EL FUTURO DE LA CIBERSEGURIDAD: MARCO NORMATIVO Y TECNOLOGÍAS EMERGENTES

Webinar de capacitación y sensibilización en materia de ciberseguridad

16 de julio de 2026

Financiado por la Unión Europea NextGenerationEU

CONTENIDOS

Introducción a RED ARGOS

BLOQUE I: Marco normativo vigente y en tramitación:

- NIS2 (Directiva UE 2022/2555) y su transposición al ordenamiento español.
- Esquema Nacional de Seguridad (ENS) — RD 311/2022: obligaciones y niveles.
- Familia de normas ISO 27000 y 27001: qué implica la certificación.
- Reglamento de Ciberresiliencia (Cyber Resilience Act — Reglamento UE 2024/2847).
- Estrategia de Especialización Inteligente de Castilla y León 2021-2027 (RIS3).
- Estrategia Deep Tech España 2026-2030.
- Proyecto de Ley IA.

BLOQUE II: Tecnologías emergentes con impacto en ciberseguridad:

- Inteligencia Artificial aplicada a la ciberseguridad (detección de amenazas, ataques con IA).
- Arquitectura de Confianza Cero (Zero Trust)
- Tecnologías cuánticas: amenazas a la criptografía actual y criptografía post-cuántica.

BLOQUE III: Implicaciones prácticas para las pymes:

- Qué deben hacer ahora y cómo prepararse.
- Implicaciones técnicas, legales y régimen sancionador.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

PROYECTO RED ARGOS

¿Qué es?

Quién lo impulsa: Coordinado por ICECYL, con la participación de Andalucía y País Vasco.

Objetivo: Fortalecer el ecosistema nacional de ciberseguridad empresarial.

Programa en que se enmarca: Nodo 1 del programa RETECH, cofinanciado por INCIBE con fondos NextGenerationEU.

CCAA participantes y Áreas de especialización

Castilla y León

Movilidad

Andalucía

Smart Cities y Salud

País Vasco

Industria Inteligente y Energía

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OBJETIVOS DEL PROYECTO RED ARGOS

OBJETIVOS ESTRATÉGICOS

- Fortalecer la industria nacional de ciberseguridad
- Ampliar la ciberseguridad a todos los sectores.
- Consolidar la colaboración interregional a través de la red de nodos.

OBJETIVOS OPERATIVOS

- Mejora de las capacidades.
- Incrementar la adopción de medidas de ciberseguridad.
- Atraer y generar talento.
- Impulsar la aceleración y el emprendimiento en ciberseguridad.
- Liderazgo internacional del ecosistema regional.
- Desplegar una red de nodos especializados.

Financiado por la Unión Europea NextGenerationEU

Texto

Plan de Recuperación, Transformación y Resiliencia

ACTUACIONES RED ARGOS

Financiación
Ayudas para proyectos de ciberseguridad

Internacionalización
Visibilidad de tu empresa en el exterior

Formación
Capacitación en competencias clave

Mapa de recursos
Oferta regional en ciberseguridad

Emprendimiento
Apoyo a nuevas ideas de negocio

Sensibilización
Cultura de ciberseguridad en empresas

Centros de excelencia
Talento y tecnología por sectores clave

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

MARCO NORMATIVO VIGENTE Y EN TRAMITACIÓN

BLOQUE I

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

NIS2- Marco europeo de ciberseguridad obligatorio
(Directiva UE 2022/2555, de 14 de diciembre) y su transposición al ordenamiento español

- **Contenidos:** medidas estrictas para proteger las redes y sistemas de información de empresas y organizaciones, ampliando los **requisitos de protección** y **notificación** de incidentes a **sectores clave**.
- **Ámbito de aplicación:** Entidades **públicas** o **privadas**, de tamaño mediano o grande (**+50 empleados** o +**10M€ de facturación**).

Las organizaciones deben adoptar un enfoque de gestión de riesgos que incluya:

Reporte de incidentes: notificación inicial a las autoridades (como el INCIBE-CERT) en un plazo máximo de 24 horas.

Gestión de riesgos y cadena de suministro: evaluación de vulnerabilidades en los sistemas de información y en los proveedores.

Responsabilidad directiva: los órganos de dirección son responsables directos del cumplimiento y deben recibir formación obligatoria.

Continuidad de negocio: planes de respaldo, gestión de crisis y cifrado de datos.

NIS2- Marco europeo de ciberseguridad obligatorio
(Directiva UE 2022/2555, de 14 de diciembre) y su transposición al ordenamiento español

El Consejo de Ministros aprueba el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad

Situación actual:
- Pendiente de aprobación parlamentaria.
- Entrada en vigor estimada: 2026

Objetivo
- Reforzar la protección de redes y sistemas de información.
- Mejorar la respuesta frente a ciberamenazas mediante medidas adaptadas, coordinadas e innovadoras.

