CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridad Industrial

Guía Normativa de Ciberseguridad Industrial

Marzo 2026

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

Edita: Xunta de Galicia

Agencia para la Modernización Tecnológica de Galicia (AMTEGA)

Lugar: Santiago de Compostela

Año: 2026

Índice

1 Introducción

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

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

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

--

La **Guía normativa de ciberseguridad industrial** tiene como objetivo servir como una referencia estructurada y práctica para las organizaciones públicas y privadas de Galicia que operan en entornos industriales, especialmente aquellas que disponen de sistemas o procesos basados en **Tecnología Operacional (OT)**. Su propósito principal es **identificar e interpretar la normativa aplicable**, así como ofrecer **pautas claras para su cumplimiento y mejora continua**.

El informe está pensado para **facilitar la comprensión del complejo marco normativo vigente**, promoviendo no sólo el cumplimiento legal, sino también una evolución progresiva hacia **modelos de excelencia y madurez en seguridad** de los activos y procesos industriales frente a las amenazas digitales.

Va dirigido tanto a **administraciones públicas gallegas** —sobre todo aquellas que gestionan infraestructuras críticas o servicios esenciales— como a **empresas privadas industriales**, con especial atención a las **pequeñas y medianas empresas (PyMEs)** que operan en sectores estratégicos o críticos para Galicia. Estas organizaciones, a

menudo con una capacidad más limitada para abordar la carga regulatoria, encontrarán en esta guía una ayuda clara y aplicable.

Hay que destacar que la **variedad normativa según el sector industrial puede ser muy amplia**, afectando de manera desigual a cada subsector productivo. Por este motivo, el enfoque del informe se centra en **aspectos normativos troncales y buenas prácticas comunes**, que serán de interés o aplicabilidad para la **práctica totalidad de la audiencia destinataria, independientemente del sector de actividad**.

En su elaboración se empleó una metodología basada en el análisis documental de la legislación nacional y europea (**ENS**, **NIS2**, **CER**, **RGPD**, etc.), la revisión de estándares internacionales reconocidos (**NIST CSF**, **ISO/IEC 27001**, **IEC 62443**, **CIS Controls**, entre otros), y la consulta de publicaciones técnicas de organismos como **ENISA**, **INCIBE**, **CCN-CERT**, **CISA** o el **Centro de Ciberseguridad Industrial (CCI)**.

El contenido se estructura en torno a un **enfoque dual**: por un lado, se presenta una **descripción a alto nivel de diferentes normas y obligaciones asociadas** que deben cumplir las organizaciones industriales para adherirse a marcos de referencia nacionales, europeos e internacionales; y por otro, se proporciona una **guía de implantación práctica para la adopción de dichas buenas prácticas y estándares reconocidos**.

Ambas perspectivas se complementan para ofrecer una **guía comprensible, aplicable y útil**, pensada para reforzar la **resiliencia del tejido industrial gallego** en un contexto normativo y tecnológico en constante evolución.

2 Visión general de la ciberseguridad industrial

La ciberseguridad industrial presenta características distintivas frente a la seguridad de la información tradicional (IT), tanto desde una perspectiva técnica como organizativa.

- Mientras que en entornos **IT** la prioridad principal suele ser **la confidencialidad de los datos**, los sistemas **OT (Tecnología Operacional)** ponen el foco en **la disponibilidad y continuidad de la operación**, ya que cualquier interrupción puede tener **impactos directos sobre procesos industriales, seguridad física o servicios críticos para la ciudadanía**.
- Las diferencias técnicas se manifiestan en múltiples capas. **Los dispositivos OT (como PLCs, sensores industriales o SCADA) no fueron diseñados inicialmente con criterios de ciberseguridad**, sino para funcionar de forma estable, en tiempo real y durante décadas. Las comunicaciones se basan en protocolos industriales como **Modbus, DNP3 o Profinet**, muchos de ellos sin cifrado ni autenticación. Por el contrario, los sistemas IT operan con estándares de seguridad más consolidados (TLS, HTTPS, autenticación fuerte, etc.). Además, las redes OT tienden a estar segregadas o compartimentadas por razones operativas, aunque **su progresiva integración con redes corporativas (convergencia IT/OT) introduce nuevas superficies de ataque.**
- A nivel organizativo, muchas empresas industriales gallegas presentan **estructuras separadas entre los equipos de operación (OT)** y los de **tecnología (IT)**. Ello se traduce en **organigramas disjuntos, procesos de toma de decisiones diferenciados, y frecuentemente, en prioridades enfrentadas**: mientras el personal de operación prioriza la continuidad de la producción, el de IT se enfoca en la seguridad de la red y de los datos. Esta dicotomía complica la adopción de enfoques unificados de ciberseguridad y requiere una **mayor cultura compartida y gobernanza transversal**.

Hay que recordar que muchas de las instalaciones industriales gallegas tienen impacto directo sobre **infraestructuras críticas y servicios esenciales** (agua, energía, alimentación, transporte), y por tanto, cualquier incidente de ciberseguridad puede tener consecuencias **económicas, sociales e incluso para la seguridad de la población**. Esta realidad coloca a la ciberseguridad OT como un asunto estratégico que trasciende el plano tecnológico.

Amenazas actuales a los sistemas industriales

Según los informes del Observatorio de Ciberseguridad Industrial de **Ciberalertas** [1] e **Inteligencia de amenazas** [2], algunos de los principales vectores de riesgo para los sistemas industriales en Galicia y en el contexto europeo son:

- **Ransomware dirigido**: con afectación a redes OT, paralización de cadenas de producción y chantaje a operadores industriales.
- **APT (Advanced Persistent Threats)**: grupos organizados, frecuentemente vinculados a estados, que buscan persistencia y espionaje industrial prolongado.
- **Ataques a sistemas ICS/SCADA**: mediante explotación de vulnerabilidades en componentes críticos de automatización industrial.
- **Accesos remotos inseguros**: el uso creciente de acceso remoto para mantenimiento técnico expone muchas instalaciones a vulnerabilidades sin parchear.

El análisis de estos informes evidencia que **los ataques a los sistemas industriales no son hipotéticos, sino una realidad creciente**, que requiere **capacidad de detección, respuesta y mitigación adaptadas al mundo OT**, y no simplemente trasladadas desde el ámbito IT.

Cumplimiento frente a madurez: un salto de visión

Teniendo en cuenta el panorama anterior, las organizaciones deben actuar. Muchas entidades abordan la ciberseguridad como un **objetivo de cumplimiento mínimo**, orientado a pasar auditorías o evitar sanciones. Este enfoque, aunque mal menor, resulta **insuficiente para garantizar la resiliencia frente a amenazas sofisticadas**.

Cumplir una norma (como el **ENS** o la **Directiva NIS2**) en una amplia mayoría de escenarios equivale a **marcar la casilla**, pero no implica necesariamente tener capacidad para **anticiparse, adaptarse y mejorar continuamente**. Por ello, estas guías invitan a ir un paso más allá, incorporando en futuras ediciones modelos de madurez reconocidos internacionalmente como:

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

Estos modelos permiten **evaluar el grado real de capacidad de una organización**, identificar debilidades estructurales y diseñar una hoja de ruta realista de mejora continua basada en el ciclo **PDCA (Plan-Do-Check-Act)**.

3 Normativa nacional

El marco legal español en materia de ciberseguridad ha experimentado una evolución constante en los últimos años, con el objetivo de dar respuesta a los riesgos crecientes derivados de la digitalización de la sociedad y de la industria. La legislación nacional se articula alrededor de un conjunto de normas que afectan tanto **al sector público** como al **privado**, con una especial atención a las **infraestructuras críticas**, los **servicios esenciales** y los **sistemas de información de alto impacto**.

En esta sección revisaremos los principales textos legales y reguladores que conforman esta arquitectura normativa:

- En primer lugar, el **Esquema Nacional de Seguridad (ENS)**, que establece los principios básicos y requisitos mínimos que deben cumplir las Administraciones Públicas y sus proveedores tecnológicos para garantizar la seguridad de los sistemas, datos y servicios. El ENS sirve, además, como base para muchas de las obligaciones que posteriormente se extienden al sector privado.

- Analizaremos también **la transposición de la Directiva NIS** al ordenamiento jurídico español, que se materializa **en el Real Decreto Ley 12/2018** sobre seguridad de redes y sistemas de información, y en su desarrollo reglamentario a través del **Real Decreto 43/2021**. Estas disposiciones afectan especialmente a **los operadores de servicios esenciales y** a los **proveedores de servicios digitales**, y recogen medidas de prevención, gestión de riesgos, notificación de incidentes y supervisión.

  ** Esta normativa sigue vigente hasta que se publique la nueva legislación que adapte NIS2 en España.* ***Derogará o modificará parcialmente*** *sus preceptos en función de cómo se redacte la nueva norma que implemente NIS2, la cual se encuentra actualmente en proceso de elaboración (la competencia es del Ministerio de Asuntos Económicos y Transformación Digital).*

- Por último, completaremos el panorama con la referencia a otras normas nacionales relevantes para el ámbito industrial, como **la Ley de Protección de Infraestructuras Críticas (Ley PIC)**, la **Estrategia Nacional de Ciberseguridad y la Ley Orgánica 3/2018 (LOPD-GDD)**, especialmente en su vínculo con los sistemas de control industrial y la protección de datos personales que puedan coexistir en los procesos de negocio.

Este conjunto de normas representa el **núcleo del cumplimiento legal básico en materia de ciberseguridad en España de manera general,** y resulta esencial para cualquier organización industrial que trabaje con determinadas entidades, y/o aspire a garantizar su conformidad, proteger sus activos digitales e integrarse en un ecosistema seguro a nivel nacional y europeo.

A continuación, se presentan los diferentes corpus normativos con sus características principales a alto nivel, para referencia del lector.

3.1 Esquema Nacional de Seguridad

En esta sección analizaremos con mayor profundidad el **Esquema Nacional de Seguridad (ENS)**, al tratarse de la **normativa nacional de referencia** en materia de ciberseguridad, especialmente en el ámbito del sector público y de las entidades que cilaboran con él. Es certificable, con una validez de dos años.

El ENS constituye además la base sobre la que **el Centro Criptológico Nacional (CCN)** articula el **cumplimiento de la Directiva europea NIS2** en España, sirviendo como instrumento clave para garantizar un nivel común y elevado de seguridad de las redes y sistemas de información, tal y como exige el marco normativo supranacional mencionado.

3.1.1 Introducción

El **Esquema Nacional de Seguridad (ENS)** fue creado al amparo de la Ley 11/2007 y regulado inicialmente por el **RD 3/2010** [5], posteriormente modificado por el **RD 951/2015**, y finalmente sustituido por el **RD 311/2022** [6], que actualiza el marco a las nuevas necesidades tecnológicas y normativas.

Su objetivo principal **es garantizar la confianza en el uso de los medios electrónicos** mediante políticas y medidas que aseguren **la seguridad de la información, sistemas, comunicaciones y servicios electrónicos**, facilitando así el ejercicio de derechos y deberes de la ciudadanía y de las administraciones.

Abarca tanto **controles técnicos como organizativos**, y aunque es compatible con la norma **ISO/IEC 27001** que se verá posteriormente en la sección de marcos y estándares internacionales, difiere en su **ámbito de aplicación y enfoque**. Las entidades certificadas en ISO 27001 tendrán facilitado el proceso de adaptación al ENS.

El Esquema se basa en seis **principios fundamentales** que orientan su implantación en cualquier organización:

1. **Seguridad como proceso integral**: la seguridad debe abarcar todos los elementos de la organización (personas, tecnología, procesos, estructura). Se excluye cualquier enfoque puntual o parcial.
2. **Gestión basada en riesgos**: el análisis y tratamiento de riesgos debe ser continuo, actualizado y proporcional a la naturaleza de la información y los servicios que se protegen.
3. **Prevención, detección, respuesta y conservación:** es imprescindible anticiparse a las amenazas, detectarlas a tiempo, responder eficazmente ante incidentes y garantizar la conservación de la información y la continuidad de los servicios.
4. **Defensa en profundidad**: los sistemas deben contar con múltiples capas de seguridad (organizativas, físicas y lógicas) para minimizar el impacto de cualquier fallo o incidente.
5. **Vigilancia continua y revisión periódica**: es necesario supervisar continuamente la seguridad, detectar anomalías y actualizar las medidas ante nuevos riesgos o vulnerabilidades.
6. **Diferenciación de responsabilidades**: deben estar claramente definidos los roles de responsabilidad sobre la información, servicios, seguridad y sistemas, sin solapamientos y con mecanismos de coordinación.

Estos principios conforman la base estructural de un sistema de seguridad robusto, orientado a la mejora continua y adaptado a las necesidades de cada organización.

Para determinar el impacto de un incidente de seguridad y establecer la **categoría del sistema**, el ENS tiene en cuenta cinco **dimensiones de seguridad** clave:

- **Disponibilidad (D)**: garantizar que los activos estén accesibles cuando los necesiten las entidades autorizadas.
- **Autenticidad (A)**: asegurar que una entidad es quien dice ser o que el origen de los datos es confiable.
- **Integridad (I)**: verificar que la información no ha sido modificada de forma no autorizada.
- **Confidencialidad (C)**: impedir que la información sea accesible o divulgada a personas o sistemas no autorizados.

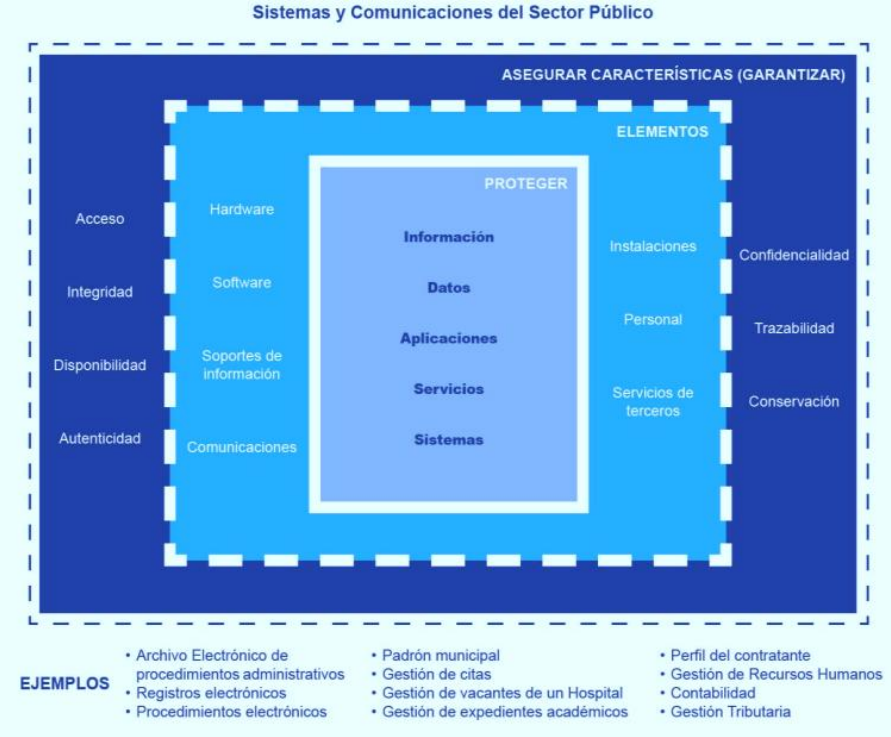
- **Trazabilidad (T)**: permitir atribuir las acciones realizadas a una entidad concreta.

Estas dimensiones son la base para **evaluar y categorizar los sistemas y activos** según su nivel de sensibilidad y los requisitos de seguridad que deben cumplir.

3.1.2 Categorización de activos y sistemas

Según el ENS, los **activos de alto nivel** se clasifican en tres grandes bloques: **información, servicios y sistemas de información**.

- La **información** representa los datos con significado que sustentan los procesos administrativos. Las dimensiones clave para evaluar este activo son la **confidencialidad y la integridad**.
- Los **servicios** permiten el tratamiento de la información y su dimensión prioritaria es la **disponibilidad**.
- Los **sistemas de información** son el conjunto de aplicaciones e infraestructuras que ofrecen capacidades para gestionar tanto información como servicios.



Activos y sistemas a proteger en la administración pública. Fuente: CCN (2022)

A cada uno de estos elementos se le asigna un **nivel de seguridad** (bajo, medio o alto), en función del grado de impacto que podría tener un incidente que afecte a alguna de las

dimensiones de seguridad (D, A, I, C, T). El **nivel más alto asignado a una dimensión determinará la categoría final del sistema**.

Las categorías de los sistemas pueden ser:

- **Básica**, si el nivel más alto de las dimensiones es bajo.
- **Media**, si el nivel más alto es medio.
- **Alta**, si alguna dimensión alcanza el nivel alto.

Los criterios de impacto se presentan en términos de:

- Cumplimiento de objetivos.
- Protección de activos.
- Prestación de servicios.
- Cumplimiento legal.
- Protección de los derechos de las personas.

Cada categoría implica diferentes niveles de exigencia en los controles de seguridad. Las organizaciones pueden optar voluntariamente por **aplicar una categoría superior** a la que le correspondería según su análisis de riesgos e impacto. Esta categorización condiciona los **requisitos mínimos y las medidas de seguridad obligatorias** según el ENS.

3.1.3 Requisitos de seguridad

El **Esquema Nacional de Seguridad (ENS)** establece un conjunto de requisitos mínimos que deben cumplir las organizaciones para garantizar la seguridad de sus sistemas de información. Estos requisitos se derivan de los principios básicos del ENS y se desarrollan en medidas concretas, organizadas alfabéticamente de la siguiente forma:

a) Organización e implantación del proceso de seguridad: Define los roles y responsabilidades, incluyendo los responsables de información, servicio, seguridad y sistema. Es obligatorio evitar relaciones jerárquicas entre el responsable de seguridad y el del sistema. En los servicios externalizados, debe designarse un **POC (Punto de Contacto)** de seguridad.

b) Análisis y gestión de riesgos: La gestión del riesgo debe ser continua, basada en metodologías reconocidas y justificada en función de la categoría del sistema y de la naturaleza de los servicios y datos tratados.

c) Gestión de personal: El personal (interno y externo) debe ser formado, informado y supervisado en el uso seguro de los sistemas, aplicando normas y procedimientos aprobados.

d) Profesionalidad: La seguridad debe ser gestionada por profesionales cualificados a lo largo de todo el ciclo de vida del sistema. Los proveedores deben demostrar madurez y cualificación técnica.

e) Autorización y control de accesos: El acceso a los sistemas debe estar limitado a entidades autorizadas, con funciones y permisos definidos.

f) Protección de las instalaciones: Los sistemas y su infraestructura deben situarse en áreas controladas y contar con medidas físicas de protección acordes a los riesgos.

g) Adquisición de productos y contratación de servicios de seguridad: Sólo deben emplearse productos y servicios con funcionalidades de seguridad certificadas, adecuadas a la categoría del sistema.

h) Mínimo privilegio: Los sistemas deben ser configurados para que los usuarios dispongan sólo de los permisos imprescindibles, desactivando funciones innecesarias.

i) Integridad y actualización del sistema: Todo cambio o incorporación debe estar autorizado. La seguridad debe ajustarse mediante evaluación y monitorización constantes.

j) Protección de la información almacenada y en tránsito: La información, especialmente en dispositivos móviles o medios extraíbles, debe estar protegida. Deben aplicarse procedimientos de conservación y recuperación de datos.

k) Prevención ante otros sistemas interconectados: Debe protegerse el perímetro de los sistemas conectados a redes públicas u otros entornos, minimizando riesgos derivados de la interconexión.

l) Registro de actividad y detección de código dañino: Es obligatorio registrar las acciones de los usuarios, detectar comportamientos anómalos y prevenir ataques mediante análisis de tráfico y contenido.

m) Gestión de incidentes de seguridad: Las organizaciones deben contar con procedimientos para detectar, clasificar, analizar, comunicar y resolver incidentes, registrando actuaciones para mejora continua.

n) Continuidad de la actividad: Deben disponer de copias de seguridad y planes de continuidad operativa ante fallos o interrupciones.

o) Mejora continua del proceso de seguridad: El sistema de seguridad debe actualizarse y perfeccionarse de forma periódica, basándose en estándares reconocidos.

p) Cumplimiento de requisitos mínimos: Las medidas adoptadas deben ajustarse a la categoría del sistema y al análisis de riesgos. Su implementación se refleja en la **Declaración de Aplicabilidad**, pudiendo incluir medidas adicionales o compensatorias.

q) Infraestructuras y servicios comunes: El uso de servicios compartidos entre administraciones facilita el cumplimiento de los requisitos del ENS.

r) Perfiles de cumplimiento específicos y acreditación de entidades: Permite adaptar el ENS a sectores concretos mediante perfiles definidos por el CCN y esquemas de validación de entidades y productos.

Estas medidas constituyen el núcleo operativo del ENS y deben ser aplicadas de forma proporcional a la categoría de los sistemas (básica, media o alta) y a la sensibilidad de la información tratada.

3.1.4 Novedades ENS 2022

La actualización del RD del ENS en 2022 busca alinear el marco normativo español con los estándares europeos vigentes y reforzar su eficacia frente a las nuevas amenazas en ciberseguridad. Entre los textos europeos de referencia figuran:

- Reglamento (UE) 2019/881 sobre ciberseguridad y ENISA [7]
- Directiva (UE) 2016/1148 – Directiva NIS [8]

La revisión del ENS forma parte del Marco Estratégico Nacional definido por la **Estrategia de Seguridad Nacional de 2017** [9], la **Estrategia Nacional de Ciberseguridad 2019** [10], y el **Plan Nacional de Ciberseguridad** [11] aprobado en marzo de 2022, que prevé cerca de 150 actuaciones.

La reforma persigue tres grandes objetivos:

1. **Alineación normativa y clarificación del ámbito de aplicación**, adaptando el ENS al marco legal vigente y simplificando sus mandatos.
2. **Flexibilización mediante la figura del perfil de cumplimiento específico**, que permite aplicar con eficiencia los requisitos del ENS según la naturaleza o

sector de la organización. Definido en el Anexo IV del RD, este perfil es un conjunto de medidas de seguridad —incluidas o no en el Anexo II— determinadas tras un análisis de riesgos y validadas por el CCN.

3. **Adaptación a las tendencias de ciberseguridad**, con refuerzo de la vigilancia continua, revisión de los principios, requisitos mínimos y medidas.

Entre las principales **novedades técnicas y organizativas** destacan:

- Inclusión expresa de los **sistemas de información clasificada** en el ámbito de aplicación.
- Obligatoriedad de **vigilancia continua mediante sistemas de detección de amenazas**.
- Ampliación de las políticas de seguridad para abordar el **riesgo en el tratamiento de datos personales**.
- Designación de un **punto de contacto (POC)** como responsable de seguridad de la organización.
- Regulación detallada de la **gestión de incidentes**, incluyendo **la notificación obligatoria al CCN-CERT**, también para entidades privadas que trabajen con la Administración.
- **Revisión anual obligatoria** de la categoría de los sistemas.
- Nuevo sistema de **codificación de los requisitos de seguridad**, basado en requisitos y refuerzos.

Los recursos más relevantes para profundizar en estos cambios son:

- Infografías generales sobre el ENS [12].
- Resumen gráfico de las novedades del ENS 2022 [13].
- Comparativa ENS 2010 vs ENS 2022 [14].
- Proceso de adecuación al ENS en el portal de la administración electrónica [15].

Adicionalmente, en la web de Gobernanza de la Ciberseguridad Nacional del CCN-CERT hay un magnífico recurso llamado **ENS navegable, que de manera cómoda y visual permite revisar por en detalle cada una de las medidas de seguridad de aplicación del Real Decreto [16].**

Todos los controles de seguridad evaluables se encuentran recogidos en la guía **CCN-STIC-804** [17], de implantación del ENS. En total, son **74 medidas de seguridad** (organizativas, operacionales y de protección). En general, cabe destacar que **las guías de la serie 800 del CCN** amplían el contenido del Real Decreto con información complementaria de utilidad para llevar a la práctica la implementación del ENS.

3.2 RD 12/2018 (Directiva NIS)

La **Directiva (UE) 2016/1148** [18] del Parlamento Europeo y del Consejo, del 6 de julio de 2016, conocida como **NIS**, relativa a medidas para garantizar un **nivel elevado común de seguridad en redes y sistemas de información**, se transpuso al ordenamiento jurídico español mediante **el Real Decreto-ley 12/2018, de 7 de septiembre** [19], sobre seguridad de las redes y sistemas de información.

Aunque la directiva mencionada fue sustituida por la NIS2 que se verá en el apartado siguiente de Normativa europea, la traemos a colación por su relevancia e impacto, dado que muchas de las medidas que se proponen en la segunda versión, estaban presentes ya en la regulación original.

Finalidad:

Esta Directiva establecía medidas con el objetivo de **conseguir un nivel elevado común de seguridad en** las redes y sistemas de información de la Unión Europea, a fin de **mejorar el funcionamiento del mercado interior**. Para ello, obligaba a los Estados miembros a:

- **adoptar una estrategia nacional de seguridad de** las redes y sistemas de información;
- crear un **Grupo de Cooperación** para apoyar y facilitar la cooperación estratégica y el intercambio de información;
- establecer una **red de CSIRT** (equipos de respuesta a incidentes de seguridad informática);
- imponer **requisitos de seguridad y notificación** tanto para **operadores de servicios esenciales** como para **proveedores de servicios digitales**;
- y obligar a que cada Estado miembro **designe autoridades nacionales competentes**, **puntos de contacto únicos y CSIRT** con funciones específicas en este ámbito.

El **RD 12/2018** establece un **doble objetivo**:

a. **Regular la seguridad de las redes y sistemas de información** que soportan servicios esenciales y servicios digitales,

b. **Establecer un sistema de notificación de incidentes**, y un marco institucional de coordinación entre autoridades competentes y con los órganos europeos correspondientes.

En cuanto a los **CSIRT de referencia en España,** son equipos de respuesta a incidentes de seguridad informática, asignados según la tipología de entidad:

- El **CCN-CERT**, del Centro Criptológico Nacional, para entidades del sector público conforme a la Ley 40/2015.
- El **INCIBE-CERT**, para entidades privadas no incluidas en la anterior, operado conjuntamente con el **CNPIC** en casos que afecten a operadores críticos.
- El **ESPDEF-CERT**, del Ministerio de Defensa, que coopera con los anteriores especialmente cuando los incidentes afectan a la defensa nacional.

