadea é a **verificación independente** das medidas implantadas. A certificación conforme á IEC 62443 permite demostrar, mediante avaliacións de terceira parte, que:

- os procesos seguen prácticas recoñecidas,

- os sistemas cumpren requisitos técnicos definidos,
- ou os produtos incorporan capacidades de seguridade adecuadas.

A certificación non é obrigatoria para aplicar a norma, pero achega unha **evidencia sólida de conformidade**, especialmente relevante en entornos reguladas ou contratos con terceiros.

A modo de exemplo, un fabricante pode certificar un produto conforme á IEC 62443-4-2, mentres que un operador pode optar por certificar un sistema concreto na IEC 62443-3-3 trala súa implantación nunha infraestrutura crítica.

Esta secuencia *risco → SL → requisitos → verificación*, garante que as medidas de seguridade:

- están xustificadas polo risco,
- son proporcionais ao impacto,
- están aliñadas cos obxectivos operativos,
- e poden ser auditadas e demostradas.

Cabe destacar para cerrar este epígrafe, que a familia IEC 62443 está deseñada para ser aplicada por distintos actores, cada un cun rol específico no ecosistema industrial:

- **Operador (propietario do activo)**: responsable da avaliación do risco, da definición dos niveis de seguridade, da operación segura dos sistemas e da gobernanza global da ciberseguridade OT.
- **Integrador (provedor de servizos)**: centra a súa responsabilidade nos procesos de integración, mantemento e acceso aos sistemas, garantindo que as súas actuacións non introducen riscos adicionais e que se cumpren os requisitos contractuais e normativos.
- **Fabricante:** debe integrar a seguridade desde o deseño dos produtos, implementando ciclos de desenvolvemento seguro e proporcionando compoñentes con capacidades técnicas acordes aos niveis de seguridade requiridos.
- **Administración (regulador):** utiliza a IEC 62443 como marco de referencia para harmonizar criterios, elaborar políticas públicas, establecer requisitos mínimos e supervisar o cumprimento en sectores críticos.

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

Este enfoque por roles reforza a idea de que a ciberseguridade industrial é unha **responsabilidade compartida**, na que cada actor contribúe á protección global do sistema desde o seu ámbito de competencia.

Como se pode apreciar, a familia IEC 62443 proporciona un marco integral que permite abordar a ciberseguridade industrial desde unha perspectiva técnica, organizativa e de ciclo de vida. Por iso se considera a norma máis importante para entornos ICS/OT, ao marxe das sectoriais específicas. A súa aplicación estruturada constitúe un elemento central para calquera estratexia de cumprimento normativo en entornos OT.

5.5 SANS ICS Top 5 Controls

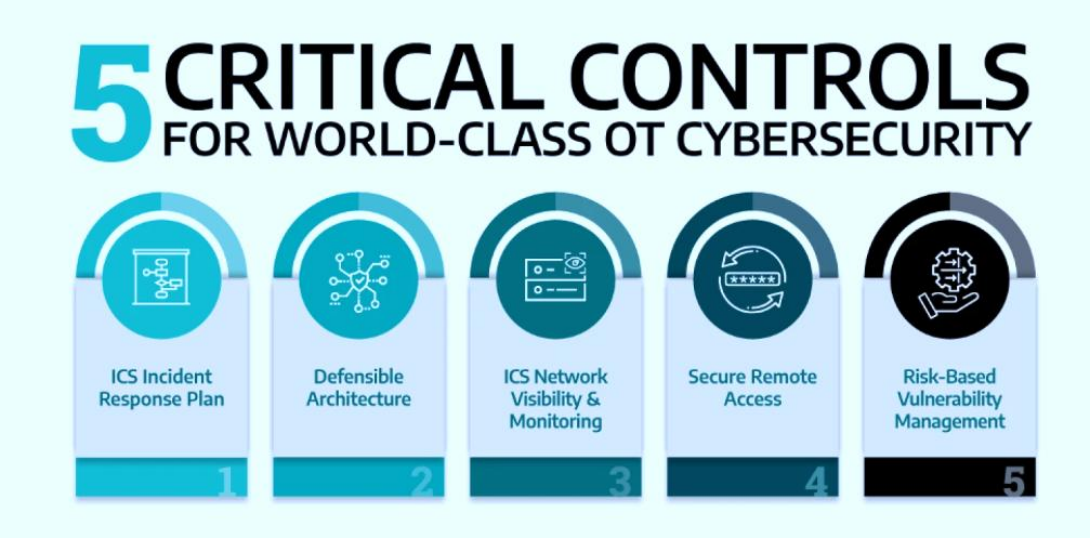
En outubro de 2022, o SANS Institute – coñecido organismo de formación en ciberseguridade – publicou un *whitepaper* no que definía cinco controis de ciberseguridade especialmente relevantes para protexer **sistemas de control industrial (ICS)** e **tecnoloxías operativas (OT)** [58][59].

Este marco, desenvolvido polos expertos de SANS Robert M. Lee e Tim Conway, naceu tras unha análise exhaustiva dos ciberataques coñecidos contra contornos ICS a nivel global. O seu propósito é proporcionar un conxunto conciso de medidas **esenciais** – deseñadas especificamente para prevención, detección e resposta a incidentes en ámbitos industriais – que sirvan de base para un programa efectivo de ciberseguridade OT.

En contraste cos catálogos extensos doutros estándares xenéricos, os **SANS ICS 5 Critical Controls** enfocan os esforzos nas áreas críticas de maior impacto práctico, aportando ás organizacións industriais unha guía clara de "por onde comezar" para mellorar a súa postura de **ciberseguridade industrial**. Ademais, este conxunto de controis foi concibido para ser flexible e adaptable aos distintos perfís de risco e necesidades de cada organización, mantendo sempre o foco nas particularidades únicas dos sistemas ICS/OT en canto a seguridade e continuidade operativa.

A continuación descríbense os cinco controis críticos de SANS ICS, detallando o seu contido técnico e exemplos de aplicación en contornos industriais reais. Tamén se analiza como estes controis funcionan como marco complementario a estándares máis amplos (ISO/IEC 27001, ISA/IEC 62443, etc.) no ámbito das infraestruturas industriais.

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



5 controis críticos para entornos ICS. Fonte: Dragos (2023)

5.5.1 Control crítico #1: Plan de resposta a incidentes específico para ICS

O primeiro control esixe contar cun **plan de resposta a incidentes ciber** adaptado ás particularidades dos sistemas industriais (ICS).

É fundamental que as organizacións dispoñan dun plan de resposta pensado especificamente para entornos ICS/OT, e que este **non** se conciba simplemente como a última etapa dun programa de seguridade, senón como un alicerce central do mesmo. Un erro común é considerar a resposta a incidentes como "o final do camiño", o que provoca que moitas das medidas de seguridade implementadas previamente non estean aliñadas coas necesidades reais á hora de xestionar un incidente industrial. Pola contra, integrar desde o inicio a perspectiva de *incident response* no plan xeral de seguridade asegura que a arquitectura, a monitorización e outros controis proporcionen a visibilidade e os datos necesarios para investigar e responder eficazmente cando ocorre un incidente.

Nos entornos OT, as prioridades ante un incidente difiren das de IT. Mentres os plans tradicionais de TI enfatizan identificación do adversario, contención e erradicación, un **plan de resposta ICS** debe poñer en primeiro lugar a seguridade das persoas e a continuidade do proceso industrial baixo control. Isto implica que as accións de resposta en OT se **priorizan segundo o impacto potencial na operación**, buscando manter os sistemas funcionais aínda baixo ataque para reducir ao mínimo os efectos sobre a produción e a seguridade física. Un beneficio engadido desta estratexia é que unha boa resposta a incidentes ICS non só minimiza o risco ciber, senón que tamén mellora a

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

resiliencia operativa global ao facilitar análises de causa raíz de calquera fallo, sexa ou non causado por un atacante.