SANCIÓN: La CE decidió, el 8 de julio, llevar a Irlanda, **España,** Francia y Países Bajos ante el TJUE por no haber notificado las medidas de transposición al Derecho nacional de la Directiva NIS2. Los Estados miembros tenían de plazo hasta el 17 de octubre de 2024. Incluye una solicitud al Tribunal para imponer **sanciones financieras** consistentes en una cantidad a tanto alzado y multas diarias hasta la notificación de la transposición completa.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

NIS2: notificación de incidentes, fases y plazos

La Directiva NIS2 unifica en **tres hitos sucesivos** la **obligación de notificar los incidentes significativos**, sustituyendo la falta de plazos homogéneos del marco anterior.

1. Alerta temprana

Plazo: **24 horas**

Notificación inicial al CSIRT competente (INCIBE-CERT / CCN-CERT según sector); indica si hay sospecha de acción ilícita/hostil o efectos transfronterizos

2. Notificación de incidente

Plazo: **72 horas**

Actualización de la información anterior, con una primera **valoración del incidente**, su gravedad, impacto y, cuando se disponga de ellos, los **indicadores de compromiso**.

3. Informe final

Plazo: **1 mes**

Descripción detallada del incidente, su gravedad e impacto, el **tipo de amenaza** u **origen** probable, y las **medidas de mitigación** aplicadas y en curso.

Notificaciones acumulables: si el incidente afecta también a datos personales, debe notificarse en paralelo a la AEPD en el plazo de **72 horas** que exige el RGPD. Son procedimientos independientes que pueden generar obligaciones simultáneas.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad

Sectores afectados por NIS2: Anexos I y II

La Directiva NIS2 distingue dos niveles de exigencia según el sector de actividad, con independencia del tamaño en determinados casos.

Anexo I: Sectores de Alta Criticidad

- Energía
- Transporte
- Banca
- Infraestructuras de los mercados financieros
- Sanidad
- Agua Potable
- Aguas residuales
- Infraestructura digital
- Gestión de servicios TIC
- Administración pública
- Espacio

Anexo II: Otros Sectores Críticos

- Servicios postales y de mensajería
- Gestión de residuos
- Fabricación e industria química
- Producción y distribución de alimentos
- Fabricación de productos (incluida la industria manufacturera)
- Proveedores de servicios digitales Investigación.

Umbral general

+50 empleados o +**10M€ de facturación**, dentro de un sector designado.
Algunas **entidades** quedan **incluidas sin importar su tamaño** — ej. proveedores de registro de nombres de dominio o servicios de confianza cualificados.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Plan de Acción de la UE sobre Ciberseguridad e Inteligencia Artificial
(publicado el 7 de julio de 2026, COM(2026) 577)

Complementa el marco jurídico vigente de la UE para impulsar un uso seguro de la IA y reforzar la ciberseguridad europea, a través de **tres objetivos complementarios:**

OBJETIVOS	MEDIDAS
Promover el uso seguro y responsable de la IA avanzada	• Plan Europeo de Acceso Seguro a Sistemas Avanzados de IA (con ENISA). • Plataforma de pruebas para sectores críticos. • Evaluación de modelos de IA antes de su comercialización.
Reforzar la ciberseguridad y la resiliencia de la UE	• Aplicación de NIS2, CRA, etc. • Uso de IA para detectar vulnerabilidades y responder a incidentes.
Ampliación de las capacidades de IA de Europa en materia de ciberseguridad	• Gran desafío europeo de IA para ciberseguridad. • Reunir empresas, investigadores y otros actores. • Inversión en capacidades soberanas de IA.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Esquema Nacional de Seguridad (ENS) — RD 311/2022, de 3 de mayo: obligaciones y niveles

Marco de referencia para garantizar la **seguridad de los sistemas de información** del s**ector público** y de sus **proveedores**.

Ámbito de aplicación: todas las Administraciones Públicas y sus proveedores tecnológicos que gestionen información sensible.

Plazos: las organizaciones debían adecuar sus sistemas a esta nueva versión antes del 4 de mayo de 2024 (derogaba el anterior RD 3/2010).

Principios: se basa en la seguridad integral, la gestión basada en riesgos y la vigilancia continua.

Esquema Nacional de Seguridad (ENS)
Anexo II del RD 311/2022: Arquitectura de las medidas

Marco organizativo

Organización global de la ciberseguridad

- Política de seguridad.
- Normativa de seguridad.
- Procedimientos de seguridad.
- Proceso de autorización.

Marco operacional

Operación del sistema como conjunto integral

- Control de accesos.
- Servicios externos.
- Protección de la operación.
- Continuidad del servicio.
- Monitorización.

Medidas de protección

Activos concretos según su naturaleza

- Protección de instalaciones.
- Gestión de personal.
- Protección de equipos.
- Protección de aplicaciones. informáticas.

Niveles de exigencia según riesgos

Básica **Media** **Alta**

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Principios Básicos ENS

- Seguridad como proceso integral
- Gestión basada en los riesgos
- Diferenciación de responsabilidades
- Prevención, detección, respuesta y conservación
- Vigilancia continua
- Líneas de defensa

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

ENS: Categorización de Sistemas y Perfiles de Cumplimiento

El Esquema Nacional de Seguridad **no aplica un nivel único**: cada **sistema** se categoriza y, además, puede ajustarse a **perfiles específicos** según el tipo de organización:

Cinco dimensiones de seguridad

Cada sistema se valora de forma independiente en **confidencialidad**, **integridad**, **disponibilidad**, **autenticidad** y **trazabilidad**, y el nivel más alto alcanzado en cualquiera de ellas determina la categoría global del sistema (básica, media o alta).