El **INCIBE-CERT** también actúa como equipo de referencia para la ciudadanía y otras entidades privadas no incluidas en los casos anteriores.

Estos CSIRT se coordinarán entre sí y con los demás equipos nacionales e internacionales. En casos de especial gravedad, el **CCN-CERT** asumirá la **coordinación nacional de la respuesta técnica**. Además, el CCN ejercerá como **punto de enlace para la cooperación transfronteriza** de los CSIRT de las Administraciones Públicas.

Principales novedades introducidas por la Directiva NIS:

- Necesidad de una **Estrategia Nacional de Seguridad de** las redes y sistemas de información.
- Designación de una o varias **autoridades competentes y** de un **punto único de contacto** para garantizar la cooperación transfronteriza.
- Designación de **CSIRT en red** con recursos e infraestructura adecuada.
- Creación **de un Grupo de cooperación** formado por representantes de los Estados miembros, Comisión Europea y ENISA.
- Establecimiento de requisitos y medidas en materia de seguridad y notificación para **operadores de servicios esenciales y proveedores de servicios digitales**.

- Introducción de un **régimen sancionador efectivo y disuasorio**.

En relación con los **operadores de servicios esenciales**, deberán aplicar medidas técnicas y organizativas adecuadas y proporcionadas para gestionar riesgos, garantizar la continuidad del servicio y notificar incidentes significativos a las autoridades competentes o al CSIRT. Dichas autoridades podrán exigir documentación, realizar auditorías o solicitar pruebas de la implantación de las políticas de seguridad, e impartir **instrucciones vinculantes** para corregir deficiencias. Asimismo, colaborarán con las autoridades de protección de datos en los casos de violación de datos personales.

En cuanto a los **proveedores de servicios digitales**, deberán aplicar medidas técnicas y organizativas para garantizar la seguridad de las redes y sistemas que emplean para prestar servicios en la UE. Tendrán que notificar los incidentes que **tengan un impacto significativo**, teniendo en cuenta parámetros como el número de usuarios afectados, la duración del incidente, su extensión geográfica, la perturbación en el funcionamiento del servicio y el impacto económico y social. Esta obligación no se aplicará a **microempresas y pequeñas empresas**, según la Recomendación 2003/361/CE.

Las autoridades competentes podrán supervisar el cumplimiento mediante actividades a posteriori y exigir información o medidas correctoras. En caso de que el proveedor de servicios digitales esté establecido fuera de la UE, deberá designar un **representante legal en un** Estado miembro donde preste servicios. La jurisdicción se aplicará en función de la ubicación de este representante.

Este marco, desarrollado a través del RD 12/2018, constituye la primera transposición de la Directiva NIS, que será posteriormente sustituida por la **Directiva NIS2** y su Reglamento correspondiente. El decreto sigue **formalmente vigente**, pero se encuentra en **proceso de revisión y sustitución** para adaptarse a los requisitos de la **nueva Directiva (UE) 2022/2555 (NIS2)**.

3.3 Ley de Protección de Infraestructuras Críticas

La **Ley 8/2011, de protección de infraestructuras críticas** [20], junto con el **Real Decreto 704/2011** [21] y otras disposiciones posteriores, establece el marco normativo por el que se regulan las **obligaciones especiales** que deben asumir tanto las Administraciones **públicas** como los **operadores de infraestructuras críticas (IICC)**.

Se declara **infraestructura crítica** aquella *"infraestructura estratégica cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales"*.

Se define **servicio esencial** como aquel *"servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de la ciudadanía, o el funcionamiento eficaz de las instituciones del Estado y de las Administraciones Públicas"*.

La información sobre la totalidad de las infraestructuras críticas está clasificada como secreta, debido a la alta sensibilidad que representa para la **seguridad nacional**. **España se estima que cuenta con más de 3.500 infraestructuras críticas reconocidas**.

Los sectores en los que se engloban entidades pertenecientes a sectores críticos de actividad son los siguientes [22]:

Lista de áreas estratégicas con infraestructuras críticas. Fuente: Lisa Institute (n.d.)

A continuación, relación de entidades afectadas de forma más exhaustiva, siguiendo el orden del gráfico anterior:

- **Financiero**: Mercados regulados, pago y compensación.

- **Administración**: Altas Instituciones del Estado, defensa, interior, partidos políticos, servicios de emergencia.
- **Agua**: Depósitos, embalses, tratamiento y distribución.
- **Alimentación**: Centros de almacenamiento y distribución.
- **Energía**: Eléctrico, hidrocarburos, gas.
- **Espacio**: Centros de control y telecomunicaciones.
- **Nuclear**: Producción y almacenamiento radiológico.
- **Químico**: Sustancias químicas, armas y explosivos.
- **Investigación**: Laboratorios y almacenamientos.
- **Salud**: Biológico, asistencia hospitalaria, vacunas y laboratorios.
- **TIC (Tecnologías de la Información y Comunicación)**: Telefonía, radio, televisión.
- **Transporte**: Aeropuertos, puertos, ferrocarril y carreteras.

La normativa exige **elaborar y mantener actualizados**, los siguientes documentos:

- **Plan Nacional de Protección de Infraestructuras Críticas (PNPIC)**: Elaborado por el Parlamento y el Gobierno, este plan es el marco estratégico superior de la protección de las IICC en España. Define la política nacional en este ámbito y sirve de base para el desarrollo normativo posterior, como la Ley 8/2011 (LPIC) y el Real Decreto 704/2011 (RDPIC).
- **Planes sectoriales**: Son responsabilidad del Grupo de Trabajo de Protección de Infraestructuras Críticas (GTPIC), que debe elaborar una lista de operadores críticos por sector. El plazo establecido para su elaboración es de 12 meses desde la entrada en vigor del Real Decreto. Incluyen un análisis sectorial de riesgos.
- **Planes de Seguridad del Operador (PSO)**: Cada operador crítico designado debe identificar sus infraestructuras críticas y redactar este plan estratégico. El PSO define las políticas generales de seguridad aplicables al conjunto de instalaciones o sistemas gestionados por el operador. El plazo para su presentación es de 6 meses desde su designación oficial.

- **Planes de Protección Específicos (PPE)**: Por cada infraestructura crítica identificada, el operador debe desarrollar un PPE que detalle las medidas concretas —tanto físicas como lógicas— para garantizar su seguridad integral. Estos planes deben elaborarse en un plazo de 4 meses tras la aprobación del correspondiente PSO.
- **Planes de Apoyo Operativo**: Son elaborados por las Fuerzas y Cuerpos de Seguridad del Estado (FCS) o por las Delegaciones del Gobierno. Establecen la respuesta operativa ante posibles incidentes que afecten a infraestructuras críticas. Deben estar listos en un plazo de 4 meses tras la aprobación del PPE correspondiente.

Este modelo piramidal de planificación asegura una cobertura progresiva y coordinada de la seguridad de las infraestructuras críticas, combinando responsabilidades del sector público y privado. Todo plan debe estar coordinado con las autoridades competentes y contribuyen a garantizar **la resiliencia y continuidad de los servicios esenciales**, reforzando la seguridad tanto en el campo físico como en el digital.

3.4 Estrategia y Planes Nacionales

La creciente dependencia digital de la sociedad y la economía ha convertido a la ciberseguridad en una prioridad estratégica. En España, este compromiso se articula a través de una **Estrategia Nacional de Ciberseguridad (ENC)** que, desde 2019, sirve de guía para proteger los intereses nacionales en el ciberespacio.

3.4.1 Estrategia Nacional de Ciberseguridad 2019

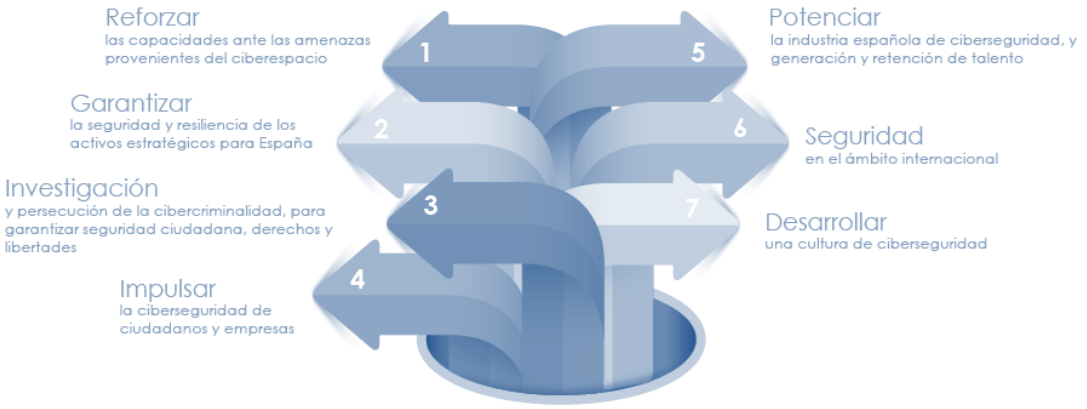
La **ENC 2019** fue aprobada por el Consejo de Seguridad Nacional el 12 de abril de 2019 y publicada por Orden PCI/487/2019, de 26 de abril. Actualiza la versión de 2013, y establece un **marco integral de actuación** para afrontar los riesgos y amenazas en el ciberespacio, tanto en el sector público como en el privado. Su propósito es reforzar la resiliencia del país frente a los riesgos emergentes, fomentar la confianza digital y asegurar la protección de los derechos y libertades de la ciudadanía [23][24].

Amenazas con fines maliciosos en el ciberespacio. Fuente: Departamento de Seguridad Nacional (2019)

La Estrategia se estructura en torno a un **objetivo general**, cinco **objetivos específicos y siete líneas de acción**, que se traducen en **65 medidas concretas**:

- **Objetivo general:** Garantizar la seguridad y resiliencia del ciberespacio nacional como parte esencial de la seguridad nacional.
- **Objetivos específicos:**
    1. Fortalecer la seguridad y resiliencia de las redes y sistemas del sector público y de los servicios esenciales.
    2. Uso seguro y fiable del ciberespacio frente a usos ilícitos o maliciosos.
    3. Fomentar la ciberseguridad de la ciudadanía y del tejido empresarial.
    4. Promover la cultura de la ciberseguridad y la formación de profesionales, potenciando capacidades humanas y tecnológicas.
    5. Reforzar la ciberseguridad en el ámbito internacional y la participación activa en foros multilaterales.

Las **siete líneas de actuación de la ENC 2019**, se recogen en la siguiente gráfica:



Líneas de actuación de la ENC. Fuente: Foro Nacional de Ciberseguridad (2019)

3.4.2 Plan Nacional de Ciberseguridad

Para desarrollar y aplicar la Estrategia, **el Consejo de Ministros aprobó el 29 de marzo de 2022 el Plan Nacional de Ciberseguridad (PNC)**. Este plan traduce los principios estratégicos de la ENC en un **conjunto de actuaciones concretas**, con horizonte a tres años, y está coordinado por el Departamento de Seguridad Nacional de la Presidencia del Gobierno [25].

El Plan contempla **147 actuaciones estructuradas en cinco ejes estratégicos**:

1. Desarrollo normativo y refuerzo institucional.
2. Protección de las capacidades tecnológicas nacionales.
3. Respuesta eficaz ante ciberincidentes.
4. Impulso a la ciberseguridad para la ciudadanía, PyMEs y sectores estratégicos.
5. Coordinación internacional y cooperación.

Incluye además la creación del **Foro Nacional de Ciberseguridad** (derivado de la cuarta línea de actuación de la ENC), que promueve el diálogo entre Administraciones, sector privado, academia y sociedad civil, y fomenta la implementación de las medidas del Plan.

Medidas adicionales al Plan Nacional de Ciberseguridad

Al amparo de la **Orden Ministerial PJC/448/2025, de 6 de mayo de 2025**, se aprobó una ampliación de las actuaciones contempladas en el PNC [26], con el objetivo de **adaptar la respuesta del Estado a los nuevos riesgos y amenazas en el ciberespacio**. La motivación principal de esta ampliación radica en una serie de factores:

- **Incremento de los ciberataques** impulsados tanto por Estados como por grupos de ciberdelincuentes, con objetivos como el robo de datos, sabotajes, espionaje y disrupción de servicios críticos.
- **Transformación del escenario digital**, que diluye las fronteras entre el ámbito civil y militar, y aumenta la superficie de exposición a ataques.
- **Emergencia de tecnologías disruptivas** como la inteligencia artificial y la computación cuántica, que elevan el nivel de sofisticación de los ataques y obligan a anticipar la transición a **criptografía postcuántica**.
- **Evolución del contexto geopolítico**, con mayor tensión en materia de defensa y seguridad del ciberespacio.
- **Obligaciones normativas recientes**, tanto nacionales (ENS, ENS 5G, RD 7/2022 sobre redes 5G) como europeas (Directiva NIS 2, Reglamentos de Ciberresiliencia y Cibersolidaridad).

Estas actuaciones buscan mejorar las capacidades nacionales en todo el ciclo de ciberseguridad y ciberdefensa: **conciencia situacional, prevención, detección, protección, respuesta, recuperación y disuasión**, con un enfoque coordinado y sostenido en el tiempo.

Las medidas están alineadas con el **Plan de Recuperación, Transformación y Resiliencia**, especialmente con su Componente 11 (Modernización de la Administración General del Estado), y estarán sometidas al marco del Real Decreto-ley 36/2020 relacionado.

3.5 Protección de datos personales

3.5.1 Introducción

En los procesos industriales, **cuando se manejan datos personales de empleados, clientes o proveedores**, resulta esencial tener en cuenta la legislación vigente sobre protección de datos. Esta normativa garantiza derechos fundamentales e impone obligaciones específicas a las organizaciones.

A continuación, se analizan los aspectos más relevantes de la legislación española y europea en materia de **protección de datos personales**.

La protección de las personas físicas en relación con el tratamiento de datos personales es un **derecho fundamental**, reconocido en el artículo **18.4 de la Constitución**

Española, en **el artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea** y **en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea**.

Este derecho surgió a partir de las **directrices de la OCDE en los años 80** y constituye un derecho **independiente del derecho a la intimidad**, tanto personal como familiar. En conjunto con el derecho a la privacidad y a la inviolabilidad de las comunicaciones, la protección de datos proporciona a la ciudadanía **defensa frente al uso no autorizado de su información personal por terceros**.

> ➢ ***Datos personales*** *(definición de la Comisión Europea en el marco del* ***Reglamento General de Protección de Datos – GDPR*** *[27]): Se declara dato personal* ***cualquier información relativa a una persona física viva identificada o identificable****. Incluso informaciones diversas que, combinadas, puedan llevar a la identificación de una persona concreta, también se consideran datos personales.*

Los datos personales que fueran **anonimizados, cifrados o seudonimizados**, pero que puedan utilizarse para **volver a identificar a la persona**, siguen estando protegidos por el GDPR. Sólo cuando **la anonimización sea irreversible**, la información deja de ser considerada dato personal.

El **reglamento** es **tecnológicamente neutro**: protege los datos con independencia de la tecnología utilizada, ya sea tratamiento automatizado o manual, siempre que se organicen según criterios predeterminados (por ejemplo, alfabéticamente). **Tampoco importa el soporte**, si los datos están en un sistema informático, en una grabación de videovigilancia o en papel, seguirán sometidos a los requisitos.

La normativa legal no sólo prevé el uso indebido por parte de terceros, **sino que otorga al titular de los datos (interesado) el control sobre los mismos**, a través de mecanismos como:

- La **necesidad de consentimiento expreso** para el tratamiento.
- El **deber de información** sobre el uso y destino de los datos.
- El ejercicio de los **derechos ARCOPOL**: acceso, rectificación, cancelación (supresión), oposición, portabilidad, olvido y limitación del tratamiento.

La legislación europea es **mucho más proteccionista** que la de otras regiones, como los **Estados Unidos**, donde no existe un marco normativo común sino leyes sectoriales, sin autoridad de control ni exigencia de consentimiento previo.

Las normativas de referencia en España en este campo son:

- La **Constitución Española**
- **La Ley Orgánica 3/2018**, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (**LOPD-GDD**) [28]
- Las **instrucciones de la AEPD** (Agencia Española de Protección de Datos) [29]

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

- El **Reglamento (UE) 2016/679**, conocido como **Reglamento General de Protección de Datos (RGPD)** o **GDPR** en sus siglas en inglés, **en vigor desde abril de 2016 y de aplicación obligatoria desde mayo de 2018**. Sustituye a la antigua **Directiva 95/46/CE**, ya derogada [30]. Su objetivo **es eliminar las asimetrías normativas** entre países miembros y **armonizar los derechos y obligaciones en materia de protección de datos personales**.

Es relevante destacar el carácter disuasorio del régimen sancionador del RGPD para garantizar el cumplimiento efectivo de la normativa, promoviendo una cultura de responsabilidad proactiva en las entidades que tratan datos personales. Se podrán imponer sanciones que pueden alcanzar hasta **20 millones de euros o el 4 % de la facturación anual global de la entidad para incidentes muy graves**, prevaleciendo el importe más elevado.

3.5.2 Licitud del tratamiento de datos personales

El **interesado** es aquella **persona física cuya identidad puede derivarse directa o indirectamente de datos que van a ser objeto de tratamiento** (es decir, **datos personales**).

Según **el Reglamento General de Protección de Datos (RGPD) y en consecuencia la LOPD-GDD**, sólo existen determinados escenarios en los que el **tratamiento de datos personales de interesados es lícito**:

1. **Seudonimización de los datos personales**: cuando los datos han sido procesados de tal manera que **no son atribuibles directamente a la persona, sino** que requieren información adicional, protegida por medidas técnicas y organizativas adecuadas.
2. **Consentimiento del interesado**: la **manifestación de voluntad libre, específica, informada e inequívoca** por parte del interesado, expresada

mediante una declaración o una acción afirmativa clara, que indique su aceptación del tratamiento de datos personales para **uno o varios fines concretos**.

3. **Necesidad contractual**: cuando el tratamiento resulta necesario para la **ejecución de un contrato** en el que el interesado es parte, o para aplicar medidas precontractuales solicitadas por éste.
4. **Obligación legal**: cuando el tratamiento es necesario para **el cumplimiento de una obligación legal aplicable al responsable del tratamiento**.
5. **Intereses vitales**: cuando el tratamiento es necesario para **proteger intereses vitales del interesado o de otra persona física**.
6. **Interés o función públicos**: cuando el tratamiento es necesario para el **cumplimiento de una misión realizada en interés público o en** el ejercicio de **poderes públicos conferidos al responsable del tratamiento**.
7. **Interés legítimo**: cuando el tratamiento es necesario para **la satisfacción de intereses legítimos del responsable del tratamiento o de un tercero**, siempre que **no prevalezcan los intereses o derechos fundamentales del interesado**, especialmente cuando éste sea un menor. **Esta base legal no será aplicable al tratamiento realizado por autoridades públicas en el ejercicio de sus funciones.**

En relación con la **oferta directa a menores de servicios de la sociedad de la información**, se establece que:

- El tratamiento de datos personales de un niño será lícito cuando **éste tenga al menos 16 años**.
- Si el niño **es menor de 16 años**, el tratamiento **sólo será lícito si el consentimiento es otorgado o autorizado por los titulares de la patria potestad o tutela**, y sólo en la medida en que se otorgue dicho consentimiento.

Los Estados miembros pueden establecer por ley una edad inferior, **sin que ésta pueda ser inferior a los 13 años**. En el caso de España, **la Ley Orgánica 3/2018 establece la edad mínima en 14 años**.

3.5.3 Derechos de los interesados

A continuación, se resumen a muy alto nivel los **derechos ARCOPOL** (Acceso, Rectificación, Cancelación Supresión, Oposición, Portabilidad, y Limitación del tratamiento) según el Reglamento General de Protección de Datos (GDPR) y la Ley Orgánica 3/2018 (LOPD-GDD):

- **Derecho de acceso**: permite al interesado saber si sus datos están siendo tratados, con qué finalidad, por cuánto tiempo, quién los recibe, de dónde proceden, si existen decisiones automatizadas y obtener una copia de ellos. Puede facilitarse mediante acceso remoto y directo. Puede limitarse por abusos (por ejemplo, reiteración injustificada en menos de 6 meses).
- **Derecho de rectificación**: da derecho a corregir datos inexactos o incompletos. El interesado debe indicar cuáles son y aportar documentación justificativa, en su caso.
- **Derecho de supresión** ("derecho al olvido"): permite eliminar datos cuando ya no son necesarios, se retira el consentimiento, el tratamiento es ilícito, o existen obligaciones legales que así lo requieran. También se aplica a datos publicados, obligando al responsable a solicitar su eliminación a terceros. No aplica cuando prevalecen derechos fundamentales, interés público, u obligaciones legales. En ciertos casos, se establece el deber de bloqueo previo a la destrucción definitiva.
- **Derecho de oposición**: el interesado puede oponerse al tratamiento de sus datos por razones particulares, o en cualquier momento si se trata de mercadotecnia directa. También puede oponerse a la elaboración de perfiles, salvo excepciones. El responsable debe dejar de tratar los datos salvo causa legítima prevalente.
- **Derecho de portabilidad**: permite al interesado recibir sus datos personales en formato estructurado y transmisible a otro responsable, cuando el tratamiento se base en el consentimiento o en un contrato, y se realice por medios automatizados.
- **Derecho de limitación del tratamiento**: permite al interesado solicitar la suspensión temporal del tratamiento de sus datos en ciertas condiciones (por ejemplo, cuando impugna su exactitud, se opone a la supresión o mientras se evalúa una oposición). Los datos sólo podrán conservarse o tratarse con el consentimiento o para reclamaciones.

Una de las novedades más destacables de la Ley 3/2018 es la **inclusión explícita del reconocimiento de los Derechos Digitales de la ciudadanía**, convirtiéndose España en el primer país europeo en hacerlo. Estos derechos constituyen un conjunto de libertades aplicables al ámbito de Internet, con el objetivo de reconocer y garantizar un catálogo de derechos digitales conforme al mandato establecido en la Constitución.

A continuación, se resumen los **17 derechos digitales reconocidos por la LOPD-GDD**, agrupados según su naturaleza general o específica del ámbito laboral:

Derechos digitales generales

1. **Derecho a la neutralidad de Internet**: acceso libre y no discriminatorio a la red por parte de los proveedores de servicios.
2. **Derecho de acceso universal a Internet**: garantía de acceso a Internet para toda la población, sin discriminación y con atención a la brecha de género, generacional o discapacidad.
3. **Derecho a la seguridad digital**: protección de las comunicaciones transmitidas y recibidas en línea.
4. **Derecho a la educación digital**: integración de la competencia digital en el currículo, formación del profesorado y seguridad en el uso de las TIC.
5. **Protección de los menores en Internet**: uso equilibrado y seguro de los dispositivos y redes sociales, con intervención del Ministerio Fiscal si hay vulneraciones.
6. **Derecho de rectificación en Internet**: posibilidad de corregir información inexacta en redes y medios digitales.
7. **Derecho a la actualización de informaciones**: solicitar la inclusión de un preaviso visible que actualice datos publicados que ya no reflejen la realidad.
8. **Protección de datos de los menores**: exigencia de consentimiento para la publicación de datos de menores en redes o plataformas digitales.
9. **Derecho al olvido en buscadores**: eliminación de enlaces en los resultados de búsquedas basadas en el nombre, cuando la información sea inadecuada u obsoleta.

10. **Derecho al olvido en redes sociales**: supresión de datos publicados por los propios usuarios o terceros, especialmente si fueron aportados durante la minoría de edad.
11. **Derecho a la portabilidad en redes sociales**: posibilidad de transferir contenidos facilitados a otro proveedor designado.
12. **Derecho al testamento digital**: acceso y gestión de los contenidos digitales de personas fallecidas por parte de herederos o personas designadas.

Derechos en el ámbito laboral

13. **Derecho a la desconexión digital**: respecto al tiempo de descanso y conciliación, con políticas internas que regulen el uso razonable de las tecnologías.
14. **Derecho a la intimidad en el uso de dispositivos digitales**: protección de la privacidad en los dispositivos facilitados por el empleador, con criterios claros de uso.
15. **Derecho a la intimidad ante videovigilancia y grabación de sonido**: limitación del uso de estos sistemas y prohibición en espacios de descanso o íntimos.
16. **Derecho a la intimidad ante sistemas de geolocalización**: uso legítimo condicionado a la información previa sobre el sistema y derechos asociados.
17. **Derechos digitales en la negociación colectiva**: los convenios colectivos podrán incluir garantías adicionales en materia de protección de datos y derechos digitales.

Estos derechos suponen un avance en la protección de los ciudadanos en el entorno digital, reconociendo nuevas dimensiones de la intimidad, libertad y seguridad en la sociedad de la información.

3.5.4 Obligaciones para las entidades

Las organizaciones que tratan datos personales, como son muchas del ámbito industrial mencionadas anteriormente, deben cumplir una serie de obligaciones legales establecidas tanto **en el Reglamento General de Protección de Datos (GDPR)** como **en la Ley Orgánica 3/2018 (LOPD-GDD)**. A continuación, se indican las más relevantes.

1. Deber de información

Las entidades deben informar a las personas interesadas, en el momento de la recogida de los datos o, si proceden de otros orígenes, en un plazo razonable o primera comunicación, sobre la identidad y datos de contacto del responsable del tratamiento, así como del delegado de protección de datos, si lo hubiere.

Deben indicar también los fines del tratamiento y su base legal, los destinatarios previstos de los datos y, en su caso, la intención de transferirlos a terceros países, así como el plazo de conservación previsto. También deberán informar sobre los derechos que asisten al interesado (acceso, rectificación, supresión, oposición, portabilidad, etc.), la posibilidad de retirar el consentimiento en cualquier momento y la existencia de elaboración de perfiles o decisiones automatizadas, en su caso.

LA LOPD-GDD permite que esta información se proporcione **por capas**: una **información básica inicial y** el resto mediante un medio accesible, como un enlace web.

2. Registro de las actividades de tratamiento

Tanto los responsables como los encargados del tratamiento están obligados a mantener un registro documental que contemple los fines del tratamiento, las categorías de interesados y de datos personales, los destinatarios previstos (incluyendo transferencias internacionales, si las hubiere), los plazos de conservación y las medidas técnicas y organizativas implantadas.