Exemplo aplicado: para preparar este plan, SANS recomenda empregar escenarios baseados en incidentes reais. En primeiro lugar, a organización debe identificar e analizar os escenarios de ameaza **que máis risco supoñen** para os seus procesos industriais – por exemplo, un ataque de ransomware que afecte as redes OT – tomando como referencia casos ocorridos no sector. Estes escenarios "intelixencia-dirixidos" (baseados en ataques reais) deben terse por prioritarios, xa que ao ter sucedido nalgures demostran ser posibles e incluso repetibles. A modo ilustrativo, **todas as organizacións industriais deberían dispoñer dun escenario de ransomware que afecte a OT**; unha empresa petroquímica debería incluír un escenario de manipulación do sistema de seguridade inspirado no malware TRISIS, e practicamente todas as compañías eléctricas deberían adestrar cun escenario baseado nos apagóns de Ucraína de 2015-2016 [60][61]. En segundo lugar, recoméndase contemplar tamén algún **escenario de consecuencia** hipotético de alto impacto aínda que non exista precedente histórico (por exemplo, un fallo grave de seguridade nunha planta que puidese causar danos físicos ou paradas prolongadas). Estes escenarios de "¿e si…?" axudan a avaliar que é teoricamente posible e a anticipar mesmo ataques inéditos, aínda que deben dosificarse para non desbordar de supostos irreais; o consello é limitarse a un ou dous escenarios de máxima consecuencia, mantendo os pés na terra do contexto e procesos reais da organización.

Finalmente, o plan de resposta a incidentes ICS debe ser **posto á proba mediante exercicios prácticos (*table-top exercises*)**. Unha vez definidos os escenarios relevantes, cómpre realizar simulacros nos que todos os departamentos implicados (operacións, seguridade, mantemento, dirección, legal, etc.) colaboren para debullar como afectaría cada escenario ás súas áreas e que requerimentos terían para xestionar o incidente. Estas **probas de mesa** permiten verificar se os equipos dispoñen da información e recursos necesarios a tempo (por exemplo, logs históricos de certos sistemas, contactos de emerxencia, procedementos de illamento, etc.), e descubrir posibles eivas a corrixir. Ademais, axudan a identificar cales son os sistemas críticos ("as xoias da coroa") en cada sitio industrial e, polo tanto, onde se debe focalizar con prioridade a aplicación dos restantes controis críticos.

O Control #1 establece unha visión compartida dos riscos principais e dos resultados que a organización quere acadar ante incidentes, servindo de guía para materializar os demais controis críticos.

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

5.5.2 Control crítico #2: Arquitectura defendible

O segundo control consiste en deseñar e manter unha **arquitectura de rede defendible** para os sistemas industriais. Unha arquitectura está ben "defendida" cando, mediante o seu deseño e configuración, **minimiza ao máximo os riscos** e facilita o labor dos responsables de seguridade na protección das instalacións. Neste sentido, existen diversos marcos de referencia en uso – desde o clásico modelo Purdue de segmentación por niveis, ata arquitecturas modernas baseadas na norma ISA/IEC 62443 – pero o esencial é a súa correcta implementación práctica para reforzar realmente a seguridade da organización. En outras palabras, non abondan os debuxos ou estándares no papel: é preciso materializalos adecuadamente na rede industrial concreta.

Algúns **atributos clave** que caracterizan unha arquitectura ICS defendible son os seguintes:

- **Identificación e inventario de activos:** coñecer todos os dispositivos, sistemas e aplicacións presentes na rede industrial, especialmente nos enclaves críticos. Un inventario actualizado serve de base para protexer e monitorizar eficazmente.
- **Segmentación de redes e zonas:** subdividir o entorno ICS en segmentos ou celas illadas, limitando estritamente os puntos de conexión entre elas (entry/exit points). Isto reduce a superficie de ataque e evita a propagación libre dunha ameaza se entra nalgún segmento. Por exemplo, é recomendable implantar **DMZ industriais** ou redes perimetrais que fagan de ponte segura entre a rede corporativa TI e a rede OT, controlando o intercambio de datos entre ambas.
- **Control da comunicación bidireccional:** determinar con criterio cales son as ligazóns que realmente precisan tráfico en ambos sentidos entre diferentes segmentos (por exemplo, entre a zona de supervisión e a de control) e restrinxir aquelas conexións innecesarias ou perigosas. Só se deben permitir os fluxos imprescindibles para a operación.
- **Capacidade de inspección e recollida de tráfico:** dispoñer de mecanismos para capturar e examinar o tráfico de rede e as comunicacións industriais. Isto inclúe implementar **inspección profunda de paquetes** (DPI) para protocolos ICS – que achega visibilidade detallada sobre comandos e valores que atravesan a rede – e gardar rexistros de actividade que poidan ser analizados posteriormente.

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

- **Rexistro e análise de eventos críticos:** a arquitectura debe facilitar o *log* dos sucesos relevantes e a súa correlación, xa sexan alertas de intrusión, cambios de configuración ou fallos de equipos. Unha boa **telemetría** é crucial para detectar intrusións ou anomalías a tempo e investigar incidentes a fondo.
- **Postura de seguridade restritiva:** configurar a rede e os sistemas aplicando o principio de privilexio mínimo, eliminando dispositivos ou servizos non esenciais e **restrinxindo conexións innecesarias** por defecto. Por exemplo, deshabilitar portos e protocolos non utilizados, aplicar listas de control de acceso (ACLs) estritas entre segmentos, e asegurar que todo acceso remoto ou de terceiros estea debidamente controlado. Unha arquitectura "limpa" e ben segmentada dificulta enormemente o movemento lateral dun atacante e reduce vías de entrada.

Unha arquitectura industrial defendible non só protexe mellor, senón que **simplifica a monitorización e resposta a incidentes**. Cómpre salientar que este control está moi ligado co Control #3 (visibilidade da rede): unha arquitectura ben deseñada permite colocar sensores e puntos de inspección nos lugares axeitados, facilitando unha vixilancia efectiva do tráfico e dos sistemas. Pola contra, sen unha correcta segmentación e sen inventario, pouco pode axudar a mellor ferramenta de monitorización. En definitiva, a Arquitectura Defendible crea os *alicerces* sobre os que operarán os demais controis técnicos de seguridade.

5.5.3 Control crítico #3: Visibilidade e monitorización da rede ICS

O terceiro control céntrase en lograr unha **visibilidade completa do que sucede nas redes industriais e en implementar monitorización continua** para detectar a tempo posibles ameazas. Dado que os entornos ICS/OT actuais son cada vez máis complexas e están recheas de protocolos e equipos heteroxéneos, ter unha visión clara do tráfico e das interaccións entre sistemas é vital para varios propósitos: identificar a priori comportamentos anómalos ou non desexados, validar que a **arquitectura defendible** do Control #2 está a funcionar (por exemplo, comprobar que a segmentación está a bloquear fluxos indebidos), e mellorar tanto a eficacia da resposta a incidentes (Control #1) como doutras medidas como o control de accesos remotos ou xestión de parches.

En palabras simples, non se pode protexer o que non se ve: sen visibilidade profunda da rede OT, unha organización quedará cegada ante intrusións ata que sexa tarde de máis.