Perfiles de cumplimiento específicos

El RD 311/2022 incorporó la posibilidad de ajustar los requisitos del ENS a las **necesidades concretas** de determinados **colectivos**, como Entidades Locales, Universidades u Organismos Pagadores, o a ámbitos tecnológicos específicos como los servicios en la nube.

Por qué importa

Una **pyme** que proporcione servicios o soluciones tecnológicas al sector público debe **identificar** primero la **categoría del sistema** al que da soporte, ya que de ella dependen las **medidas de seguridad exigibles** y la necesidad de auditoría.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Familia de normas ISO 27000 y 27001: qué implica la certificación

Son estándares internacionales que estructuran la gestión de la seguridad de la información:

Norma	Objetivo y relevancia
ISO 27000 - Vocabulario y Fundamentos	Define los términos y el **lenguaje común** de la serie.
ISO 27001 – Requisitos de SGSI	Especifica los requisitos para establecer, implementar, mantener y mejorar un **SGSI** (Sistema de Gestión de la Seguridad de la Información). Adopta la Estructura de Alto Nivel (HLS). Es **voluntaria** y es la **única norma certificable**.
ISO 27002 - Guía de Prácticas. Controles de seguridad	Proporciona directrices detalladas (controles) para **implementar** las medidas de seguridad mencionadas en el **Anexo A de ISO 27001**. No es certificable.
ISO 27005 - Guía de Gestión de Riesgos	Ofrece directrices para la **gestión de riesgos de seguridad de la información** con un enfoque estructurado.

Certificarse en la **Norma ISO/IEC 27001** es una herramienta poderosa para **demostrar el cumplimiento de otras normativas obligatorias** (Reglamento General de Protección de Datos; Esquema Nacional de Seguridad;…).

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

ISO/IEC 27001:2022: el Anexo A y el Ciclo de Certificación

La versión de 2022 de la norma reestructuró por completo el catálogo de controles de seguridad frente a la edición anterior de 2013.

- **93 controles en 4 categorías:** **organizativos** (37 controles: políticas, roles, relación con proveedores), de **personas** (8 controles: selección, formación y concienciación), **físicos** (14 controles: perímetro, equipos, soportes) y **tecnológicos** (34 controles: control de acceso, criptografía, registro de eventos).
- **Declaración de Aplicabilidad (SoA):** la empresa debe justificar, para cada uno de los 93 controles, si lo aplica o lo excluye y por qué, en función de su propio análisis de riesgos; **no es obligatorio implementar los 93 controles**, sino los que resulten pertinentes.
- **Ciclo de certificación:** **auditoría inicia**l en dos fases (revisión documental y auditoría in situ), **certificado** con una **validez de tres años**, y **auditorías de seguimiento anuales** para comprobar que el sistema de gestión sigue funcionando.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad

Reglamento de Ciberresiliencia (Cyber Resilience Act — Reglamento UE 2024/2847, de 20 de noviembre).

Es la normativa europea que establece **requisitos obligatorios** de ciberseguridad para **hardware** y **software**. Su aplicación plena será exigible a partir del **11 de diciembre de 2027**, con el objetivo es garantizar que los **productos conectados** sean **seguros** a lo largo de **todo su ciclo de vida**. Los aspectos más relevantes son:

Alcance	Afecta a cualquier producto comercializado en la UE que contenga **elementos digitales**, tanto de hardware (ej. dispositivos IoT, electrodomésticos inteligentes…) como de software.
Ciclo de vida seguro	Obliga a los fabricantes a incorporar la ciberseguridad desde el diseño inicial, solucionar vulnerabilidades conocidas y proporcionar actualizaciones de seguridad periódicas.
Obligaciones de notificación	Los fabricantes deben reportar de forma obligatoria **cualquier incidente de ciberseguridad** activo o vulnerabilidad explotada a la Agencia de Ciberseguridad de la Unión Europea (**ENISA**) y a los equipos de respuesta a emergencias informáticas (**CSIRT**) correspondientes.
Marca CE	Tras cumplir con los estándares de esta ley, los productos digitales deberán llevar el marcado CE para poder venderse dentro del mercado europeo.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Reglamento de Ciberresiliencia: requisitos esenciales del Anexo I

El Anexo I del Reglamento fija los requisitos esenciales de ciberseguridad que debe cumplir cualquier producto con elementos digitales, divididos en dos bloques.

Parte I - Propiedades de seguridad del producto

- Diseño y fabricación sin vulnerabilidades explotables conocidas.
- Configuración segura por defecto.
- Protección de confidencialidad e integridad de datos (ej. cifrado).
- Minimización de datos.
- Disponibilidad y resiliencia frente a fallos.
- Limitación de la superficie de ataque.

Parte II - Gestión de vulnerabilidades

- Identificar y documentar componentes (incl. SBOM legible por máquina).
- Corregir vulnerabilidades sin demora mediante actualizaciones.
- Pruebas de seguridad periódicas.
- Publicar información sobre vulnerabilidades corregidas.