Esta obligación no se aplica a las entidades con menos de 250 empleados, salvo que el tratamiento no sea ocasional, implique riesgos o se manejen datos sensibles (categoría especial).

3. Cooperación con la autoridad de control

Las entidades deben colaborar con la **Agencia Española de Protección de Datos (AEPD)** o con el organismo autonómico competente (no es el caso en Galicia) cuando éste les solicite información o actuaciones en el ejercicio de sus funciones.

4. Protección de datos desde el diseño y por defecto

El responsable del tratamiento debe aplicar medidas técnicas y organizativas adecuadas ya desde la concepción de los sistemas o servicios, para integrar la protección de datos de forma efectiva y garantizar que sólo se traten los datos personales necesarios para

cada finalidad específica. Por defecto, los datos no deben ser accesibles a personas no autorizadas.

5. Evaluación de impacto y consulta previa

En los casos en los que un tratamiento pueda suponer un alto riesgo para los derechos y libertades de las personas, como la elaboración de perfiles automatizados, tratamientos a gran escala de datos sensibles o vigilancia sistemática en espacios públicos, es obligatorio realizar una **evaluación de impacto en protección de datos (EIPD, o DPIA en inglés)**.

Si persisten los riesgos tras esta evaluación, deberá realizarse una consulta previa a la autoridad de control (AEPD en Galicia), para verificar si es procedente el tratamiento en cuestión.

Dada la importancia de esta obligación para las organizaciones, se le dedica un apartado específico a continuación.

6. Seguridad del tratamiento

Deberán aplicarse medidas técnicas y organizativas para garantizar la seguridad de los datos, teniendo en cuenta los riesgos potenciales. Estas medidas incluirán, entre otras, seudonimización o cifrado, la capacidad de garantizar la confidencialidad, integridad y disponibilidad permanente de los sistemas, la posibilidad de restaurar datos tras incidentes y otras, así como la revisión periódica de la eficacia de estas medidas.

7. Gestión de brechas de seguridad

Una **brecha de seguridad** se define según el Reglamento, como **cualquier violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a tales datos.**

En caso de violación:

- **Notificación a la autoridad de control** (AEPD o autonómica correspondiente):
    - En menos de 72 horas desde que se tenga constancia.
    - Incluyendo detalles de la naturaleza de la brecha, consecuencias y medidas correctoras.
- **Comunicación a las personas afectadas**:

- Sin dilación indebida si existe alto riesgo para sus derechos.
- Salvo si los datos estaban cifrados o se adoptaron medidas suficientes para neutralizar el riesgo.

El responsable deberá documentar todas las brechas de seguridad, aunque no sea necesario notificar a las personas afectadas.

3.5.5 EIPD

En los **artículos 35 y 36 del RGPD** se establece la necesidad de conducir una EIPD **(Evaluación de Impacto de Protección de Datos)** en ciertos supuestos, antes de poder llevar a cabo el tratamiento de datos personales. A continuación, se incluye una pequeña guía sobre cómo realizarla.

El **Reglamento (UE) 2016/679** como se ha indicado, incorpora una nueva obligación para los responsables de tratamiento: **evaluar el impacto de las operaciones de tratamiento en la protección de los datos personales**, cuando sea probable que el tratamiento suponga un riesgo **significativo para los derechos y libertades de las personas**.

Podemos clasificar los riesgos asociados a un tratamiento en dos tipos: **los riesgos inherentes al tratamiento** (cómo ha sido diseñado) y **los riesgos asociados a la seguridad de los datos**. El enfoque en el riesgo que propone el Reglamento exige **analizar los riesgos** y, si son demasiado altos, **reducirlos**.

El tratamiento de los riesgos puede llevarse a cabo mediante diferentes metodologías, como la **ISO 31000** [31] o **MAGERIT** [32]. La **APDCAT** (Agencia de Protección de Datos Catalana) propone una metodología alternativa para organizaciones pequeñas, que puede ser de interés por su simplicidad [33], aunque lógicamente la AEPD, tiene sus propias recomendaciones [34].

Definición

La **EIPD** es un procedimiento que busca **identificar y controlar los riesgos** para los derechos y libertades de las personas, asociados a un tratamiento de datos.

No nos limitamos a los derechos reconocidos por el Reglamento, sino a **cualquier efecto que el tratamiento pueda tener sobre los derechos y libertades fundamentales de las personas**: derecho a la libertad de expresión, a la libertad de pensamiento, a la prohibición de sufrir discriminación, a la libertad de conciencia, a la libertad de religión, etc.

Al **identificar los riesgos**, debemos considerar cualquier **impacto** que el tratamiento pueda tener sobre las personas (físico, económico, emocional, etc.). Algunos **impactos potenciales** son:

- Imposibilidad de acceder a servicios u otras oportunidades
- Discriminación
- Robo de identidad y otros fraudes
- Pérdidas económicas
- Daños a la reputación
- Daños físicos
- Pérdida de la confidencialidad
- Imposibilidad de ejercer algún derecho

Los impactos pueden materializarse por dos razones:

- **Mal diseño del tratamiento de datos**. Para mitigar este riesgo, debemos establecer los controles para asegurar que el tratamiento se realiza conforme al RGPD.
- **Mala seguridad de los datos**. Para mitigarlo, debe hacerse un análisis del riesgo para su identificación, valoración, y el establecimiento de los oportunos controles de seguridad.

Escenarios de aplicación

El RGPD, salvo tres supuestos concretos indicados en el artículo 35.3, se limita a indicar que debe llevarse a cabo la EIPD cuando el tratamiento **pueda conllevar un riesgo alto** para los derechos y libertades de las personas.

Según el **GT29** (grupo de trabajo a este respecto a nivel comunitario), aunque idealmente se realice siempre la EIPD, debería ejecutarse cuando se den al menos uno de los siguientes supuestos (en ciertos casos), o **dos o más** (en ese caso, habría que realizar la EIPD siempre):

- **Evaluación o puntuación**, incluidas la elaboración de perfiles y predicciones
- **Toma de decisiones automatizada** con efectos jurídicos o que afecta de manera similar y significativa a la persona física

- **Observación sistemática de un área de acceso público**
- **Datos sensibles** (categorías especiales del artículo 9 del RGPD)
- **Tratamiento de datos a gran escala**
- **Conjuntos de datos que se han enlazado o combinado**
- **Datos relacionados con personas vulnerables**
- **Uso innovador de tecnologías**
- **Tratamiento que en sí mismo impide el ejercicio de un derecho o el uso de un servicio o contrato**

Observaciones:

- Aunque el artículo 35.4 del RGPD indica que la **AEPD** publicará una lista de tratamientos para los que debe realizar EIPD, la tendencia general es adoptar la propuesta anterior.
- La **transferencia internacional de datos** era un supuesto para realización de la AIPD, que fue suprimido.
- Si **no aplica el RGPD**, o bien la naturaleza, el alcance, el contexto y las finalidades del tratamiento son muy similares a otro tratamiento para el que ya se ha hecho una EIPD, o bien el tratamiento tiene una **base jurídica** en el derecho de la UE o de un estado miembro, y ya se ha hecho una EIPD en el momento de adoptar esa base jurídica: en estos supuestos, la EIPD **no es necesaria**.
- **No llevar a cabo la EIPD en casos de obligación es una conducta sancionable.**

Cuándo y quién la elabora

La **EIPD** debe efectuarse **en cuanto sea posible**. En el caso de nuevos tratamientos de datos, deberá realizarse **siempre previamente** a los mismos.

Para tratamientos ya en curso, debe realizarse en cuanto se tenga constancia de la existencia de un **riesgo grave** para los derechos y libertades de las personas. Teniendo en cuenta que al igual que la seguridad es un proceso continuo, los **análisis de riesgos también lo son**, hay que reevaluar los tratamientos y las EIPD cuando se produzca un **cambio de contexto organizativo o social**.

La **responsabilidad de la ejecución** de la Evaluación de Impacto es plenamente del **responsable del tratamiento**, con la ayuda del encargado si procede, y el asesoramiento del **Delegado de Protección de Datos**.

El responsable deberá **documentar** si solicitó la opinión de los interesados, **y justificar** por qué no lo hizo, si corresponde. De cualquier forma, el tratamiento debe tener **base legal**, independientemente de la opinión de los afectados.

También puede recogerse la opinión de **agentes externos o internos a la entidad**, expertos independientes o responsables de seguridad.

Contenidos obligatorios

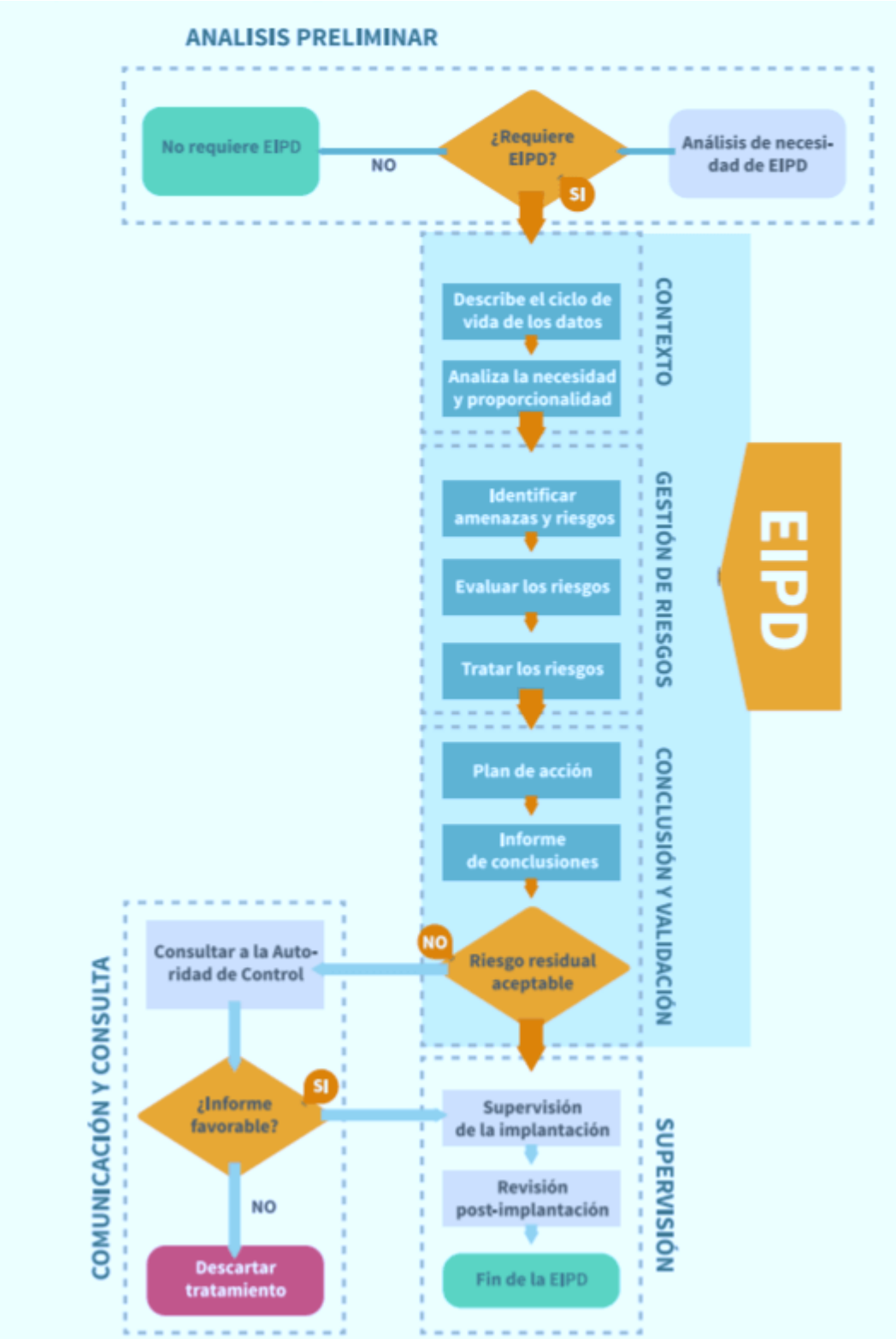
La EIPD es un **informe** que recoge unos **contenidos mínimos según el RGPD**, que son:

- **Descripción de las operaciones de tratamiento de datos.**
- **Evaluación de la necesidad y la proporcionalidad del tratamiento.**
- **Evaluación del riesgo para los derechos y libertades de las personas.**
- **Medidas adoptadas para mitigar los riesgos.**

Ejecución de la EIPD

La elaboración práctica de una EIPD excede del ámbito de este informe. No es compleja, pues en esencia se trata de realizar un análisis de riesgos asociado al tratamiento de datos personales. En cualquier caso, se aconseja contar con asesoramiento experto en la materia.

El flujo de actividades para la ejecución de la EIPD, se muestra a continuación:



Etapas de elaboración de la EIPD. Fuente: Agencia de Protección de datos de Cataluña (2022)

Hay que destacar que la **AEPD tiene disponible en su sitio web varios recursos en forma de guías y herramientas de interés**, que facilitan tanto evaluaciones de impacto, como comunicaciones de brechas de datos, así como otros asuntos relativos a cifrado de información personal, etc. [37][38].

4 Normativa europea

4.1 NIS2

La **Directiva (UE) 2022/2555**, conocida como **NIS2** [39], es la nueva normativa marco de ciberseguridad de la Unión Europea, que sustituye y amplía el alcance de la Directiva NIS original. Su objetivo principal **es garantizar un nivel elevado y común de seguridad de las redes y sistemas de información** en toda la UE, respondiendo a la creciente sofisticación y frecuencia de las ciberamenazas y eliminando las disparidades entre Estados en la aplicación de la anterior directiva.

La NIS2 fue publicada en el Diario Oficial de la UE el *27 de diciembre de 2022*, entrando en vigor el *16 de enero de 2023* [40]. Los Estados miembros disponían hasta *el 17 de octubre de 2024* para transponer la directiva a su ordenamiento jurídico, fecha a partir de la cual las medidas serán de aplicación obligatoria. A fecha de elaboración de este informe, la directiva todavía no ha sido transpuesta a nuestro ordenamiento jurídico (ver última subsección).

4.1.1 Alcance de la directiva

La Directiva NIS2 **amplía notablemente su ámbito de aplicación respecto de** la NIS1, abarcando un abanico mucho más amplio de sectores y servicios críticos para la sociedad y la economía.

Incluye tanto entidades *públicas* como *privadas* de sectores considerados de alta criticidad (en el anexo I) y de otros sectores críticos (en el anexo II), reflejando la creciente digitalización en todos los ámbitos. De este modo, sectores como **la energía, transporte, banca, infraestructuras de los mercados financieros, salud, el suministro de agua potable,** entre otros, siguen estando cubiertos como esenciales, y se incorporan nuevos sectores y actividades no contemplados en la normativa anterior: por ejemplo, se incluyen las **infraestructuras digitales** (proveedores de servicios de nube, DNS, redes de comunicación electrónicas, etc.), los **servicios de redes sociales**, las **Administraciones públicas** (central y regional) o **la gestión de residuos**, la **industria química** y la alimentaria**, el sector espacial** y **la investigación**, por mencionar algunos. También se añaden los *proveedores de servicios digitales* que antes estaban limitados a tres categorías (mercados en línea, buscadores y cloud) incorporando ahora, por ejemplo, las plataformas de redes sociales como nuevo tipo de servicio cubierto. En consecuencia, la NIS2 **elimina la distinción previa entre**

"operadores de servicios esenciales" y "proveedores de servicios digitales" que establecía NIS1, unificando todos estos agentes bajo el mismo marco y requisitos de ciberseguridad.

Otro aspecto clave del alcance es que, con carácter general, la directiva **se aplica a todas las organizaciones medianas y grandes** que operen en los sectores indicados (ya sean públicas o privadas). Ello significa que cualquier empresa con más de 50 empleados o cuyo volumen de negocio anual supere los 10 millones de euros, perteneciente a alguno de los sectores críticos listados, debe considerarse dentro del ámbito de NIS2. Por el contrario, las pequeñas empresas y microempresas quedan exentas por defecto.

Sin embargo, **existen excepciones importantes**: la directiva permite incluir también organizaciones de menor tamaño cuando desempeñen un papel clave para la sociedad o la economía o para ciertos servicios. En particular, independientemente del tamaño, podrían estar afectadas pequeñas entidades que sean las únicas proveedoras de un servicio esencial en un Estado, aquellas cuya interrupción pueda tener un impacto significativo en la *seguridad pública, orden o salud públicos*, o que puedan generar riesgos *sistémicos* en otros sectores o regiones [41].

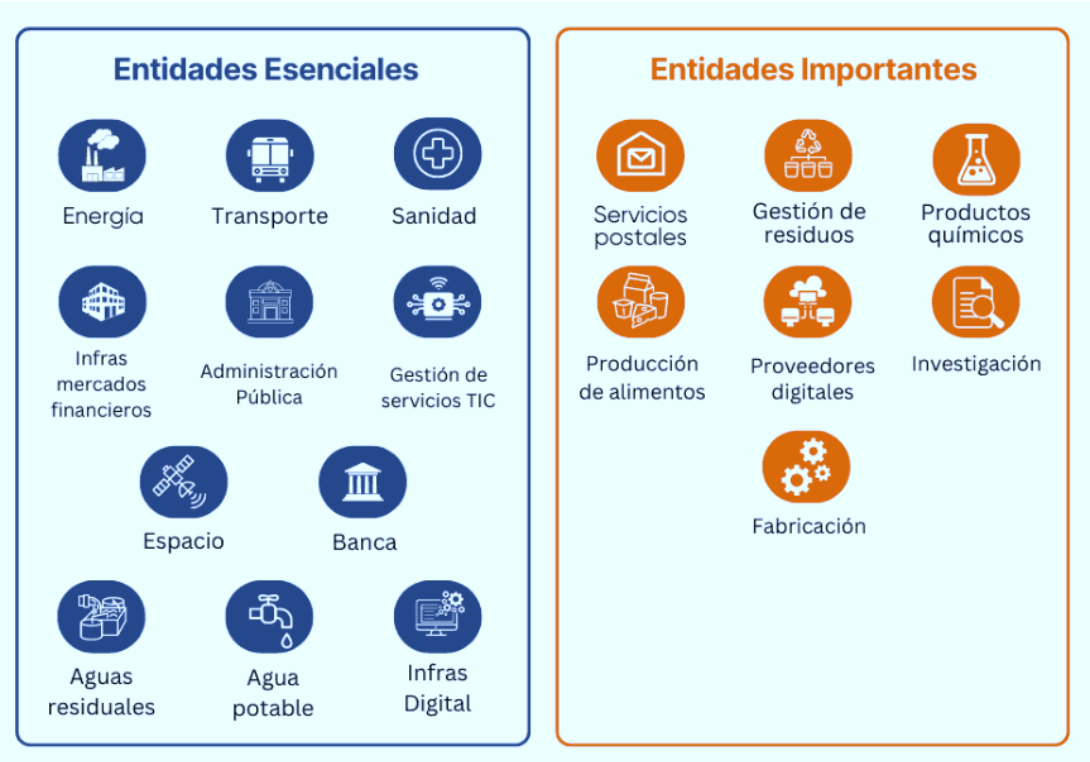
Además, cada Estado miembro tiene la facultad de designar como *esencial* o *importante* cualquier otra entidad no incluida explícitamente en los anexos si considera que su interrupción tendría consecuencias críticas a nivel nacional o regional. De esta forma se asegura que ninguna organización vital quede fuera de la protección de la directiva por mera cuestión de tamaño.

4.1.2 Entidades afectadas y categorización

NIS2 establece dos categorías de entidades afectadas, en función de la criticidad del sector y del servicio que proporcionan, así como de su tamaño e impacto potencial de un incidente:

- **Entidades esenciales**: Son aquellas pertenecientes a los sectores de **alta criticidad** (anexo I de la directiva). Se incluyen aquí, por ejemplo, las Administraciones públicas centrales y regionales, y empresas de sectores como energía, transporte, finanzas (banca e infraestructuras de mercados financieros), sanidad, suministro de agua potable, gestión de residuales, infraestructuras digitales, espacio, etc. Por su relevancia, dichas entidades se consideran vitales para el mantenimiento de actividades socioeconómicas críticas.

- **Entidades importantes**: Corresponden a los **otros sectores críticos** enumerados en el anexo II. Son entidades de sectores no tan sensibles como los anteriores, pero igualmente relevantes, y que superan también el umbral de mediana empresa. Ejemplos de este grupo son los proveedores de **servicios postales y de mensajería**, empresas de **gestión de residuos**, ciertos fabricantes industriales (por ejemplo, del sector químico, alimentario o de productos sanitarios y farmacéuticos), así como muchos **proveedores de servicios TIC** (*IT managed services*, computación en la nube, etc.) e incluso operadores del sector de la **investigación** o tecnológico [42].



Entidades esenciales e importantes según la directiva NIS2. Fuente: Wallix (2025)

En términos prácticos, la directiva impone los *mismos deberes de ciberseguridad* a entidades esenciales e importantes, diferenciándose ambos grupos principalmente en el régimen de supervisión y en las consecuencias ante incumplimientos. Las **entidades esenciales** estarán sujetas a una supervisión más estricta y periódica por parte de las autoridades competentes (enfoque *proactivo* y *reactivo*), mientras que las **entidades importantes** estarán sometidas a una supervisión *reactiva*, es decir, sólo se intervendrá sobre ellas a posteriori, cuando la autoridad tenga conocimiento o evidencias de un posible incumplimiento. En otras palabras, las autoridades podrán inspeccionar proactivamente a las entidades esenciales para verificar que cumplen con los requisitos, mientras que en las importantes actuarán fundamentalmente **después de un incidente**

grave o denuncia, pero no con control continuo. Esta distinción implica también que las sanciones más severas (como la inhabilitación de directivos, explicada más adelante) únicamente aplicará a las entidades esenciales, reforzando la protección en los sectores de mayor criticidad.

Es de destacar que, a diferencia de la directiva precedente, ahora son las propias organizaciones quienes deben **autoevaluar si entran en el ámbito de NIS2 y, por tanto, identificarse como esenciales o importantes** de acuerdo con los criterios establecidos. Ya no es preciso aguardar a una designación formal por parte de la Administración, algo que bajo NIS1 había generado demoras y desigualdades en la aplicación. Esta autoidentificación obligatoria contribuye a una implantación más homogénea e inmediata de la normativa en toda la UE, reduciendo la fragmentación que existía previamente.

4.1.3 Obligaciones en materia de ciberseguridad

La Directiva NIS2 establece una serie de **obligaciones concretas de gestión de seguridad y reporte de incidentes** para todas las entidades que entren en su ámbito, con el fin último de reforzar su *ciber-resiliencia*. En líneas generales, todas las entidades esenciales e importantes deberán llevar a cabo:

- **Gestión de riesgos y medidas de seguridad:** Adoptar medidas técnicas, operativas y organizativas adecuadas y proporcionales para gestionar los riesgos de ciberseguridad en sus operaciones. La directiva detalla un listado mínimo de controles que deben implementarse (descritos en el capítulo IV de la norma, artículo 21), que incluyen [43]:

  a) las **políticas de seguridad de los sistemas de información** y el **análisis de riesgos**;

  b) **la gestión de incidentes**;

  c) la **continuidad de las actividades**, como **la gestión de copias de seguridad**, la **recuperación en caso de catástrofe y la gestión de crisis**;

  d) la **seguridad de la cadena de suministro**, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus **proveedores o prestadores de servicios directos**;

e) **la seguridad en la adquisición, desarrollo y mantenimiento de sistemas de redes y de información**, incluida **la gestión y divulgación de las vulnerabilidades**;

f) las **políticas y procedimientos para evaluar la eficacia** de las medidas para **la gestión de riesgos de ciberseguridad**;

g) las **prácticas básicas de ciber higiene** y **la formación en ciberseguridad**;

h) las **políticas y procedimientos relativos al uso de la criptografía y**, en su caso, del **cifrado**;

i) la **seguridad de los recursos humanos**, **las políticas de control de acceso y la gestión de activos**;

j) el uso de **soluciones de autenticación multifactor o de autenticación continua**, **comunicaciones seguras** (voz, vídeo y texto), y **sistemas seguros de comunicaciones de emergencia** en la entidad, cuando proceda.

Todas estas medidas deben aplicarse siguiendo un enfoque basado en el riesgo (es decir, proporcionales a la magnitud de los riesgos identificados, al tamaño de la organización y al potencial impacto de los incidentes) y teniendo en cuenta *el estado del arte* tecnológico y las normas europeas/internacionales aplicables. En definitiva, se busca que las entidades integren la ciberseguridad en sus prácticas corporativas de forma continua y preventiva, con el compromiso explícito de la Alta Dirección.

- **Notificación de incidentes:** Establecer procedimientos para **notificar a la autoridad competente o al CSIRT** correspondiente aquellos incidentes de seguridad que tengan un impacto significativo en la prestación de sus servicios. La NIS2 fija *plazos estrictos y* un **procedimiento escalonado de reporte**: la entidad debe emitir una **alerta inicial** o *alerta temprana* en un plazo máximo de **24 horas** desde que tenga constancia del incidente, para informar de que ocurrió o está ocurriendo un incidente grave. Posteriormente, en un período no superior a **72 horas**, deberá enviar una **notificación complementaria** en la que actualice la información con una evaluación inicial más detallada de la gravedad e impacto del incidente. Finalmente, en un plazo máximo de **1 mes**, la entidad deberá remitir un **informe final** en el que se incluyan todos los detalles sobre la incidencia, su causa raíz, el alcance de los daños causados y las medidas correctivas adoptadas. Este proceso en tres fases garantiza que las autoridades

reciban información inmediata para reaccionar con agilidad, así como datos más completos una vez la entidad investigó en profundidad lo sucedido.

Cabe destacar que el incumplimiento de estos plazos de notificación, o la ocultación deliberada de incidentes significativos, podrá llevar aparejadas sanciones importantes. Asimismo, la directiva prevé que se informe al público cuando un incidente pueda tener gran trascendencia (por ejemplo, por afectar a usuarios o ciudadanos); en este sentido, las autoridades o CSIRT podrán hacer público el incidente, o requerir a la propia entidad que lo comunique, si consideran que es de interés general.