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

Implementar este control implica despregar ferramentas e tecnoloxías especializadas de monitorización industrial. Un aspecto clave é a capacidade de **inspección de protocolos ICS** en profundidade – por exemplo, comprender tramas Modbus, OPC UA, S7, DNP3, etc. – xa que desta forma pódense detectar comandos ou valores anómalos propios do dominio industrial (e non só paquetes TCP/IP xenéricos). Estas ferramentas de monitorización (que adoitan incluír funcionalidades de inventario automático, IDS/IPS adaptados a ICS, análise de tráfico e incluso machine learning) como se indicou no Informe de Ciberalertas desde mesmo Observatorio [1], deben operar preferiblemente de forma non intrusiva ou en modo espello, para non interferir cos sistemas sensibles.

Algúns elementos que unha boa solución de visibilidade e monitorización ICS debería proporcionar son:

- **Inventario dinámico de activos e mapas de comunicación:** identificación de todos os dispositivos conectados e visualización das comunicacións entre eles nun mapa ou diagrama. Isto permite verificar a arquitectura (p.ex. ver que só existen comunicacións permitidas entre as zonas definidas) e detectar dispositivos descoñecidos ou non autorizados.
- **Detección de anomalías e intrusións:** supervisar o tráfico en tempo real para identificar patróns sospeitosos, tanto procedentes do exterior (ataques) coma internos (comportamentos fóra do normal dos equipos). Un IDS/IPS especializado en protocolos ICS pode lanzar alertas temperás ante, por exemplo, un comando inesperado nun PLC ou un escaneo de rede na planta.
- **Mecanismos de engano e detección proactiva:** algunhas ferramentas inclúen *honeypots* ou señuelos dentro da rede industrial para atraer posibles atacantes e estudar as súas técnicas sen risco para a operación real. Isto axuda a identificar ataques dirixidos antes de que afecten sistemas de produción, dando máis marxe de manobra á defensa.
- **Bloqueo de tráfico malicioso:** aínda que a función principal é detectar, en ocasións tamén se pode optar por intervir activamente para **cortar comunicacións non autorizadas** ou claramente maliciosas (por exemplo, mediante listas de bloqueos ou segmentación dinámica). Deste xeito redúcese a superficie de ataque en tempo real.
- **Correlación e análise forense de eventos:** integración cos sistemas de rexistro (SIEM/SCADA logging) para correlacionar eventos de distintas fontes e realizar

análises forenses completas tras un incidente. Nun entorno ICS, isto pode significar correlacionar alertas da rede con alarmas do sistema de control de procesos, logrando unha visión unificada do incidente que fortaleza a resposta e as accións de remediación.

A visibilidade OT acada un valor moi superior cando non permanece illada, senón que se integra cos servizos corporativos de seguridade da organización. **A conexión das ferramentas OT de monitorización con SIEM, SOC e sistemas de análise e resposta permite correlacionar alertas de rede industrial, cambios en protocolos ICS, eventos de autenticación, actividade en endpoints e incidentes en servizos corporativos, construíndo unha visión unificada do ataque.** Isto é especialmente **útil en escenarios de converxencia IT/OT, nos que unha intrusión pode iniciarse por correo electrónico, acceso remoto ou credenciais comprometidas e materializarse despois no ámbito industrial.** Para este fin, poden empregarse **plataformas CPS PP (de protección de sistemas ciberfísicos) con solucións especializadas de mercado —como a galega InprOTech Guardian, Nozomi, Claroty, Armis ou Darktrace/OT—** sempre baixo criterios de despregamento non intrusivo, segmentación, mínimo privilexio e compatibilidade co proceso industrial.

Este control busca dotar ao equipo de seguridade industrial dunha **"torre de vixilancia"** dende a que observar en continuo o estado da rede e dos sistemas ICS. Con ela poderán descubrir máis rapidamente actividades anómalas – por exemplo, a presenza dun dispositivo alleo conectado na rede de automatización, ou unha subestación enviando máis datos ca habitual – e **actuar con antelación** antes de que unha ameaza se materialice en impacto real. Ademais, unha boa visibilidade reduce significativamente o tempo e custe de investigar incidentes (por exemplo, para achar a causa raíz dunha parada inesperada nunha planta), algo crítico cando cada minuto de produción perdido conta [62][63].

5.5.4 Control crítico #4: Acceso remoto seguro

O cuarto control aborda un dos vectores de ameaza máis frecuentes na industria moderna: o **acceso remoto** a sistemas OT. Coa dixitalización e a necesidade de interconectar plantas, subministradores e persoal de operación distribuído, **hoxe en día é habitual que as infraestruturas industriais dispoñan de accesos remotos para mantemento, soporte de provedores ou xestión centralizada.** En moitos casos poderían limitarse ou eliminarse algúns accesos, pero na maioría de organizacións industriais **son inevitables** dadas as necesidades do negocio actual.

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

Por suposto, esta conectividade remota trae tamén consigo importantes riscos: desde intrusións vía VPN ou escritorio remoto, ata uso indebido de credenciais por terceiras partes, entre outros. O obxectivo do control #4 é asegurar que todos estes accesos se xestionen coa máxima seguridade posíbel, reducindo a superficie de ataque asociada.

As recomendacións principais inclúen establecer medidas de control de identidade robustas e limitar ao mínimo os privilexios e orixe deses accesos. En particular, **implantar autenticación multi-factor (MFA)** é unha contramedida hoxe indispensable en calquera acceso remoto a entornos ICS. Ademais, **deben cifrarse** tódalas comunicacións remotas (usando VPNs seguras, SSH, TLS, etc.) e **restrinxirse os accesos** só a aqueles usuarios, dispositivos e horarios realmente necesarios, seguindo o principio de mínimo privilexio. Por exemplo, se un provedor ten que dar soporte a un PLC nunha fábrica, poderíaselle habilitar un acceso VPN unicamente durante as xanelas acordadas e só á rede desa planta concreta, nunca á rede completa.

Outras boas prácticas son o emprego de servidores de salto ou pasarelas intermedias para acceder aos equipos OT (evitando conexións directas desde Internet aos controladores), o **rexistro exhaustivo de todas as sesións remotas** (para auditoría e posíbeis forenses), **e a monitorización continua destas sesións** mediante o Control #3 anterior. Cando algún tipo de acceso remoto non sexa compatible cunha medida como MFA – por exemplo, algúns equipos ICS moi antigos que non admitan autenticación robusta – a organización debe establecer **controles compensatorios apropiados**. Isto pode incluír desde illar ese equipo nunha rede moi restrinxida e monitorizada, ata utilizar métodos alternativos de validación manual ou acceso físico supervisado.

En definitiva, o Control #4 procura **pechar a porta de entrada** máis explotada polos adversarios (os accesos remotos) sen sacrificar a operativa.

5.5.5 Control crítico #5: Xestión de vulnerabilidades baseada no risco

O último dos cinco controis céntricos de SANS enfócase na **identificación e tratamento das vulnerabilidades** presentes nos sistemas industriais, empregando un enfoque baseado no risco. A xestión de vulnerabilidades en ICS/OT presenta retos particulares: os sistemas de control industrial adoitan ter ciclos de vida moi longos (décadas), empregan hardware/software propietario que ás veces non se pode actualizar facilmente, e moitas instalacións só poden aplicarlle parches durante paradas programadas pouco frecuentes. Por iso, un programa de vulnerabilidades en OT debe ir

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

máis alá do simple scanning periódico e parcheo inmediato que se aplicaría nun entorno TI convencional.