Política de divulgación coordinada

Los fabricantes deben establecer un punto de contacto y un procedimiento de divulgación coordinada de vulnerabilidades, para que terceros puedan reportarlas de forma responsable.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad

DORA: Reglamento de Resiliencia Operativa Digital

El Reglamento (UE) 2022/2554, de 14 de diciembre de 2022, sobre la **resiliencia operativa digital del sector financiero** (conocido como DORA), es de aplicación directa en toda la Unión Europea desde el 17 de enero de 2025.

A quién obliga: a entidades financieras (bancos, aseguradoras, empresas de inversión, entidades de pago, proveedores de criptoactivos, entre otras) y a sus proveedores externos de servicios TIC.

Qué exige: un marco de gestión del riesgo TIC, la notificación de incidentes graves a las autoridades competentes, pruebas periódicas de resiliencia digital (incluidas pruebas de penetración guiadas por amenazas para las entidades designadas) y la supervisión del riesgo de terceros proveedores tecnológicos.

Relación con NIS2: para las entidades financieras identificadas como esenciales o importantes, DORA se considera la normativa sectorial de referencia (lex specialis) y prevalece sobre NIS2 en materia de gestión y notificación de riesgos TIC.

Por qué interesa a tu pyme: si tu empresa presta servicios tecnológicos a bancos, aseguradoras u otras entidades financieras, es probable que tu cliente te exija por contrato requisitos alineados con DORA.

Ciberseguridad 5G: Real Decreto-ley 7/2022 y RD 443/2024

Norma	Qué establece
RD-ley 7/2022 (29 mar.) **"Ley de Ciberseguridad 5G"**	Requisitos de seguridad para instalación, despliegue y explotación de redes 5G; incorpora la Recomendación (UE) 2019/534
RD 443/2024 (30 abr.) **En vigor desde el 2 may. 2024**	Aprueba el **Esquema Nacional de Seguridad de redes y servicios 5G** (**ENS5G**): tratamiento integral de seguridad para operadores, suministradores y usuarios corporativos

Aspectos clave del ENS5G

- Análisis y gestión de riesgos a nivel nacional
- Catalogación de elementos críticos de la red
- Control de la cadena de suministro (diversificación de proveedores)
- Evaluación del riesgo de suministradores según su nivel de riesgo

Revisión periódica

El Esquema se revisará, como mínimo, cada cuatro años, o antes si las circunstancias lo aconsejan.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad

Estrategia de Especialización Inteligente de Castilla y León 2021-2027 (RIS3) - Acción estratégica en Ciberseguridad

Aprobada el 23 de septiembre de 2021, engloba la Acción Estratégica en Ciberseguridad como una de las **iniciativas emblemáticas clave** de la RIS3 de Castilla y León, que consolida a Castilla y León como **polo europeo** de referencia en investigación, innovación y desarrollo empresarial en ciberseguridad.. La estrategia articula sus objetivos a través de **tres líneas de trabajo fundamentales**:

Línea	Foco
1. Innovación y ciberseguridad industrial	Tecnologías para proteger procesos industriales e infraestructuras críticas; soluciones de doble uso (civil/defensa).
2. Talento, formación y capacitación	Programas educativos adaptados al mercado; reducir la brecha de talento.
3. Transferencia tecnológica al tejido empresarial	Extender capacidades de ciberseguridad a pymes de otros sectores (ej. agroalimentación, fabricación avanzada).

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad

Estrategia de Especialización Inteligente de Castilla y León 2021-2027 (RIS3) - Ecosistema de agentes y actualización 2025-2027

El éxito de la acción estratégica se apoya en un modelo de ecosistema con **4 tipos de agentes.**

- **Empresas:** Grandes compañías tractoras + tejido de pymes innovadoras
- **Academia y centros tecnológicos:** Universidades (ej. Universidad de León) e instituciones I+D+i
- **Administración pública:** Junta de CyL — Consejería de Educación y Comisionado para la Ciencia y la Tecnología
- **Entidades de apoyo:** Agrupaciones empresariales innovadoras y Digital Innovation Hubs (DIH)

Actualización 2025-2027

Tras su evaluación intermedia, la estrategia fue actualizada y aprobada para el periodo 2025 2027. En esta nueva fase, se potencia el rol de la ciberseguridad dentro de la prioridad transversal denominada "Castilla y León, una apuesta por la fabricación inteligente y la ciberseguridad".

Financiado por la Unión Europea NextGenerationEU

Estrategia Deep Tech España 2026-2030

La Estrategia, aprobada el 19 de mayo de 2026. Plantea un **marco estable e integrador** para que el **potencial científico español** se traduzca en **impacto económico**, empleo de calidad y autonomía tecnológica, conectando investigación, mercado y sociedad.