- **Gobernanza y recursos:** Implicar activamente a los **órganos de gobierno y dirección de** la entidad en la gestión de la ciberseguridad. La Alta Dirección tiene ahora una responsabilidad expresa de aprobar las políticas de gestión de riesgos y supervisar su implantación efectiva. La Directiva NIS2 subraya que la ciberseguridad debe ser asumida como una cuestión estratégica, por lo que los miembros del órgano de administración deben tener un conocimiento adecuado en esta materia (por ejemplo, recibiendo formación específica) y garantizando que la organización destina los recursos necesarios para cumplir con sus deberes de seguridad. De hecho, la norma establece que los directivos podrán ser considerados **responsables personalmente** en el caso de incumplimientos graves de las obligaciones de ciberseguridad por su organización. Esta responsabilidad de los gestores se traduce, entre otras medidas, en la posibilidad de sanciones específicas para ellos (por ejemplo, la *inhabilitación temporal* para ejercer cargos directivos en una entidad esencial, en caso de infracciones muy graves).

  Por este motivo, muchas organizaciones están creando o reforzando la figura del **Chief Information Security Officer (CISO)** o responsable de seguridad de la información, que asesore a la Dirección y lidere la implementación de estas medidas, asegurando el cumplimiento normativo.

- **Colaboración y reporte entre Estados:** La directiva también refuerza la cooperación a nivel nacional y europeo en materia de ciberseguridad. Las entidades deberán colaborar con los organismos competentes de su Estado y, cuando sea pertinente, intercambiar información sobre amenazas e incidentes con otras partes interesadas. Se establecen mecanismos para la **divulgación coordinada de vulnerabilidades** (vulnerability disclosure) entre las

organizaciones afectadas y sus proveedores o clientes, de forma que los fallos de seguridad se comuniquen responsablemente y se corrijan cuanto antes.

En el plano supranacional, se crea la **Red europea de organizaciones de gestión de crisis cibernéticas (EU-CyCLONe)** para apoyar la coordinación de la respuesta a incidentes o crisis de ciberseguridad a gran escala que afecten a múltiples países. También se fortalece el papel del **Grupo de Cooperación NIS** de la UE, que facilitará la toma de decisiones conjuntas y el intercambio de información entre Estados miembros, por ejemplo compartiendo alertas tempranas o buenas prácticas. En cada país, sigue exigiéndose tener una estrategia nacional de ciberseguridad, una o varias **autoridades competentes NIS** encargadas de supervisar el cumplimiento en las entidades, puntos de contacto únicos de enlace internacional, y **equipos de respuesta a incidentes CSIRT** nacionales que gestionen las notificaciones y asistencia a las entidades. Con esta estructura, se pretende una respuesta más coordinada y efectiva ante ciberataques transfronterizos o de gran impacto, evitando la respuesta aislada de cada país.

En síntesis, las obligaciones de la NIS2 abarcan desde la **prevención y preparación** (medidas de seguridad obligatorias, evaluación de riesgos, planes de continuidad, formación...) hasta **la reacción y reporte** ante incidentes (notificación rápida y gestión coordinada), así como una gobernanza clara de la seguridad de la información dentro de las organizaciones. El cumplimiento de estos requisitos será exigible legalmente una vez se transponga la directiva, y estará respaldado por un importante régimen sancionador en caso de incumplimiento (algo que también ocurre con la normativa de protección de datos, LOPD-GDD / RGPD).

4.1.4 Régimen de sanciones y control del cumplimiento

La Directiva NIS2 introduce un régimen de **supervisión y sanciones** mucho más estricto que el de su predecesora, con el objetivo de garantizar que las entidades cumplan efectivamente las obligaciones mencionadas. Cada Estado miembro deberá designar autoridades competentes con facultades de inspección, auditoría e imposición de sanciones administrativas. Dichas autoridades podrán realizar controles de forma proactiva en el caso de las entidades esenciales, e investigarán posibles incumplimientos (por denuncia, incidentes notificados, etc.) en el caso de las importantes.

La directiva establece una lista de poderes mínimos de estas autoridades, que incluye la posibilidad de emitir **apercibimientos e instrucciones vinculantes** a las entidades

para subsanar deficiencias, ordenar la adopción de medidas de seguridad o la notificación de incidentes en un plazo determinado, requerir información y evidencias sobre el estado de seguridad, o incluso **suspender temporalmente actividades** o certificaciones si se detectan incumplimientos graves. En casos extremos, y sólo para entidades esenciales, podrán imponerse sanciones como la mencionada prohibición temporal para determinados directivos responsables.

En cuanto a las multas, la NIS2 exige establecer sanciones **administrativas proporcionadas y disuasorias**. Específicamente, fija unos *umbrales mínimos armonizados* para las multas máximas que cada legislación nacional debe contemplar: en el caso de las **entidades esenciales**, se pueden imponer multas de hasta **10 millones de euros o el 2 % del volumen de negocio anual mundial** de la empresa (la cantidad que sea mayor); para las entidades **importantes**, las multas máximas serán de hasta **7 millones de euros o el 1,4 % del volumen de negocio anual,** escogiendo igualmente la cifra de mayor cuantía en cada caso.

Estas cifras representan los mínimos que los Estados deben aplicar, pudiendo cada país establecerlas en valores superiores si así lo decide al transponer la directiva. Además de las multas, podrán imponerse otras medidas sancionadoras como la publicación de las infracciones (para daño reputacional), requerimientos de corrección auditados por terceros, o incluso la paralización temporal de alguna actividad hasta que se resuelvan las deficiencias de seguridad.

Este endurecimiento de las sanciones viene acompañado de un claro llamamiento a la responsabilidad de los directivos, tal y como se ha indicado. La normativa deja explícito que la **alta dirección responde en última instancia** del (incumplimiento del) deber de ciberseguridad en su organización. Así, si una empresa incumple gravemente las obligaciones de gestión de riesgos o de notificación, los supervisores podrán aplicar sanciones que afecten no sólo a la entidad sino también a sus gestores (por ejemplo, multas personales o inhabilitaciones). Todo ello pretende incitar a las empresas a las que doten de medios suficientes a la seguridad y fomenten una cultura de cumplimiento, sabiendo que las consecuencias legales de no hacerlo pueden ser severas.

4.1.5 Ayudas al cumplimiento: guía CCN-STIC 892 (PCE-NIS2)

Para facilitar a las organizaciones españolas la adaptación a los nuevos requisitos de NIS2, especialmente aquellas sujetas al Esquema Nacional de Seguridad (ENS), el Centro Criptológico Nacional publicará una guía específica de ayuda al cumplimiento. Se trata de la guía **CCN-STIC 892**, que define el Perfil de Cumplimiento Específico NIS2 (PCE-

NIS2) para entidades en el ámbito de aplicación de la directiva [44]. Este perfil de cumplimiento ofrecerá un **mapeo detallado entre los requisitos de la NIS2 y los del ENS**, proporcionando directrices claras para la implementación de las medidas de la directiva en el contexto del marco español de seguridad. Incluirá la correspondencia entre los controles de seguridad del ENS y las obligaciones específicas de NIS2, ayudando así a las entidades (sobre todo públicas, obligadas a ENS) a establecer un solo sistema de gestión de seguridad que satisfaga ambas normativas. Además, el CCN-CERT ofrece con esta guía un marco común de certificación o auditoría de cumplimiento, de forma que las organizaciones puedan demostrar que están alineadas con los requerimientos europeos de ciberseguridad. La versión nueva de la guía CCN-STIC 892, sustituirá la versión previa (que quedó obsoleta con la entrada de NIS2) y será de facto una referencia práctica esencial para encarar el proceso de adecuación antes de la entrada en vigor de la nueva ley en España.

4.1.6 Transposición de la NIS2 en España

Dado que una directiva europea no es de aplicación directa, cada país debe transponer NIS2 a su legislación interna. En España, este proceso de transposición está en marcha y se materializará en una nueva Ley de Ciberseguridad. El Gobierno español aprobó la elaboración del **Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad** el 16 de enero de 2025, con el propósito de incorporar los requisitos de la NIS2 al marco jurídico nacional [45].

El texto del anteproyecto fue sometido a audiencia e información pública en enero-febrero de 2025, y actualmente se encuentra en trámite parlamentario para su aprobación definitiva. La presente Ley, una vez aprobada, sustituirá y actualizará la normativa anterior (Real Decreto-ley 12/2018 y RD 43/2021, que transponía NIS1) y establecerá las obligaciones específicas en territorio español para las entidades esenciales e importantes definidas por NIS2.

El contenido del anteproyecto de Ley sigue de cerca las disposiciones de la Directiva europea. En líneas generales, contempla el refuerzo de la **gobernanza de la ciberseguridad** – atribuyendo claramente a la alta dirección de las entidades la responsabilidad en el cumplimiento –; establece las **medidas de seguridad** que deben implantarse para la gestión de los riesgos (alineadas con las mencionadas en la sección anterior); requiere designar un **responsable de seguridad de la información** (figura equivalente al CISO); y define los **plazos y procedimientos de notificación de incidentes** conforme a la NIS2. Asimismo, la futura ley española detallará el modelo de

supervisión y el catálogo de sanciones aplicables en caso de incumplimiento, siguiendo los baremos mínimos (multas de hasta 10 millones/ 2% del negocio) impuestos por la directiva.

Es importante notar que España, al igual que la mayoría de los países de la UE, **no llegó a tiempo de transponer** la NIS2 antes de la fecha límite de octubre de 2024. Ello motivó que la Comisión Europea haya iniciado procedimientos de infracción en 2024 contra 23 Estados miembros (entre ellos España) por la demora en la incorporación de la normativa. En respuesta, se están a acelerando los trabajos legislativos para aprobar la Ley lo antes posible.

Mientras la transposición no finaliza, las obligaciones de NIS2 aún **no son exigibles directamente** a las entidades españolas (la directiva por sí sola carece de efecto directo, a diferencia de un reglamento). Sin embargo, se recomienda encarecidamente que las organizaciones no aguarden por la ley nacional y **vayan adelantando a los deberes de adaptación a las nuevas exigencias.**

La NIS2 ya marca el estándar europeo de ciberseguridad desde enero de 2023, y las empresas deben aprovechar este tiempo para fortalecer sus capacidades: **identificar si están afectadas, evaluar su nivel de madurez en cada control requerido, e implementar mejoras en sus planes de seguridad**. Las organizaciones que operan en sectores críticos deben prepararse para este nuevo escenario en el que la ciberseguridad será no sólo una obligación legal, sino un elemento central de su continuidad de negocio y confianza del mercado.

4.2 CRA

** Esta normativa afecta tangencialmente a los dispositivos industriales, al ser relativa a ciberseguridad de productos. Se incluye de manera somera como referencia, aunque se trabajará con más profundidad desde otro ámbito del Laboratorio de Ciberseguridad Industrial de la AMTEGA.*

El **15 de septiembre de 2022**, la Unión Europea publicó una **propuesta legislativa para mejorar el nivel de ciberseguridad de los dispositivos IoT** (Internet de las Cosas) y de los productos electrónicos en general. La denominada **Ley de Ciberresiliencia (Cyber Resilience Act, CRA)** es un reglamento que fue finalmente **aprobado el 12 de marzo de 2024**, marcando un hito al establecer **requisitos obligatorios de ciberseguridad para productos con elementos digitales**, tanto de

hardware como de software, con el objetivo de reforzar la seguridad del mercado interior europeo [46].

Según la presentación oficial de la CRA, esta iniciativa:

- **Refuerza las normas de ciberseguridad** para garantizar productos más seguros.
- Responde a la creciente exposición de productos digitales a ciberataques, que causaron **costes globales estimados de 5,5 billones de euros en 2021**.

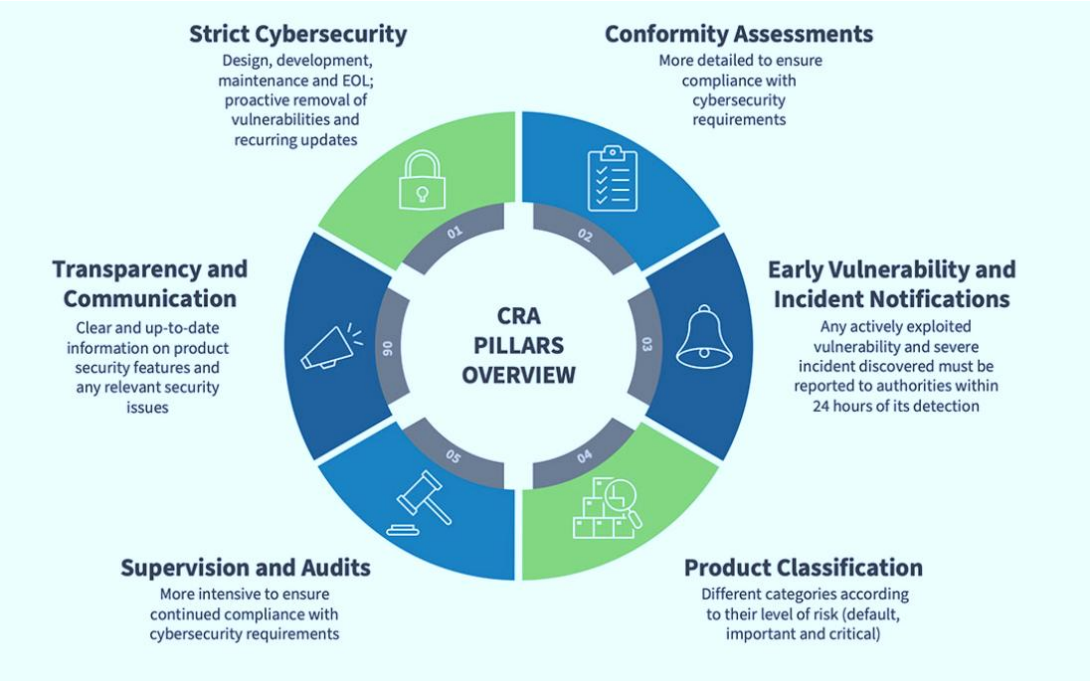
Se han detectado **dos problemáticas principales**: por una parte, un **bajo nivel de ciberseguridad general** de los productos, con vulnerabilidades comunes y ausencia o ineficiencia de las actualizaciones de seguridad. Por otro, **falta de transparencia e información clara para los usuarios**, que dificulta la elección y uso seguro de productos con propiedades de seguridad adecuadas.

La mayoría de los productos con elementos digitales no estaban cubiertos por legislación europea en materia de ciberseguridad, especialmente el **software no embebido**, pese a ser uno de los objetivos principales de ataques. Los **objetivos principales de la CRA**, son:

1. **Crear condiciones para el desarrollo de productos seguros**, con menos vulnerabilidades y un compromiso activo por parte de los fabricantes durante todo el ciclo de vida del producto.
2. **Permitir a los usuarios valorar la ciberseguridad** al elegir y emplear productos con elementos digitales.

De manera más específica, lo que se busca con el reglamento es:

1. Garantizar que los fabricantes **mejoran la seguridad desde el diseño y a lo largo de todo el ciclo de vida de** los productos.
2. Establecer un **marco normativo coherente** que facilite el cumplimiento legal por parte de fabricantes de hardware y software.
3. **Mejorar la transparencia de las propiedades de seguridad de** los productos.
4. Permitir que **consumidores y empresas utilicen productos digitales con seguridad**.



Pilares del reglamento CRA de ciberseguridad. Fuente: Digi International (2025)

Los fabricantes estarán obligados a **evaluar los riesgos de ciberseguridad antes de poner el producto en el mercado**, manteniendo **registros detallados de la fabricación y de los componentes durante al menos diez años**. Será obligatorio **notificar vulnerabilidades explotadas o incidentes graves a la ENISA y a los CERT nacionales en un plazo máximo de 24 horas** desde que se tenga conocimiento, y deberán **designar representantes autorizados como puntos de contacto** con las autoridades.

Asimismo, los productos deberán contar con una **certificación de seguridad**, que podrá ser obtenida mediante mecanismos internos o externos, dependiendo del nivel de riesgo del servicio. Los productos críticos o de alta importancia estarán sometidos a procedimientos de evaluación de la conformidad más exigentes que aquellos de menor riesgo.

La CRA introduce por primera vez un enfoque específico para **la seguridad de la cadena de suministro**, obligando a los fabricantes a considerar la ciberseguridad no sólo como un asunto interno, sino también en las relaciones con los proveedores de servicios y componentes. El cumplimiento de la CRA se convertirá así en un criterio clave a la hora de establecer relaciones comerciales en el ecosistema digital europeo.

Este reglamento supone un cambio de paradigma al establecer **obligaciones específicas y vinculantes** para fabricantes, importadores y distribuidores. A diferencia de otras regulaciones que ofrecían directrices no obligatorias, esta legislación europea

aplica medidas de obligado cumplimiento, orientadas a la prevención, transparencia y respuesta ante incidentes, consolidándose como el marco más ambicioso hasta la fecha en ciberseguridad de productos.

Calendario de aplicación de la CRA

Aunque la aplicación plena de la CRA no se producirá hasta **diciembre de 2027**, existen disposiciones que entrarán en vigor **antes**, según el siguiente calendario:

- A partir del **11 de junio de 2026** serán aplicables las disposiciones relativas a la **notificación de los organismos de evaluación de la conformidad**.
- A partir del **11 de septiembre de 2026** se aplicarán las **obligaciones de información de los fabricantes**.
- A partir del **11 de diciembre de 2027** será de **plena aplicación el conjunto del reglamento**.

Este calendario responde a la necesidad de **conceder a los fabricantes un plazo de hasta 36 meses desde** la entrada en vigor de la norma para adaptar sus productos y procesos a su cumplimiento.

4.3 CER

La **normativa CER** (Critical Entities Resilience) establece un nuevo marco legal europeo para **mejorar la protección y resiliencia de las entidades críticas** frente a cualquier tipo de amenaza, sea de naturaleza **física, natural, tecnológica, sanitaria o híbrida**.

La base legal de la CER es la **Directiva (UE) 2022/2557**, del Parlamento Europeo y del Consejo, publicada el **27 de diciembre de 2022** [47]. Sustituye a la anterior Directiva 2008/114/CE, modernizando el enfoque para adaptarse a las nuevas amenazas complejas e interdependientes. Es de interés visitar el sitio web con información asociada [48].

Esta directiva busca **reforzar la seguridad del mercado interior de la UE** garantizando la continuidad de los servicios esenciales ante cualquier interrupción grave. En España, está en tramitación **el Anteproyecto de Ley de Protección y Resiliencia de Entidades Críticas** desde el 27 de Mayo de 2025 [49], que desarrollará esta normativa a nivel estatal.

Ámbito de aplicación

La normativa CER se aplica a las entidades públicas y privadas que prestan **servicios esenciales para el mantenimiento de funciones sociales vitales, actividades económicas, salud pública o seguridad**, en sectores definidos en **el Anexo de la Directiva mencionada**.

Además, los Estados miembros pueden **designar entidades adicionales como críticas**, incluso fuera de estos sectores, si consideran que su interrupción puede tener consecuencias significativas. En el caso de la transposición española, **se incluye expresamente el sector de la seguridad privada** como ámbito de aplicación de la norma.

El anteproyecto de ley española especifica:

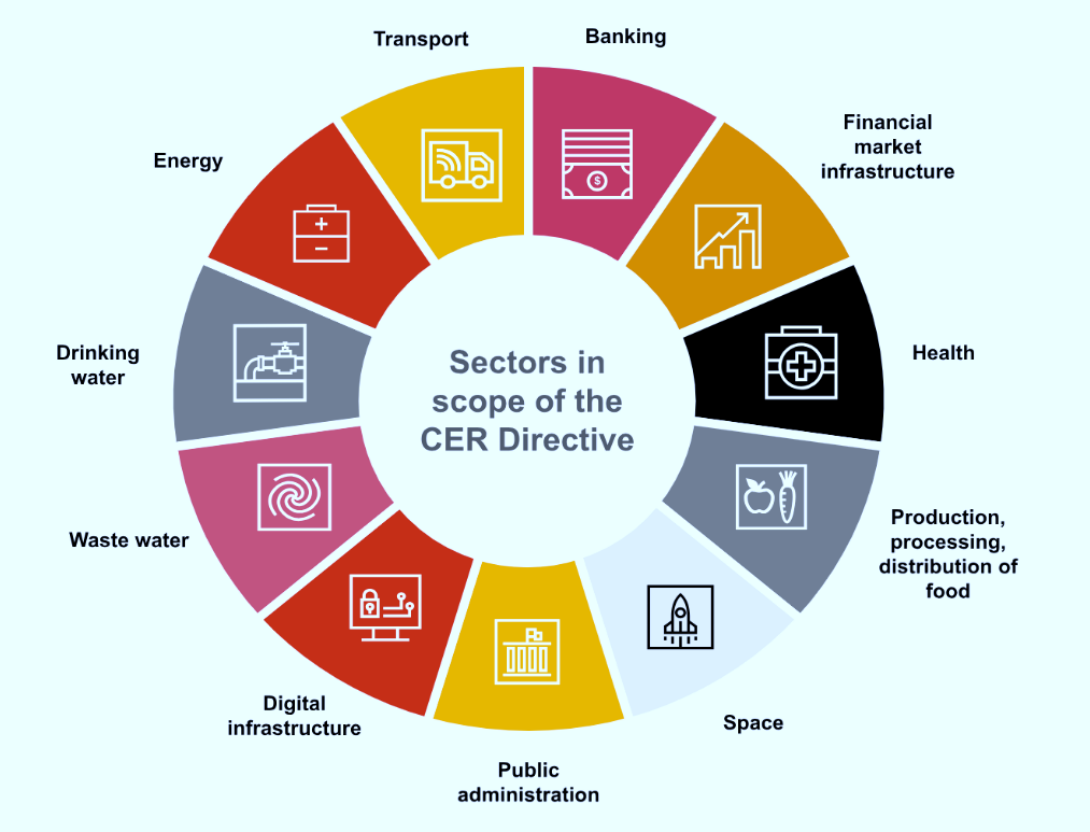
1. La presente Ley es aplicable a las entidades críticas situadas en el territorio nacional, vinculadas a los sectores y subsectores definidos en el anexo.

2. Quedan excluidas:

a) Las entidades críticas dependientes del Ministerio de Defensa, de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos de Policía autonómica con competencias reconocidas para protección y orden público.

b) Las materias reguladas por la Ley de Transposición de la Directiva (UE) 2022/2555 (NIS2), sin perjuicio de lo dispuesto en la disposición adicional cuarta.

c) No se aplicará tampoco cuando otras normas sectoriales impongan obligaciones equivalentes a las previstas en esta Ley, reconocidas en la normativa o mediante resolución de la Secretaría de Estado de Seguridad.



Ámbito de aplicación original de Directiva CER. Fuente: Price Waterhouse Cooper (2025)

En la práctica, algunos de los sectores afectados incluyen **energía, transporte, agua, sanidad, hidrógeno, aguas residuales, sistemas urbanos de climatización y seguridad privada.**

Obligaciones y medidas

La CER se articula sobre tres ejes fundamentales:

a) Medidas estratégicas: A nivel institucional, establece la elaboración de la **Estrategia Nacional de Resiliencia**, a cargo de la Secretaría de Estado de Seguridad y aprobada por el Consejo de Seguridad Nacional, así como una **evaluación nacional de riesgos** cada cuatro años, identificando amenazas naturales, tecnológicas y humanas. El **CNPIC** es sustituido por el nuevo **Centro Nacional para la Protección y Resiliencia de Entidades Críticas (CNPREC)**.

b) Medidas de resiliencia para entidades críticas: Las entidades identificadas deberán **evaluar periódicamente los riesgos**, incluyendo amenazas naturales, tecnológicas, híbridas o de ciberseguridad, e implementar **medidas organizativas, técnicas y físicas** para mitigarlos. Están obligadas a desarrollar **Planes de Resiliencia** con medidas de prevención, respuesta y recuperación en el plazo de seis meses tras ser

designadas. Asimismo, deberán identificar un **responsable de seguridad y resiliencia**, que actuará como interlocutor con las autoridades competentes.

Los **planes de resiliencia** deberán incluir:

1. Medidas para **evitar incidentes**, considerando la reducción de riesgos y adaptación al cambio climático.
2. Medidas para **proteger físicamente las infraestructuras**, como barreras, sistemas de vigilancia y controles de acceso.
3. Procedimientos para **responder y resistir a los incidentes**, con protocolos de alerta y gestión de crisis.
4. Acciones para **recuperar la prestación del servicio esencial**, incluyendo continuidad operativa y cadenas de suministro alternativos.
5. Medidas para **proteger al personal**, definiendo funciones esenciales, accesos, verificación de antecedentes y formación. Esto incluye también personal de proveedores externos.
6. Programas de **concienciación y formación**, mediante cursos, ejercicios y materiales informativos.

c) Comunicación de incidentes: Las entidades críticas están obligadas a **notificar a la autoridad competente cualquier incidente que pueda afectar significativamente a la prestación de sus servicios** en el plazo de 24 horas desde que dispongan de indicios razonables. Además, deben enviar un informe más completo tras la resolución o contención del incidente, **como muy tarde en un plazo de un mes**.

d) Medidas de control y supervisión: Se incluye la **comprobación de antecedentes** del personal que desempeñe funciones sensibles, mediante verificación de identidad, historial penal y datos de inteligencia.

Estas obligaciones buscan **reforzar la preparación y capacidad** de respuesta frente a amenazas sistémicas y evitar disrupciones graves que afecten a la seguridad o el bienestar de la población.

Las **sanciones por incumplimiento** pueden alcanzar los **10 millones de euros**, especialmente en los casos de no notificar incidentes o no adoptar medidas exigidas por la normativa.

Período de implantación

La Directiva CER entró en vigor el **16 de enero de 2023** y los Estados miembros, incluida España, debían **trasponerla a su ordenamiento jurídico nacional antes del**

17 de octubre de 2024, coincidiendo con el plazo establecido para la transposición de la Directiva NIS2.

Este alineamiento estratégico entre NIS2 y CER persigue garantizar una **implementación coordinada y coherente** de la resiliencia ciberfísica en Europa.

