

CÓMO PROTEGER TU EMPRESA: SERVICIOS, ASESORAMIENTO Y APOYO EXPERTO EN CIBERSEGURIDAD



Webinar de capacitación y sensibilización en materia de ciberseguridad

9 de julio de 2026



**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



INSTITUTO NACIONAL DE CIBERSEGURIDAD

CONTENIDOS

Introducción a RED ARGOS

BLOQUE I: Soluciones en ciberseguridad para proteger tu empresa:

- Gestión de identidades y accesos.
- Formación y concienciación interna.
- Respuesta ante incitendes.
- Casos de éxito y buenas practices
- Servicios SOC.

BLOQUE II: Recursos y servicios de apoyo para las empresas:

- Servicios del ICECYL en el marco de RED ARGOS: acompañamiento, asesoría técnica, convocatorias
- Servicios de la Junta de Castilla y León en materia de ciberseguridad empresarial.

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



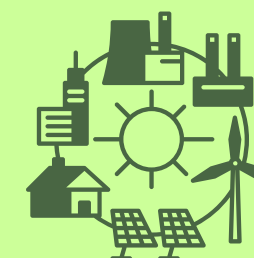
Andalucía

Smart Cities y Salud



País Vasco

Industria Inteligente y Energía



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.

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

SOLUCIONES EN CIBERSEGURIDAD PARA PROTEGER TU EMPRESA

BLOQUE I

Ponente: Julio César Miguel Pérez. CEO de la empresa Grupo CFI y presidente de la Asociación Palentina de Empresarios de las Tecnologías de la Información y Comunicación (APETIC)



grupocfi.es

20 años ayudando a empresas, organizaciones y Administraciones Públicas a **gestionar** la Ciberseguridad y la Protección de datos personales

LA CIBERSEGURIDAD YA NO ES SOLO TECNOLOGÍA

Para una pyme, es continuidad, confianza y responsabilidad.

Cuando falla la seguridad, no se para “el ordenador”: se puede parar la empresa.



- **Continuidad de negocio:** paradas, pérdida de información y dependencia de terceros.



- **Confianza:** clientes, administraciones y grandes empresas piden garantías.



- **Responsabilidad:** la dirección debe conocer y priorizar los riesgos que asume.

La ciberseguridad es una decisión de negocio



¿QUÉ ES LA CIBERSEGURIDAD?



La ciberseguridad **NO PUEDE COMPRARSE**,
sin embargo,
puede **GESTIONARSE**

Porque **NO ES UN PRODUCTO**,
es un **PROCESO**

ÁMBITOS DE GESTIÓN



**Políticas y
organización de la
seguridad**



Personal



**Infraestructura
física**



Tecnologías



Políticas y organización de la seguridad

ÁMBITOS DE GESTIÓN

- Políticas de seguridad
- Roles y responsabilidades
- Clasificación de la información
- Inventario de activos
- Uso aceptable de la información y los activos asociados
- Control de acceso y permisos
- Proveedores y requisitos de seguridad
- Servicios cloud
- Gestión de incidentes
- Protección de datos

ÁMBITOS DE GESTIÓN



Personal

- Responsabilidades en relación a la seguridad de la información
- Concienciación y formación
- Proceso disciplinario
- Acuerdos de confidencialidad
- Teletrabajo
- Notificación de eventos de seguridad de la información

ÁMBITOS DE GESTIÓN



**Infraestructura
física**

- Perímetro de seguridad físico
- Protección contra amenazas físicas y ambientales (fuego, agua, etc.)
- Puesto de trabajo despejado y pantalla limpia
- Soportes de almacenamiento
- Eliminación o reutilización de soportes y equipos informáticos

ÁMBITOS DE GESTIÓN



Tecnologías

- Securizar los dispositivos del usuario
- Gestión de privilegios de acceso
- Autenticación segura
- **Antimalware**
- Gestión de vulnerabilidades técnicas
- Gestión de la configuración
- Copias de seguridad
- Seguridad de las redes y vigilancia
- Filtrado de webs
- Cifrado de la información
- Instalación de software

QUÉ NECESITA REALMENTE UNA PYME

Cuatro necesidades que ordenan todos los servicios.

Antes de hablar de servicios, conviene hablar de necesidades.

- 01 Saber cómo está**
diagnóstico, riesgos, madurez y brechas
- 02 Protegerse**
medidas técnicas y organizativas realistas
- 03 Cumplir**
RGPD, ENS, ISO 27001, NIS2, DORA...
- 04 Estar acompañada**
seguimiento, soporte y mejora continua

La clave es pasar de la reacción a la planificación.