En primeiro lugar, é necesario **inventariar e avaliar as vulnerabilidades** de forma continua. Cada día anúncianse novas vulnerabilidades que poden afectar a PLCs, SCADAs, sistemas SCADA, protocolos, etc., polo que o labor de threat intelligence e escaneo debe ser permanente. Unha vez identificadas, hai que **priorizalas segundo o risco**: non todas as debilidades nunha rede industrial teñen a mesma criticidade. Debe prestarse atención prioritaria ás vulnerabilidades que realmente **poden poñer en perigo o proceso industrial ou a seguridade** – por exemplo, aquelas que permitirían a un atacante acceder á rede de control ou executar código nos sistemas de automatización – fronte a outras menores ou de difícil explotación. Isto implica coñecer ben o contexto: unha vulnerabilidade crítica nun sistema exposto en DMZ pode ser irrelevante nun PLC illado sen conexión, e viceversa.

Seguidamente, hai que **escoitar as restricións operativas**: en moitos casos non será factible aplicar parches de inmediato porque iso implicaría deter a produción ou invalidar certificacións do fabricante. Cando parchear non sexa posible a curto prazo, o enfoque baseado no risco propón implementar **medidas de mitigación alternativas** para cada vulnerabilidade crítica identificada. Por exemplo, se un determinado controlador ten unha vulnerabilidade sen parche dispoñible, pódese mitigar segmentando ese equipo nunha subrede illada, reforzando a monitorización do seu tráfico (para detectar intentos de explotación) ou limitando estritamente quen pode comunicarse con el. Estas contramedidas reducen o risco ata que se poida aplicar o parche definitivo nunha parada planificada.

En paralelo, debe establecerse **vixilancia continua**: manterse alerta ante novos exploits ou ferramentas de ataque relacionadas coa vulnerabilidade, e monitorizar calquera signo de intento de explotación nos sistemas da planta (aquí de novo xoga un papel o Control #3 de monitorización).

O importante é adoptar unha visión máis ampla que a simple xestión dos parcheos. A *filosofía* deste control é: "non deixemos cabos soltos". En última instancia, o programa de xestión de vulnerabilidades OT debe lograr un equilibrio óptimo entre **seguridade e continuidade operativa**. Trátase de reducir a exposición a ameazas coñecidas – enfocándose nas máis perigosas – sen poñer en risco a estabilidade dos procesos industriais por querer aplicar medidas apresuradas. Este equilibrio é especialmente crucial en infraestruturas críticas, onde calquera cambio debe ser avaliado con lupa. En

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

resumo, o Control #5 asegura que a organización coñeza as súas debilidades técnicas e actúe de forma intelixente sobre elas, priorizando o que realmente importa para evitar incidentes graves.

5.5.6 Complementariedade con outros estándares

Os *SANS ICS 5 Critical Controls* naceron **como complemento pragmático**, non para substituír os marcos normativos existentes. De feito, os autores desenvolveron estes controis conscientes de que existían múltiples estándares e guías de seguridade industrial – por exemplo a familia **ISA/IEC 62443**, ISO/IEC 27001/27002, NIST CSF, entre outros – que ofrecen unha visión moi ampla da ciberseguridade en entornos industriais. Porén, moitos deses estándares foron creados nun momento no que a visibilidade de ameazas ICS era limitada, polo que en gran medida *herdaron controis xenéricos de IT aplicados indirectamente a OT*. O resultado é que ás veces cumprimentar todos os requirimentos dun estándar non garante abordar os riscos máis evidentes fronte ás ameazas OT actuais. Ademais, a maioría destes marcos fan fincapé na **prevención** (ata un 60–95% dos controis son preventivos segundo SANS) e dedicaron menos atención a capacidades de **detección e resposta** específicas de entornos ICS. Isto pode xerar unha falsa sensación de seguridade, se as organizacións invisten moito en prevención pero carecen de visibilidade para decatarse cando esas defensas fallan.

Fronte a esa situación, os cinco controis críticos de SANS veñen **equilibrar e focalizar** os esforzos de seguridade industrial nun conxunto interdependente de medidas preventivas, detectivas e responsivas. Non se trata dun novo estándar que haxa que certificar, senón dun **lexo común** e práctico para comunicar prioridades e comprobar progresos. Son unha especie de "lista de tarefas urxentes" que complementa os requisitos obrigatorios: para sectores non regulados, proporcionan un enfoque claro e programático da seguridade OT; e para aqueles con regulación madura, sinalan en que aspectos **ir máis aló do mínimo normativo** para estar por riba dun adversario que tamén coñece os estándares ao dedillo.

Estes controis, cando se implementan de forma coordinada e priorizada, axudan a construír un programa de seguridade robusto adaptado ós riscos reais do entorno industrial. En lugar de tentar "facelo todo" segundo interminables listaxes de controis, o marco de SANS enfócanos no que realmente importa: estar preparados para responder a incidentes graves, ter arquitecturas resilientes, observar de preto as redes, protexer os accesos máis vulnerables, e xestionar intelixentemente as debilidades técnicas do tecido industrial da nosa terra.

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

6 Guía de implantación práctica

A complexidade do ecosistema normativo en materia de ciberseguridade, obriga ás organizacións industriais a **abordar a súa adaptación dunha forma estruturada, priorizada e realista**. O presente apartado ofrece unha aproximación práctica para iniciar e consolidar este proceso, **centrándose exclusivamente nas seguintes normas descritas ao longo deste documento**: **ISO 27001, ENS, NIS2, RGPD, LPIC, CER, CRA, NIST CSF, CIS Controls, IEC 62443 e SANS ICS Top 5 Controls**.

Trátase dun posible enfoque, pero non é o único válido. Pretende servir como punto de partida para o deseño de follas de ruta personalizadas, que dependerán de múltiples factores como o tamaño da organización, o seu grao de madurez, o sector no que opera ou se está suxeita a obrigas reguladoras específicas. Para iso, **analizaranse as características comparadas das distintas normas**, e **proporanse itinerarios progresivos de implantación e adaptación**, con orientacións sobre o seu **orde de magnitude a nivel de esforzo temporal (baixo, medio, alto)**, sen entrar en estimacións ríxidas que poidan ser irreais ou inexactas, ao seren fortemente dependentes da situación particular.

O obxectivo é dotar ás organizacións dun **marco orientativo adaptado ao contexto da ciberseguridade industrial**, facilitando a toma de decisións estratéxicas e operativas para o cumprimento e mellora continua nesta materia.

6.1 Cadro comparativo de normas

Para facilitar a toma de decisións en materia de cumprimento normativo e fortalecemento da seguridade, preséntase a continuación unha táboa comparativa das **principais normas e marcos analizados previamente**, enfocadas á protección de sistemas de información e datos persoais, infraestruturas críticas, e/ou contornos industriais OT/ICS, segundo o caso.

A táboa analiza cada norma segundo os seguintes criterios:

- **Norma / Marco**: identificación da norma ou conxunto normativo.
- **Obrigatoriedade**: se é **legalmente obrigatoria**, depende de **contexto**, ou é **voluntaria**.
- **Sector ou ámbito**: ámbito ao que aplica, como administración pública, infraestruturas críticas, industria ou calquera organización.

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

- **Certificable**: se é posible obter unha **certificación oficial externa** trala auditoría.
- **Enfoque principal**: obxectivo ou área de acción principal da norma.
- **Nivel de detalle**: grao de **especificidade técnica** (alto, medio ou básico).