5 Marcos y estándares internacionales

Antes de abordar el contenido específico de cada marco o estándar de los que se describen a continuación, hay que destacar que, **aunque no todos han sido diseñados exclusivamente para el ámbito industrial**, estas referencias normativas **tienen un elevado grado de aplicación y utilidad en entornos ICS/OT**, especialmente en los procesos de gobernanza, gestión del riesgo y seguridad técnica.

Su carácter internacional y su reconocimiento en el sector las convierte en **guías fundamentales para establecer prácticas robustas de ciberseguridad industrial**, adaptables según las necesidades y características de cada organización. Partiremos de marcos generales, y finalizaremos con dos específicos de ICS/OT.

5.1 ISO/IEC 27001

5.1.1 Introducción

Un **Sistema de Gestión de la Seguridad de la Información (SGSI)** es un conjunto de políticas, procedimientos, estructuras organizativas, procesos y recursos que una organización establece para **proteger la confidencialidad, integridad y disponibilidad de su información**.

Su finalidad es garantizar que los **datos sensibles o críticos** se gestionan de forma segura, protegiendo tanto los activos tecnológicos como los humanos frente a amenazas internas o externas. Además, permite demostrar **cumplimiento normativo**, mejorar la confianza de los clientes y partes interesadas, y reducir el riesgo de incidentes de seguridad. Un SGSI adopta implantarse según los requisitos de la norma internacional **ISO/IEC 27001**.

Se trata de un **estándar internacional para la Seguridad de la Información**, posiblemente el más conocido, que **especifica los requisitos para definir, implantar, mantener y mejorar un SGSI** (ISMS, Information Security Management System, en inglés).

Es la **primera norma de la serie ISO 27000**, originada a partir de la **ISO BS7799-2:2002**, desarrollada por la **BSI (British Standards Institution)**. Es la **norma principal de la familia**, que define los **requisitos del ISMS y su proceso de auditoría**. Está compuesta por una serie de preceptos reconocidos internacionalmente en las

prácticas de seguridad de la información, aplicando una **metodología de cuatro fases (PDCA: Plan-Do-Check-Act)**.

La **ISO 27001 es certificable**, y define el SGSI: estructura, procesos, documentación, auditoría... La versión actual de la norma **ISO/IEC 27001 es la de 2022** [50]. El resto de las normas de la serie, son **de apoyo**.

No es posible obtener certificación de la ISO 27002 [51], ya que ésta se limita a recoger una serie de **controles de seguridad como buenas prácticas**, sin ser una norma de gestión. Estos **controles son idénticos a los del anexo A de la ISO 27001**, tanto en denominación como en alcance.

La **ISO 27001 está diseñada como una aproximación concreta a la creación de una estructura segura de gestión de la información** dentro de una organización. **Todos los controles de la ISO 27002 y del anexo A deben identificarse en un documento llamado SOA (Statement of Applicability – Declaración de Aplicabilidad)**, tanto si aplican como si no. La correcta definición e implantación de estos controles se **verifica mediante auditorías**.

El modelo de implantación tiene en cuenta los planos **tecnológico, organizativo, legal y humano**:

- En **el aspecto humano**, se presentan factores como **la formación, roles y responsabilidades, control y la supervisión, y la concienciación**.
- En el **ámbito técnico**: protocolos, redes, criptografía, estandarización, desarrollo seguro...
- En relación con la **legislación**: cumplimiento de leyes, reglamentos y normativas aplicables.
- Y en el **plano organizativo**, se establece una **jerarquía documental** que incluye políticas, normas, procesos, procedimientos, planes de contingencia y relaciones con terceros.

Clausulado de la norma ISO 27001:2022. Fuente: Spectral, Check Point (2025)

El **SGSI forma parte del sistema de gestión global de una organización**, e incluye políticas, estructura organizativa, procesos, recursos y objetivos para garantizar la seguridad de la información. La **ISO 27001 guía en la implantación, seguimiento, mejora y auditoría del sistema**.

Se puede concluir que esta norma recoge los **requisitos comunes para un SGSI aplicable a cualquier industria**, y puede **complementarse con otras como la ISO 22301 de Continuidad de Negocio** [52]. Constituye un **marco estándar para desarrollar normas de seguridad sectoriales** y permite implementar un método de gestión **eficaz, auditable y certificable** de los sistemas de información.

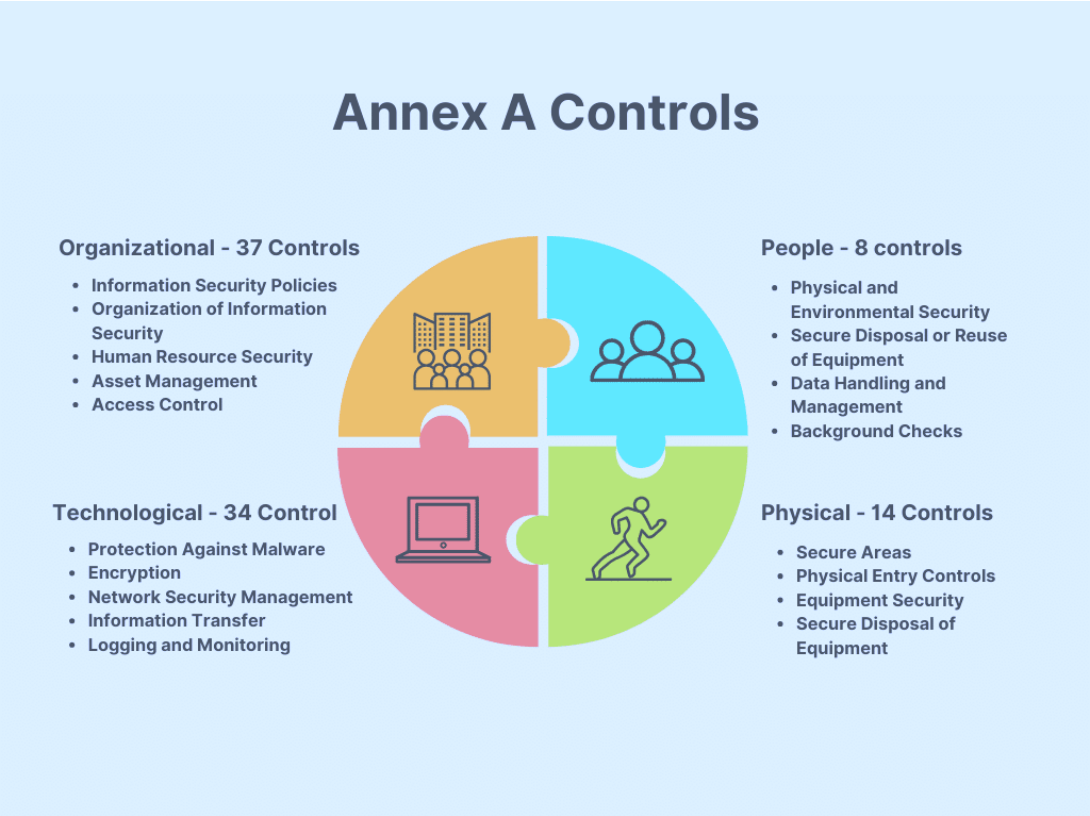
5.1.2 Componentes del SGSI

La estructura de un **SGSI** (Sistema de Gestión de la Seguridad de la Información) bajo la norma **ISO 27001** consta de los siguientes componentes:

1. **Alcance:** Tal y como se indica en el capítulo 4 de la norma, debe definir qué parte de la organización quedará protegida por el SGSI, en cuanto a características de la organización, localizaciones, activos de información y sistemas, y procesos o actividades. Esto es fundamental para delimitar su ámbito de aplicación. Es una decisión de gestión, y no implica necesariamente que toda la organización esté certificada.

2. **Organización:** Se evalúan los aspectos organizativos de la seguridad de la información, tanto internos como en relación con clientes y proveedores. Roles clave:
    - **Dirección de seguridad:** Tiene responsabilidades clave como la convalidación de políticas, aprobación de riesgos residuales, demostración de compromiso, revisión periódica del SGSI y aprobación de los planes asociados.
    - **Responsables del SGSI:** Se encargan de la gestión de usuarios y permisos, disponibilidad de los sistemas, definición de nuevos requerimientos y coordinación de la seguridad.
    - **Propietario de los activos:** Define accesos, normativa aplicable, reporta incidentes y supervisa los controles implementados.
    - **Personal:** Tanto interno como externo, debe conocer y seguir las normas y comunicar incidentes en tiempo y forma.
3. **Diseño de controles de seguridad:** Los controles son medidas para prevenir, detener o mitigar amenazas. Distinguiremos entre:
    - **Controles físicos:** tornos, cámaras, puertas, extintores...
    - **Controles lógicos:** firewalls, IDS, antimalware, contraseñas...
    - **Controles organizativos**: políticas, procedimientos, etc.
4. **Objetivos de control:** En la versión 2013 de la norma, se agrupaban en 14 dominios (a5 a a18). La versión 2022 presenta 4 categorías (organizacionales, de personas, físicos y tecnológicos), con 93 controles. Las diferencias son:
    - **11 nuevos controles:** inteligencia sobre amenazas, seguridad en servicios en la nube, continuidad TIC, supervisión física, hardening, eliminación de datos, enmascaramiento, prevención de fugas, supervisión, filtrado web, codificación segura.
    - Se añade un propósito y atributos relacionados con ciberseguridad a cada control.

    El anexo A ofrece una guía de uso de los atributos, y el anexo B un mapeo con los controles de 2013 vs 2022.



Controles ISO 27001:2022. Fuente: Spectral, Check Point (2025)

5. **Declaración de aplicabilidad (SOA, *Statement of Applicability*):** Documento clave que refleja qué controles se aplican, con estructura tabular:
    - Nombre del control
    - Aplicable (SI/NO)
    - Justificación
    - Objetivo
    - Descripción de la implementación
    - Estado actual

    Es el nexo entre evaluación, tratamiento e implantación de la seguridad.

6. **Cuerpo normativo:** La documentación de gobierno se estructura como una pirámide:
    - **Manual de seguridad:** Incluye política de seguridad, alcance, evaluación de riesgos (normalmente no pública), y el SOA.

- **Política de seguridad:** Documento estratégico validado por la Dirección, revisado periódicamente, de dominio público.
- **Procesos:** Normas internas obligatorias que indican como actuar, clasificables como primarios, de guía o de apoyo.
- **Procedimientos:** Desarrollan aspectos concretos de las políticas, asociados a plataformas y sistemas.
- **Instrucciones técnicas:** Guías detalladas para tareas específicas.
- **Registros (logs):** Soporte para monitorización y control, recogen acciones, activos, usuarios, fechas, etc. y se revisan de forma periódica.

5.1.3 Documentación

La documentación que debe estar siempre disponible para ser auditada relativa al SGSI de acuerdo con la norma ISO 27001, en una organización con un alcance ambicioso de implantación, es:

- El **manual de seguridad** (alcance del SGSI, políticas y objetivos de seguridad de la información, metodología de evaluación y tratamiento de riesgos, declaraciones de aplicabilidad - SOA -, plan de tratamiento del riesgo, informe de evaluación y tratamiento del riesgo).
- **Definición de funciones y responsabilidades de seguridad**.
- **Inventario de activos** y uso aceptable de los mismos.
- **Procedimientos operativos para gestión de TI**.
- **Principios de ingeniería para sistemas seguros**.
- **Políticas de seguridad para proveedores**.
- **Procedimientos de gestión de incidentes**.
- **Procedimientos para la continuidad del negocio**.
- **Requerimientos legales, normativos y contractuales**.
- **Registros de capacitación, habilidades, experiencia y cualificaciones**.
- **Resultados de supervisión y medición**.
- **Programa de auditoría interna**, resultados de auditorías internas.

- **Resultados de revisión por parte de la Dirección**.
- **Resultados de acciones correctivas**.
- **Registros sobre actividades de usuarios**.
- **Excepciones y eventos de seguridad**.

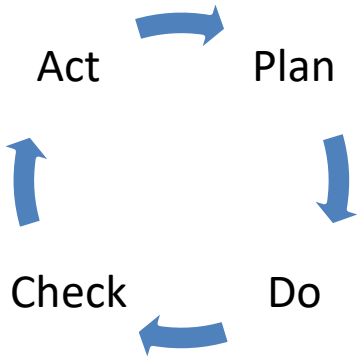
Los documentos no obligatorios de uso habitual pueden incluir:

- Procedimientos para control de documentos.
- Controles para gestión de registros.
- Procedimientos para auditorías internas.
- Procedimientos para medidas correctivas.
- Políticas **BYOD** (Bring Your Own Device).
- Políticas de **dispositivos móviles y teletrabajo**.
- Políticas de **clasificación de la información**.
- Políticas de **claves criptográficas**.
- Políticas de **eliminación y destrucción**.
- Procedimientos de **trabajo en áreas seguras**.
- Políticas de **pantalla y escritorio limpio**.
- Políticas de **gestión de cambios**.
- Política de **copias de seguridad (backups)**.
- Políticas de **transferencia de información**.
- **Análisis de impacto de negocio**.
- **Planes de pruebas y verificación**.
- **Planes de mantenimiento y revisión**.

5.1.4 Certificación

La **certificación de un SGSI es** el proceso mediante el cual una entidad de certificación externa, independiente y acreditada audita el sistema con el objetivo de determinar su conformidad con **ISO/IEC 27001**, su grado de implantación real y su eficacia y, en el caso positivo, emite el correspondiente certificado.

La norma ISO/IEC 27001 como se indicó es **certificable** y se implanta en un modelo iterativo de **mejora continua** en cuatro fases (**Plan-Do-Check-Act, PDCA**):



Ciclo de mejora continua PDCA. Fuente: elaboración propia (2026)

- **PLAN**: Planificación, diseño inicial de la primera o siguiente iteración del SGSI. Incluye la gestión del riesgo.
- **DO**: Implantación y ejecución. Las actividades definidas se ponen en práctica.
- **CHECK**: Seguimiento y revisión, evaluación de la madurez del SGSI.
- **ACT**: Mejora. Con el feedback de la evaluación previa y el feedback de los interesados, se proponen cambios incrementales sobre el SGSI, que se incluyen en la siguiente planificación de un nuevo ciclo PDCA.

Cada ciclo PDCA ha adoptado desarrollase a lo largo de **6 a 12 meses**. En organizaciones grandes o entornos complejos, si el alcance de la certificación abarca toda la compañía, la implantación del SGSI conforme a la norma puede **implicar varios años de trabajo**.

Las partes **interesadas** aportarán sus expectativas, necesidades en cuanto a la seguridad de la información y los requerimientos que impongan a los sistemas de la información (que deben estar alineados con los objetivos de negocio y el marco normativo).

En la fase de seguimiento y revisión se realizan **auditorías**, si el nivel de madurez es suficiente. Estas pueden ser:

- **Internas/externas**: Son obligatorias según ISO 27001. Deben ser realizadas por personal externo o con independencia jerárquica del área auditada. El informe resultante es más simplificado que el de certificación. Se comparten con los directivos para evaluar y mejorar el sistema (fases CHECK y ACT).

- **De certificación**: Sólo pueden ser realizadas por entidades reconocidas conforme a la **ISO 27006** (como **AENOR**, **Applus+** o **TÜV Rheinland**). Estas acreditan que el SGSI se ajusta a los requisitos de la norma. La certificación es válida por **3 años**, con auditorías anuales:
    - **Año 1**: Evaluación completa del SGSI (gestión + todos los controles).
    - **Año 2**: Evaluación parcial (parte de la gestión + parte de los controles).
    - **Año 3**: Evaluación parcial (resto de la gestión + otro subconjunto de controles).
    - **Año 4**: Recertificación completa (gestión + 100% de controles).

Las primeras auditorías suelen ser internas/externas. Se contratan antes de la certificación y, una vez implantado el SGSI, pueden asumirse las revisiones por personal interno para **reducir costes**.

Entre las **ventajas asociadas a la certificación**, se encuentran las siguientes:

- **Mejora la reputación** de la organización demostrando el compromiso con la seguridad de la información ante los clientes.
- **Prueba el apoyo de la Dirección** a la seguridad de la información.
- **Evidencia el cumplimiento de leyes y reglamentos** aplicables.
- Acredita el **cumplimiento de requisitos de gestión corporativa** y continuidad operativa.
- Muestra una **gestión eficaz de los riesgos** empresariales.
- Manifiesta un **compromiso con la mejora continua**, a través de la evaluación periódica del rendimiento e implementación de mejoras.

5.2 NIST CSF

El **CSF (Cybersecurity Framework)** del **NIST (Instituto Nacional de Estándares y Tecnologías de los Estados Unidos)** es un marco de gestión de la seguridad de la información, que se utiliza especialmente en entidades anglosajonas.

El **NIST Cybersecurity Framework (CSF) 2.0** fue lanzado oficialmente el **26 de febrero de 2024** [53][54]. Esta actualización representa un **avance muy significativo respecto de la versión 1.1**, que se había oficializado en el año 2018. El **NIST CSF 2.0**

está diseñado para ser utilizado por **organizaciones de todos los tamaños y sectores**, con independencia de su nivel de sofisticación en materia de ciberseguridad.

Utiliza los **motores de negocio como guía para las actividades de ciberseguridad** dentro de las compañías, considerando los **riesgos asociados a la tecnología como parte fundamental del proceso de gestión de riesgos generales**.

Los componentes del modelo CSF son **tres**: el **Core**, las **capas de implementación (Tiers)**, y el **Framework Profile**.

5.2.1 Core

En el **Core** de este Framework se define un conjunto de **actividades de ciberseguridad y resultados esperados**, comunes a las organizaciones de cualquier sector. Se indican una serie de **estándares industriales y guías de buenas prácticas** que permiten la ejecución y comunicación adecuada de las actividades de ciberseguridad en toda la compañía, desde la capa ejecutiva hasta la de implementación y operaciones.

El **Core define seis Funciones concurrentes y continuas** (que se descomponen posteriormente en **Categorías** y **Subcategorías**) que, cuando se consideran conjuntamente, proporcionan una **visión estratégica y sistemática para la gestión del ciclo de vida y de las operaciones de gestión de riesgos de ciberseguridad en las organizaciones**.

Las seis funciones y sus categorías asociadas son **muy populares** y aparecen con frecuencia en la literatura técnica de ciberseguridad, especialmente en las **descripciones de servicios**. Se presentan a continuación:

Funciones NIST CSF 2.0. Fuente: NIST (2024)

Hay que destacar que en el Anexo A se describen las **funciones, categorías y subcategorías del Core** del framework, así como **referencias informativas** (ya sean del **NIST** o de otros organismos o estándares), para completar y ampliar la documentación al 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

Funciones y categorías NIST CSF 2.0. Fuente: NIST (2024)

5.2.2 Niveles de Implementación

Los **niveles de implementación o *Tiers*** se definen como se indica a continuación. **Proporcionan el contexto de cómo una organización entiende el riesgo de ciberseguridad** y los procesos establecidos para gestionar ese riesgo. Los niveles van desde **el parcial (nivel 1)** hasta el **adaptativo (nivel 4)**.

Esta escala describe **un grado creciente de rigor y sofisticación en las prácticas de gestión de riesgos de ciberseguridad**. Ayuda a determinar hasta qué punto la gestión de riesgos de ciberseguridad **se basa en las necesidades de la empresa y está integrada en las prácticas generales de gestión de riesgos de la organización**.

El proceso de selección de niveles tiene en cuenta:

- las prácticas actuales de gestión de riesgos de la organización,
- el entorno de amenazas,
- los requisitos legales y reglamentarios,
- las prácticas de intercambio de información,
- los objetivos de negocio o misión,
- los requisitos de ciberseguridad de la cadena de suministro, y
- las limitaciones de la organización.

Las organizaciones deben **determinar el nivel deseado**, asegurándose de que:

- **cumple los objetivos de la organización**,
- es **factible de implementar**, y
- **reduce el riesgo de ciberseguridad** sobre los activos críticos y recursos hasta niveles aceptables.

Aunque se **anima a las organizaciones identificadas como Nivel 1 (Parcial)** a considerar avanzar hacia el **Nivel 2 o Superior**, los niveles **no representan niveles de madurez**. **Están pensados para apoyar la toma de decisiones organizativas sobre cómo gestionar el riesgo de ciberseguridad, así como identificar que dimensiones deben priorizarse y recibir recursos adicionales.**

La progresión hacia niveles superiores se recomienda cuando un análisis coste-beneficio indica una reducción viable y rentable del riesgo de ciberseguridad.

Como se comentaba más arriba, existen cuatro **niveles**, en un esquema que recuerda ligeramente al modelo de madurez **CMMI**:

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

Las características de cada nivel se describen en el framework en base a:

- el **grado de madurez del proceso de gestión del riesgo**,
- su **integración en el programa de gestión de la organización**, y

- el **grado de participación e implicación con stakeholders externos** en la gestión del riesgo de ciberseguridad.

5.2.3 Perfil del Framework

El **"Perfil"** es la alineación de las Funciones, Categorías y Subcategorías con los requisitos empresariales, la tolerancia al riesgo y los recursos de la organización**.**

Un **Perfil permite a las organizaciones establecer una hoja de ruta para reducir el riesgo de ciberseguridad**, alineada con los objetivos de la organización y del sector, que tenga en cuenta los requisitos legales/regulatorios y las mejores prácticas de la industria, y refleje las prioridades de la gestión de riesgos.

Dada la complejidad de muchas organizaciones, éstas **pueden optar por tener múltiples perfiles**, adaptados a **componentes o unidades concretas**, reconociendo sus **necesidades específicas**.

Los perfiles **permiten describir el estado de la gestión de riesgos de ciberseguridad de una compañía en un momento dado**. La comparación entre el **perfil actual y el deseado en el futuro** se emplea habitualmente para **identificar GAPs**, que serán cubiertos mediante **proyectos de mejora específicos**, siempre teniendo en **cuenta el nivel de riesgo y el coste/beneficio** de cada acción.

5.3 CIS Controls

El **Center for Internet Security (CIS)** es una organización sin fines de lucro reconocida internacionalmente por su labor en la mejora de la ciberseguridad a través de guías, recursos y buenas prácticas accesibles [55]. Entre sus principales aportes destacan los **Controles Críticos de Seguridad (CIS Controls)**, un conjunto de medidas priorizadas destinadas a **proteger las infraestructuras digitales frente a amenazas comunes**.

La versión 8.1 de estos controles, publicada en 2024 [56] **no es certificable**, pero **su implementación efectiva permite elevar de manera sustancial el nivel de protección de una organización**, sea industrial o no.

Aunque originalmente diseñados para entornos empresariales en general, los CIS Controls son perfectamente **aplicables en entornos industriales OT/ICS**, contribuyendo a fortalecer la defensa de las infraestructuras críticas contra amenazas cada vez más sofisticadas y persistentes.

En este caso, es clave la adaptación a estos entornos particulares, para **garantizar la disponibilidad, integridad y continuidad de los procesos industriales**. A continuación, se presenta el listado completo de controles propuestos.

1. Inventario y control de activos industriales: mantener una visibilidad completa y actualizada de todos los dispositivos OT, como PLCs, sensores, SCADA, HMIs y RTUs, resulta esencial para identificar posibles riesgos. La implementación de herramientas de descubrimiento pasivo que no interfieran con la operación industrial, facilita la creación de mapas detallados de la red y de sus activos.

2. Inventario y control de software de sistemas industriales: es deseable mantener registros de firmware, sistemas operativos y software de aplicaciones industriales. Este control requiere establecer listas de software autorizado, gestionar licencias y validar cualquier modificación mediante procesos de control de cambios. Los SCADA y sistemas DCS deben incluirse en esta revisión.

3. Protección de datos industriales sensibles: los datos operativos, como parámetros de procesos o registros históricos, deben estar cifrados en tránsito y en reposo. Deben establecerse políticas claras de clasificación de la información, restricciones de acceso y registros de auditoría para garantizar su confidencialidad e integridad.

4. Configuración segura de dispositivos industriales: emplear configuraciones por defecto seguras, desactivar servicios innecesarios y aplicar políticas consistentes en todos los dispositivos OT. Estándares como los propios CIS benchmarks [57] proporcionan orientación sobre configuraciones robustas para máquinas anfitrionas o algún software de uso industrial, como bases de datos.

5. Gestión de cuentas e identidades OT: las cuentas deben ser asignadas individualmente, evitando el uso compartido. Es necesario aplicar autenticación multifactor siempre que sea posible, especialmente para accesos remotos o privilegiados. Las sesiones deben registrarse para garantizar la trazabilidad.

6. Control de accesos físicos y lógicos: establecer políticas de acceso basadas en el principio de menor privilegio. A nivel físico, controlar el acceso a salas de control o armarios de comunicaciones. A nivel lógico, utilizar segmentación de redes, listas de control de acceso y proxys industriales para limitar la exposición.

7. Gestión continua de vulnerabilidades OT: realizar evaluaciones de vulnerabilidades sin interrumpir los procesos industriales, a través de escaneos pasivos

o análisis de firmware. La colaboración con el fabricante es esencial para aplicar parches sin afectar a la estabilidad de los sistemas.

8. Registros y trazabilidad de eventos industriales: recoger logs de eventos de control, accesos, fallos y modificaciones en los sistemas. Integrar estos registros en un SIEM adaptado al contexto OT permite detectar comportamientos anómalos y responder rápidamente.

9. Protección frente a vectores de entrada externos: limitar el uso de dispositivos USB y establecer zonas desmilitarizadas (DMZ) entre redes IT y OT. Las herramientas de control de acceso físico y los sistemas de escaneo de medios de almacenamiento portables, son recomendables.

10. Defensa contra malware en sistemas OT: utilizar soluciones antivirus compatibles con sistemas que operan en tiempo real. Los entornos OT requieren soluciones no intrusivas que no comprometan la continuidad de los procesos. Es recomendable también aislar las estaciones de trabajo críticas.

11. Copias de seguridad y recuperación de configuraciones industriales: realizar backups periódicos de los sistemas y configuraciones de dispositivos. Estos deben almacenarse de forma segura y comprobarse regularmente mediante pruebas de restauración.

12. Gestión segura de las redes industriales: definir arquitecturas en capas, segmentar las redes por zonas y conductos según ISA/IEC 62443, y emplear firewalls industriales para controlar el tráfico entre segmentos.

13. Monitorización continua y detección de intrusiones: integrar soluciones de detección de intrusiones específicas de OT (como IDS industriales) que reconozcan protocolos como Modbus, DNP3 u OPC-UA. La respuesta automática debe ser proporcional al riesgo.

14. Formación y concienciación del personal de operaciones: implementar programas de formación específicos para personal OT, sobre seguridad física, manipulación segura de dispositivos, respuesta a incidentes y política de control de accesos.

15. Supervisión de proveedores e integradores industriales: establecer contratos con cláusulas de seguridad, revisar los protocolos de acceso remoto de los proveedores y exigir cumplimiento normativo en los procesos de mantenimiento o integración de nuevos sistemas.

16. Desarrollo y mantenimiento seguro de aplicaciones industriales: aplicar revisiones de código, convalidaciones y pruebas de seguridad en las modificaciones de lógica de PLCs o sistemas SCADA. Implantar controles de cambio rigurosos para mantener la trazabilidad.

17. Preparación y respuesta ante incidentes OT: definir procedimientos claros de respuesta, aislamiento y recuperación. Simular incidentes como fallos de comunicación, ransomware o sabotaje interno. Contar con contactos clave de fabricantes y autoridades.

18. Evaluación y test de seguridad en infraestructuras OT: realizar pruebas de penetración en entornos de laboratorio o mediante revisiones manuales y automáticas. Evaluar regularmente los controles aplicados y los planes de mejora continua.

Es destacable el hecho de que cada control CIS, dispone de un número variable de salvaguardas para su implantación. La distribución de esas salvaguardas según los tres **grupos de implementación (*Implementation Groups*, IGs)**, es la siguiente:

- **IG1 (Grupo 1)**: salvaguardas básicas, recomendadas para todas las organizaciones, especialmente pequeñas y medianas sin infraestructura compleja.
- **IG2 (Grupo 2)**: salvaguardas intermedias, para organizaciones con más recursos, necesidades regulatorias o exposición al riesgo.
- **IG3 (Grupo 3)**: salvaguardas avanzadas, para organizaciones que gestionan datos sensibles u operan en sectores críticos como algunos del ámbito industrial, sanitario o financiero.

A continuación, un resumen gráfico de todo lo anterior:

Controles CIS, salvaguardas y grupos de implementación. Fuente: CIS (2024)

5.4 ISA/IEC 62443

La presente sección tiene como objetivo ofrecer una **visión estructurada y orientativa de la familia de normas IEC 62443**, que constituyen las normas transversales más relevantes en el contexto de la ciberseguridad industrial. El fin es facilitar su comprensión, adopción progresiva y alineamiento con los marcos de cumplimiento normativo vigentes.

Esta guía no sustituye, ni pretende sustituir, el texto íntegro de las normas IEC 62443 ni de sus correspondientes adopciones nacionales o europeas. A efectos de certificación, evaluación formal de conformidad, auditoría o interpretación normativa vinculante, deberán consultarse siempre las versiones íntegras y oficiales publicadas por los organismos de normalización correspondientes.

5.4.1 Introducción

La *International Society of Automation* (ISA) y la *International Electrotechnical Commission* (IEC) son dos organizaciones internacionales de referencia en el ámbito de la estandarización técnica e industrial [64][65]**.**

La ISA es una asociación profesional internacional especializada en automatización y sistemas de control, con un papel histórico destacado en el desarrollo de buenas prácticas y estándares orientados a la seguridad y fiabilidad de los sistemas industriales. Por su parte, la IEC es el organismo internacional responsable de la elaboración de normas globales en el ámbito de la tecnología eléctrica, electrónica y de automatización, con el objetivo de armonizar criterios técnicos y facilitar la interoperabilidad y la seguridad a nivel mundial.

La colaboración entre ambas organizaciones ha permitido trasladar el conocimiento experto de la ISA al marco normativo internacional de la IEC, dando lugar a estándares ampliamente aceptados como la familia IEC 62443 [66].

La familia de normas ISA/IEC 62443 constituye el estándar internacional más completo y específico para la protección de ciberseguridad de los sistemas de automatización y control industrial (IACS/ICS/OT).

Su principal diferencia frente a otros marcos de seguridad reside en que **ha sido concebida desde su origen para entornos industriales**, donde los impactos de un fallo de seguridad no se limitan a la información, sino que pueden afectar directamente a la seguridad de las personas, al medio ambiente y a la continuidad del proceso productivo.

La norma **proporciona un lenguaje común y un marco estructurado que permite alinear la seguridad técnica, organización y los procesos operativos**, integrando la ciberseguridad a lo largo de todo el ciclo de vida de los sistemas industriales: diseño, integración, operación, mantenimiento y retirada.

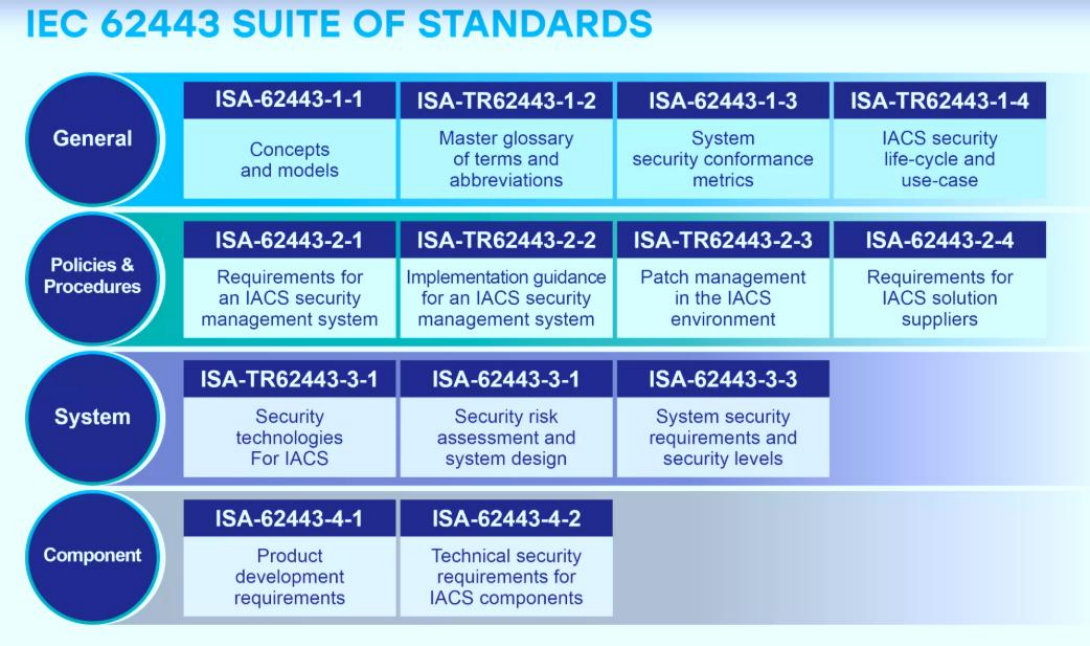
5.4.2 Estructura de la familia de normas

La familia IEC 62443 se estructura en cuatro grandes bloques que responden a una lógica progresiva y complementaria:

- En primer lugar, las normas de la **Parte 1 (General)** establecen la base conceptual del estándar. En ellas **se definen la terminología común, los principios fundamentales y los modelos que se emplearán en el resto de la familia**. Estas normas no introducen requisitos técnicos ni organizativos directos, pero son imprescindibles para interpretar correctamente el estándar.
- En segundo lugar, **la Parte 2 (Políticas y procesos)** aborda **la dimensión organizativa de la ciberseguridad industrial**. Este bloque se centra en cómo deben estructurarse los programas de seguridad, los roles, responsabilidades,

procesos y relaciones entre propietarios de activos, integradores y proveedores de servicios.

- A continuación, **la Parte 3 (Sistemas)** constituye el **núcleo técnico-operativo de la norma para operadores y propietarios de activos**. En ella se definen la metodología de evaluación de riesgos y los requisitos técnicos que deben cumplir los sistemas industriales en función del riesgo identificado.
- Finalmente, **la Parte 4 (Componentes y Desarrollo)** está **orientada principalmente a fabricantes de productos OT**, estableciendo requisitos tanto para el desarrollo seguro como para las capacidades de seguridad de los componentes.



Estructura de estándares ISA/IEC 62443. Fuente: Thales Cybersecurity (2024)

Esta disposición permite aplicar el estándar de manera selectiva y proporcional, evitando enfoques indiscriminados y favoreciendo una adopción realista.

5.4.3 Conceptos fundamentales de la IEC 62443

5.4.3.1 Defensa en profundidad

El principio de defensa en profundidad es uno de los pilares de la IEC 62443. Este concepto establece que la **seguridad no debe depender de un único mecanismo o control, sino de una combinación de medidas técnicas, organizativas y procedimentales distribuidas en diferentes capas.**

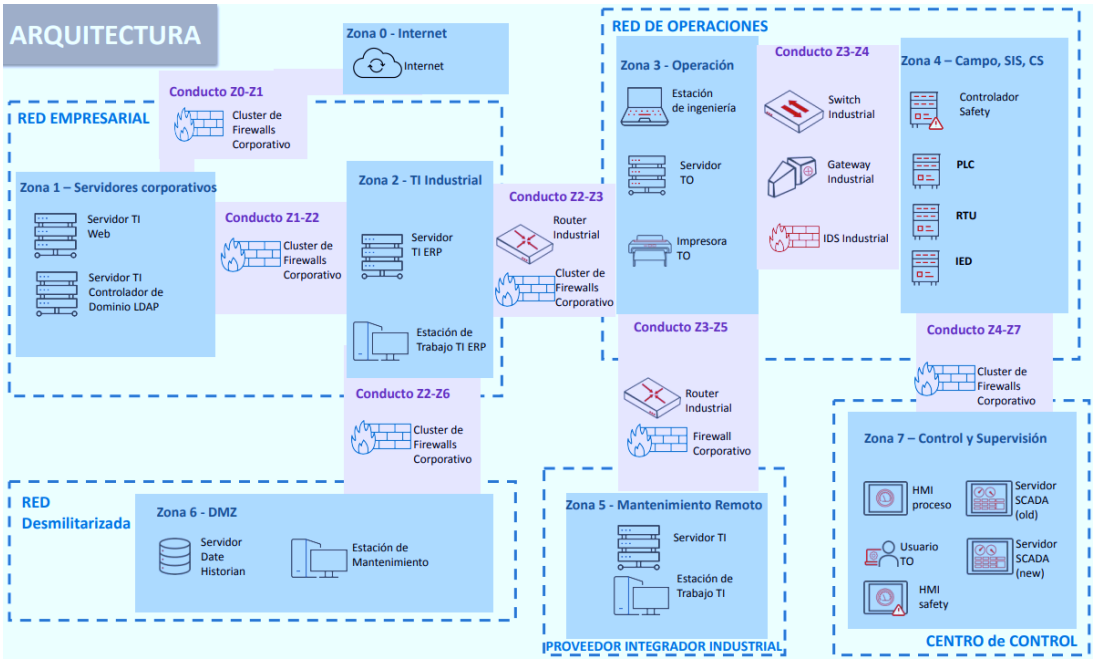
En entornos OT, esto se traduce en la combinación de segmentación de red, control de accesos, mecanismos de autenticación, procedimientos operativos seguros, monitorización y capacidades de respuesta. El objetivo no es impedir absolutamente cualquier incidente, sino limitar su impacto y evitar la propagación de un fallo o ataque a todo el sistema.

5.4.3.2 Zonas y conductos

El modelo de zonas y conductos es una de las aportaciones más distintivas de la IEC 62443. Una **zona** se define como un **conjunto de activos, físicos o lógicos, que comparten requisitos de seguridad comunes.** Los **conductos representan los canales de comunicación entre zonas y deben ser protegidos acorde a los riesgos** asociados.

Este modelo permite estructurar la seguridad de un sistema industrial de forma comprensible y verificable, facilitando tanto el diseño de arquitecturas seguras como su evaluación posterior.

A continuación, un ejemplo de arquitectura basado en zonas y conductos:



Arquitectura de red ICS basada en zonas y conductos. Fuente: CCI (n.d.)

5.4.3.3 Niveles de seguridad (*Security Levels*, SL)

Los **niveles de seguridad (*Security Levels*, SL) describen el grado de protección requerido frente a distintos perfiles de amenaza**, caracterizados por el nivel de recursos, conocimientos y motivación del atacante. La IEC 62443 define cinco niveles:

- **SL 0**: no se requiere **ningún requisito específico de seguridad**. Sólo es aceptable en entornos aislados o sin impacto relevante.
- **SL 1**: **protección frente a errores o usos no intencionados**. Abarca medidas básicas como control de accesos elementales y buenas prácticas operativas.
- **SL 2**: **protección frente a ataques intencionados simples**, realizados con herramientas comunes y conocimientos generales. Requiere controles técnicos básicos de autenticación, segmentación y registro.
- **SL 3**: **protección frente a ataques dirigidos con conocimientos específicos** de sistemas OT. Implica medidas avanzadas de control de acceso, monitorización, defensa en profundidad y protección de la integridad.
- **SL 4**: **protección frente a ataques altamente sofisticados y dirigidos, con amplios recursos y alta motivación**. Normalmente se restringe a escenarios muy críticos.

Los SL no son objetivos arbitrarios: deben derivarse de una evaluación de riesgos y aplicarse de forma diferenciada a zonas, conductos, sistemas y componentes.

5.4.3.4 Niveles de madurez organizativa

Además de los niveles de seguridad técnica, la familia IEC 62443 introduce un **modelo de madurez organizativa** que **permite evaluar hasta qué punto una organización tiene integrados e institucionalizados los procesos de ciberseguridad industrial**. Este modelo es especialmente relevante para proveedores de servicios y fabricantes, aunque también resulta útil como referencia para operadores y administraciones.

Los niveles de madurez definidos son los siguientes:

- **Nivel de madurez 1 – Inicial**: la seguridad se gestiones de manera reactiva y ad hoc. Los procesos no están formalizados, dependen de las personas y existe poca o ninguna documentación. Las actuaciones en seguridad se producen habitualmente tras incidentes.
- **Nivel de Madurez 2 – Gestionado**: existen procesos documentados y directrices formales. El personal conoce los procedimientos básicos y se aplican de manera repetible, aunque con variabilidad entre proyectos o áreas.
- **Nivel de Madurez 3 – Definido**: los procesos de seguridad están estandarizados en toda la organización, se integran en el ciclo de vida de los sistemas y existe evidencia sistemática de su aplicación.

- **Nivel de Madurez 4 – Mejora continua:** la organización mide la eficacia y eficiencia de sus procesos de seguridad, utiliza indicadores y métricas, y aplica mejoras continuas basadas en datos y revisiones periódicas.

Este modelo permite evaluar no sólo si existen controles, sino si estos son sostenibles en el tiempo y son gestionados de modo oportuno.

5.4.4 Certificación en la IEC 62443

La familia IEC 62443 dispone de un esquema de certificación específico, gestionado por ISASecure, que permite certificar distintos objetos:

- **Procesos**: certificación del ciclo de vida de desarrollo seguro (basado en IEC 62443-4-1).
- **Productos y componentes**: certificación de las capacidades técnicas de seguridad (IEC 62443-4-2).
- **Sistemas**: certificación de sistemas industriales completos conforme a requisitos de sistema (IEC 62443-3-3). Posteriormente nos centraremos en este, por ser lo más relevante para las organizaciones que quieran proteger al entorno operativo.

Las certificaciones se realizan por entidades acreditadas independientes y tienen carácter temporal, requiriendo **renovación periódica**, habitualmente anual o plurianual según el esquema, incluyendo revisiones documentales y, cuando procede, auditorías técnicas.

En contraste como vimos, certificaciones como **ISO/IEC 27001** o el **Esquema Nacional de Seguridad** tienen una vigencia de tres y dos años, respectivamente. Éstas no evalúan directamente la seguridad técnica de un sistema industrial ni de un producto concreto, sino la existencia de un marco de gestión adecuado.

5.4.5 Documentos principales de la familia IEC 62443

A continuación, se presenta una descripción breve de los principales documentos de la familia IEC 62443 que se consideran más relevantes a efectos de cumplimiento normativo.

5.4.5.1 IEC 62443-1-1 – Conceptos, terminología y modelos fundamentales

Establece la **base conceptual de la familia IEC 62443, definiendo la terminología común, los principios fundamentales de ciberseguridad industrial y el modelo**

general de aplicación del estándar. Introduce conceptos clave como defensa en profundidad, zonas y conductos, niveles de seguridad y la relación entre riesgos y requisitos, actuando como marco interpretativo imprescindible para el resto de las normas de la serie. Más detalle de alguna de estas cuestiones en la siguiente sección.

5.4.5.2 IEC 62443-1-5 – Perfiles de seguridad

Introduce **el concepto de perfiles de seguridad** como mecanismo para adaptar la IEC 62443 **a sectores, regulaciones o contextos específicos**.

5.4.5.3 IEC 62443-2-1 – Sistema de gestión de la seguridad del propietario del activo

Este documento define los **requisitos para establecer y mantener un sistema de gestión de la seguridad OT por parte del propietario de los activos.** Proporciona el marco organizativo que conecta la evaluación de riesgos, requisitos técnicos y la operación segura.

5.4.5.4 IEC 62443-2-4 – Requisitos de seguridad para proveedores de servicios IACS

Aborda la dimensión **organizativa y operativa de los integradores, empresas de mantenimiento y proveedores de servicios OT, uno de los vectores de riesgo más relevantes** en entornos industriales.

5.4.5.5 IEC 62443-3-2 – Evaluación del riesgo de seguridad para el diseño de sistemas

Establece la **metodología para realizar evaluaciones de riesgo específicas para sistemas OT**, sirviendo de punto de partida para el diseño de arquitecturas seguras basadas en zonas, conductos y niveles de seguridad.

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

Define los **requisitos técnicos que deben cumplir los sistemas industriales para alcanzar los niveles de seguridad establecidos** tras la evaluación de riesgos. Fundamental para proteger y certificar una planta productiva. Profundizaremos en esta cuestión en la siguiente sección.

5.4.5.7 IEC 62443-4-1 – Ciclo de vida de desarrollo seguro de productos

Establece los requisitos que deben cumplir los fabricantes para **integrar la seguridad en el desarrollo de productos OT** desde las fases iniciales.

5.4.5.8 IEC 62443-4-2 – Requisitos técnicos de seguridad para componentes

Define las **capacidades de seguridad que deben ofrecer los componentes industriales**, como PLC, HMI, dispositivos de red o software.

5.4.6 Aplicación de la IEC 62443 a sistemas industriales

La aplicación práctica de la familia de normas IEC 62443 **no debe entenderse como la implantación aislada de un conjunto de controles técnicos**, sino como un **proceso estructurado y coherente**, en el que cada decisión de seguridad deriva del riesgo y puede ser justificada técnica y organizativamente. Este enfoque se articula como una **cadena lógica de pasos**, que permite garantizar proporcionalidad, trazabilidad y evidencias de cumplimiento.

5.4.6.1 Evaluación del riesgo

El punto de partida es siempre **la evaluación del riesgo de ciberseguridad**, conforme a la IEC 62443-3-2. En esta fase se identifican los activos industriales, sus funciones críticas, las amenazas relevantes, las vulnerabilidades existentes y los impactos potenciales sobre la seguridad de las personas, la continuidad del proceso, el medio ambiente o la calidad del servicio.

Ejemplo: en una planta de tratamiento de agua, se identifica que la pérdida de control sobre determinados PLC puede provocar la interrupción del suministro o la dosificación incorrecta de productos químicos. Las amenazas incluyen accesos remotos no controlados y malware introducido a través de portátiles de mantenimiento.

5.4.6.2 Determinación del nivel de seguridad objetivo (SL-T)

Una vez analizado el riesgo, se establece el **nivel de seguridad objetivo (SL-T)** para cada zona y conducto. Este nivel expresa el grado de protección necesario frente al perfil de amenaza considerado, evitando tanto la infraprotección como la sobreprotección innecesaria.

Ejemplo: la red de supervisión puede requerir un SL-2, mientras que la zona de control de procesos críticos puede necesitar un SL-3 debido al mayor impacto operativo y a la posibilidad de ataques dirigidos.

A estos efectos, **veamos qué indica la norma sobre los niveles de seguridad (SL).** En el anexo A de la IEC 62443-3-3, reza lo siguiente:

Los niveles de seguridad suponen un enfoque cualitativo a la hora de abordar la seguridad de una zona. Como método cualitativo, la definición del nivel de seguridad puede aplicarse para comparar y gestionar la seguridad de las zonas dentro de una organización. A medida que se disponga de más datos y se desarrollen las representaciones matemáticas del riesgo, de las amenazas y de los incidentes de seguridad, este concepto pasará a tener un enfoque cuantitativo para la selección y verificación de los niveles de seguridad (SL). Podrá ser

aplicado tanto por las organizaciones usuarias finales como por los proveedores de IACS y de productos de seguridad. Se empleará para seleccionar los dispositivos IACS y las contramedidas a utilizar en una zona y para identificar y comparar la seguridad de las zonas en distintas organizaciones del sector.

Los SL se clasifican en tres categorías: **niveles objetivo**, **niveles alcanzados** y **niveles de capacidad**. Aunque estas categorías están relacionadas entre sí, hacen referencia a distintos aspectos del ciclo de vida de la seguridad.

- **Los niveles de seguridad objetivo (SL-T)** representan los niveles de seguridad que se desea para un sistema determinado. Normalmente, este nivel se determina a través de una evaluación de riesgos del sistema, mediante la cual se establece que es necesario un determinado nivel de seguridad para garantizar un funcionamiento correcto.
- **Los niveles de seguridad alcanzados (SL-A)** son el nivel de seguridad real de un sistema determinado. Estos niveles se miden una vez que se dispone de un diseño del sistema o cuando el sistema está implantado. Se emplean para determinar si un sistema de seguridad está cumpliendo los objetivos que se hayan establecido inicialmente en los niveles de seguridad objetivo.
- **Los niveles de seguridad de capacidad (SL-C)** son los niveles de seguridad que pueden proporcionar los componentes o los sistemas cuando están configurados correctamente. Estos niveles expresan que un componente o sistema determinado es capaz de conseguir los SL objetivo de forma nativa, sin emplear contramedidas compensatorias adicionales, siempre que esté configurado e integrado de manera correcta.

Los distintos tipos de niveles de seguridad (SL) se aplican en diferentes fases del ciclo de vida de la seguridad. En primer lugar, se define el nivel de seguridad objetivo (SL-T) a partir de la evaluación de riesgos. A continuación, se diseña el sistema de manera iterativa para alcanzar ese nivel, seleccionando componentes y sistemas con el nivel de capacidad (SL-C) adecuado o, de ser necesario, aplicando contra medidas compensatorias. Una vez el sistema entra en operación, se mide el nivel de seguridad alcanzado (SL-A) y se comprará con el SL objetivo para verificar el cumplimiento de los requisitos establecidos.

5.4.6.3 Aplicación de requisitos técnicos y organizativos

A continuación, se procede a la **selección e implantación de los requisitos de seguridad** adecuados para alcanzar el SL-T definido. Estos requisitos pueden ser de naturaleza técnica (IEC 62443-3-3 y 4-2) u organizativa y procedimental (IEC 62443-2-4, 4-1).

5.4.6.3.1 Requerimientos y formato vector del SL

Existe una forma compacta de describir los niveles de seguridad. Tal y como se define en la Norma **IEC 62443-1-1**, los niveles de seguridad (SL) previamente descritos se basan en siete **requisitos fundamentales (FR)** para la seguridad:

1. **control de identificación y autenticación (IAC);**
2. **control de uso (UC);**
3. **integridad del sistema (SI);**
4. **confidencialidad de los datos (DC);**
5. **flujo de datos restringido (RDF);**
6. **respuesta oportuna a los eventos (TRE);** y
7. **disponibilidad de recursos (RA).**

En lugar de reducir los SL a un único valor numérico, **es posible emplear un vector de SL que utilice los siete FR mencionados en lugar de un único factor de protección**. Este vector de SL permite establecer separaciones definibles entre los SL para los distintos FR mediante un lenguaje específico. Este lenguaje puede basarse en consecuencias adicionales asociadas a los sistemas de seguridad o en distintos tipos de ataques contra los objetivos de seguridad abordados por los FR, y puede incluir explicaciones prácticas sobre cómo un sistema puede ser más seguro que otro sin necesidad de relacionar todo con consecuencias para la salud, la seguridad y el medio ambiente (HSE).

Es preferible emplear un **vector** para describir los requisitos de seguridad de una zona, de un conducto, de un componente o de un sistema, en lugar de utilizar un único número que proporciona menor detalle. Este vector puede contener un requisito específico de SL o un valor igual a cero para cada requisito fundamental.

El formato vector del SL, es:

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

Donde:

- **SL-? = (Requerido)** representa el tipo de SL. Los formatos posibles son:
    - **SL-T** = SL objetivo
    - **SL-A** = SL alcanzado
    - **SL-C** = SL de capacidad
- **[FR] = (Opcional)** Campo que indica el requisito fundamental al que se aplica el valor del SL. Los FR se escriben de forma abreviada, en lugar de emplear una notación numérica, para facilitar la comprensión.
- **dominio = (Requerido)** El dominio al que se aplica el SL. Los dominios pueden hacer referencia a zonas, sistemas de control, subsistemas o componentes.

  En esta norma en particular, todos los requisitos hacen referencia al sistema de control, por lo que el término "dominio" no se utiliza como en otros documentos de la serie de Normas IEC 62443.

Ejemplos:

- SL-T (Zona BPCS) = { 2 2 0 1 3 1 3 }
- SL-C (Puesto de trabajo técnico del SIS) = { 3 3 2 3 0 0 1 }
- SL-C (RA, FS-PLC) = 4

5.4.6.3.2 Implantación de la ciberseguridad

El **Anexo B de la IEC 62443-3-3** describe cómo se construyen los **niveles de seguridad (SL 1 a SL 4)** a partir de la asignación progresiva de **requisitos del sistema (SR) y** de sus **mejoras (RE)** a los **siete requisitos fundamentales (FR)** definidos en el estándar, enumerados arriba.