Movilizará más de **8.000 millones de euros** hasta 2030

Objetivo

Construir una cadena de valor capaz de conectar investigación, mercado y sociedad

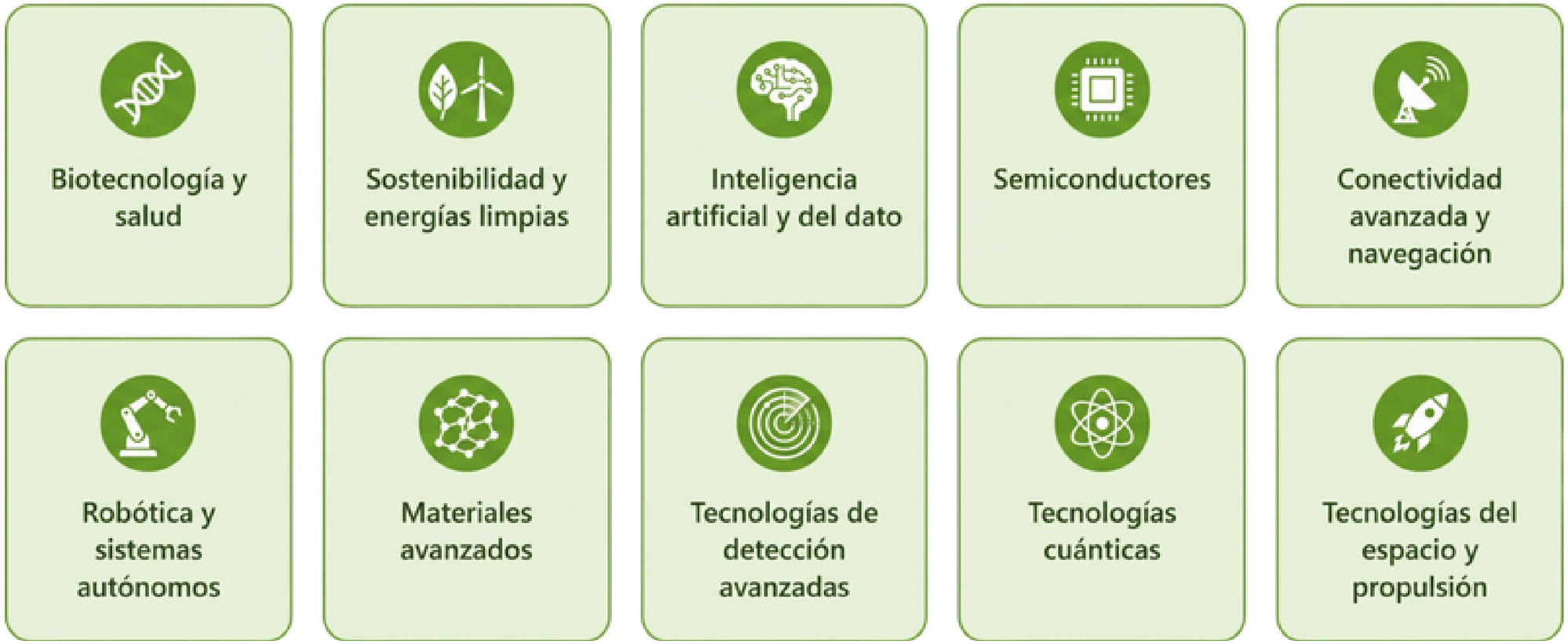
Énfasis clave

- Transferencia tecnológica
- Atracción de talento
- Coordinación público-privada (universidades, OPIs, centros tecnológicos, startups)

Estrategia Deep Tech España 2026-2030 — 3 ejes estratégicos

Eje	Foco
1. Capacidades científicas y tecnológicas	Formación especializada, talento internacional, infraestructuras de investigación; transferencia de conocimiento y nuevos centros de excelencia
2. Tejido empresarial	Colaboración público-privada, compra pública de innovación, entornos de validación; refuerzo de capital vía INNVIERTE, Next Tech y el nuevo fondo Deep Start
3. Transversal	Nueva gobernanza institucional, vigilancia tecnológica, regulación ágil; Observatorio Nacional Deep Tech, Red de Venture Builders y Deep Tech Factories, espacios de experimentación regulatoria

Estrategia Deep Tech España 2026-2030 — Diez áreas prioritarias



Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Proyecto de Ley Orgánica para el buen uso y la gobernanza de la Inteligencia Artificial (26 de mayo de 2026, Consejo de Ministros) — Contexto y uso confiable

Aprobado el 26 de mayo de 2026 (Consejo de Ministros) — alineado con el Reglamento (UE) 2024/1689 (RIA), en vigor desde agosto de 2024

Uso confiable de la IA

- Supervisión humana
- Transparencia algorítmica reforzada
- Protección reforzada de derechos
- Medidas específicas de protección de menores

Marco nacional de gobernanza

Autoridad	Rol
AESIA	Agencia Española de Supervisión de la IA — autoridad principal
AEPD	Interviene según ámbito (protección de datos)
CGPJ	Interviene según ámbito (poder judicial)

Financiado por la Unión Europea NextGenerationEU

Proyecto de Ley Orgánica para el buen uso y la gobernanza de la Inteligencia Artificial (26 de mayo de 2026, Consejo de Ministros) — Sanciones, sector público y sandboxes

Medidas específicas para el sector público estatal

Incorpora el "buen uso" de la IA en la administración

- **Inventario** de **sistemas de IA** (más allá de alto riesgo) — desarrollo por RD
- **Figura del delegado de IA** — coordina normativa, asesora en proyectos y contratación pública
- Impulso a **formación y concienciación** del personal público

Sandboxes y fomento de la innovación segura

Sandbox nacional obligatorio (RIA), operado por AESIA

- Posibilidad de **sandboxes sectoriales** adicionales
- Requiere **participación de autoridades** sectoriales y de derechos fundamentales

Régimen sancionador

Criterios: proporcionalidad, intencionalidad, reincidencia — con atención especial a **pymes** y **startups**

Leve | **Grave** | **Muy Grave**

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad

Reglamento europeo de IA: niveles de riesgo y sanciones

El Reglamento (UE) 2024/1689 clasifica los sistemas de Inteligencia Artificial en niveles de riesgo, con obligaciones proporcionales a cada nivel.

Nivel Riesgo	Sanción	Régimen Sancionador
Riesgo inaceptable (prohibido)	Sistemas que manipulan el comportamiento mediante técnicas subliminales, explotan vulnerabilidades de colectivos concretos, puntúan socialmente a las personas o realizan identificación biométrica remota en tiempo real en espacios públicos (con excepciones). Prohibido desde el 2 de febrero de 2025.	Hasta 35 millones de euros o el 7% de la facturación mundial
Riesgo alto	Sistemas usados en infraestructuras críticas, educación, empleo, calificación crediticia o aplicación de la ley, sujetos a obligaciones de gestión de riesgos, documentación técnica y supervisión humana. Plenamente exigibles desde el 2 de agosto de 2026.	Hasta 15 millones o el 3%
Riesgo limitado	Sistemas como chatbots o generadores de contenido sintético (deepfakes), sujetos a obligaciones de transparencia: informar de que se interactúa con IA y etiquetar el contenido generado.	Hasta 7,5 millones o el 1,5%
Riesgo mínimo	La mayoría de aplicaciones actuales (videojuegos, filtros de spam), sin obligaciones específicas.	-

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad

TECNOLOGÍAS EMERGENTES CON IMPACTO EN CIBERSEGURIDAD

BLOQUE II

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Inteligencia Artificial aplicada a la ciberseguridad (detección de amenazas, ataques con IA)

La **IA es clave en la ciberdefensa moderna**. protege detectando amenazas en tiempo real, pero también potencia ataques cada vez más sofisticados.

Detección de amenazas (Defensa)

Aprendizaje automático (Machine Learning):
- Aprende el comportamiento normal de la red.
- Detecta anomalías y amenazas.

Respuesta autónoma:
- Aísla dispositivos infectados.
- Bloquea IP maliciosas automáticamente.

Reducción de falsos positivos:
- Filtra alertas irrelevantes.
- Permite centrarse en incidentes reales.

IA en la ofensiva (Ataques)

Malware polimórfico:
- Modifica continuamente su código.
- Evita la detección por antivirus

Ingeniería social avanzada:
- Phishing hiperrealista.
- BEC mediante clonación de voz (deepfakes).

Ataques rápidos:
- Escaneo masivo de vulnerabilidades.
- Desarrollo automático de herramientas de explotación.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad

Arquitectura de Confianza Cero (Zero Trust)

El NIST (Instituto Nacional de Estándares y Tecnología de Estados Unidos) define en su publicación especial SP 800-207 (2020) el modelo de referencia de Confianza Cero, cada vez más recomendado frente a los modelos tradicionales de perímetro.

Principio central: no existe confianza implícita por el mero hecho de estar dentro de la red corporativa; cada solicitud de acceso a un recurso debe autenticarse y autorizarse de forma explícita.

Verificación continua: la identidad del usuario y el estado del dispositivo se comprueban en cada sesión, no solo en el inicio, incorporando el contexto (ubicación, comportamiento, nivel de riesgo).

Mínimo privilegio: cada usuario o servicio recibe solo los permisos estrictamente necesarios para su función, durante el tiempo necesario.

Por qué interesa a tu pyme: el trabajo en remoto, el uso de dispositivos personales (BYOD) y los servicios en la nube diluyen el perímetro tradicional de la red; adoptar principios de Confianza Cero, aunque sea de forma progresiva, refuerza directamente varios de los controles exigidos por NIS2 y el ENS.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Tecnologías cuánticas: amenazas a la criptografía actual y criptografía post-cuántica

Los futuros ordenadores cuánticos amenazan el cifrado de clave pública actual mediante diferentes algoritmos. La seguridad digital moderna se sostiene sobre **dos pilares criptográficos** que los ordenadores cuánticos podrán romper cuando alcancen suficiente potencia y tolerancia a fallos:

Cifrado asimétrico (Clave pública)

- Algoritmos como RSA y la criptografía de curvas elípticas (ECC)
- Basan su seguridad en problemas matemáticos complejos.
- Algoritmo de Shor: podría romper estas claves cuando existan ordenadores cuánticos suficientemente potentes.

Cifrado simétrico

- Algoritmos como AES se verían afectados por el algoritmo de Grover, que acelera la búsqueda en bases de datos no estructuradas
- Mitigación: utilizar claves más largas (ej. AES-256).

¿Cómo protegerse?

Para protegerse, debe implementarse la **Criptografía Post-Cuántica (PQC)**, nuevos estándares matemáticos resistentes a ordenadores clásicos y cuánticos, impulsados por agencias como el INCIBE.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad

IMPLICACIONES PRÁCTICAS PARA LAS PYMES

BLOQUE III

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Qué deben hacer ahora las PYMES y cómo prepararse

El cumplimiento normativo en ciberseguridad obliga a las PYMES a implementar **medidas técnicas y organizativas** para proteger datos sensibles. Esto exige el uso de **autenticación multifactor**, **cifrado de datos**, **copias de seguridad** y **formación del personal**. Su fin es evitar multas millonarias y garantizar la continuidad del negocio.

Recursos útiles

Para evitar sanciones y entender exactamente qué leyes aplican a tu negocio, puedes apoyarte en fuentes oficiales:

- **Evaluación de riesgos:** Utiliza el catálogo y las herramientas de diagnóstico del INCIBE.
- **Legislación y cumplimiento normativo:** Infórmate sobre cómo leyes específicas afectan a tu sector específico.
- **Certificación:** valora certificar un SGSI conforme a ISO/IEC 27001 o adherirte al Esquema Nacional de Seguridad, ya que ambos marcos facilitan acreditar el cumplimiento ante clientes y administraciones públicas.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Implicaciones Técnicas

Para cumplir con normativas como el RGPD o la normativa NIS2, tu empresa debe aplicar acciones concretas:

Control de accesos
Limitar el acceso a la información confidencial solo a quien la necesite, con contraseñas robustas y Autenticación Multifactor (2FA).

Protección de la información
Implementar cifrado para bases de datos y comunicaciones.

Copias de seguridad
Backups periódicos y cifrados, comprobando que se pueden restaurar rápidamente ante ransomware o desastre.

Gestión de vulnerabilidades
Mantener sistemas y aplicaciones actualizados, priorizando parches de vulnerabilidades ya explotadas.

Notificación de incidentes
Procedimiento interno para detectar y comunicar incidentes al CSIRT competente y, si afectan a datos personales, a la AEPD.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Ciclo de gestión de un incidente de ciberseguridad

El NIST estructura la respuesta a incidentes en fases de referencia para cualquier organización.

1. Preparación

Políticas, roles y herramientas definidos antes del incidente: backups probados, contacto con el CSIRT, inventario de sistemas.

2. Detección y análisis

Identificar el incidente, confirmarlo descartando falsos positivos, y clasificar su gravedad e impacto.

3. Contención, erradicación y recuperación

Aislar los sistemas afectados, eliminar la causa raíz y restaurar desde copias verificadas.

4. Actividad posterior

Documentar lo ocurrido, extraer lecciones aprendidas y notificar a las autoridades si procede.

Actualización de referencia: en abril de 2025, el NIST publicó la revisión 3 de su guía (SP 800-61), integrando estas fases en el NIST Cybersecurity Framework 2.0 (Gobernar, Identificar, Proteger, Detectar, Responder, Recuperar).

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad

Implicaciones Legales y de Gestión

El cumplimiento en ciberseguridad significa alinear tus salvaguardas técnicas y organizativas con las leyes, normativas y políticas internas que rigen tus datos y sistemas. En la práctica responde a tres preguntas: **¿qué estás obligado a proteger? ¿cómo lo estás protegiendo? ¿puedes demostrarlo?**

Evaluación y Políticas
Redactar y aprobar Políticas de Seguridad internas que establezcan cómo se tratan los datos y activos corporativos.

Notificación de Incidentes
En caso de brecha de seguridad, el marco legal europeo obliga a reportarla a las autoridades y usuarios afectados en un plazo muy estricto.

Cadena de Suministro
Se exige auditar y asegurar que los proveedores externos que manejan tus datos también cumplen con normativas de ciberseguridad.

Sanciones y Riesgos

El incumplimiento de normativas de ciberseguridad y protección de datos puede acarrear sanciones muy graves. Más allá de la multa, una brecha de seguridad provoca paralización de la actividad y graves daños reputacionales, algo crítico para las PYMES.

Gravedad variable
Las cuantías varían según la norma aplicable y siempre se aplica la cifra mayor entre el importe fijo y el porcentaje de facturación.

Cuantías de referencia
RGPD: hasta 20M€ o 4%. NIS2: hasta 10M€ o 2% (esenciales), 7M€ o 1,4% (importantes). Reglamento de Ciberresiliencia: hasta 15M€ o 2,5%.

Régimen sancionador comparado

En los regímenes con cuantía porcentual se aplica siempre la cifra que resulte mayor entre el importe fijo y el porcentaje de facturación.

Norma	Régimen sancionador
RGPD	Infracciones graves: hasta 20 millones de euros o el 4% de la facturación anual mundial.
NIS2	Hasta 10 millones € o 2% (entidades esenciales); hasta 7 millones € o 1,4% (entidades importantes).
Reglamento de Ciberresiliencia	Hasta 15 millones € o 2,5% por incumplir requisitos esenciales; hasta 10 millones o 2% por otras obligaciones; hasta 5 millones o 1% por información incorrecta.
Esquema Nacional de Seguridad	No contempla régimen propio de multas: responsabilidad administrativa e imposibilidad de certificar o contratar con el sector público.