Norma / Marco	Obrigatorio/a	Sector ou ámbito	Certificable	Enfoque principal	Nivel de detalle
ISO/IEC 27001	Voluntaria, pero esixida en contratos ou auditorías	Calquera sector	Si	Sistema de xestión da seguridade da información (SXSI)	Medio
ENS (Esquema Nacional de Seguridade)	Obrigatoria para sector público e provedores TIC	Administración pública e contratistas tecnolóxicos	Si	Requisitos mínimos de seguridade da información no sector público	Alto
NIS2	Obrigatoria para entidades designadas	Sectores esenciais e importantes en UE	Non	Ciberseguridade en entidades críticas, obrigas de xestión de risco e notificación	Medio-alto
RGPD	Obrigatoria por lexislación da UE	Calquera entidade que trate datos persoais	Non	Protección de datos persoais e dereitos dixitais	Medio
LPIC	Obrigatoria	Entidades críticas físicas	Non	Protección e resiliencia de entidades críticas físicas	Medio
CER (Directiva UE 2022/2557)	Obrigatoria (directiva europea en transposición)	Infraestruturas físicas esenciais	Non	Avaliación de risco físico, resiliencia e coordinación nacional	Medio

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

CRA (Cyber Resilience Act)	Obrigatoria desde 2026-2027	Fabricantes e importadores de HW/SW con elementos dixitais	Parcialmente	Requisitos de ciberseguridade en produtos con elementos dixitais	Alto
NIST CSF 2.0	Voluntaria	Calquera organización	Non	Marco de xestión de riscos de ciberseguridade	Medio
CIS Controls v8.1	Voluntaria	Calquera organización, aplicable a OT/ICS	Non	Medidas técnicas priorizadas para protección fronte a ameazas comúns	Medio
IEC 62443	Voluntaria, recomendada en industria e contratos	Entornos OT/ICS industriais	Parcialmente	Ciberseguridade industrial, defensa en profundidade en contornos ICS	Alto
SANS ICS Top 5 Controls	Voluntaria	Entornos industriais e infraestruturas críticas	Non	Controis mínimos esenciais para seguridade en ICS/OT	Básico-medio

Táboa comparativa de normas e marcos normativos de ciberseguridade. Fonte: elaboración propia (2026)

Esta análise permite comparar de maneira rápida o **alcance, rigor técnico e aplicabilidade práctica** das normas, facilitando a súa selección en función das características e madurez de cada organización.

6.2 Identificación do punto de partida

As necesidades normativas e estratéxicas varían notablemente en función do **tamaño da organización, sector de actividade** e do **tipo de cliente ao que se dirixe**. Neste apartado analízase como debería afrontarse a adaptación normativa en empresas industriais, atendendo a diferentes casuísticas. De novo, trátase de una aproximación de moi alto nivel, que haberá que revisar ou adaptar en cada escenario.

Advertir que antes de decidir que norma abordar primeiro e con que nivel de ambición, é conveniente partir dun diagnóstico inicial estruturado. Este diagnóstico p**ode adoptar a forma dunha avaliación de madurez, dunha revisión de controis existentes ou dunha análise GAP fronte ós marcos de referencia**

seleccionados. O seu valor reside en ofrecer unha fotografía obxectiva da situación de partida, identificando fortalezas, carencias, controis xa implantados, evidencias dispoñibles e ámbitos con maior exposición ao risco. **Sobre esta base, a organización pode construír unha folla de ruta máis realista a nivel de tempos e esforzos, priorizada e defendible**, evitando tanto implantacións excesivamente teóricas como investimentos desordenados sen criterio metodolóxico.

O primeiro que cabe subliñar, é que independentemente do tamaño, hai certas normas ou regulamentos que son de obrigado cumprimento se caemos dentro do ámbito de aplicación, como son:

- **RGPD**, se os procesos industriais involucran datos persoais.
- **LPIC (e CER)**, se se tratase de infraestruturas críticas (e físicas).
- **ENS**, en certos modelos B2G (relación coa administración pública ou subministrador da mesma).
- **NIS2**, en caso de tratarse de unha entidade esencial e importante segundo a definición da Directiva.
- **CRA,** se a entidade manufactura dispositivos IoT e/ou produtos electrónicos.

Con respecto ao resto de normas, de maneira xeral o que se pode tamén dicir é que a **ISO 27001** cun alcance máis ou menos ambicioso debería ser o punto de partida recomendable para calquera organización independentemente do seu nivel de madurez. Por outra banda, no mundo anglosaxón utilízase de xeito equivalente aínda que non o sexa, o marco **NIST CSF**.

En caso de requirir **ENS**, certificarse previamente en **ISO 27001** aplana bastante o camiño de cara ao cumprimento. E tendo ENS, pasar a adherirse á **Directiva NIS2**, a falta de aterrar o anteproxecto de Lei en curso, é un GAP relativamente pequeno, á luz do que se comentou da equivalencia NIS2 <> ENS proposta polo CCN.

Se falamos por último dos marcos máis técnicos, os **CIS controls** permiten acadar un nivel de seguridade razoable a nivel técnico cun esforzo máis ou menos acotado, pero deixando certamente algo de lado a parte de goberno e xestión da seguridade (controis organizativos e procedimentais), polo que nunca recomendaríamos implementalos por separado.

E en caso de apostar xa claramente por securizar o entorno ICS/OT, habendo previamente resolto a cuestión do SXSI, apostaríamos en función das capacidades técnicas, presupostarias e de recursos, polos **SANS ICS Top 5 Controls**, ou **IEC 62443** (de menor a maior grao de esixencia), e tendo en conta que en determinados ámbitos ou

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

relación con cliente, a segunda pode ser obrigatoria. E dende logo, é a que denota un maior grao de compromiso coa protección destas infraestruturas.

6.2.1 Segundo o tipo de empresa e necesidades

A adaptación e cumprimento das distintas normativas e estándares de ciberseguridade debe considerar o **perfil da empresa segundo as súas características estruturais e operativas**. Para iso, realizaremos unha clasificación segundo o **tamaño organizativo** (pequena, mediana ou grande empresa) e segundo o **tipo de cliente obxectivo principal**, tendo en conta se opera **con administración pública (modelo B2G)**, **con outras empresas (modelo B2B)**, **co consumidor final (modelo B2C)** e se traballa con **clientes internacionais**, sexan **europeos** (suxeitos a regulacións comúns como RGPD ou NIS2) ou **anglosaxóns** (que poden dar prioridade a marcos como NIST ou SANS).

Perfilaremos a continuación un retrato robot de entidades por tamaño, centrándonos na actividade industrial. Téñanse en conta en calquera caso, as salvedades apuntadas no apartado previo.

- As **pequenas empresas industriais**, adoitan contar con recursos limitados en ciberseguridade, sen persoal dedicado en exclusiva e con dependencias de provedores externos. En moitos casos, a dixitalización é incipiente e a presenza de sistemas conectados a internet é reducida, pero non por iso exenta de riscos. Cómpre priorizar marcos lixeiros e progresivos como os **CIS Controls**, apoiándose nunha adaptación parcial a estándares máis ambiciosos como **ISO 27001** (sempre recomendable para contar un SXSI en base a boas prácticas internacionais como base) ou **SANS ICS Top 5 Controls** no caso de organización mais ambiciosas.
- As **empresas medianas industriais**, comezan a incorporar arquitecturas OT máis complexas, interconectadas con redes TI en moitos casos, cun número crecente de activos industriais e exposición á cadea de subministración. Este tipo de empresas pode estar xa afectado por obrigas legais como **NIS2**, ou **CRA se manufacturan produtos electrónicos**, e interesa tamén preparar o terreo para certificacións voluntarias (ISO, IEC). Ademais, se traballan con administracións públicas ou en sectores regulados, veranse afectadas por marcos como **ENS, CER** ou **LPIC**.
- As **grandes empresas industriais**, normalmente contan cun sistema maduro de gobernanza e seguridade, equipos especializados e capacidades de xestión integral de riscos. Están afectadas por **moitas regulacións normativas**

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

vixentes e adoitan implementar esquemas certificados como **ISO 27001**, **IEC 62443** ou estruturas de madurez como **NIST CSF**. Tamén se espera delas que dispoñan de **plans de resiliencia e resposta a incidentes**, especialmente se prestan servizos esenciais ou críticos **(LPIC, CER)**.

No relativo ao **cliente obxectivo**:

- Se a empresa opera con **administración pública**, debe considerar de forma prioritaria o **ENS**, e se presta servizos ou produtos relacionados coa seguridade física, tamén **LPIC** e **CER**.
- En caso de traballar con **outras empresas (modelo B2B)**, especialmente en sectores como enerxía, transporte ou saúde, o grao de esixencia normativa é alto, sendo habitual a esixencia contractual de **certificacións (ISO, IEC, CRA)** ou **avaliacións de conformidade co NIST CSF**.
- As empresas **que venden ao consumidor final (modelo B2C)** deben ter especial coidado co cumprimento do **RGPD** e da **CRA**, no caso de ofrecer produtos con compoñentes dixitais conectados.
- Se a empresa traballa con **clientes internacionais europeos**, as directivas como **ISO, NIS2**, **RGPD**, **CRA** e **CER** deben ser referencia principal. Pola contra, se os clientes son **anglosaxóns**, pode existir unha preferencia clara por **NIST CSF**, **CIS Controls** ou marcos ou **ISA,** como **IEC 62443**.

6.3 Estimación de esforzos

A adaptación efectiva aos distintos marcos e normativas de ciberseguridade require unha análise previa do **esforzo estimado** que pode supoñer a súa implantación para cada organización. Este esforzo **varía significativamente** en función de múltiples factores: o grao de madurez da empresa, a súa estrutura interna, o seu sector, o seu tamaño, o nivel de dixitalización e, sobre todo, o **nivel de compromiso e intensidade de aplicación** que se pretenda alcanzar.

Así, o esforzo pode oscilar entre **poucos meses de traballo ben enfocado**, en casos de cumprimento mínimo e con apoio externo, ata **proxectos progresivos de longo percorrido** que se estenden ao longo de **2 ou 3 anos ou máis**, especialmente cando se aspira a integrar as normas de forma transversal e completa na cultura da organización.

Para **representar este esforzo de forma práctica**, utilizaremos unha **clasificación cualitativa** en tres niveis orientativos:

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

- **Baixo** → Esforzo relativamente reducido, asumible con recursos limitados nun prazo estimado de ata 12 meses.
- **Medio** → Require planificación, coordinación e maior carga de traballo (entre 12 e 24 meses).
- **Alto** → Implica despregue organizativo amplo, integración progresiva e varios ciclos de mellora (24–36 meses ou máis).

Esta estimación realizarase tendo en conta as seguintes **dimensións clave** para cada normativa ou marco:

- **Obrigatoriedade**: se o seu cumprimento é esixido por normativa ou contrato, ou é voluntario.
- **Certificabilidade**: se implica auditorías ou emisión formal de certificación por terceiro acreditado.
- **Enfoque predominante**: legal, técnico, organizativo ou híbrido.
- **Impacto organizativo**: grao de transformación nos procesos, responsabilidades, recursos e cultura interna.
- **Complexidade de implantación**: número e dificultade dos controis, dependencia de provedores, tecnoloxía e grao de detalle esixido.

Dito todo o anterior, tómese a seguinte táboa como unha referencia de orde de magnitude grosa.

Norma / Marco	Esforzo estimado	Certificable	Enfoque principal	Impacto organizativo	Notas relevantes
ISO/IEC 27001	Medio	Si	Técnico + xestión	Alto	Implica un SXSI completo
ENS	Medio / Alto	Si	Técnico + xestión	Medio/Alto	Esixido en contratos públicos. Ter ISO previamente acurta plazos. Plazos dependen do nivel ENS a acadar
NIS2	Medio / Alto	Non (directa)	Legal + técnico + xestión	Alto	Altamente regulado para entidades medianas e grandes. Ter ENS axiliza.

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

RGPD	Medio	Non	Legal	Medio	Revisión continua de procesos e datos, máis AIPDs nalgúns casos
LPIC	Medio	Non	Legal + técnico	Medio/Alto	Require planificación de plans e designación de responsables
CER	Alto	Non	Legal + técnico + físico	Alto	Para entidades críticas, esixe plans e informes
CRA	Medio / Alto	Si (produto)	Legal + produto (técnico)	Alto (para fabricantes)	Aplicable a hardware/software con conectividade
NIST CSF	Medio	Non	Técnico + xestión	Medio	Referencia flexible, non obrigatoria
CIS Controls	Baixo / Medio	Non	Técnico práctico	Baixo / Medio	Ideal para pequenas e medianas empresas
IEC 62443	Alto	Si (parcial)	Técnico + xestión OT	Alto	Alto nivel técnico e segmentado por rol
SANS ICS Top 5	Medio	Non	Técnico + xestión OT	Baixo / Medio	Ideal para primeira capa de defensa OT. Flexible

Estimación de esforzo de implantación de marcos normativos. Fonte: elaboración propia (2026)

En calquera caso, unha vez se comprenden os diferentes marcos normativos, regulacións e boas prácticas, o ideal é **contactar con algún proveedor de servicios de adecuamento normativo ou ciberseguridade técnica, de cara a definir tanto un alcance como unha planificación temporal máis axustada á casuística concreta** e necesidades da organización.

Para este fin, pódese facer uso do **magnífico recurso que proporciona o Mapa de capacidades dixitais de Galicia, auspiciado pola Xunta de Galicia (Gaiastech)** [68].

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

7 Conclusións

A presente **Guía normativa de ciberseguridade industrial** foi elaborada co obxectivo de proporcionar ás organizacións públicas e privadas de Galicia unha **panorámica ampla e clara** para **comprender e abordar as obrigas normativas e as boas prácticas en materia de ciberseguridade en entornos industriais e de Tecnoloxía Operacional (OT)**.

A guía aborda de maneira sintética o **marco normativo nacional, con especial atención ao Esquema Nacional de Seguridade (ENS)** e á súa evolución recente, **así como á normativa de protección de infraestruturas críticas e á lexislación en materia de protección de datos persoais**. Complementariamente, analízase o **marco normativo europeo**, destacando a **Directiva NIS2, o Regulamento CER** e outras iniciativas que introducen novas obrigas para entidades industriais e operadores de servizos esenciais.

No ámbito dos **marcos e estándares internacionais**, a guía integra e relaciona estándares amplamente recoñecidos como **ISO/IEC 27001**, **NIST CSF, IEC 62443** e outros marcos de referencia, explicando o seu alcance, complementariedade e aplicabilidade práctica en entornos industriais. **Este exercicio de síntese permite ás entidades destinatarias identificar con maior claridade que estándares lles resultan de aplicación ou interese, e como poden aliñalos de maneira coherente.**

Finalmente, a guía incorpora unha **orientación práctica á implantación**, achegando criterios, exemplos e recomendacións que **facilitan a adopción dos marcos ou alomenos, o establecemento dunha folla de ruta, axeitada ás obrigas, ao nivel de risco e mais ó grao de madurez de cada organización.**

A análise realizada ó longo da Guía permite extraer unha **serie de conclusións relevantes que afectan directamente ás entidades galegas** que operan en sectores industriais ou xestionan infraestruturas e servizos críticos.

En primeiro lugar, queda patente que a **seguridade da información no eido industrial deixou de ser unha cuestión puramente técnica** para converterse nun elemento estratéxico de xestión do risco, con implicacións legais, operativas e reputacionais. O incremento das esixencias regulamentarias, especialmente a partir da NIS2, obriga ás organizacións a adoptar enfoques máis estruturados e documentados.

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

En segundo lugar, a guía evidencia que **non existe unha única norma ou estándar que resolva de forma illada todas as obrigas**, senón que é necesario un enfoque integrado que combine regulación, estándares internacionais e boas prácticas. Neste contexto, marcos como a IEC 62443 xogan un papel central ao proporcionar un modelo específico para entornos OT, complementando enfoques máis xerais como ISO/IEC 27001.

Outra conclusión clave é a importancia de adoptar un **enfoque baseado no risco e na madurez**, evitando aproximacións uniformes ou excesivamente prescritivas. A guía promove unha implantación progresiva, adaptada á realidade de cada organización, o que resulta especialmente relevante para as PEMEs industriais galegas, con recursos máis limitados.

Así mesmo, ponse de relevo a necesidade de **clarificar roles e responsabilidades** entre operadores, integradores, fabricantes e administracións públicas. **A ciberseguridade industrial debe entenderse como unha responsabilidade compartida ao longo de toda a cadea de valor**, na que cada actor desempeña un papel específico e complementario.

Dende unha perspectiva territorial, a guía pretende contribuir a **fortalecer o ecosistema galego de ciberseguridade industrial**, ofrecendo unha referencia común que en caso de aproveitamento, mellorará a preparación fronte a auditorías e inspeccións, reforzando así a confianza na protección de procesos e servizos críticos.

Finalmente, esta Guía Normativa **non debe entenderse como un documento estático, senón como unha base evolutiva que deberá adaptarse á progresiva evolución das ameazas e aos cambios regulatorios todavía por chegar.** En futuras edicións da guía podería plantexarse incorporar plantillas detalladas para a adherencia normativa, ou modelos de madurez para o seu desenvolvemento progresivo e faseado dentro dunha organización.

Do que non cabe dúbida, é de que **a comprensión e aplicación efectiva dos marcos propostos, permitirá avanzar cara a modelos máis resilientes, seguros e competitivos, contribuíndo á protección do tecido industrial galego e ao desenvolvemento sostible da súa economía.**

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

Bibliografía

[1] Observatorio de Ciberseguridade Industrial de Galicia (2025). *Informe de Ciberalertas - I*. Recuperado de https://ciberseguridadegalicia.gal/es

[2] Observatorio de Ciberseguridade Industrial de Galicia (2025). *Informe de Intelixencia de Ameazas - I*. Recuperado de https://ciberseguridadegalicia.gal/es

[3] U.S. Department of Energy (2022). *Cybersecurity Capability Maturity Model (C2M2)*. Recuperado de https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

[4] Cybersecurity and Infrastructure Security Agency (CISA) (2021). *Cyber Security Evaluation Tool (CSET)*. Recuperado de https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset

[5] Boletín Oficial do Estado (2010). *Real Decreto 3/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade no ámbito da Administración Electrónica.* Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1331

[6] Boletín Oficial do Estado (2022). *Real Decreto 311/2022, do 3 de maio, polo que se regula o Esquema Nacional de Seguridade.* Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191

[7] Parlamento Europeo e Consello da UE (2019). *Regulamento (UE) 2019/881 relativo a ENISA e á certificación da ciberseguridade da información e as comunicacións.* Recuperado de https://eur-lex.europa.eu/legal-content/GL/TXT/?uri=CELEX%3A32019R0881

[8] Parlamento Europeo e Consello da UE (2016). *Directiva (UE) 2016/1148 relativa a medidas para garantir un nivel común elevado de seguridade das redes e sistemas de información na Unión (Directiva NIS).* Recuperado de https://eur-lex.europa.eu/legal-content/GL/TXT/?uri=CELEX%3A32016L1148

[9] Goberno de España (2017). *Estratexia de Seguridade Nacional 2017.* Recuperado de https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/presidenciadelgobierno/documents/2017-1824_estrategia_de_seguridad_nacional_esn_doble_pag.pdf

[10] Goberno de España (2019). *Estratexia Nacional de Ciberseguridade, publicada mediante Orde PCI/487/2019, do 26 de abril.* Recuperado de

https://www.famp.es/export/sites/famp/.galleries/documentos-lab-eficiencia-energetica/Estrategia-Nacional-de-Ciberseguridad-2019-Interactivo_0.pdf

[11] Goberno de España (2022). *Aprobación do Plan Nacional de Ciberseguridade.* Recuperado de https://www.mpr.gob.es/prencom/notas/paginas/2022/290322-ciberseguridad.aspx

[12] Centro Criptolóxico Nacional (n.d.). *ENS – Infografías.* Recuperado de https://ens.ccn.cni.es/es/que-es-el-ens/infografias

[13] Centro Criptolóxico Nacional (2022). *Infografía 03 – ENS 2022: Novedades.* Recuperado de https://ens.ccn.cni.es/es/docman/documentos-publicos/19-infografia-03-ens-2022-novedades/file

[14] Centro Criptolóxico Nacional (2022). Infografía 04 – ENS 2010 vs ENS 2022: Diferencias e evolución. Recuperado de https://ens.ccn.cni.es/es/docman/documentos-publicos/20-infografia-04-ens-2010-ens-2022-diferencias-y-evolucion/file

[15] Portal da Administración Electrónica (n.d.). E*squema Nacional de Seguridade.* Recuperado de https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad.html#.ZFE_aHZByP0

[16] 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

[17] Centro Criptolóxico Nacional (2017). *Guía CCN-STIC-804 – Implantación do ENS.* Recuperado de https://www.ccn-cert.cni.es/es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file?format=html

[18] Boletín Oficial do Estado (2018). *Real Decreto-ley 12/2018, de 7 de setembro, de seguridade das redes e sistemas de información.* Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257

[19] EUR-Lex (2016). *Directiva NIS.* Recuperado de https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[20] Boletín Oficial do Estado (2011). *Lei 8/2011, do 28 de abril, pola que se establecen medidas para a protección das infraestruturas críticas.* Recuperado de: https://www.boe.es/eli/es/l/2011/04/28/8/con

[21] Boletín Oficial do Estado (2011). *Real Decreto 704/2011, do 20 de maio, polo que se aproba o Regulamento de protección das infraestruturas críticas.* Recuperado de: https://www.boe.es/eli/es/rd/2011/05/20/704/con

[22] LISA Institute. *Infraestruturas críticas: definición, plans, riscos, ameazas e lexislación.* Recuperado de: https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas

[23] Departamento de Seguridade Nacional (2019). *Estratexia Nacional de Ciberseguridade 2019.* Recuperado de: https://www.dsn.gob.es/sites/default/files/documents/Estrategia%20Nacional%20de%20Ciberseguridad%202019.pdf

[24] Departamento de Seguridade Nacional (2019). *Estratexia Nacional de Ciberseguridade 2019 (Versión interactiva).* Recuperado de: https://www.dsn.gob.es/sites/default/files/2025-04/Estrategia%20Nacional%20de%20Ciberseguridad%202019%20-%20%20Interactivo_0%20%281%29_0.pdf

[25] Ministerio da Presidencia, Relacións coas Cortes e Memoria Democrática (2022). *Nota de prensa: Aprobación do Plan Nacional de Ciberseguridade.* Recuperado de: https://www.mpr.gob.es/prencom/notas/paginas/2022/290322-ciberseguridad.aspx

[26] Boletín Oficial do Estado (2025). *PJC/448/2025, do 6 de mayo, polo que se aproban actuación para complementar as recollidas no Plan Nacional de Ciberseguridade*. Recuperado de: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2025-9088

[27] Unión Europea (2016). *Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello, de 27 de abril de 2016, relativo á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos (Regulamento Xeral de Protección de Datos - RXPD)*. Recuperado de https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04

[28] Boletín Oficial do Estado (2018). *Lei Orgánica 3/2018, do 5 de decembro, de protección de datos persoais e garantía dos dereitos dixitais (LOPD-GDD)*. Recuperado de https://www.boe.es/eli/es/lo/2018/12/05/3/con

[29] Axencia Española de Protección de Datos (AEPD) (1993). *Sitio web oficial da Axencia Española de Protección de Datos*. Recuperado de https://www.aepd.es

[30] Boletín Oficial do Estado (1995). *Directiva 95/46/CE, relativa á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos*. https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678

[31] Organización Internacional de Normalización (ISO) (2018). *ISO 31000:2018. Xestión do risco. Principios e directrices*. Recuperado de https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

[32] Centro Criptológico Nacional (CCN) (2022). *MAGERIT – Metodoloxía de Análise e Xestión de Riscos da Administración TIC. Versión 3.0*. Recuperado de https://pilar.ccn-cert.cni.es/docman/documentos/1-magerit-v3-libro-i-metodo/file

[33] Agència Catalana de Protecció de Dades (APDCAT) (2022). *Guía práctica de avaliación de impacto relativa á protección de datos*. Recuperado de https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guia-EIPD_castellano.pdf

[34] Axencia Española de Protección de Datos (AEPD) (2022). *Xestión do risco e avaliación de impacto en tratamentos de datos persoais*. Recuperado de https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

[35] Comisión Europea (n.d.). *Que son os datos persoais*. Recuperado de https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es

[36] Congreso dos Deputados (2003). *Constitución Española. Dereitos e liberdades*. Recuperado de https://app.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=18&tipo=2

[37] Axencia Española de Protección de Datos (AEPD) (1993). *Guías de interese*. Recuperado de https://www.aepd.es/es/guias-y-herramientas/guias

[38] Axencia Española de Protección de Datos (AEPD) (1993). *Ferramentas de interese*. Recuperado de https://www.aepd.es/es/guias-y-herramientas/herramientas

[39] EUR-Lex (2022). *Directiva NIS2*. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32022L2555

[40] INCIBE (2022). *Aprobación da Directiva NIS2*. Recuperado de https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/aprobacion-directiva-nis2

[41] INCIBE (2024). *FAQs NIS2*. Recuperado de https://www.incibe.es/incibe-cert/sectores-estrategicos/FAQNIS2

[42] INCIBE (2024). *Entidades esenciais e importantes no ámbito de NIS2.* Recuperado de https://www.incibe.es/sites/default/files/2024-08/Entidades_NIS2_ACC.pdf

[43] INCIBE (2023). *Guía para empresas sobre NIS2*. Recuperado de https://www.incibe.es/empresas/tematicas/cumpliendo-NIS2

[44] CCN-CERT (2024). *Guía CCN-STIC 892: PCE-NIS2*. Recuperado de https://www.ccn-cert.cni.es/es/seguridad-al-dia/novedades-ccn-cert/12945-el-ccn-publica-un-nuevo-perfil-de-cumplimiento-especifico-para-organizaciones-en-el-ambito-de-aplicacion-de-la-directiva-nis2.html

[45] Ministerio do Interior (2025). *Anteproxecto de Lei de coordinación e gobernanza da ciberseguridade*. Recuperado de https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/participacion-ciudadana/Participacion-publica-en-proyectos-normativos/Audiencia-e-informacion-publica/01_2025_Anteproyecto_ley_coordinacion_gobernanza_ciberseguridad.pdf

[46] Parlamento Europeo e Consello (2024). *Regulamento (UE) 2024/1680 do Parlamento Europeo e do Consello, do 12 de marzo de 2024, relativo aos requisitos de ciberseguridade para produtos con elementos dixitais (Lei de Ciberresiliencia)*. Recuperado de https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81720

[47] Parlamento Europeo e Consello (2022). *Directiva (UE) 2022/2557 sobre a resiliencia das entidades críticas*. Recuperado de https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81965

[48] Comisión Europea (2022). *Portal oficial da Directiva CER sobre resiliencia das entidades críticas*. Recuperado de https://www.critical-entities-resilience-directive.com/

[49] Ministerio do Interior (2025). *Anteproxecto de Lei de protección e resiliencia de entidades críticas*. Recuperado de

https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/participacion-ciudadana/Participacion-publica-en-proyectos-normativos/Audiencia-e-informacion-publica/08_2025_Anteproyecto_ley_proteccion_resiliencia_entidades_criticas.pdf

[50] ISO/IEC (2022). *ISO/IEC 27001:2022. Tecnoloxía da información — Técnicas de seguridade — Sistemas de xestión da seguridade da información — Requisitos*. Recuperado de https://www.iso.org/standard/27001

[51] ISO/IEC (2022). *ISO/IEC 27002:2022. Seguridade da información, ciberseguridade e protección da privacidade — Controis de seguridade da información*. Recuperado de https://www.iso.org/standard/75652.html

[52] ISO (2019). *ISO 22301:2019. Seguridade e resiliencia — Sistemas de xestión da continuidade do negocio — Requisitos*. Recuperado de https://www.iso.org/standard/75106.html

[53] NIST (2024). *O NIST publica a versión 2.0 do seu marco histórico de ciberseguridade*. Recuperado de https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

[54] NIST (2024). *NIST Cybersecurity Framework, versión 2.0*. Recuperado de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[55] Center for Internet Security (2000). *Sitio web oficial do Center for Internet Security*. Recuperado de: https://www.cisecurity.org/

[56] Center for Internet Security (2024). *CIS Critical Security Controls List*. Recuperado de: https://www.cisecurity.org/controls/cis-controls-list

[57] Center for Internet Security (n.d.). *CIS Benchmarks*. Recuperado de: https://www.cisecurity.org/cis-benchmarks

[58] SANS Institute (2024). *Sitio web oficial do SANS Institute*. Recuperado de: https://www.sans.org/

[59] SANS Institute (2022). *Whitepapers sobre os 5 controis críticos ICS*. Recuperado de: https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

[60] MIT Technology Review (n.d.). *Así se propaga Triton, o malware que ameaza a industria mundial*. Recuperado de: https://technologyreview.es/article/asi-se-propaga-triton-el-malware-que-amenaza-la-industria-mundial/

[61] ESET – WeLiveSecurity (2016). *Ciberataque causou cortes de luz en Ucraína*. Recuperado de: https://www.welivesecurity.com/la-es/2016/03/02/ciberataque-causo-cortes-de-luz-ucrania/

[62] ENISA (2016). *The cost of incidents affecting Critical Information Infrastructures (CII)*. Recuperado de: https://www.enisa.europa.eu/sites/default/files/publications/The%20cost%20of%20incidents%20affecting%20CIIs.pdf

[63] CISA (2020). *Cost of Cyber Incidents Study*. Recuperado de: https://www.cisa.gov/sites/default/files/2024-10/CISA-OCE%20Cost%20of%20Cyber%20Incidents%20Study_508.pdf

[64] ISA – International Society of Automation (n.d.). *Industrial Automation and Control Systems Security*. Recuperado de: https://www.isa.org/

[65] IEC – International Electrotechnical Commission (n.d.). *International Standards and Conformity Assessment for Electrotechnology*. Recuperado de: https://www.iec.ch/

[66] 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

[67] CCI – Centro de Ciberseguridad Industrial (n.d.). *Aplicando o estándar IEC 62443 nun proxecto de dixitalización industrial*. Recuperado de: https://www.cci-es.org/wp-content/uploads/Aplicando-el-estandar-IEC62443-en-un-proyecto-de-digitalizacion-industrial-v3.pptx.pdf

[68] Xunta de Galicia – GAIASTECH. (2024). *Mapa de capacidades dixitais de Galicia*. Recuperado de: https://gaiastech.xunta.gal/es/mapa-de-capacidades-digitales-de-galicia

CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridade Industrial
Guía Normativa de Ciberseguridade Industrial

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