Mapa de servicios de ciberseguridad

De necesidades empresariales a soluciones
concretas



SERVICIOS AGRUPADOS POR NECESIDAD

Qué problema resuelve cada servicio.

DIAGNOSTICO

**Saber dónde está el
riesgo**

Análisis de riesgos ·
Auditoría inicial · Plan
Director



CUMPLIMIENTO

**Ordenar y demostrar
la seguridad**

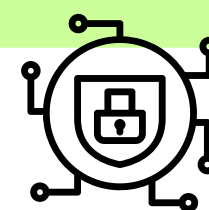
ISO 27001 · ENS · NIS2 ·
DORA · RGPD



SEGURIDAD TECNICA

**Comprobar si los
sistemas resisten**

Vulnerabilidades ·
Pentesting · Revisión
cloud/M365



ACOMPANAMIENTO

**Mantener la
seguridad viva**

CISO externo ·
Mantenimiento SGSI ·
Formación



Un servicio no se entiende por su nombre, sino por el riesgo que reduce.

1. DIAGNÓSTICO Y PUNTO DE PARTIDA

Antes de invertir, saber dónde están las prioridades.

Objetivo: convertir la preocupación en una hoja de ruta.



Diagnóstico de ciberseguridad y madurez.



Análisis de riesgos y revisión de exposición.



Auditoría inicial frente a buenas prácticas o requisitos.



Plan Director con acciones priorizadas por impacto, urgencia y coste.

**No empezar comprando herramientas;
empezar sabiendo dónde está el riesgo.**



2. CUMPLIMIENTO Y SISTEMAS DE GESTIÓN

Convertir la seguridad en un sistema ordenado, documentado y auditable.

Marcos y obligaciones que pueden afectar a una pyme:

ISO 27001	ENS
NIS 2	RIA
RGPD	ISO 27701



Políticas, procedimientos, registros y evidencias.



Preparación para auditorías, licitaciones, clientes y obligaciones sectoriales.



EJEMPLO: RGPD, RIA, NIS2



3. SEGURIDAD TÉCNICA

Comprobar antes de que lo haga un atacante.

La documentación es necesaria, pero la seguridad también debe probarse.

- 01** **Análisis de vulnerabilidades**
identificación de debilidades en sistemas, servicios y aplicaciones
- 02** **Pentesting**
pruebas controladas para validar impacto real y priorizar correcciones
- 03** **Revisión de configuración**
Microsoft 365, cloud, copias, accesos, endpoints y redes

Objetivo: proteger lo que realmente expone a la empresa.



4. INCIDENTES Y CONTINUIDAD

No solo evitar un incidente: saber responder si ocurre.

El valor está en reducir el tiempo de reacción.

Preparar



roles, contactos, copias y criterios

Detectar



alertas, señales y evidencias

Responder



contener, comunicar y recuperar

Aprender



mejoras, lecciones y seguimiento

Planes de respuesta, continuidad, crisis y formación.



5. ACOMPAÑAMIENTO CONTINUO

La ciberseguridad no es un proyecto de una vez.

La pyme necesita seguimiento, no solo una implantación.

- 01 CISO externo**
dirección y criterio sin incorporar un perfil interno a tiempo completo
- 02 Mantenimiento SGSI / ENS**
riesgos, evidencias, controles, indicadores, auditorías y mejora
- 03 Formación y concienciación**
sesiones, simulaciones y refuerzo periódico adaptado a perfiles

**Objetivo: que la empresa no se quede sola tras el diagnóstico
o la implantación.**



SERVICIOS AGRUPADOS POR NECESIDAD

Qué problema resuelve cada servicio.

DIAGNOSTICO

**Saber dónde está el
riesgo**

Análisis de riesgos ·
Auditoría inicial · Plan
Director



CUMPLIMIENTO

**Ordenar y demostrar
la seguridad**

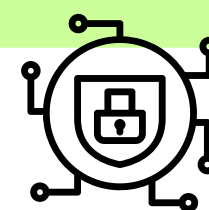
ISO 27001 · ENS · NIS2 ·
DORA · RGPD



SEGURIDAD TECNICA

**Comprobar si los
sistemas resisten**

Vulnerabilidades ·
Pentesting · Revisión
cloud/M365



ACOMPANAMIENTO

**Mantener la
seguridad viva**

CISO externo ·
Mantenimiento SGSI ·
Formación



Un servicio no se entiende por su nombre, sino por el riesgo que reduce.

NUESTRO ENFOQUE DE TRABAJO

Especialización, proporcionalidad y acompañamiento práctico.



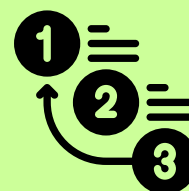
1.Escuchar

sector, tamaño,
clientes y
obligaciones



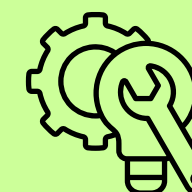
2.Medir

riesgos, brechas
y exposición



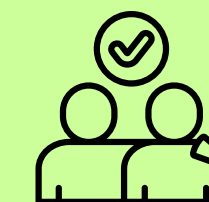
3.Priorizar

acciones
realistas y con
impacto



4.Implantar

medidas técnicas
y organizativas



5.Acompañar

seguimiento,
auditoría y
mejora

No se trata de hacer “más seguridad”, sino de hacer la seguridad adecuada para cada pyme.

SERVICIOS



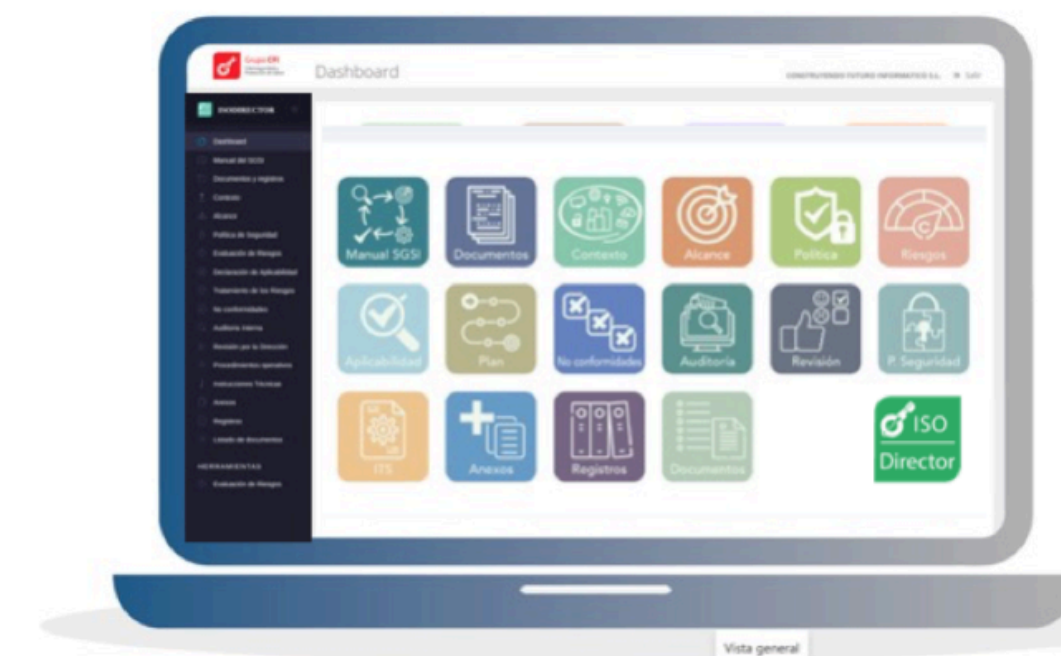
Grupo CFI

Ciberseguridad y
Protección de datos

grupocfi.es



Papel Cero



SERVICIOS OFRECIDOS



Grupo **CFI**

Ciberseguridad y
Protección de datos

grupocfi.es



Consultoría y Auditoría en:

- Esquema Nacional de Seguridad
- ISO 27001 - ISO 27701
- ISO 9001
- LOPDGDD
- LSSICE
- TISAX, DORA, NIS2, CRA, PCI DSS, RIA

SERVICIOS OFRECIDOS



Grupo CFI
Ciberseguridad y
Protección de datos

grupocfi.es



Auditorías de Ciberseguridad
Análisis de Riesgos
Investigación Forense Digital



SERVICIOS OFRECIDOS



Grupo CFI
Ciberseguridad y
Protección de datos

grupocfi.es



Formación en:

- Ciberseguridad
- Protección de Datos



INSTITUTO SUPERIOR
DE CIBERSEGURIDAD

RGPD/LOPD ▾

CIBERSEGURIDAD ▾

LSSI ▾

TARIFA PLANA

NOSOTROS

CONTACTO

BLOG



Instituto Superior de Ciberseguridad

Escuela de formación sobre Ciberseguridad, Protección de Datos Personales, LOPD, LSSI.

Cursos online con profesores profesionales del sector. Aprende de los mejores.

VER CURSOS ▸



isciberseguridad.es

SERVICIOS OFRECIDOS



Grupo CFI

Ciberseguridad y
Protección de datos

grupocfi.es



Delegado de Protección de Datos Externo
Responsable de Seguridad de la Información Externo



SERVICIOS OFRECIDOS



Grupo **CFI**

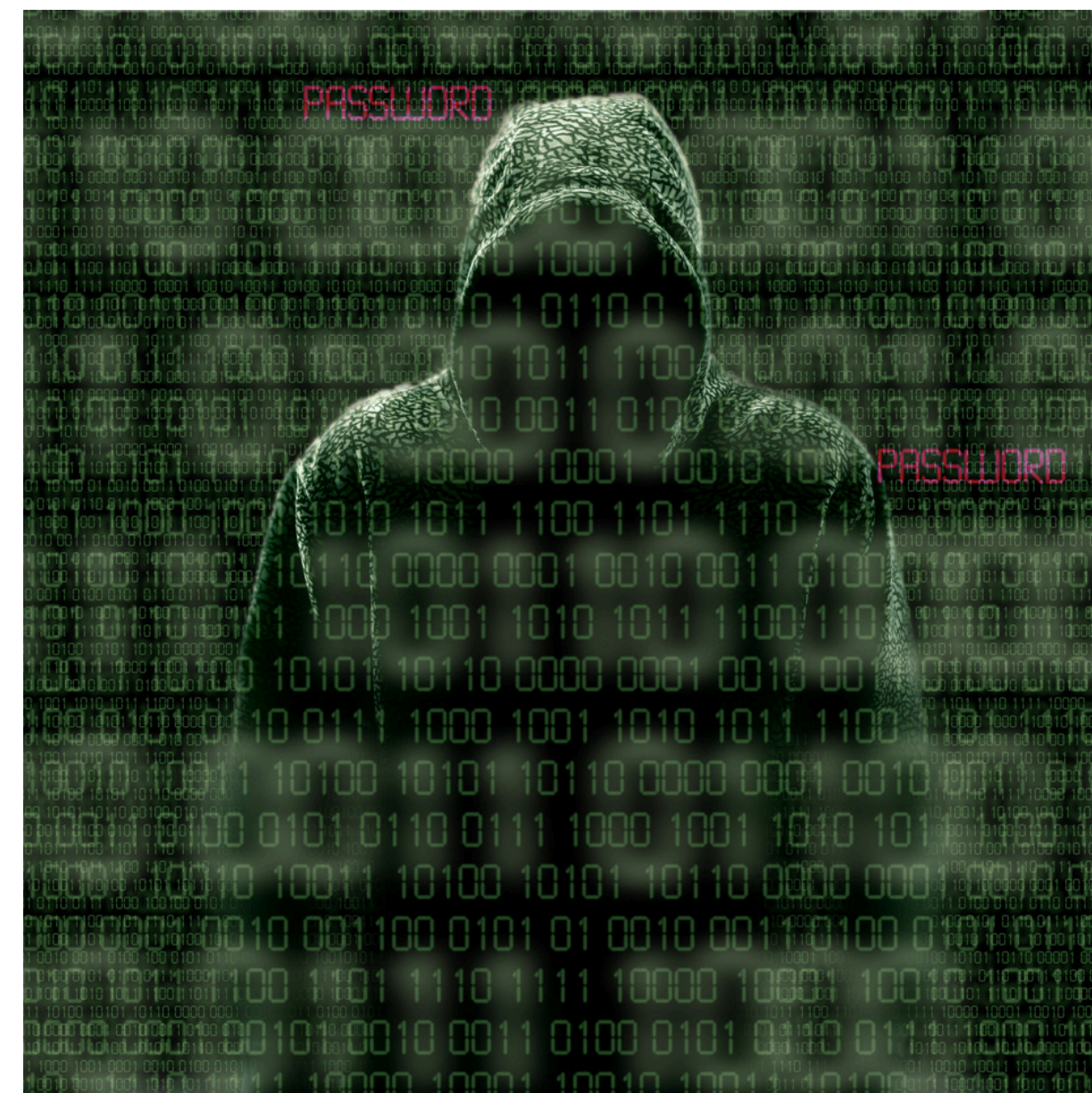
Ciberseguridad y
Protección de datos

grupocfi.es



Hacking Ético:

- Análisis de Vulnerabilidades
- Test de Intrusión



SERVICIOS OFRECIDOS



Grupo **CFI**
Ciberseguridad y
Protección de datos

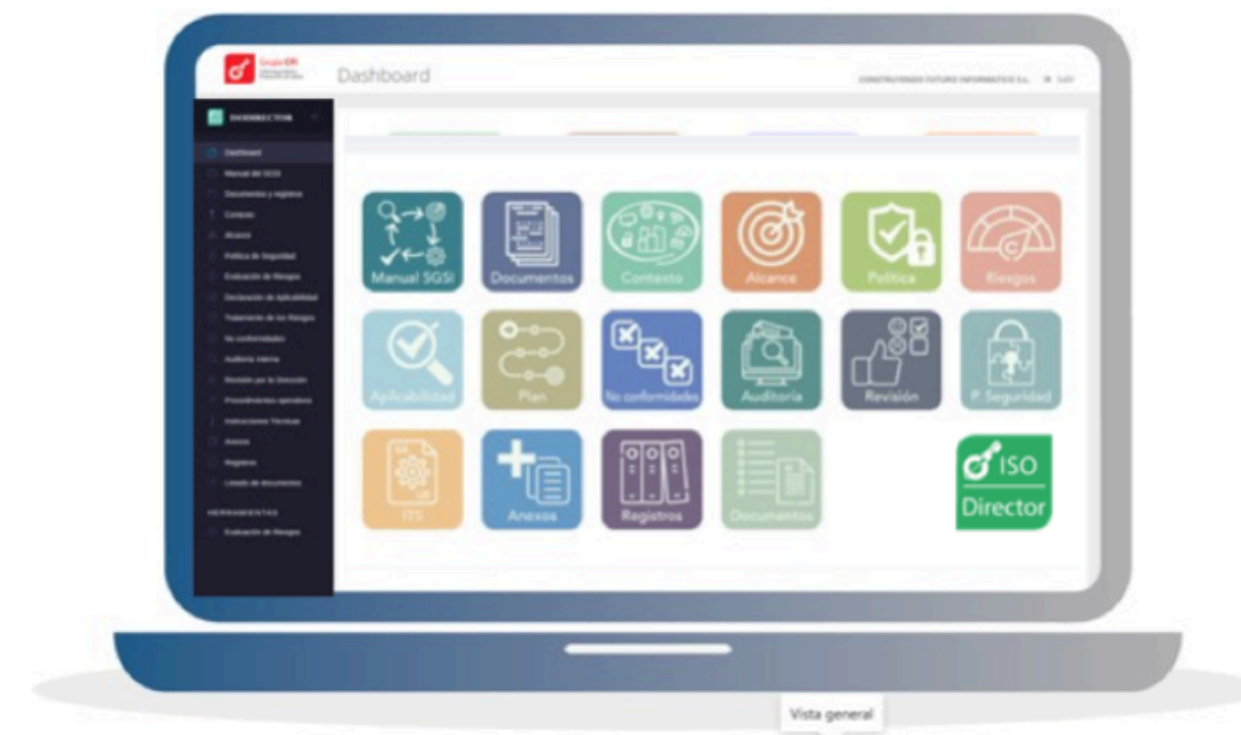
grupocfi.es



Desarrollo de software

- LOPD Manager
- HubLOPD
- ISO Director

Papel Cero



PRIMER PASO RECOMENDADO

Un diagnóstico breve para convertir la preocupación en un plan de acción.

**La mejor puerta de entrada no es “comprar algo”:
es entender el punto de partida.**

- 01 Reunión inicial**
actividad, sistemas, clientes, obligaciones y preocupaciones
- 02 Revisión de madurez**
riesgos prioritarios y brechas más relevantes
- 03 Hoja de ruta**
medidas por impacto, urgencia, coste y cumplimiento



grupocfi.es

¿Hablamos?

El primer paso es saber en qué punto está tu empresa.

RECURSOS Y SERVICIOS DE APOYO PARA LAS EMPRESAS

**BLOQUE II.1: Línea de Ayudas de Proyectos de I+D en
Ciberseguridad dentro del Proyecto Red Argos (Programa
Retech), con cargo al PRTR**

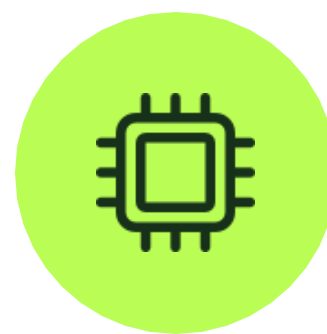
Ponente: Victoria Molpeceres Arroyo . Responsable de Departamento de Innovación y Emprendimiento del Instituto para la Competitividad Empresarial de la Junta de Castilla y León

RED ARGOS: Tu mejor aliado en ciberseguridad

Aprovecha esta oportunidad única para que tu negocio crezca de manera segura



Mejora de las capacidades:
infraestructura, equipamiento y recursos



Incremento de la adopción global de
medidas de ciberseguridad, desde el
diseño y en el resto de etapas.
Desarrollo de nuevas soluciones



Generación de talento, fórmate en
ciberseguridad



Impulsa la aceleración de empresas y el
emprendimiento en ciberseguridad



Conoce el ecosistema nacional en
materia de ciberseguridad con el fin de
obtener un liderazgo internacional



Conoce la red de nodos especializados
en ciberseguridad



Impulsando la ciberseguridad empresarial

RED ARGOS en Castilla y León

2. Financiación

2.2. PROYECTOS DE I+D EN CIBERSEGURIDAD (Presupuesto: 3.550.000 €)

Objeto: Subvenciones destinadas a financiar proyectos empresariales de I+D en ciberseguridad

Beneficiarios: PYMES y grandes empresas (en colaboración)

Proyectos subvencionables:

Proyectos estratégicos de investigación aplicada y desarrollo experimental en el área de la ciberseguridad, enfocados en fomentar una investigación que proponga soluciones a desafíos transversales y estratégicos, mejorando la base de conocimiento y tecnología en la que se apoyan las empresas de Castilla y León en esta materia.



PROYECTOS de I+D individuales: presentados por una única pequeña o mediana empresa.



PROYECTOS de I+D colaborativos: presentados por un consorcio de un mínimo de tres y un máximo de cinco empresas de cualquier tamaño, siendo al menos dos de ellas pymes.

RED ARGOS en Castilla y León

2. Financiación

2.2. PROYECTOS DE I+D EN CIBERSEGURIDAD

Tipo de ayuda:

La ayuda consistirá en una subvención a fondo perdido que se determinará como un porcentaje fijo mínimo al que se sumará un porcentaje variable:



PYMES: porcentaje mínimo del 70% de la actuación subvencionada, pudiendo alcanzar hasta un 80% de financiación



GRANDES: porcentaje mínimo 50% de la actuación subvencionada, pudiendo alcanzar hasta un 60% de financiación

RED ARGOS en Castilla y León

2. Financiación

2.2. PROYECTOS DE I+D EN CIBERSEGURIDAD

Gastos elegibles:



Gastos de personal (investigadores, técnicos, personal auxiliar) conforme a la dedicación que exija su participación en el proyecto



Costes de adquisición de hardware o software vinculado al proyecto subvencionado



Costes externos de consultores especializados, no vinculados o asociados a la empresa beneficiaria



Gastos de gestión para la tramitación del expediente de ayuda, realizados por una entidad gestora externa.



Gastos de auditoría para la realización de un informe final obligatorio de auditoría económica de la subvención

RED ARGOS en Castilla y León

2. Financiación

2.2. PROYECTOS DE I+D EN CIBERSEGURIDAD

Presupuestos elegibles mínimos y máximos

Tipología de proyecto	TIPO	MÍNIMO	MÁXIMO
Proyectos individuales	Pymes	100.000 €	425.000 €
Proyectos colaborativos	Pymes y Grandes empresas	100.000 €	1.300.000 €

Estas ayudas están sujetas al régimen de minimis

El importe total de las ayudas de minimis concedidas a una única empresa no excederá de trescientos mil euros (300.000 €) durante cualquier periodo de 3 años.

RED ARGOS en Castilla y León

2. Financiación

2.3. PROYECTOS PRESENTADOS

Tipología de proyecto	Nº PROYECTOS PRESENTADOS	PRESUPUESTO PRESENTADO	PRESUPUESTO APROBADO	SUBVENCIÓN CONCEDIDA
Proyectos INNOVACIÓN	23	1.358.921,68 €	1.313.999,10 €	1.013.767,25 €
Proyectos I+D	13	3.214.466,34 €	2.780.073,93 €	2.095.820,24 €

RED ARGOS en Castilla y León

5. Otras actuaciones:

Vigilancia Tecnológica en materia de ciberseguridad:

- Mapa de ayudas públicas relacionadas con ciberseguridad.
- Análisis de la legislación y normativa relacionada con ciberseguridad.
- Análisis de los avances tecnológicos y aplicaciones de la ciberseguridad.
- Boletín mensual con noticias de interés relacionadas con ciberseguridad.

Impulso del Grupo de Trabajo Regional sobre ciberseguridad.

Plan de Sensibilización en Ciberseguridad y Fomento de la Demanda.

Internacionalización y visibilización del ecosistema:

- Identificación de eventos europeos e internacionales de interés.
- Colaboración directa con agentes de la Red de Emprendimiento e Innovación de Castilla y León.
- Visibilización y posicionamiento de RED ARGOS a nivel internacional.

Maapeo de Recursos y Capacidades del ecosistema regional de Ciberseguridad:

- Mapa de recursos y capacidades disponible y actualizado.
- Identificación de nuevos agentes del ecosistema regional de la ciberseguridad.
- Identificación de servicios y soluciones que proporcionan todos los agentes.

RECURSOS Y SERVICIOS DE APOYO PARA LAS EMPRESAS

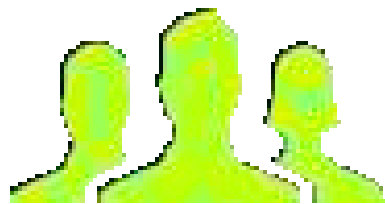
**BLOQUE II.2: Línea de Ayudas de Proyectos de I+D en
Ámbitos de Tecnologías Fundamentales para las provincias
de León y Palencia (Fondo de Transición Justa)**

Ponente: Pablo Merinero Sáinz. Responsable de Seguimiento de Ayudas a la Innovación.

Proyectos de I+D en ámbitos de tecnologías fundamentales en los territorios de la Comunidad de Castilla y León (provincias de León y Palencia), incluidos en el programa del Fondo de Transición Justa de España 2021-2027



Proyectos de I+D en ámbitos de tecnologías fundamentales en los territorios de la Comunidad de Castilla y León (provincias de León y Palencia), incluidos en el programa del Fondo de Transición Justa de España 2021-2027



Empresas León y Palencia

- Micro empresa
- Pequeña empresa
- Mediana empresa
- Grandes empresas



Proyectos de I+D en ámbitos de tecnologías fundamentales en los territorios de la Comunidad de Castilla y León (provincias de León y Palencia), incluidos en el programa del Fondo de Transición Justa de España 2021-2027

Proyectos de I+D STEP en Le y Pa



Proyectos Subvencionables

Proyectos
individuales

Micro empresa
Pequeña empresa
Mediana empresa

20.0000 – 1.000.000

Grandes empresas

200.000 – 2.000.000

Proyectos
Colaboración
Efectiva

Al menos 2 empresas
Al menos 1 pyme
≤ 70 %

250.0000 – 2.500.000

Proyectos de I+D en ámbitos de tecnologías fundamentales en los territorios de la Comunidad de Castilla y León (provincias de León y Palencia), incluidos en el programa del Fondo de Transición Justa de España 2021-2027



Proyectos Subvencionables

Proyectos de I+D STEP en Le y Pa

Plazo presentación: hasta 30/06/2028, salvo cierre anticipado

Plazo ejecución: 30 meses, con fecha tope de 30/03/2030

Crédito: ≈ 13 M€

Proyectos de I+D en ámbitos de tecnologías fundamentales en los territorios de la Comunidad de Castilla y León (provincias de León y Palencia), incluidos en el programa del Fondo de Transición Justa de España 2021-2027



Costes subvencionables

1. Gastos de personal

Categoría de coste	Requisitos	Coste máx. €/h
Director Técnico y Personal Cualificado	Titulado universitario y grupo cotización Seguridad Social 1 o 2	45
Personal Técnico	Grupo cotización Seguridad Social 3,4 o 5	30
Personal Auxiliar	Resto del personal.	20

1. Tipo fijo

40 % de los gastos de personal aprobados

Proyectos de I+D en ámbitos de tecnologías fundamentales en los territorios de la Comunidad de Castilla y León (provincias de León y Palencia), incluidos en el programa del Fondo de Transición Justa de España 2021-2027



Subvención

1. Proyectos individuales

a. Porcentaje mínimo

Categoría del Proyecto	Tamaño de la empresa			
	Micro	Pequeña	Mediana	Grande
Investigación Industrial	60 %	55 %	50 %	40 %
Desarrollo Experimental	45 %	40 %	35 %	25 %

a. Porcentaje variable

- Criterio territorial: 5%
- Criterio igualdad: 5%
- % personal con discapacidad: 5%

Proyectos de I+D en ámbitos de tecnologías fundamentales en los territorios de la Comunidad de Castilla y León (provincias de León y Palencia), incluidos en el programa del Fondo de Transición Justa de España 2021-2027



Subvención

1. Proyectos colaboración efectiva

a. Porcentaje mínimo

Categoría del Proyecto	Tamaño de la empresa			
	Micro	Pequeña	Mediana	Grande
Investigación Industrial	65 %	60 %	55 %	45 %
Desarrollo Experimental	55 %	50 %	45 %	35 %

a. Porcentaje variable

- Criterio territorial: 5%
- Criterio igualdad: 5%
- % personal con discapacidad: 5%

Proyectos de I+D en ámbitos de tecnologías fundamentales en los territorios de la Comunidad de Castilla y León (provincias de León y Palencia), incluidos en el programa del Fondo de Transición Justa de España 2021-2027



Subvención

1. Límites de la subvención

a. Porcentaje máximo

	Intensidad máxima de ayuda bruta		
Categoría de Investigación	Microempresa y Pequeña empresa	Mediana empresa	Gran Empresa
Investigación Industrial	75 %	65 %	55 %
Investigación Industrial en colaboración efectiva	80 %	75 %	65 %
Desarrollo experimental	50 %	40 %	30 %
Desarrollo experimental en colaboración efectiva	60 %	50 %	40 %

Incompatibilidad

Proyectos I+D – FTJ-STEP

3 NIVELES

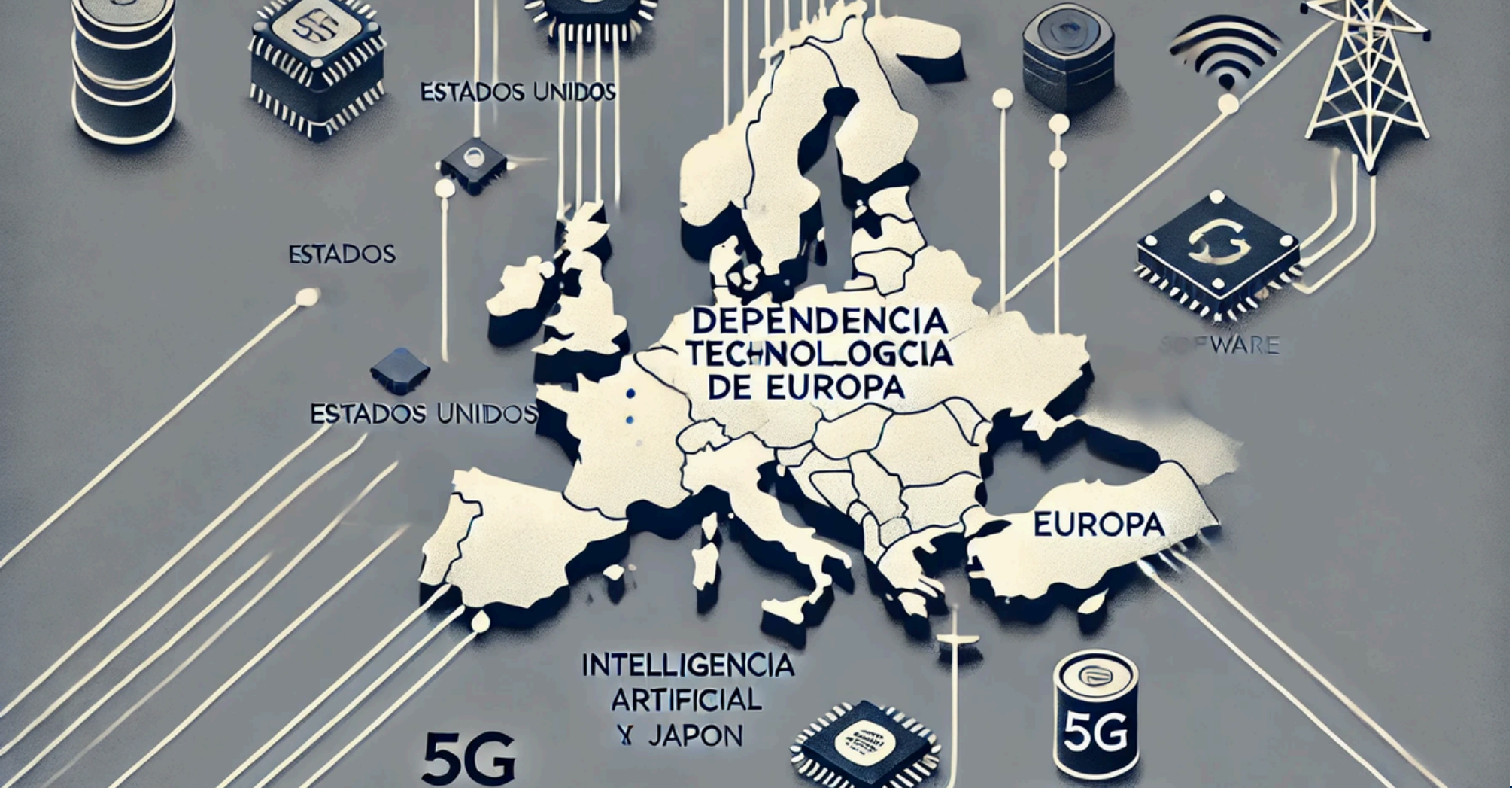
• Sector Tecnológico

Tecnologías limpias y eficientes en el uso de los recursos
Tecnologías digitales y profundas
Biotecnologías
Tecnologías de defensa

• Ámbito

• Tecnología fundamental

Nivel 1: Sector Tecnológico	Nivel 2: Ámbito	Nivel 3: Tecnología Específica
Biotecnologías.	Proteínas y otras moléculas.	Secuenciación/síntesis/ingeniería/fabricación de proteínas y péptidos (incluidas las hormonas moléculas grandes).



Para más información acerca de RED ARGOS:



info@redargos.com



<https://redargos.com/>