Calendario de hitos normativos

Julio de 2026 (actualidad)
El anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad (NIS2) sigue en tramitación; el Proyecto de Ley Orgánica de IA está en fase de comisión.

2 de agosto de 2026
Nuevo hito del Reglamento europeo de IA: obligaciones para sistemas de alto riesgo y autoridades nacionales de gobernanza.

11 de septiembre de 2026
Entra en vigor la obligación del Reglamento de Ciberresiliencia de notificar a ENISA vulnerabilidades explotadas e incidentes graves.

11 de diciembre de 2027
Aplicación plena del Reglamento de Ciberresiliencia para todos los productos con elementos digitales comercializados en la UE.

Cada dos años (recurrente)
España debe actualizar la lista de entidades esenciales e importantes sujetas a NIS2.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad

Normas y estándares técnicos complementarios

Junto a las normas de cumplimiento obligatorio, estos estándares técnicos completan el marco de referencia para las pymes:

ISO/IEC 27002
Guía de controles de seguridad que desarrolla el Anexo A de ISO/IEC 27001; no es certificable por sí sola.

ISO/IEC 27017 e ISO/IEC 27018
Controles de seguridad y protección de datos personales específicos para servicios en la nube.

ISO/IEC 27701
Extensión de gestión de la privacidad integrada con el SGSI de ISO/IEC 27001, alineada con el RGPD.

NIST Cybersecurity Framework (CSF) 2.0
Marco voluntario internacional (feb. 2024): Gobernar, Identificar, Proteger, Detectar, Responder, Recuperar.

Guías CCN-STIC
Serie de guías técnicas del Centro Criptológico Nacional (CCN) para implementar las medidas del ENS.

CCN-CERT e INCIBE-CERT
Equipos de respuesta a incidentes de referencia: sector público (CCN-CERT) y empresas/ciudadanos (INCIBE-CERT).

Financiado por la Unión Europea NextGenerationEU

Autoridades y organismos de referencia

Ante una duda o un incidente, estos son los organismos a los que puede dirigirse tu empresa según el ámbito:

INCIBE-CERT
Punto de contacto para empresas y ciudadanos; catálogo de soluciones, autodiagnóstico y Línea 017.

CCN-CERT
Respuesta a incidentes del Centro Criptológico Nacional; referente para Administraciones Públicas y sus proveedores.

AEPD
Agencia Española de Protección de Datos: autoridad a la que notificar brechas que afecten a datos personales (RGPD).

AESIA
Agencia Española de Supervisión de la IA: autoridad de referencia para los sistemas de Inteligencia Artificial en España.

ENISA
Agencia de la UE para la ciberseguridad; opera la plataforma de notificación del Reglamento de Ciberresiliencia.

RED ARGOS e ICECYL
Para dudas sobre el programa, financiación o actividades de sensibilización: info@redargos.com.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Resumen: acciones prioritarias para tu pyme

1. Identifica qué te aplica
Revisa si tu empresa entra en el ámbito de NIS2 (sector y tamaño), si trabajas con el sector público (ENS) o si tus productos incorporan elementos digitales (Reglamento de Ciberresiliencia).

2. Implementa medidas técnicas básicas
Autenticación multifactor, cifrado de datos, copias de seguridad probadas y gestión activa de vulnerabilidades.

3. Documenta y forma
Redacta políticas de seguridad por escrito y forma periódicamente al personal y, si corresponde, al órgano de dirección.

4. Prepara la respuesta a incidentes
Ten identificado el CSIRT de referencia (INCIBE-CERT o CCN-CERT) y los plazos de notificación aplicables.

5. Valora la certificación
ISO/IEC 27001 o el Esquema Nacional de Seguridad facilitan acreditar el cumplimiento ante clientes y administraciones públicas.

6. Apóyate en RED ARGOS
Aprovecha las herramientas de diagnóstico, la financiación y los recursos de sensibilización del programa.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad

Preguntas frecuentes

¿Me afecta NIS2 si tengo menos de 50 empleados o facturo menos de 10M€?
Con carácter general no, salvo excepciones tasadas (registro de dominios, servicios de confianza) o que formes parte de la cadena de suministro de una entidad esencial o importante.

¿Es obligatorio certificarse en ISO/IEC 27001?
No, es voluntaria. Lo obligatorio, según sector y tamaño, es cumplir con NIS2, el ENS o el RGPD; la certificación ISO facilita demostrar ese cumplimiento.

¿Qué hago si sufro un ciberincidente?
Contacta con el CSIRT que corresponda (INCIBE-CERT o CCN-CERT) y, si hay datos personales afectados, notifica a la AEPD en 72 horas conforme al RGPD.

¿El Reglamento de Ciberresiliencia me afecta si no fabrico hardware?
Sí, si desarrollas o comercializas software que se conecta a otros dispositivos o redes, tu producto entra dentro de su ámbito.

¿Dónde puedo resolver dudas sobre estas normativas?
A través del catálogo de INCIBE, el punto de contacto de RED ARGOS (info@redargos.com) o un asesor especializado.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad

Para **más información acerca** de RED ARGOS:

info@redargos.com

https://redargos.com/

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD