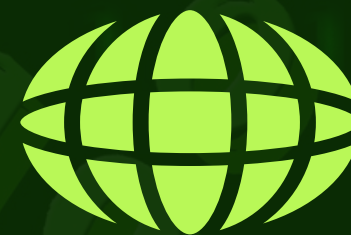


DEL RIESGO A LA OPORTUNIDAD: CLAVES PARA PROTEGER TU EMPRESA Y FINANCIACIÓN PARA INNOVAR



Webinar de capacitación y sensibilización en materia de ciberseguridad

2 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: Ciberamenazas y retos irresueltos en la actualidad:

- Panorama actual de amenazas.
- Retos por abordar.
- Casos reales de incidentes en ámbito industrial.

BLOQUE II: Innovación ayudas y financiación disponibles:

- Qué es la CPI
- Convocatoria I+D+i RED ARGOS
- Convocatoria I+D en ámbito de tecnologías fundamentales.
- Compra Pública de Innovación (CPI) en ciberseguridad.
- Programa Horizon Europe.
- European Digital Programme (DEP).

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



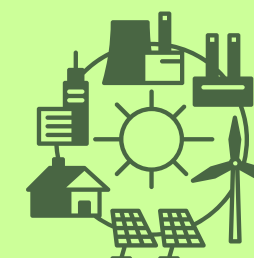
Andalucía

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

CIBERAMENAZAS Y RETOS IRRESUELTOS

BLOQUE I

PANORAMA ACTUAL DE AMENAZAS



Ransomware y extorsión digital: Cifrado o robo de información con petición de rescate.

Impacto: parada de actividad, pérdida de datos, daño reputacional y costes de recuperación.



Ataque a la cadena de suministro (*Supply Chain Attack*): Exposición a fallos de seguridad originados en proveedores, software o servicios de terceros.

Riesgo asociado: la vulnerabilidad de un tercero se traslada directamente a la empresa, sin que el fallo se origine en ella, y puede extenderse a sus propios clientes y colaboradores.



Ataques avanzados: Phishing, robo de credenciales, explotación de vulnerabilidades y uso de herramientas legítimas para moverse dentro de la red.

Consecuencia directa: acceso no autorizado a sistemas, que con frecuencia deriva en fraude, robo de datos o ransomware.

Ransomware y extorsión digital I

¿Qué es?

Es un tipo de *software* malicioso o *malware* que **cifra y secuestra los datos** de una empresa, haciéndolos inaccesibles, y **exige un rescate económico** para devolverlos a su estado original.

Las Pymes, el blanco perfecto.

Cuentan con **menos recursos y protección** en ciberseguridad, convirtiéndolas en objetivos más vulnerables. Aunque sean pequeñas, estas empresas a menudo manejan **información sensible**, de **gran valor para los ciberdelincuentes**.

Vías de entrada más comunes.

- Los correos electrónicos fraudulentos, de tipo phishing.
- Vulnerabilidades en software no actualizado.

Ransomware y extorsión digital II: Medidas de prevención y mitigación

Vías de entrada	Medidas de prevención
Phishing (correos engañosos)	Formación continua del personal y simulacros de phishing
Robo de credenciales	Autenticación multifactor (MFA), gestores de contraseñas y políticas de contraseñas robustas y rotación periódica
Vulnerabilidades de software	Actualizaciones y parches de seguridad periódicos
Fraude del CEO / RRHH (suplantación de identidad)	Verificación en dos pasos para transferencias y solicitudes sensibles

Medidas de mitigación: Cuando la prevención no es suficiente, las **copias de seguridad cifradas** y desconectadas de la red mejoran la capacidad de recuperacion y permiten mantener la continuidad del negocio.

Ataque a la cadena de suministro (Supply Chain Attack)

¿Qué es?

Riesgo de infección de virus o ataques a través de los sistemas de un tercero, **un proveedor de confianza** que cuenta con menores medidas de seguridad o accesos remotos permitidos.

¿Cómo se produce la infección?



Software de terceros comprometido: Modifican el código de un programa legítimo o de una actualización técnica de un proveedor habitual.



Suplantación de identidad: Interceptan el correo del proveedor y correos idénticos a las reales con malware camuflado en adjuntos.

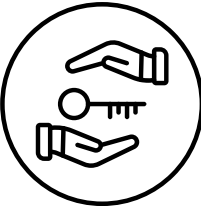


Accesos remotos desprotegidos: Roban las credenciales al proveedor, los atacantes entran directamente a los sistemas de la empresa sin levantar sospechas.



Robo de información indirecto: Brecha en el sistema del proveedor que revela datos confidenciales.

Ataque a la cadena de suministro (Supply Chain Attack): Medidas de prevención

	Relación con el proveedor	Medidas de prevención
	Antes de contratar	Exigir mínimos de ciberseguridad y evaluar reputación: certificaciones y cumplimiento normativo de proveedores críticos.
	Durante la contratación	- Establecer cláusulas de seguridad sobre acceso a datos, responsabilidades, controles, auditorías y penalizaciones. - Definir ANS/SLA (Acuerdo de Nivel de Servicio / Service Level Agreement).
	Durante la relación	Supervisar y auditar el servicio de forma continua, extendiendo el control a toda la cadena de suministro.
	Al finalizar el contrato	Retirar accesos , recuperar activos y garantizar el borrado de toda información sensible.

Ataques avanzados I



Ransomware de Extorsión Múltiple

¿Cómo funciona?

Roban la información confidencial antes de cifrarla, no solo bloquean el acceso.

Doble extorsión

Aún con copias de seguridad, amenazan con **filtrar secretos comerciales o datos de clientes**.

Triple extorsión

Contactan directamente a **clientes y proveedores** de la empresa para forzar el pago.



Compromiso de Correo Empresarial (BEC)

¿Cómo funciona?

Utlizan **IA generativa** imita con exactitud el tono, jerga y estilo de directivos o proveedores habituales.

Amenaza avanzada

Sin errores ortográficos ni saludos genéricos, es **casi imposible detectar el fraude** a simple vista.

MFA Fatigue

Bombardean el móvil del empleado con **solicitudes de acceso** hasta que aprueba una por error.

Ataques avanzados II



Ingeniería Social Multimedia Deepfakes y Vishing

¿Cómo funciona?

Llamadas con **tecnología deepfake** que suplanta la voz e imagen exacta de un socio, banco o el propio CEO.

Amenaza Avanzada

La legitimidad **visual y auditiva** combinada con la **presión psicológica** logra vulnerar los controles manuales del empleado.

Solicitudes Urgentes

Transferencias de fondos, cambios en cuentas bancarias de facturación o restablecimiento de contraseñas críticas.



Ataques mediante Código QR Quishing y Smishing

¿Cómo funciona?

Correos/SMS corporativos con un **código QR** para una gestión urgente nóminas, seguro médico, acceso a sistemas.

Amenaza avanzada

Los **filtros de seguridad** del correo no pueden leer el **enlace oculto** tras la imagen del QR

Exposición de credenciales

El empleado escanea el QR con su móvil personal o de trabajo, dando acceso a sus credenciales corporativas sin saberlo.

RETOS A ALCANZAR



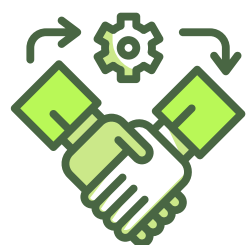
OT/IoT conectado

Maquinaria, sensores y dispositivos conectados amplían la superficie de ataque.



Identidades y accesos

Controlar quién accede, desde dónde y con qué permisos.



Continuidad y recuperación

Prepararse para responder y recuperar la actividad ante un incidente.

El reto para las pymes no es solo prevenir ataques, sino mantener la actividad y recuperarse rápido si ocurre un incidente.

Retos OT/IoT: Brechas de acceso más comunes

Contraseñas débiles o predeterminadas



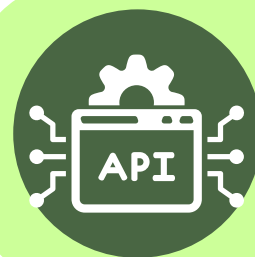
Equipos que mantienen credenciales de fábrica o contraseñas fijas en el firmware que no pueden modificarse.

Actualizaciones inseguras



Sin actualizaciones firmadas criptográficamente, pueden instalar firmware modificado o malicioso en el dispositivo.

Puertos y APIs expuestos



Puertos de red abiertos innecesariamente y APIs vulnerables en la nube que facilitan accesos remotos no autorizados.

Datos transmitidos sin cifrar



Información sensible enviada en texto plano por la red, vulnerable a interceptaciones mediante ataques Man-in-the-Middle.

Software obsoleto



Sistemas operativos y componentes sin soporte, con vulnerabilidades conocidas públicamente y sin parche disponible.

Falta de protección física



Dispositivos instalados en lugares accesibles sin protección, expuestos a manipulación directa o extracción de tarjetas de memoria.

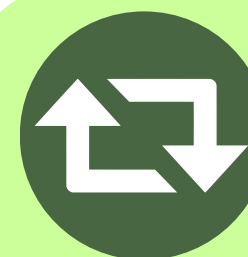
Gestión de Accesos e Identidades: Fallos Críticos

Ausencia de doble factor (MFA)



Una sola contraseña filtrada es suficiente para que un atacante acceda al correo o a los sistemas internos de la empresa.

Reutilización de contraseñas



Usar la misma clave en el correo corporativo, redes sociales y cuentas personales multiplica el riesgo ante cualquier filtración.

Privilegios excesivos



Permisos de administrador para tareas diarias que no lo requieren, ampliando innecesariamente la superficie de ataque.

Falta de offboarding



Cuentas de ex-empleados que permanecen activas meses después de su salida, con acceso pleno a sistemas y correo.

Credenciales compartidas



Equipos que comparten una única cuenta genérica imposibilitan rastrear quién hizo qué en caso de incidente.

Shadow IT sin control



Uso de aplicaciones externas con su correo corporativo sin aprobación de IT, creando accesos invisibles para la empresa.



Soluciones de bajo coste y alto impacto

MFA obligatorio

Activa el **doble factor de autenticación** en todas las herramientas en la nube y cualquier acceso remoto:
Google Authenticator,
Microsoft Authenticator

Gestor de contraseñas

Uso obligatorio de herramientas gratuitas como **KeePass** o **PassBolt** eliminan contraseñas anotadas y reutilizadas en post-its o correos.

Mínimo privilegio

Restringe el acceso a datos financieros y de clientes solo a quien lo necesite. Revisa permisos al menos una vez al año.

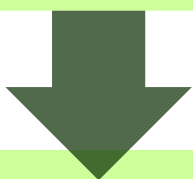
Continuidad del negocio y recuperación

1.El día del ataque

Plan de Respuesta

Aislamiento

Desconectar equipos de la red
sin apagarlo



Cadena de mando

Definir quién decide parar la
operación



Contactos clave

Soporte técnico, seguro,
abogados y AEPD

2.Actividad tras el ataque

Operar en modo degradado

Procedimientos manuales

Plantillas en papel para pedidos,
facturas e inventario

Sistemas alternativos

Dispositivos no afectados con
acceso a servicios en la nube

Comunicación alternativa

Mensajería cifrada ajena a los
servidores locales

3.Vuelta a la normalidad

Mecanismos de recuperación

Análisis forense

Identificar la vía de entrada
antes de restaurar ningún
sistema

Limpieza total

Formatear y reinstalar desde
cero. Nunca reutilizar un sistema
comprometido

Restauración progresiva

Primero facturación y atención al
cliente, después el resto

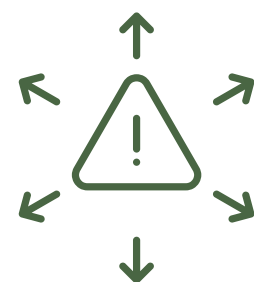
CASOS REALES I

Norsk Hydro



¿Qué pasó?

Un virus de rescate (ransomware) bloqueó la red corporativa. Aunque las máquinas de producción no se infectaron, toda la fábrica se detuvo porque los operarios no podían ver los pedidos de los clientes, las órdenes de fabricación ni las direcciones de envío



Impacto operativo

- Parálisis total: bloqueo de 3.000 servidores corporativos en segundos.
- Vuelta al pasado: tuvieron que producir usando papel, bolígrafo y procesos manuales.
- Efecto dominó: pérdida de comunicación con clientes, proveedores y sistemas de envío.



Respuesta

- Cero pagos. Reconstruyeron todo con copias de seguridad.
- Gestionaron los pedidos llamando al cliente uno a uno.
- Usaron pizarras, libretas y operaron las máquinas en manual.

Si tu sistema informático se apaga hoy, tu única salvaguarda real serán tus copias de seguridad aisladas de la red.

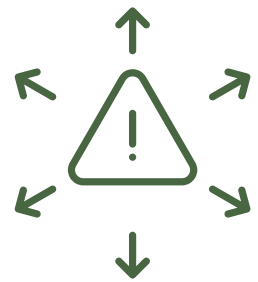
CASOS REALES II

JBS Foods



¿Qué pasó?

El 30 de mayo de 2021, el gigante cárnico JBS Foods sufrió un masivo ciberataque de tipo ransomware ejecutado por el grupo cibercriminal de origen ruso REvil, el cual encriptó sus servidores de soporte informático y obligó a suspender la actividad de múltiples plantas de procesamiento a nivel global.



Impacto operativo

- Colapso de la producción norteamericana: El cierre de las nueve plantas de Estados Unidos y la mayor de Canadá suprimió repentinamente el 25% de la producción de ternera y el 20% de cerdo.
- Parálisis laboral y ganadera internacional: La caída informática forzó la suspensión laboral de 7.000 trabajadores y bloqueó las granjas al impedir la entrega de animales para el sacrificio.



Respuesta

- Aislamiento informático: JBS desconectó sus sistemas de TI para frenar el virus, salvando los servidores de respaldo externos y evitando la filtración de datos de clientes.
- Pago de rescate: Tras avisar al FBI, la directiva pagó 11 millones de dólares en Bitcoin.

Las copias de seguridad salvan datos, pero solo una ciberseguridad proactiva salva el negocio.

INNOVACIÓN, AYUDAS Y FINANCIACIÓN DISPONIBLES

BLOQUE II.1: Concepto de Compra Pública de Innovación

LA COMPRA PÚBLICA DE INNOVACIÓN (CPI) I

¿Qué es?

Un **mecanismo específico de contratación pública** que permite al sector público adquirir **soluciones que no existen actualmente en el mercado**, así como soluciones en fase de desarrollo.



Objetivos

- Impulsar la **innovación** desde el sector público.
- Favorecer la **colaboración** con empresas y centros de investigación.
- Resolver retos y **necesidades no cubiertas**.
- **Mejorar los servicios públicos** mediante las nuevas tecnologías.



Marco legal

Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación (art. 36.sexies): La compra pública de innovación (CPI) podrá tener por objeto la adquisición de bienes o servicios innovadores, que no existan actualmente en el mercado como producto o servicio final, o la investigación de soluciones a futuras necesidades públicas.

LA COMPRA PÚBLICA DE INNOVACIÓN (CPI) I

¿Qué es?

Un **mecanismo específico de contratación pública** que permite al sector público adquirir **soluciones que no existen actualmente en el mercado**, así como soluciones en fase de desarrollo.



Objetivos

- Impulsar la **innovación** desde el sector público.
- Favorecer la **colaboración** con empresas y centros de investigación.
- Resolver retos y **necesidades no cubiertas**.
- **Mejorar los servicios públicos** mediante las nuevas tecnologías.



Marco legal

Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación (art. 36.sexies): La compra pública de innovación (CPI) podrá tener por objeto la adquisición de bienes o servicios innovadores, que no existan actualmente en el mercado como producto o servicio final, o la investigación de soluciones a futuras necesidades públicas.

LA COMPRA PÚBLICA DE INNOVACIÓN (CPI) II



A nivel europeo, la CPI se suele definir como:

La contratación en la que concurren uno o los dos siguientes aspectos:

- ✓ La compra del proceso de innovación (servicios de I+D) con sus resultados (parciales).
- ✓ La compra de los resultados de la innovación.



Algunos errores comunes:

- ✗ **No es un único procedimiento de contratación pública:** una Administración puede hacer uso de todos sus instrumentos jurídicos para adquirir estos productos y servicios innovadores.
- ✗ **No tiene un modelo fijo que deba seguirse obligatoriamente:** hay múltiples modelos y la academia y los profesionales están creando nuevos modelos cada año.

LA COMPRA PÚBLICA DE INNOVACIÓN (CPI) III

MODALIDADES DE CPI

Compra Pública Precomercial (CPP)

- Contratación de servicios de I+D.
- Se financia el desarrollo de soluciones innovadoras.



Compra Pública de Tecnología Innovadora (CPTI)

Adquisición de productos o servicios innovadores próximos al mercado.



Procedimiento de contratación específico

Asociación para la innovación (arts. 177-182 LCSP)



Introducción a la madurez tecnológica - TRLs

TECHNOLOGY READINESS LEVELS IN THE EUROPEAN COMMISSION (EC)	
TECHNOLOGY READINESS LEVEL	DESCRIPTION
TRL 1.	Basic principles observed
TRL 2.	Technology concept formulated
TRL 3.	Experimental proof of concept
TRL 4.	Technology validated in lab
TRL 5.	Technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)
TRL 6.	Technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)
TRL 7.	System prototype demonstration in operational environment
TRL 8.	System complete and qualified
TRL 9.	Actual system proven in operational environment (competitive manufacturing in case of key enabling technologies; or in space)

COMPRA PÚBLICA PRECOMERCIAL - CPP

Compra pública precomercial (CPP)	
Definición	- Contratación de los servicios de I+D con vistas a un producto o servicio que está aún lejos de ser comercializado en el mercado, pero cuya compra favorece el desarrollo del sector. - Inversión en I+D.
Objeto	- Investigación de soluciones a futuras demandas públicas. - La CPP promueve la formación tecnológica de las empresas.
Tipo de contrato	- Contratos excluidos de la Ley de Contratos del Sector Público (art. 8 LCSP / art. 20 RD 3/2020 / art. 7.1.k) Ley 24/2011) - Contrato plenamente sujeto a Dº privado (salvo principios generales de la contratación pública) - El comprador y el operador económico comparten los riesgos y beneficios que derivan del proceso de I+D.
TRL	Limitado hasta TRL 7-8, sin adquisición de la solución por el comprador público.
Procedimientos de contratación	Cualquiera de los previstos en la LCSP, así como cualquiera que defina el órgano de contratación y cumpla con los principios de la contratación pública

COMPRA PÚBLICA DE TECNOLOGÍA INNOVADORA - CPTI

Compra pública de tecnología innovadora (CPTI)	
Definición	Adquisición de soluciones innovadoras que están próximas al mercado o que existen ya en un número reducido y que no requieren de una fase de I+D amplia.
Objeto	- Adquisición de bienes y servicios innovadores. - Mejora la prestación de servicios públicos y fortalece la posición del operador económico.
Tipo de contrato	Contrato sujeto a la LCSP.
TRL	TRL 7-9, incluyendo adquisición de la solución resultante
Procedimientos de contratación	- Abierto - Restringido - Con negociación - Diálogo competitivo

ASOCIACIÓN PARA LA INNOVACIÓN

Asociación para la Innovación	
Definición	◦ Procedimiento de contratación que combina la I+D para el desarrollo de un nuevo producto o servicio con la subsiguiente adquisición por el comprador público.
Objeto	◦ Adquisición de bienes y servicios innovadores que no están aún en el mercado, incluyendo su desarrollo previo.
Tipo de contrato	◦ Procedimiento regulado en la LCSP (arts. 177 y ss.). ◦ Se desarrolla en al menos dos fases diferenciadas: Fase de I+D y Fase de ejecución de las obras, servicios o suministros derivados. ◦ Incluye una negociación de las propuestas de solución con los operadores económicos. ◦ La adquisición de las soluciones se supedita a la consecución de los niveles de rendimiento y costes máximos acordados entre las partes.
TRL	◦ Desde TRLs bajos hasta TRL 9

INNOVACIÓN, AYUDAS Y FINANCIACIÓN DISPONIBLES

**BLOQUE II.2: Compra Pública de Innovación
aplicada a Ciberseguridad**

COMPRA PÚBLICA DE INNOVACIÓN EN CIBERSEGURIDAD

¿Qué es?

La Administración lanza **retos de ciberseguridad** y contrata el desarrollo o adquisición de **soluciones innovadoras** que todavía no existen en el mercado o requieren evolución tecnológica.

¿Cómo participar?



Identificar **retos** y **consultas** preliminares de mercado.



Preparar una **propuesta técnica y económica** alineada con la necesidad pública.



Participar **individualmente** o en **consorcio**, cuando la licitación lo permita.



Superar **hitos de I+D**, validación y, en su caso, despliegue de la solución.

CIBERMOV ARGOS I



CIBERMOV es un proyecto de **compra pública precomercial** para diseñar, desarrollar e implantar un **Centro de Excelencia en Ciberseguridad** aplicada a la **Movilidad Conectada** en **Castilla y León**, en modalidad de prototipo funcional. Forma parte de la **Red Argos**, dentro del programa **RETECH**.



Organismo convocante

Instituto para la Competitividad Empresarial de Castilla y León (ICECYL).



Presupuesto

2.892.561,98 €.



Adjudicatario

UTE Renault España – Orange Espagne, S.A.U.



Duración y estado

Licitado y adjudicado en 2025. Actualmente **en ejecución**.

CIBERMOV ARGOS II

Objetivos

- Crear un **entorno de referencia** para el desarrollo, validación y prueba de tecnologías de **vehículo conectado y ciberseguro**.
- Integrar **infraestructura urbana inteligente**, comunicaciones seguras y redes privadas 5G en condiciones reales de tráfico.
- Reforzar el **ecosistema regional y nacional** de ciberseguridad y automoción.

Resultados previos

- **Centro de Excelencia** especializado en **movilidad conectada**.
- **Prototipo funcional** y un **entorno urbano de pruebas** en Valladolid.
- Capacidades para **testar conectividad**, ciberseguridad y tecnologías de coche conectado en entorno real.
- **Atracción** de fabricantes, empresas auxiliares, startups y **talento** especializado en automoción y ciberseguridad.

CIBER ESCALA CPI I



CIBER ESCALA CPI es un proyecto de **compra pública precomercial**, para desarrollar un **sistema de detección de servicios ilícitos ocultos en la red TOR** (The Onion Router) versiones 2 y 3, no indexados por fuentes públicas. Cofinanciado al 50% por el **FEDER**.



Organismo convocante

Instituto para la Competitividad Empresarial de Castilla y León (ICE)



Presupuesto

442.637,43 €



Adjudicatario

GMV Soluciones Globales Internet, S.A.U.– Universidad de Murcia



Duración

13 meses.

CIBER ESCALA CPI II

Objetivos

- Desarrollar un **sistema de detección de servicios ilícitos ocultos** en la red TOR.
- Impulsar la **I+D** mediante la Compra Pública Precomercial (**CPP**), desde la demanda.
- Promover **soluciones innovadoras** en el ámbito de la ciberseguridad.
- Impulsar la **especialización regional** de Castilla y León en ciberseguridad.
- Fortalecer la **colaboración público-privada** (INCIBE y AEI Ciberseguridad).

Funcionalidades

- Detección automática de dominios .onion no indexados.
- Filtrado de servicios conocidos por fuentes públicas.
- Comprobación del estado (activo/inactivo) de los servicios detectados.
- Consulta estructurada de los resultados obtenidos.
- Generación de un prototipo software funcional.
- Capacidad de evolución tecnológica frente a cambios en TOR.
- Monitorización continua de los servicios detectados.
- Documentación técnica completa del sistema y sus componentes.

PROGRAMA DE CPI DE INCIBE I



Son programas de **I+D** articulados mediante **compra pública precomercial** entre INCIBE y grandes empresas, para desarrollar **soluciones de ciberseguridad estratégicas**, orientadas a retos del sector público, pymes y sectores NIS2.



Organismo convocante

Instituto Nacional de Ciberseguridad (INCIBE)



Presupuesto

224 millones de euros



Duración

2022-2026

PROGRAMA DE CPI DE INCIBE II

Resultados

- Conjunto de **proyectos de I+D** independientes, pero alineados en una **estrategia común**.
- Cofinanciación entre INCIBE y la empresa adjudicataria, compartiendo riesgos e inversión.
- Desarrollo de **soluciones tecnológicas** para pymes y sectores estratégicos.
- Refuerzo de la **competitividad internacional** de la ciberseguridad española.
- Impulso de la **cultura y el conocimiento** en **ciberseguridad** dentro de las empresas españolas.

Innovación

- Impulso de la **innovación** en la contratación y **compra pública estratégica**.
- Fomento de la **I+D+i en ciberseguridad**.
- Colaboración **público-privada** para fortalecer la industria y la innovación nacional.
- Creación de un **catálogo de soluciones** innovadoras de alto impacto para **pymes y sectores estratégicos** españoles y europeos.

INNOVACIÓN, AYUDAS Y FINANCIACIÓN DISPONIBLES

BLOQUE II.3.1: Convocatorias Nacionales

CONVOCATORIA I+D+i Red Argos I



Plazo

Del 26/04/2026 al 31/08/2026



Cuantía

Subvención a fondo perdido, que se determinará como un porcentaje de los costes subvencionables del proyecto de I+D.



Quién puede solicitarla

PYMES de Castilla y León o grandes empresas de Castilla y León en colaboración con PYMES.



Proyectos subvencionables

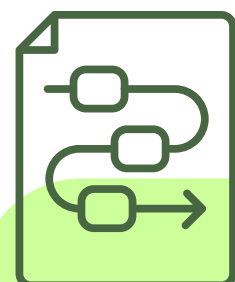
I+D aplicada y **desarrollo experimental** en **ciberseguridad**, alineados con la **RIS3 de Castilla y León**. En concreto, prioridad 3: **fabricación inteligente y ciberseguridad**.
 *Máximo 1 proyecto de I+D en ejecución por empresa.
 *El proyecto deberá obtener al menos 40 puntos conforme a los criterios de valoración.

CONVOCATORIA I+D+i Red Argos I I



Requisitos

- **Ejecución en Castilla y León:** El proyecto y sus resultados deben desarrollarse y permanecer en Castilla y León.
- **Proyecto completo y no finalizado:** Debe ser aplicable por sí mismo y no estar completamente ejecutado antes de solicitar la ayuda.
- **Inicio elegible:** A partir del 1 de junio de 2024.
- **Viabilidad acreditada:** Debe ser viable técnica, económica, financiera y medioambientalmente.
- **Personal y evaluación mínima:** El personal imputado debe estar adscrito a un centro de trabajo en Castilla y León y el proyecto debe alcanzar la puntuación mínima exigida.



Procedimiento

- Las subvenciones se tramitarán en **concurrentia no competitiva**.
- Tramitación electrónica en <https://www.tramitacastillayleon.jcyl.es/web/es/sede-electronica.html>
- Para consultar las bases reguladoras y la convocatoria: [BBRR y Convocatoria](#)

CONVOCATORIA I+D en Tecnologías Fundamentales I

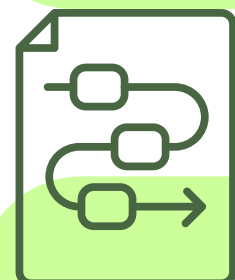
	Plazo	Del 11/06/2026 al 30/06/2028
	Cuantía	12.993.999 €
	Quién puede solicitarla	Empresas con centro de trabajo en el que se vaya a realizar el proyecto subvencionable en las provincias de León o Palencia .
	Proyectos subvencionables	Investigación industrial o de desarrollo experimental , individuales o realizados en colaboración, que estén incluidos dentro de los ámbitos de tecnologías fundamentales establecidos en el Reglamento STEP : tecnologías digitales, tecnologías limpias y eficientes en el uso de recursos y biotecnologías.

CONVOCATORIA I+D en Tecnologías Fundamentales II



Requisitos

- **Localización:** El proyecto debe realizarse en las provincias de León y/o Palencia.
- **Presupuesto subvencionable:**
 - Micropymes y pymes: Más de 20.000€ y menos de 1.000.000€
 - Grandes empresas: más de 200.000€ y menos de 2.000.000€
 - Proyectos en colaboración: entre 250.000 y 2.500.000€
- **Colaboración efectiva:** Deben participar varias empresas independientes de León y/o Palencia, con al menos una pyme. Ninguna empresa puede asumir más del 70 % de los costes subvencionables; debe existir acuerdo previo de colaboración y una empresa coordinadora. La subcontratación no cuenta como colaboración efectiva.



Procedimiento

- Las subvenciones se tramitarán en **régimen de concurrencia competitiva**.
- Tramitación electrónica en Sede electrónica | Sede Electrónica | Junta de Castilla y León
- BBRR y Convocatoria

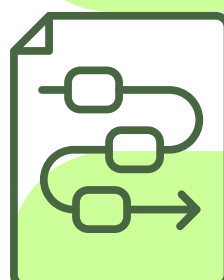
	Plazo	Del 19/05/2026 al 23/11/2026
	Cuantía	11.000.000 € (Subvención a fondo perdido del 60 % de los gastos elegibles.)
	Quién puede solicitarla	Empresas, personas físicas o jurídicas, industriales o de servicios vinculados al producto-proceso industrial. Centro de actividad en Euskadi , donde se ejecute y tenga impacto el proyecto, y estar dadas de alta en el IAE vasco.
	Proyectos subvencionables	Iniciativas que mejoren la protección, la ciberseguridad y la resiliencia operativa de la empresa o de sus productos: ◦ Diagnósticos, auditorías y planes de ciberseguridad. ◦ Gestión de riesgos, cumplimiento normativo y protección de redes, accesos y sistemas. ◦ Monitorización, detección de amenazas y respuesta ante incidentes. ◦ Copias de seguridad, continuidad de negocio y recuperación ante desastres. ◦ Certificaciones y desarrollo de productos seguros desde el diseño.

CIBERSEGURIDAD INDUSTRIAL 2026 II



Requisitos

- **Empresa elegible:** Empresas industriales o de servicios vinculados al producto-proceso industrial, dadas de alta en el IAE vasco.
- **Límite de ayudas:** No se pueden superar los **300.000 €** en ayudas de minimis durante los tres últimos años.
- **Proyecto no finalizado:** No puede estar completamente ejecutado antes de presentar la solicitud y debe finalizar en un máximo de 12 meses.
- **Colaboración efectiva:** Participación de varias empresas independientes de León y/o Palencia, con al menos una pyme. Ninguna empresa puede asumir más del 70 % de los costes subvencionables; debe existir acuerdo previo de colaboración y una empresa coordinadora. La subcontratación no cuenta como colaboración efectiva.
- **Proveedor especializado:** Los trabajos deben realizarse con proveedores externos expertos en ciberseguridad. La consultoría o ingeniería debe representar, en general, al menos el 20 % del presupuesto subvencionable.

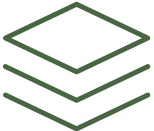


Procedimiento

- Tramitación electrónica en <https://www.spri.eus/es/>
- BBRR y Convocatoria

INNOVACIÓN, AYUDAS Y FINANCIACIÓN DISPONIBLES

BLOQUE II.3.2: Convocatorias Europeas

	Convocatoria Principal	HORIZON-CL3-2026-02-CS-ECCC Ciberseguridad y privacidad digital
	Plazo	Apertura: 03 marzo de 2026 - Cierre: 15 septiembre de 2026
	Participación PYMES	Socias tecnológicas de consorcios europeos, aportando soluciones, pilotos o casos de uso.
	Beneficiarios	Consortios de al menos 3 entidades de 3 países Horizonte Europa. Pueden incluir empresas, centros de investigación, universidades y organismos públicos.
	Ámbitos de Oportunidad	Proyectos europeos de I+D e innovación para desarrollar soluciones avanzadas en ciberseguridad: ○ Ciberseguridad en software, hardware e IoT. ○ IA, criptografía y protección de datos. ○ Resiliencia de infraestructuras y servicios críticos. ○ Tecnologías de detección, respuesta y validación

PROGRAMA HORIZON EUROPE II: Convocatorias

Enhancing the Security, Privacy and Robustness of AI Models and Systems (SecureAI)

Presupuesto: 21.200.000 €

Actuaciones subvencionables:

- Desarrollo de modelos de IA seguros y resilientes.
- Protección frente a ataques y amenazas avanzadas.
- Detección y mitigación de incidentes en tiempo real.
- Adaptación a la Ley de IA de la UE.

Approaches and tools for security in software and hardware development and assessment

Presupuesto: 20.000.000 €

Actuaciones subvencionables:

- Marcos de seguridad para cadenas de suministro de software y hardware
- Arquitecturas de chips seguras; integración de security-by-design
- Metodologías de prueba (verificación formal, IA)
- Evaluación y certificación de seguridad de hardware.

Advanced cryptographic schemes and High-Assurance high-speed cryptographic implementations

Presupuesto: 15.000.000 €

Actuaciones subvencionables:

- Criptografía post-cuántica
- Algoritmos criptográficos.
- Aceleración hardware
- Arquitecturas resistentes
- Soluciones criptográficas de alto rendimiento para sectores estratégicos

EUROPEAN DIGITAL PROGRAMME (EDP) I: Convocatorias Abiertas

Digital Skills and Jobs Platform: The National Coalitions for Digital Skills and Jobs



Plazo

Hasta el 01/10/2026



Cuantía

2.000.000 €



Quién puede solicitarla

Consorcio - mínimo de 5 solicitantes independientes (beneficiarios; no entidades afiliadas) de al menos 4 países elegibles diferentes.



Actuaciones subvencionables

Actividad 1: desarrollo web.
Actividad 2: servicios, contenido y actividades relacionadas con la comunidad.
Actividad 3: posesición y localización de contenido.

EUROPEAN DIGITAL PROGRAMME (EDP) II: Próximas Convocatorias

Cybersecure tools, technologies and services relying on AI

	Plazo	Del 01/04/2027 al 01/10/2027.
	Cuantía	15.000.000 €
	Quién puede solicitarla	Pymes, entidades públicas y privadas que implementan la Directiva NIS 2, la Ley de Resiliencia Cibernética, la investigación y el ámbito académico, etc.
	Actuaciones subvencionables	El desarrollo de un conjunto de herramientas cibernéticas como servicio para ayudar a las pymes a gestionar los riesgos cibernéticos, definir e implementar su estrategia de ciberseguridad.

EUROPEAN DIGITAL PROGRAMME (EDP) II: Próximas Convocatorias

Migration of Cyber Hubs to PQC

	Plazo	Del 01/04/2027 al 01/10/2027.
	Cuantía	4.000.000 €
	Quién puede solicitarla	Centros de Ciberseguridad, autoridades competentes, proveedores de soluciones y servicios de control de calidad de la información, y demás partes interesadas relevantes (públicas o privadas).
	Actuaciones subvencionables	- Estrategias para implementar las acciones previstas en los borradores de la Hoja de Ruta de Implementación Coordinada para la transición a PQC. - Implementación de soluciones criptográficas ágiles e híbridas. - Validación de sistemas PQC y coordinación con entidades encargadas de las actividades de certificación.

Para más información acerca de RED ARGOS:



info@redargos.com



<https://redargos.com/>