La norma establece **100 requisitos técnicos** (descritos con detalle en la norma en el cuerpo principal de la misma), resultado de la combinación de SR y RE (requisitos básicos del sistema y mejoras), que permiten materializar los distintos niveles de seguridad para cada FR. **La progresión de los SL es acumulativa: para cumplir un nivel superior es necesario cumplir todos los requisitos de los niveles inferiores más los adicionales definidos para ese nivel.**

La tabla B.1 indica, para cada FR y para cada SL, qué requisitos deben aplicarse para que un sistema pueda considerarse conforme a ese nivel. De esta forma, los SL dejan de ser un concepto abstracto y se convierten en un conjunto de **capacidades técnicas verificables**.

Este enfoque permite evaluar de forma objetiva el SL alcanzado (SL-A) de un sistema, comparar sistemas o zonas con distintos perfiles de seguridad, y garantizar coherencia entre el riesgo identificado, el nivel de seguridad exigido y las medidas técnicas implantadas.

Veamos a continuación un ejemplo:

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				✓

Muestra de asignación de SR y RE a los RF de los niveles de seguridad. Fuente: ISA 62443-3-3 (2020)

Como se puede apreciar en el ejemplo, para cumplir con el Requisito del Sistema (SR) 1.1 del Requisito Fundamental 1 (Control de identificación y autenticación, IAC), en caso de precisar un Nivel de Seguridad dado en el sistema:

- De SL1: bastaría con implementar el requisito SR 1.1.
- De SL2: se precisaría además de lo anterior, la mejora SR 1.1. RE 1.
- De SL3: a lo anterior, sumaríamos la mejora SR 1.1 RE 2.
- De SL4: necesitaríamos aplicar todo, tanto el requisito de sistema, como las tres mejoras definidas.

Así, para definir las necesidades de seguridad de nuestro sistema, debemos en base al análisis de riesgos determinar los SL-T asociados a las diferentes zonas y conductos, e implementarlas mediante las medidas correspondientes en la ISA 62443-3-3.

En conjunto, el Anexo B proporciona el puente entre los niveles de seguridad definidos conceptualmente y su **implementación técnica concreta** en sistemas industriales.

En el siguiente recurso, puede verse un ejemplo ilustrativo de un escenario real de implantación de la norma IEC 62443 en el sector energético, en colaboración con el CCI (Centro de Ciberseguridad Industrial) [67].

5.4.6.4 Certificación y verificación

La última pieza de la cadena es la **verificación independiente** de las medidas implantadas. La certificación conforme a la IEC 62443 permite demostrar, mediante evaluaciones de tercera parte, que:

- los procesos siguen prácticas reconocidas,
- los sistemas cumplen requisitos técnicos definidos,
- o los productos incorporan capacidades de seguridad adecuadas.

La certificación no es obligatoria para aplicar la norma, pero aporta una **evidencia sólida de conformidad**, especialmente relevante en entornos regulados o contratos con terceros.

A modo de ejemplo, un fabricante puede certificar un producto conforme a la IEC 62443-4-2, mientras que un operador puede optar por certificar un sistema concreto en la IEC 62443-3-3 tras su implantación en una infraestructura crítica.

Esta secuencia *riesgo → SL → requisitos → verificación*, garantiza que las medidas de seguridad:

- están justificadas por el riesgo,
- son proporcionales al impacto,
- están alineadas con los objetivos operativos,
- y pueden ser auditadas y demostradas.

Cabe destacar para cerrar este apartado, que la familia IEC 62443 está diseñada para ser aplicada por distintos actores, cada uno con un rol específico en el ecosistema industrial:

- **Operador (propietario del activo)**: responsable de la evaluación del riesgo, de la definición de los niveles de seguridad, de la operación segura de los sistemas y de la gobernanza global de la ciberseguridad OT.
- **Integrador (proveedor de servicios)**: centra su responsabilidad en los procesos de integración, mantenimiento y acceso a los sistemas, garantizando

que sus actuaciones no introducen riesgos adicionales y que se cumplen los requisitos contractuales y normativos.

- **Fabricante:** debe integrar la seguridad desde el diseño de los productos, implementando ciclos de desarrollo seguro y proporcionando componentes con capacidades técnicas acordes a los niveles de seguridad requeridos.
- **Administración (regulador):** utiliza la IEC 62443 como marco de referencia para armonizar criterios, elaborar políticas públicas, establecer requisitos mínimos y supervisar el cumplimiento en sectores críticos.

Este enfoque por roles refuerza la idea de que la ciberseguridad industrial **es una responsabilidad compartida**, en la que cada actor contribuye a la protección global del sistema desde su ámbito de competencia.

Como se puede apreciar, la familia IEC 62443 proporciona un marco integral que permite abordar la ciberseguridad industrial desde una perspectiva técnica, organizativa y de ciclo de vida. Por ello se considera la norma más importante para entornos ICS/OT, al margen de las sectoriales específicas. Su aplicación estructurada constituye un elemento central para cualquier estrategia de cumplimiento normativo en entornos OT.

5.5 SANS ICS Top 5 Controls

En octubre de 2022, el SANS Institute – conocido organismo de formación en ciberseguridad – publicó un *whitepaper* en el que definía cinco controles de ciberseguridad especialmente relevantes para proteger **sistemas de control industrial (ICS)** y **tecnologías operativas (OT)** [58][59].

Este marco, desarrollado por los expertos de SANS Robert M. Lee y Tim Conway, nació tras un análisis exhaustivo de los ciberataques conocidos contra entornos ICS a nivel global. Su propósito es proporcionar un conjunto conciso de medidas **esenciales – diseñadas específicamente para prevención, detección y respuesta a incidentes en ámbitos industriales –** que sirvan de base para un programa efectivo de ciberseguridad OT.

En contraste con los catálogos extensos de otros estándares generalistas, los **SANS ICS 5 Critical Controls** enfocan los esfuerzos en las áreas críticas de mayor impacto práctico, aportando a las organizaciones industriales una guía clara de "por dónde comenzar" para mejorar su postura de **ciberseguridad industrial**. Además, este conjunto de controles ha sido concebido para ser flexible y adaptable a los distintos

perfiles de riesgo y necesidades de cada organización, manteniendo siempre el foco en las particularidades únicas de los sistemas ICS/OT en cuanto a seguridad y continuidad operativa.

A continuación, **se describen los cinco controles críticos de SANS ICS**, detallando su contenido técnico y ejemplos de aplicación en entornos industriales reales. También se analiza **cómo estos controles funcionan como marco complementario a estándares más amplios (ISO/IEC 27001, ISA/IEC 62443, etc.)** en el ámbito de las infraestructuras industriales.

5 controles críticos para entornos ICS. Fuente: Dragos (2023)

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

El primer control exige contar con un **plan de respuesta a incidentes de ciberseguridad** adaptado a las particularidades de los sistemas industriales (ICS).

Es fundamental que las organizaciones dispongan de un plan de respuesta pensado específicamente para entornos ICS/OT, y que éste **no** se conciba simplemente como la última etapa de un programa de seguridad, sino como un cimiento central del mismo. Un error común es considerar la respuesta a incidentes como "el final del camino", lo que provoca que muchas de las medidas de seguridad implementadas previamente no estén alineadas con las necesidades reales a la hora de gestionar un incidente industrial. Por el contrario, integrar desde el inicio la perspectiva de *incident response* en el plan general de seguridad asegura que la arquitectura, la monitorización y otros controles proporcionen la visibilidad y los datos necesarios para investigar y responder eficazmente cuando ocurre un incidente.

En los entornos OT, las prioridades ante un incidente difieren de las de IT. Mientras los planes tradicionales de TI enfatizan identificación del adversario, contención y erradicación, un **plan de respuesta ICS** debe poner en primer lugar la seguridad de las personas y la continuidad del proceso industrial bajo control. Ello implica que las acciones de respuesta en OT se **priorizan según el impacto potencial en la operación**, buscando mantener los sistemas funcionales aún bajo ataque para reducir al mínimo los efectos sobre la producción y la seguridad física. Un beneficio añadido de esta estrategia es que una buena respuesta a incidentes ICS no sólo minimiza el riesgo ciber, sino que también mejora la resiliencia operativa global al facilitar análisis de causa raíz de cualquier fallo, sea o no causado por un atacante.

Ejemplo aplicado: para preparar este plan, SANS recomienda emplear escenarios basados en incidentes reales. En primer lugar, la organización debe identificar y analizar los escenarios de amenaza **que más riesgo suponen** para sus procesos industriales – por ejemplo, un ataque de ransomware que afecte a las redes OT – tomando como referencias casos ocurridos en el sector. Estos escenarios "dirigidos por inteligencia" (basados en ataques reales) deben tenerse por prioritarios, ya que al haber sucedido en algunos, demuestran ser posibles e incluso repetibles. A modo ilustrativo, **todas las organizaciones industriales deberían disponer de un escenario de ransomware que afecte a la OT**; una empresa petroquímica debería incluir un escenario de manipulación del sistema de seguridad inspirado en el malware TRISIS, y prácticamente todas las compañías eléctricas deberían entrenar con un escenario basado en los apagones de Ucrania de 2015-2016 [60][61]. En segundo lugar, se recomienda contemplar también algún **escenario de consecuencia** hipotética de alto impacto aunque no exista precedente histórico (por ejemplo, un fallo grave de seguridad en una planta que pudiera causar daños físicos o paradas prolongadas). Estos escenarios de "¿y sí...?" ayudan a evaluar qué es teóricamente posible y a anticipar incluso ataques inéditos, aunque deben dosificarse para no desbordar de supuestos irreales; el consejo es limitarse a uno o dos escenarios de máxima consecuencia, manteniendo los pies en la tierra a nivel de contexto y procesos reales de la organización.

Finalmente, el plan de respuesta a incidentes ICS debe ser **puesto a prueba mediante ejercicios prácticos (*table-top exercises*)**. Una vez definidos los escenarios relevantes, deben realizarse simulacros en los que todos los departamentos implicados (operaciones, seguridad, mantenimiento, dirección, legal, etc.) colaboren para desgranar cómo afectaría cada escenario a sus áreas y qué requerimientos tendrían para gestionar el incidente. Estas **pruebas teóricas** permiten verificar si los equipos

disponen de la información y recursos necesarios a tiempo (por ejemplo, logs históricos de ciertos sistemas, contactos de emergencia, procedimientos de aislamiento, etc.), y descubrir posibles defectos a corregir. Además, ayudan a identificar cuáles son los sistemas críticos ("las joyas de la corona") en cada planta industrial y, por lo tanto, dónde se debe focalizar con prioridad la aplicación de los restantes controles críticos.

El Control #1 establece una visión compartida de los riesgos principales y de los resultados que la organización quiere alcanzar ante incidentes, sirviendo de guía para materializar los demás controles críticos.

5.5.2 Control crítico #2: Arquitectura defendible

El segundo control consiste en diseñar y mantener una **arquitectura de red defendible** para los sistemas industriales. Una arquitectura está bien "defendida" cuando, mediante su diseño y configuración, **minimiza al máximo los riesgos** y facilita la labor de los responsables de seguridad en la protección de las instalaciones. En este sentido, existen diversos marcos de referencia – desde el clásico modelo Purdue de segmentación por niveles, hasta arquitecturas modernas basadas en la norma ISA/IEC 62443 – pero lo esencial es su correcta implementación práctica para reforzar realmente la seguridad de la organización. En otras palabras, no bastan los dibujos o estándares en el papel: es necesario materializarlos adecuadamente en la red industrial concreta.

Algunos **atributos clave** que caracterizan una arquitectura ICS defendible son los siguientes:

- **Identificación e inventario de activos:** conocer todos los dispositivos, sistemas y aplicaciones presentes en la red industrial, especialmente en los emplazamientos críticos. Un inventario actualizado sirve de base para proteger y monitorizar eficazmente.
- **Segmentación de redes y zonas:** subdividir el entorno ICS en segmentos o celdas aisladas, limitando estrictamente los puntos de conexión entre ellas (entry/exit points). Ello reduce la superficie de ataque y evita la propagación libre de una amenaza si entra en algún segmento. Por ejemplo, es recomendable implantar **DMZ industriales** o redes perimetrales que hagan de puente seguro entre la red corporativa TI y la red OT, controlando el intercambio de datos entre ambas.
- **Control de la comunicación bidireccional:** determinar con criterio cuáles son los enlaces que realmente necesitan tráfico en ambos sentidos entre diferentes

segmentos (por ejemplo, entre la zona de supervisión y la de control) y restringir aquellas conexiones innecesarias o peligrosas. Sólo deben permitir los flujos imprescindibles para la operación.

- **Capacidad de inspección y recogida de tráfico:** disponer de mecanismos para capturar y examinar el tráfico de red y las comunicaciones industriales. Esto incluye implementar **inspección profunda de paquetes** (DPI) para protocolos ICS – que aporta visibilidad detallada sobre comandos y valores que atraviesan la red – y guardar registros de actividad que puedan ser analizados posteriormente.
- **Registro y análisis de eventos críticos:** la arquitectura debe facilitar *el log* de los sucesos relevantes y su correlación, ya sean alertas de intrusión, cambios de configuración o fallos de equipos. Una buena **telemetría** es crucial para detectar intrusiones o anomalías a tiempo e investigar incidentes a fondo.
- **Postura de seguridad restrictiva:** configurar la red y los sistemas aplicando el principio de privilegio mínimo, eliminando dispositivos o servicios no esenciales y **restringiendo conexiones innecesarias** por defecto. Por ejemplo, deshabilitar puertos y protocolos no utilizados, aplicar listas de control de acceso (ACLs) estrictas entre segmentos, y asegurar que todo acceso remoto o de terceros esté debidamente controlado. Una arquitectura "limpia" y bien segmentada dificulta enormemente el movimiento lateral de un atacante y reduce vías de entrada.

Una arquitectura industrial defendible no sólo protege mejor, sino que **simplifica la monitorización y respuesta a incidentes**. Es de destacar que este control está muy ligado con el Control #3 (visibilidad de la red): una arquitectura bien diseñada permite colocar sensores y puntos de inspección en los lugares adecuados, facilitando una vigilancia efectiva del tráfico y de los sistemas. Por el contrario, sin una correcta segmentación y sin inventario, poco puede ayudar la mejor herramienta de monitorización. La Arquitectura Defendible crea las bases sobre los que operarán los demás controles técnicos de seguridad.

5.5.3 Control crítico #3: Visibilidad y monitorización de la red ICS

El tercer control se centra en lograr una **visibilidad completa de lo que sucede en las redes industriales y en implementar monitorización continua** para detectar a tiempo posibles amenazas. Dado que los entornos ICS/OT actuales son cada vez más complejos y están llenos de protocolos y equipos heterogéneos, tener una visión clara

del tráfico y de las interacciones entre sistemas es vital para varios propósitos: identificar a priori comportamientos anómalos o no deseados, validar que la **arquitectura defendible** del Control #2 está funcionando (por ejemplo, comprobar que la segmentación está deteniendo flujos indebidos), y mejorar tanto la eficacia de la respuesta a incidentes (Control #1) como de otras medidas como el control de accesos remotos o gestión de parches.

En palabras simples, no se puede proteger lo que no se ve: sin visibilidad profunda de la red OT, una organización estará ciega ante intrusiones hasta que sea demasiado tarde.

Implementar este control implica desplegar herramientas y tecnologías especializadas de monitorización industrial. Un aspecto clave es la capacidad de **inspección de protocolos ICS** en profundidad – por ejemplo, comprender tramas Modbus, OPC UA, S7, DNP3, etc. – ya que de esta forma se pueden detectar comandos o valores anómalos propios del dominio industrial (y no sólo paquetes TCP/IP genéricos). Estas herramientas de monitorización (que suelen incluir funcionalidades de inventario automático, IDS/IPS adaptados a ICS, análisis de tráfico e incluso machine learning) como se ha indicado en el Informe de Ciberaleralertas desde mismo Observatorio [1], deben operar preferiblemente de forma no intrusiva o en modo espejo, para no interferir con los sistemas sensibles.

Algunos elementos que una buena solución de visibilidad y monitorización ICS debería proporcionar son:

- **Inventario dinámico de activos y mapas de comunicación:** identificación de todos los dispositivos conectados y visualización de las comunicaciones entre ellos en un mapa o diagrama. Ello permite verificar la arquitectura (p.ej. ver que sólo existen comunicaciones permitidas entre las zonas definidas) y detectar dispositivos desconocidos o no autorizados.
- **Detección de anomalías e intrusiones:** supervisar el tráfico en tiempo real para identificar patrones sospechosos, tanto procedentes del exterior (ataques) como internos (comportamientos fuera de lo normal de los equipos). Un IDS/IPS especializado en protocolos ICS puede lanzar alertas tempranas ante, por ejemplo, un comando inesperado en un PLC o un escaneo de red en la planta.
- **Mecanismos de engaño y detección proactiva:** algunas herramientas incluyen *honeypots* o señuelos dentro de la red industrial para atraer posibles atacantes y estudiar sus técnicas sin riesgo para la operación real. Esto ayuda a identificar

ataques dirigidos antes de que afecten a sistemas de producción, dando más margen de maniobra a la defensa.

- **Bloqueo de tráfico malicioso:** aunque la función principal es detectar, en ocasiones también puede optar por intervenir activamente para **cortar comunicaciones no autorizadas** o claramente maliciosas (por ejemplo, mediante listas de bloqueos o segmentación dinámica). De esta forma se reduce la superficie de ataque en tiempo real.
- **Correlación y análisis forense de eventos:** integración con los sistemas de registro (SIEM/SCADA logging) para correlacionar eventos de distintas fuentes y realizar análisis forenses completos tras un incidente. En un entorno ICS, esto puede significar correlacionar alertas de la red con alarmas del sistema de control de procesos, logrando una visión unificada del incidente que fortalezca la respuesta y las acciones de remediación.

La visibilidad OT alcanza un valor muy superior cuando no permanece aislada, sino que se integra con los servicios corporativos de seguridad de la organización. **La conexión de las herramientas OT de monitorización con SIEM, SOC y sistemas de análisis y respuesta permite correlacionar alertas de red industrial, cambios en protocolos ICS, eventos de autenticación, actividad en endpoints e incidentes en servicios corporativos, construyendo una visión unificada del ataque.** Esto es especialmente **útil en escenarios de convergencia IT/OT, en los que una intrusión puede iniciarse por correo electrónico, acceso remoto o credenciales comprometidas y materializarse después en el ámbito industrial.** A este fin, pueden emplearse **plataformas CPS PP (de protección de sistemas ciberfísicos) con soluciones especializadas de mercado —como la gallega InprOTech Guardian, Nozomi, Claroty, Armis o Darktrace/OT—** siempre bajo criterios de despliegue no intrusivo, segmentación, mínimo privilegio y compatibilidad con el proceso industrial.

Este control busca dotar al equipo de seguridad industrial de una **"torre de vigilancia"** desde la que observar en régimen continuo el estado de la red y de los sistemas ICS. Con ella podrán descubrir más rápidamente actividades anómalas – por ejemplo, la presencia de un dispositivo ajeno conectado en la red de automatización, o una subestación enviando más datos de lo habitual – y **actuar con antelación** antes de que una amenaza se materialice en impacto real. Además, una buena visibilidad reduce significativamente el tiempo y coste de investigar incidentes (por ejemplo, para localizar

la causa raíz de una parada inesperada en una planta), algo crítico cuando cada minuto de producción perdido cuenta [62][63].

5.5.4 Control crítico #4: Acceso remoto seguro

El cuarto control aborda uno de los vectores de amenaza más frecuentes en la industria moderna: **el acceso remoto** a sistemas OT. Con la digitalización y la necesidad de interconectar plantas, suministradores y personal de operación distribuido, **hoy en día es habitual que las infraestructuras industriales dispongan de accesos remotos para mantenimiento, soporte de proveedores o gestión centralizada.** En muchos casos podrían limitarse o eliminarse algunos accesos, pero en la mayoría de las organizaciones industriales **son inevitables** dadas las necesidades del negocio actual.

Por supuesto, esta conectividad remota trae también consigo importantes riesgos: desde intrusiones vía VPN o escritorio remoto, hasta uso indebido de credenciales por terceras partes, entre otros. El objetivo del control #4 es asegurar que todos estos accesos se gestionen con la máxima seguridad posible, reduciendo la superficie de ataque asociada.

Las recomendaciones principales incluyen establecer medidas de control de identidad robustas y limitar al mínimo los privilegios y origen de esos accesos. En particular, **implantar autenticación multi-factor (MFA)** es una contramedida hoy indispensable en cualquier acceso remoto a entornos ICS. Además, **deben cifrarse** todas las comunicaciones remotas (usando VPNs seguras, SSH, TLS, etc.) y **restringirse los accesos** sólo a aquellos usuarios, dispositivos y horarios realmente necesarios, siguiendo el principio de mínimo privilegio. Por ejemplo, si un proveedor tiene que dar soporte a un PLC en una fábrica, se podría habilitar un acceso VPN únicamente durante las ventanas acordadas y sólo a la red de esa planta concreta, nunca a la red completa.

Otras buenas prácticas son el empleo de servidores de salto o pasarelas intermedias para acceder a los equipos OT (evitando conexiones directas desde Internet a los controladores), el **registro exhaustivo de todas las sesiones remotas** (para auditoría y posibles análisis forenses), y **la monitorización continua de estas sesiones** mediante el Control #3 anterior. Cuando algún tipo de acceso remoto no sea compatible con una medida como MFA – por ejemplo, algunos equipos ICS muy antiguos que no admitan autenticación robusta – la organización debe establecer **controles compensatorios apropiados**. Esto puede incluir desde aislar ese equipo en una red muy restringida y monitorizada, hasta utilizar métodos alternativos de validación manual o acceso físico supervisado.

El Control #4 trata de **cerrar la puerta de entrada** más explotada por los adversarios (los accesos remotos), sin sacrificar la operativa.

5.5.5 Control crítico #5: Gestión de vulnerabilidades basada en el riesgo

El último de los cinco controles centrales de SANS se enfoca en la **identificación y tratamiento de las vulnerabilidades** presentes en los sistemas industriales, empleando un enfoque basado en el riesgo. La gestión de vulnerabilidades en ICS/OT presenta retos particulares: los sistemas de control industrial suelen tener ciclos de vida muy largos (décadas), emplean hardware/software propietario que a veces no se puede actualizar fácilmente, y en muchas instalaciones sólo pueden aplicarle parches durante paradas programadas poco frecuentes. Por ello, un programa de vulnerabilidades en OT debe ir más allá del simple scanning periódico y parcheo inmediato que se aplicaría en un entorno TI convencional.

En primer lugar, **es necesario inventariar y evaluar las vulnerabilidades** de forma continua. Cada día se anuncian nuevas vulnerabilidades que pueden afectar a PLCs, SCADAs, sistemas SCADA, protocolos, etc., por lo que la labor de Threat intelligence y escaneo debe ser permanente. Una vez identificadas, hay que **priorizarlas según el riesgo**: no todas las debilidades en una red industrial tienen la misma criticidad. Debe prestarse atención prioritaria a las vulnerabilidades que realmente **pueden poner en peligro el proceso industrial o la seguridad** – por ejemplo, aquellas que permitirían a un atacante acceder a la red de control o ejecutar código en los sistemas de automatización – frente a otras menores o de difícil explotación. Esto implica conocer bien el contexto: una vulnerabilidad crítica en un sistema expuesto en DMZ puede ser irrelevante en un PLC aislado sin conexión, y viceversa.

Seguidamente, hay que **escuchar las restricciones operativas**: en muchos casos no será factible aplicar parches de inmediato porque ello implicaría detener la producción o invalidar certificaciones del fabricante. Cuando parchear no sea posible a corto plazo, el enfoque basado en el riesgo propone implementar **medidas de mitigación alternativas** para cada vulnerabilidad crítica identificada. Por ejemplo, si un determinado controlador tiene una vulnerabilidad sin parche disponible, puede mitigarse segmentando ese equipo en una subred aislada, reforzando la monitorización de su tráfico (para detectar intentos de explotación) o limitando estrictamente quién puede comunicarse con él. Estas contramedidas reducen el riesgo hasta que se pueda aplicar el parche definitivo en una parada planificada.

En paralelo, debe establecerse **vigilancia continua**: mantenerse alerta ante nuevos exploits o herramientas de ataque relacionadas con la vulnerabilidad, y monitorizar cualquier signo de intento de explotación en los sistemas de la planta (aquí de nuevo juega un papel el Control #3 de monitorización).

Lo importante es adoptar una visión más amplia que la mera gestión de los parcheos. La filosofía de este control es: "no dejar cabos sueltos". En última instancia, el programa de gestión de vulnerabilidades OT debe lograr un equilibrio óptimo entre **seguridad y continuidad operativa**. Se trata de reducir la exposición a amenazas conocidas – enfocándose en las más peligrosas – sin poner en riesgo la estabilidad de los procesos industriales por querer aplicar medidas apresuradas. Este equilibrio es especialmente crucial en infraestructuras críticas, donde cualquier cambio debe ser evaluado con lupa.

El Control #5 asegura que la organización conozca sus debilidades técnicas y actúe de forma inteligente sobre ellas, priorizando lo que realmente importa para evitar incidentes graves.

5.5.6 Complementariedad con otros estándares

Los *SANS ICS 5 Critical Controls* nacieron **como complemento pragmático**, no para sustituir a los marcos normativos existentes. De hecho, los autores desarrollaron estos controles conscientes de que existían múltiples estándares y guías de seguridad industrial – por ejemplo, la familia **ISA/IEC 62443**, ESO/IEC 27001/27002, NIST CSF, entre otros – que ofrecen una visión muy amplia de la ciberseguridad en entornos industriales. Sin embargo, muchos de esos estándares fueron creados en un momento en el que la visibilidad de amenazas ICS era limitada, por lo que en gran medida *heredaron controles genéricos de IT aplicados indirectamente a OT*. El resultado es que a veces adherirse a todos los requerimientos de un estándar no garantiza abordar los riesgos más evidentes frente a las amenazas OT actuales. Además, la mayoría de estos marcos hacen hincapié en la **prevención** (hasta un 60–95% de los controles son preventivos según SANS) y dedican menos atención a capacidades de **detección y respuesta** específicas de entornos ICS. Esto puede generar una falsa sensación de seguridad, si las organizaciones invierten mucho en prevención, pero carecen de visibilidad para percatarse de cuándo esas defensas fallan.

Frente a esa situación, los cinco controles críticos de SANS vienen a **equilibrar y focalizar** los esfuerzos de seguridad industrial en un conjunto interdependiente de medidas preventivas, detectivas y de respuesta. No se trata de un nuevo estándar que haya que certificar, sino de **una base común** y práctica para comunicar prioridades y

comprobar progresos. Son una especie de "lista de tareas urgentes" que complementa los requisitos obligatorios: para sectores no regulados, proporcionan un enfoque claro y programático de la seguridad OT; y para aquellos con regulación madura, señalan en que aspectos **ir más allá del mínimo normativo** para estar por encima de un adversario que también conoce los estándares.

Estos controles, cuando se implementan de forma coordinada y priorizada, ayudan a construir un programa de seguridad robusto adaptado a los riesgos reales del entorno industrial. En lugar de intentar "hacerlo todo" según interminables checklists, el marco de SANS enfoca lo que realmente importa: estar preparados para responder a incidentes graves, tener arquitecturas resilientes, observar de cerca las redes, proteger los accesos más vulnerables, y gestionar inteligentemente las debilidades técnicas del tejido industrial de la región.

6 Guía de implantación práctica

La complejidad del ecosistema normativo en materia de ciberseguridad obliga a las organizaciones industriales a **abordar su adaptación de una forma estructurada, priorizada y realista**. El presente apartado ofrece una aproximación práctica para iniciar y consolidar este proceso, **centrándose exclusivamente en las siguientes normas descritas a lo largo de este documento**: **ISO 27001, ENS, NIS2, RGPD, LPIC, CER, CRA, NIST CSF, CIS Controles, IEC 62443 y SANS ICS Top 5 Controles**.

Se trata de un posible enfoque, pero no es el único válido. Pretende servir como punto de partida para el diseño de hojas de ruta personalizadas, que dependerán de múltiples factores como el tamaño de la organización, su grado de madurez, el sector en el que opera o si está sujeta a obligaciones reguladoras específicas. Para ello, **se analizarán las características comparadas de las distintas normas**, y se **propondrán itinerarios progresivos de implantación y adaptación**, con orientaciones sobre su **orden de magnitud a nivel de esfuerzo temporal (bajo, medio, alto)**, sin entrar en estimaciones rígidas que puedan ser irreales o inexactas, al ser fuertemente dependientes de la situación particular.

El objetivo es dotar a las organizaciones de un **marco orientativo adaptado al contexto de la ciberseguridad industrial**, facilitando la toma de decisiones estratégicas y operativas para el cumplimiento y mejora continua en esta materia.

6.1 Cuadro comparativo de normas

De nuevo con el fin de facilitar la toma de decisiones en materia de cumplimiento normativo y fortalecimiento de la seguridad, se presenta a continuación una tabla comparativa de las **principales normas y marcos analizados previamente**, enfocadas a la protección de sistemas de información y datos personales, infraestructuras críticas, y/o entornos industriales OT/ICS, según el caso.

La tabla analiza cada norma según los siguientes criterios:

- **Norma / Marco**: identificación de la norma o conjunto normativo.
- **Obligatoriedad**: si es **legalmente obligatoria**, depende de **contexto**, o es **voluntaria**.
- **Sector o ámbito**: universo al que aplica, como administración pública, infraestructuras críticas, industria o cualquier organización.

- **Certificable**: si es posible obtener una **certificación oficial externa** tras la auditoría.
- **Enfoque principal**: objetivo o área de acción principal de la norma.
- **Nivel de detalle**: grado de **especificidad técnica** (alto, medio o básico).

Norma / Marco	Obligatorio/a	Sector o ámbito	Certificable	Enfoque principal	Nivel de detalle
ISO/IEC 27001	Voluntaria, pero exigida en contratos o auditorías	Cualquier sector	Sí	Sistema de gestión de la seguridad de la información (SGSI)	Medio
ENS (Esquema Nacional de Seguridad)	Obligatoria para sector público y proveedores TIC	Administración pública y contratistas tecnológicos	Sí	Requisitos mínimos de seguridad de la información en el sector público	Alto
NIS2	Obligatoria para entidades designadas	Sectores esenciales e importantes en UE	No	Ciberseguridad en entidades críticas, obligaciones de gestión de riesgo y notificación	Medio-alto
RGPD	Obligatoria por legislación de la UE	Cualquier entidad que trate datos personales	No	Protección de datos personales y derechos digitales	Medio
LPIC	Obligatoria	Entidades críticas físicas	No	Protección y resiliencia de entidades críticas físicas	Medio
CER (Directiva UE 2022/2557)	Obligatoria (directiva europea en transposición)	Infraestructuras físicas esenciales	No	Evaluación de riesgo físico, resiliencia y coordinación nacional	Medio

CRA (Cyber Resilience Act)	Obligatoria desde 2026-2027	Fabricantes e importadores de HW/SW con elementos digitales	Parcialmente	Requisitos de ciberseguridad en productos con elementos digitales	Alto
NIST CSF 2.0	Voluntaria	Cualquier organización	No	Marco de gestión de riesgos de ciberseguridad	Medio
CIS Controls v8.1	Voluntaria	Cualquier organización, aplicable a OT/ICS	No	Medidas técnicas priorizadas para protección frente a amenazas comunes	Medio
IEC 62443	Voluntaria, recomendada en industria y contratos	Entornos OT/ICS industriales	Parcialmente	Ciberseguridad industrial, defensa en profundidad en entornos ICS	Alto
SANS ICS Top 5 Controls	Voluntaria	Entornos industriales e infraestructuras críticas	No	Controles mínimos esenciales para seguridad en ICS/OT	Básico-medio

Tabla comparativa de normas y marcos normativos de ciberseguridad. Fuente: elaboración propia (2026)

Este análisis permite comparar de manera rápida **el alcance, rigor técnico y aplicabilidad práctica** de las normas, facilitando su selección en función de las características y madurez de cada organización.

6.2 Identificación del punto de partida

Las necesidades normativas y estratégicas varían notablemente en función del **tamaño de la organización, sector de actividad** y del **tipo de cliente al que se dirige**. En este apartado se analiza cómo debería afrontarse la adaptación normativa en empresas industriales, atendiendo a diferentes casuísticas. De nuevo, se trata de una aproximación de muy alto nivel, que habrá que revisar o adaptar en cada escenario.

Advertir de que antes de decidir qué norma abordar primero y con qué nivel de ambición, es conveniente de un diagnóstico inicial estructurado. Este diagnóstico puede adoptar la forma de una evaluación de madurez, de una revisión de controles

existentes o de un análisis GAP frente a **los marcos de referencia seleccionados.** Su valor reside en ofrecer una fotografía objetiva de la situación de partida, identificando fortalezas, carencias, controles ya implantados, evidencias disponibles y ámbitos con mayor exposición al riesgo. **Sobre esta base, la organización puede construir una hoja de ruta más realista a nivel de tiempos y esfuerzos, priorizada y defendible**, evitando tanto implantaciones excesivamente teóricas como inversiones desordenadas sin criterio metodológico.

Lo primero que cabe subrayar, es que independientemente del tamaño, hay ciertas normas o reglamentos que son de obligado cumplimiento si caemos dentro del ámbito de aplicación, como son:

- **RGPD**, si los procesos industriales involucran datos personales.
- **LPIC (e CER)**, si se trata de infraestructuras críticas (y físicas).
- **ENS**, en ciertos modelos B2G (relación con la Administración Pública o suministrador de la misma).
- **NIS2**, en caso de tratarse de una entidad esencial o importante según la definición de la Directiva.
- **CRA,** si la entidad manufactura dispositivos IoT y/o productos electrónicos.

Con respecto al resto de normas, de manera general lo que se puede también decir es que la **ISO 27001** con un alcance más o menos ambicioso debería ser el punto de partida recomendable para cualquier organización independientemente de su nivel de madurez. Por otro lado, en el mundo anglosajón se utiliza de forma equivalente (aunque no lo sea), el marco **NIST CSF**.

En caso de requerir **ENS**, certificarse previamente en **ISO 27001** aplana bastante el camino de cara al cumplimiento. Y teniendo ENS, pasar a adherirse a la **Directiva NIS2**, a falta de aterrizar el anteproyecto de Ley en curso, es un GAP relativamente pequeño, a la luz de lo que se comentó de la equivalencia NIS2 <> ENS propuesta por el CCN.

Si hablamos por último de los marcos más técnicos, los **CIS controls** permiten alcanzar un nivel de seguridad razonable a nivel técnico con un esfuerzo más o menos acotado, pero dejando ciertamente algo de lado la parte de gobierno y gestión de la seguridad (controles organizativos y procedimentales), por lo que nunca recomendaríamos implementarlos por separado.

Y en caso de apostar ya claramente por securizar el entorno ICS/OT, habiendo previamente resuelto la cuestión del SGSI, apostaríamos en función de las capacidades técnicas, presupuestarias y de recursos, por los **SANS ICS Top 5 Controles**, o **IEC 62443**

(de menor a mayor grado de exigencia), y teniendo en cuenta que, en determinados ámbitos o según la relación con cliente, la segunda puede ser obligatoria. Y desde luego, es la que denota un mayor grado de compromiso con la protección de estas infraestructuras.

6.2.1 Según el tipo de empresa y necesidades

La adaptación y cumplimiento de las distintas normativas y estándares de ciberseguridad debe considerar **el perfil de la empresa según sus características estructurales y operativas**. Para ello, realizaremos una clasificación según el **tamaño organizativo** (pequeña, mediana o gran empresa) y según **el tipo de cliente objetivo principal, teniendo** en cuenta si opera **con administración pública (modelo B2G)**, **con otras empresas (modelo B2B)**, **con el consumidor final (modelo B2C)** y si trabaja con **clientes internacionales**, sean **europeos** (sujetos a regulaciones comunes como RGPD o NIS2) o **anglosajones** (que pueden dar prioridad a marcos como NIST o SANS).

Perfilaremos a continuación un retrato robot de entidades por talla, centrándonos en la actividad industrial. Ténganse en cuenta en cualquier caso, las salvedades apuntadas en el apartado previo.

- Las **pequeñas empresas industriales**, suelen contar con recursos limitados en ciberseguridad, sin personal dedicado en exclusiva y con dependencias de proveedores externos. En muchos casos, la digitalización es incipiente y la presencia de sistemas conectados a internet es reducida, pero no por ello exenta de riesgos. Conviene priorizar marcos ligeros y progresivos como los **CIS Controls**, apoyándose en una adaptación parcial a estándares más ambiciosos como **ISO 27001** (siempre recomendable para contar un SGSI en base a buenas prácticas internacionales como base), o **SANS ICS Top 5 Controls** en el caso de organización más ambiciosas.
- Las empresas **medianas industriales**, comienzan a incorporar arquitecturas OT más complejas, interconectadas con redes TI en muchos casos, con un número creciente de activos industriales y exposición a la cadena de suministro. Este tipo de empresas puede estar ya afectado por obligaciones legales como **NIS2**, o **CRA si manufacturan productos electrónicos**, e interesa también preparar el terreno para certificaciones voluntarias (ISO, IEC). Además, si trabajan con Administraciones públicas o en sectores regulados, se verán afectadas por marcos como **ENS, CER** o **LPIC**.

- Las **grandes empresas industriales**, normalmente cuentan con un sistema maduro de gobernanza y seguridad, equipos especializados y capacidades de gestión integral de riesgos. Están afectadas por **muchas regulaciones normativas vigentes** y suelen implementar esquemas certificados como **ISO 27001**, **IEC 62443** o estructuras de madurez como **NIST CSF**. También se espera de ellas que dispongan de **planes de resiliencia y respuesta a incidentes**, especialmente si prestan servicios esenciales o críticos **(LPIC, CER)**.

En lo relativo al **cliente objetivo**:

- Si la empresa opera con **administración pública**, debe considerar de forma prioritaria **el ENS,** y si presta servicios o productos relacionados con la seguridad física, también **LPIC** y **CER**.
- En caso de trabajar con **otras empresas (modelo B2B)**, especialmente en sectores como energía, transporte o salud, el grado de exigencia normativa es alto, siendo habitual la exigencia contractual de **certificaciones (ISO, IEC, CRA)** o **evaluaciones de conformidad con el NIST CSF**.
- Las empresas **que venden al consumidor final (modelo B2C)** deben tener especial cuidado con el cumplimiento del **RGPD** y de la **CRA**, en el caso de ofrecer productos con componentes digitales conectados.
- Si la empresa trabaja con **clientes internacionales europeos**, las normas como **ISO, NIS2**, **RGPD**, **CRA** y **CER** deben ser referencia principal. Por el contrario, si los clientes son **anglosajones**, puede existir una preferencia clara por **NIST CSF**, **CIS Controls** o marcos **ISA,** como **IEC 62443**.

6.3 Estimación de esfuerzos

La adaptación efectiva a los distintos marcos y normativas de ciberseguridad requiere un análisis previo del **esfuerzo estimado** que puede suponer su implantación para cada organización. Este esfuerzo **varía significativamente** en función de múltiples factores: el grado de madurez de la empresa, su estructura interna, su sector, su tamaño, el nivel de digitalización y, sobre todo, el **nivel de compromiso e intensidad de aplicación** que se pretenda alcanzar.

Así, el esfuerzo puede oscilar entre **pocos meses de trabajo bien enfocado**, en casos de cumplimiento mínimo y con apoyo externo, hasta **proyectos progresivos de largo recorrido** que se extienden a lo largo de **2 o 3 años o más**, especialmente cuando se aspira a integrar las normas de forma transversal y completa en la cultura de la organización.

Para **representar este esfuerzo de forma práctica**, utilizaremos una **clasificación cualitativa** en tres niveles orientativos:

- **Bajo** → Esfuerzo relativamente reducido, asumible con recursos limitados en un plazo estimado de hasta 12 meses.
- **Medio** → Requiere planificación, coordinación y mayor carga de trabajo (entre 12 y 24 meses).
- **Alto** → Implica despliegue organizativo amplio, integración progresiva y varios ciclos de mejora (24–36 meses o más).

Esta estimación se realizará teniendo en cuenta las siguientes **dimensiones clave** para cada normativa o marco:

- **Obligatoriedad**: si su cumplimiento es exigido por normativa o contrato, o es voluntario.
- **Certificabilidad**: si implica auditorías o emisión formal de certificación por tercero acreditado.
- **Enfoque predominante**: legal, técnico, organizativo o híbrido.
- **Impacto organizativo**: grado de transformación en los procesos, responsabilidades, recursos y cultura interna.
- **Complejidad de implantación**: número y dificultad de los controles, dependencia de proveedores, tecnología y grado de detalle exigido.

Dicho todo lo anterior, se toma la siguiente tabla como una referencia de orden de magnitud grueso.

Norma / Marco	Esfuerzo estimado	Certificable	Enfoque principal	Impacto organizativo	Notas relevantes
ISO/IEC 27001	Medio	Sí	Técnico + gestión	Alto	Implica un SGSI completo
ENS	Medio / Alto	Sí	Técnico + gestión	Medio/Alto	Exigido en contratos públicos. Tener ISO previamente acorta tiempos. Plazos dependen del nivel ENS a alcanzar

NIS2	Medio / Alto	No (directa)	Legal + técnico + gestión	Alto	Altamente regulado para entidades medianas y grandes. Tener ENS agiliza.
RGPD	Medio	No	Legal	Medio	Revisión continua de procesos y datos, más EIPDs en algunos casos
LPIC	Medio	No	Legal + técnico	Medio/Alto	Requiere planificación de planes y designación de responsables
CER	Alto	No	Legal + técnico + físico	Alto	Para entidades críticas, exige planes e informes
CRA	Medio / Alto	Si (producto)	Legal + producto (técnico)	Alto (para fabricantes)	Aplicable a hardware/software con conectividad
NIST CSF	Medio	No	Técnico + gestión	Medio	Referencia flexible, no obligatoria
CIS Controls	Bajo / Medio	No	Técnico práctico	Bajo / Medio	Ideal para pequeñas y medianas empresas
IEC 62443	Alto	Si (parcial)	Técnico + gestión OT	Alto	Alto nivel técnico y segmentado por rol
SANS ICS Top 5	Medio	No	Técnico + gestión OT	Bajo / Medio	Ideal para primera capa de defensa OT. Flexible

Estimación de esfuerzo de implantación de marcos normativos. Fuente: elaboración propia (2026)

En cualquier caso, una vez se comprenden los diferentes marcos normativos, regulaciones y buenas prácticas, lo ideal es **contactar con algún proveedor de servicios de adecuamiento normativo o ciberseguridad técnica, de cara a definir**

tanto un alcance como una planificación temporal más ajustada a la casuística concreta y necesidades de la organización.

A este fin, se puede hacer uso del **magnífico recurso que proporciona el Mapa de capacidades digitales de Galicia, auspiciado por la Xunta de Galicia (Gaiastech)** [68].

7 Conclusiones

La presente **Guía normativa de ciberseguridad industrial** fue elaborada con el objetivo de proporcionar a las organizaciones públicas y privadas de Galicia una **panorámica amplia y clara** para **comprender y abordar las obligaciones normativas y las buenas prácticas en materia de ciberseguridad en entornos industriales y de Tecnología Operacional (OT)**.

La guía afronta de manera sintética el **marco normativo nacional, con especial atención al Esquema Nacional de Seguridad (ENS)** y a su evolución reciente, **así como a la normativa de protección de infraestructuras críticas y a la legislación en materia de protección de datos personales**. Complementariamente, se analiza el **marco normativo europeo**, destacando la **Directiva NIS2, el Reglamento CER** y otras iniciativas que introducen nuevas obligaciones para entidades industriales y operadores de servicios esenciales.

En el ámbito de los **marcos y estándares internacionales**, la guía integra y relaciona estándares ampliamente reconocidos como **ISO/IEC 27001**, **NIST CSF, IEC 62443 y** otros marcos de referencia, explicando su alcance, complementariedad y aplicabilidad práctica en entornos industriales. **Este ejercicio de síntesis permite a las entidades destinatarias identificar con mayor claridad qué estándares les resultan de aplicación o interés, y cómo pueden alinearlos de manera coherente.**

Finalmente, la guía incorpora una **orientación práctica para la implantación**, aportando criterios, ejemplos y recomendaciones que **facilitan la adopción de los marcos o al menos, el establecimiento de una hoja de ruta, adecuada a las obligaciones, al nivel de riesgo y al grado de madurez de cada organización.**

El análisis realizado a lo largo de la Guía permite extraer una **serie de conclusiones relevantes que afectan directamente a las entidades gallegas** que operan en sectores industriales o gestionan infraestructuras y servicios críticos.

En primer lugar, queda patente que **la seguridad de la información en el campo industrial ha dejado de ser una cuestión puramente técnica** para convertirse en un elemento estratégico de gestión del riesgo, con implicaciones legales, operativas y reputacionales. El incremento de las exigencias reglamentarias, especialmente a partir de la NIS2, obliga a las organizaciones a adoptar enfoques más estructurados y documentados.

En segundo lugar, la guía evidencia que **no existe una única norma o estándar que resuelva de forma aislada todas las obligaciones**, sino que es necesario un enfoque integrado que combine regulación, estándares internacionales y buenas prácticas. En este contexto, marcos como la IEC 62443 juegan un papel central al proporcionar un modelo específico para entornos OT, complementando enfoques más generales como ISO/IEC 27001.

Otra conclusión clave es la importancia de adoptar un **enfoque basado en el riesgo y en la madurez**, evitando aproximaciones uniformes o excesivamente prescriptivas. La guía promueve una implantación progresiva, adaptada a la realidad de cada organización, lo que resulta especialmente relevante para las PyMEs industriales gallegas, con recursos más limitados.

Asimismo, se pone de relieve la necesidad de **clarificar roles y responsabilidades** entre operadores, integradores, fabricantes y Administraciones Públicas. **La ciberseguridad industrial debe entenderse como una responsabilidad compartida a lo largo de toda la cadena de valor**, en la que cada actor desempeña un papel específico y complementario.

Desde una perspectiva territorial, la guía pretende contribuir a **fortalecer el ecosistema gallego de ciberseguridad industrial**, ofreciendo una referencia común que, en caso de aprovechamiento, mejorará la preparación frente a auditorías e inspecciones, reforzando así la confianza en la protección de procesos y servicios críticos.

Finalmente, esta Guía Normativa **no debe entenderse como un documento estático, sino como una base evolutiva que deberá adaptarse a la progresiva variación de las amenazas y a los cambios regulatorios todavía por llegar.** En futuras ediciones de la guía podría plantearse incorporar plantillas detalladas para la adherencia normativa, o modelos de madurez para su desarrollo progresivo y faseado dentro de una organización.

De lo que no cabe duda, es de que la **comprensión y aplicación efectiva de los marcos propuestos, permitirá avanzar hacia modelos más resilientes, seguros y competitivos, contribuyendo a la protección del tejido industrial gallego y al desarrollo sostenible de su economía.**

Bibliografía

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

[2] Observatorio de Ciberseguridad Industrial de Galicia (2025). *Informe de Inteligencia de Amenazas - 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 del Estado (2010). *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.* Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1331

[6] Boletín Oficial del Estado (2022). *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.* Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191

[7] Parlamento Europeo y Consejo de la UE (2019). *Reglamento (UE) 2019/881 relativo a ENISA y a la certificación de la ciberseguridad de la información y las comunicaciones.* Recuperado de https://eur-lex.europa.eu/legal-content/GL/TXT/?uri=CELEX%3A32019R0881

[8] Parlamento Europeo y Consejo de la UE (2016). *Directiva (UE) 2016/1148 relativa a medidas para garantizar un nivel común elevado de seguridad de las redes y sistemas de información en la Unión (Directiva NIS).* Recuperado de https://eur-lex.europa.eu/legal-content/GL/TXT/?uri=CELEX%3A32016L1148

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

[10] Gobierno de España (2019). *Estrategia Nacional de Ciberseguridad, publicada mediante Orden PCI/487/2019, de 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] Gobierno de España (2022). *Aprobación del Plan nacional de ciberseguridad.* Recuperado de https://www.mpr.gob.es/prencom/notas/paginas/2022/290322-ciberseguridad.aspx

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

[13] Centro Criptológico 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 Criptológico Nacional (2022). Infografía 04 – ENS 2010 vs ENS 2022: Diferencias y 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 de la Administración Electrónica (n.d.). *Esquema Nacional de Seguridad.* Recuperado de https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad.html#.ZFE_aHZByP0

[16] Centro Criptológico Nacional (2022). *ENS Navegable – Revisión visual e interactiva de las medidas de seguridad del Real Decreto 311/2022.* Recuperado de https://gobernanza.ccn-cert.cni.es/ens-navegable

[17] Centro Criptológico Nacional (2017). *Guía CCN-STIC-804 – Implantación del 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 del Estado (2018). *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y 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 del Estado (2011). *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.* Recuperado de: https://www.boe.es/eli/es/l/2011/04/28/8/con

[21] Boletín Oficial del Estado (2011). *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.* Recuperado de: https://www.boe.es/eli/es/rd/2011/05/20/704/con

[22] LISA Institute. *Infraestructuras críticas: definición, planes, riesgos, amenazas y legislación.* Recuperado de: https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas

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

[24] Departamento de Seguridad Nacional (2019). *Estrategia Nacional de Ciberseguridad 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 de la Presidencia, Relaciones con las Cortes y Memoria Democrática (2022). *Nota de prensa: Aprobación del Plan Nacional de Ciberseguridad.* Recuperado de: https://www.mpr.gob.es/prencom/notas/paginas/2022/290322-ciberseguridad.aspx

[26] Boletín Oficial del Estado (2025). *PJC/448/2025, de 6 de mayo, por el que se aprueban actuaciones para complementar las recogidas en el Plan Nacional de Ciberseguridad*. Recuperado de: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2025-9088

[27] Unión Europea (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos - RGPD)*. Recuperado de https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04

[28] Boletín Oficial del Estado (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD)*. Recuperado de https://www.boe.es/eli/es/lo/2018/12/05/3/con

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

[30] Boletín Oficial del Estado (1995). *Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678

[31] Organización Internacional de Normalización (ISO) (2018). *ESO 31000:2018. Gestión del riesgo. Principios y directrices*. Recuperado de https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

[32] Centro Criptológico Nacional (CCN) (2022). *MAGERIT – Metodología de Análisis y Gestión de Riesgos de la 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 evaluación de impacto relativa a la 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] Agencia Española de Protección de Datos (AEPD) (2022). *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*. Recuperado de https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

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

[36] Congreso de los Diputados (2003). *Constitución Española. Derechos y libertades*. Recuperado de https://app.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=18&tipo=2

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

[38] Agencia Española de Protección de Datos (AEPD) (1993). *Herramientas de interés*. 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 de la 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 esenciales e importantes en el 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 del Interior (2025). *Anteproyecto de Ley de coordinación y gobernanza de la ciberseguridad*. 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 y Consejo (2024). *Reglamento (UE) 2024/1680 del Parlamento Europeo y del Consejo, de 12 de marzo de 2024, relativo a los requisitos de ciberseguridad para productos con elementos digitales (Ley de Ciberresiliencia)*. Recuperado de https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81720

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

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

[49] Ministerio del Interior (2025). *Anteproyecto de Ley de protección y 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. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos*. Recuperado de https://www.iso.org/standard/27001

[51] ISO/IEC (2022). *ISO/IEC 27002:2022. Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información*. Recuperado de https://www.iso.org/standard/75652.html

[52] ISO (2019). *ESO 22301:2019. Seguridad y resiliencia — Sistemas de gestión de la continuidad del negocio — Requisitos*. Recuperado de https://www.iso.org/standard/75106.html

[53] NIST (2024). *El NIST publica la versión 2.0 de su marco histórico de ciberseguridad*. 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 del 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 del SANS Institute*. Recuperado de: https://www.sans.org/

[59] SANS Institute (2022). *Whitepapers sobre los 5 controles 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, el malware que amenaza la industria mundial*. Recuperado de: https://technologyreview.es/article/asi-se-propaga-triton-el-malware-que-amenaza-la-industria-mundial/

[61] ESET – WeLiveSecurity (2016). *Ciberataque causó cortes de luz en Ucrania*. 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 el estándar IEC 62443 en un proyecto de digitalización 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 digitales de Galicia*. Recuperado de: https://gaiastech.xunta.gal/es/mapa-de-capacidades-digitales-de-galicia

CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridad Industrial
Guía normativa de ciberseguridad industrial

AMTEGA – Xunta de Galicia 2026

Financiado pola Unión Europea NextGenerationEU

Plan de Recuperación, Transformación e Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA