Iniciativa RETECH para el impulso de redes territoriales de especialización tecnológica

8 de mayo de 2024

RED DE NODOS DE CIBERSEGURIDAD

RED ARGOS
Red de Nodos de Ciberseguridad

PLANTEAMIENTO ALINEADO CON

- Estrategia Europea de Ciberseguridad – EU´s Cybersecurity Strategy for the Digital Decade
- Estrategia Nacional de Ciberseguridad y las primeras conclusiones de los grupos de trabajo del Foro Nacional de Ciberseguridad.
- Plan de Recuperación, Transformación y Resiliencia
- España Digital 2026

OBJETIVO GLOBAL

El objetivo principal de la propuesta es **impulsar y fortalecer el ecosistema nacional de ciberseguridad a través del trabajo en Red de Nodos de Ciberseguridad regionales coordinados** (Castilla y León, País Vasco y Andalucía) y de la **generación de capacidades** especializadas en ámbitos estratégicos (movilidad, aeroespacial, energía, industria inteligente, salud y smartcities)

Esta red se construirá sobre la base de la **cooperación interregional, con una visión de liderazgo internacional,** apoyándose en las fortalezas de cada comunidad autónoma y haciendo que gracias a la colaboración y la complementariedad de las acciones, se desarrolle conocimiento conjunto, se compartan estrategias de éxito y en definitiva **se optimice el impacto en las pymes y se consiga un mayor efecto tractor de la ciberseguridad como oportunidad económica, profesional y empresarial.**

Objetivos estratégicos

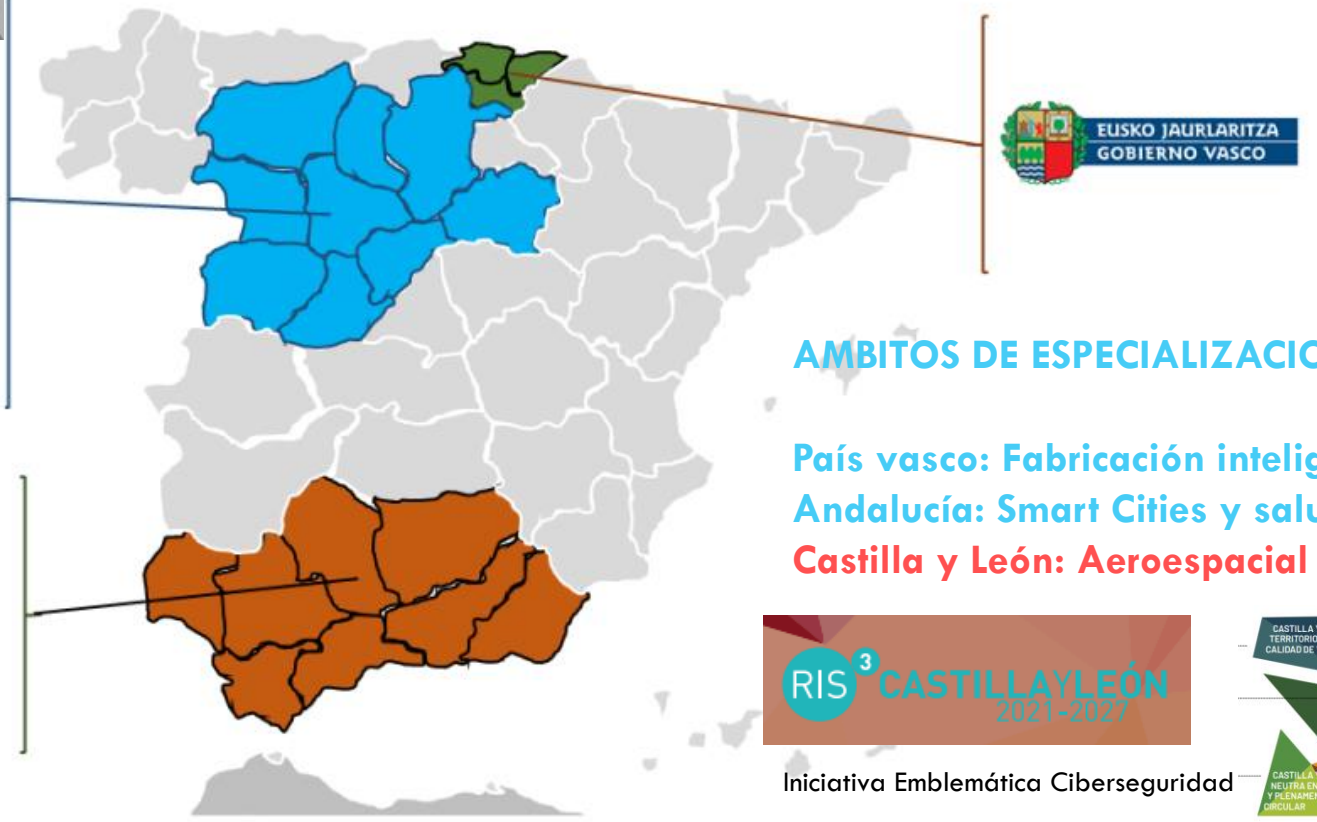
- Fortalecer la industria de ciberseguridad nacional
- Mejorar la permeabilidad de la ciberseguridad a todos los sectores económicos
- Promover, hacer crecer y consolidar la colaboración interregional a través de la red de nodos

Objetivos operativos

- Mejora de las capacidades: infraestructura, equipamiento y recursos
- Incrementar la adopción global de medidas de ciberseguridad, desde el diseño y en el resto de etapas. Desarrollo de nuevas soluciones
- Atraer y generar talento: capacitación en ciberseguridad, tanto a nivel de oferta como de demanda
- Impulsar la aceleración de empresas y el emprendimiento en ciberseguridad
- Potenciar, conectar y alinear el ecosistema nacional en materia de ciberseguridad con el fin de obtener un liderazgo internacional (visibilización y posicionamiento)
- Desplegar, explotar, posicionar una red de nodos especializados en ciberseguridad.

SOCIOS

- DEPARTAMENTO DE DESARROLLO ECONÓMICO, SOSTENIBLE Y MEDIO AMBIENTE. GRUPO SPRI. GOBIERNO VASCO
- AGENCIA DIGITAL DE ANDALUCÍA -JUNTA DE ANDALUCÍA
- INSTITUTO DE COMPETITIVIDAD EMPRESARIAL DE CASTILLA Y LEÓN



AMBITOS DE ESPECIALIZACION

País vasco: Fabricación inteligente y energía
Andalucía: Smart Cities y salud
Castilla y León: Aeroespacial y Movilidad

Iniciativa Emblemática Ciberseguridad

CONEXIÓN ENTRE 3 REGIONES EN DIFERENTE SITUACIÓN DE DESARROLLO PERO CON APUESTA CLARA POR LA CIBERSEGURIDAD

COOPERACIÓN INTERREGIONAL COMO ELEMENTO CLAVE

PRESUPUESTO Y DURACIÓN

ENTIDADES PARTICIPANTES	Presupuesto TOTAL	Presupuesto SOLICITADO	%	APORTACIÓN PROPIA	%
ICE Junta de Castilla y león	14.300.000	10.725.000	75	3.575.000	25
Gobierno Vasco	14.000.000	10.500.000	75	3.500.000	25
Junta de Andalucía	14.050.000	10.537.500	75	3.512.500	25
TOTAL	**42.350.000**	**31.762.500**	**75**	**10.587.500**	**25**

EL PROYECTO SE DESARROLLARÁ DESDE LA FIRMA DEL CONVENIO 30 NOVIEMBRE DE 2023 HASTA JUNIO 2026

ALINEAMIENTO CON PLAN DE RECUPERACIÓN

- **COMPONENTE 15. I7 (Contribución a Hitos 246 y 248)**
  - Incremento sustancial de las capacidades de ciberseguridad a través de polos de especialización
  - Fomento del desarrollo de ecosistemas
  - Mejora del liderazgo internacional en el campo de ciberseguridad

ACTUACIONES ICECYL – CASTILLA Y LEÓN

Línea de actuación 1 (WP1): Creación y fomento de una Red de Centros de excelencia en ciberseguridad y su oferta de servicios especializados por ámbitos estratégicos

1.1. Servicios de los Centros de Excelencia Regionales en Ciberseguridad	Diseño funcional y desarrollo de los Centros de Excelencia (laboratorios, centros demostrativos, herramientas de desarrollo, infraestructuras de testeo y pruebas) que permitan afrontar las necesidades prioritarias actuales del ecosistema de ciberseguridad en movilidad y aeroespacial.
1.2. Nodos de formación y generación de conocimiento experto en ciberseguridad	Construcción de un nodo de formación especializada de alto nivel, en los ámbitos de ciberseguridad aeroespacial y de movilidad. Se diseñará a través de acuerdos con los centros educativos y tecnológicos junto con los actores más relevantes del ecosistema. Esta formación estará directamente relacionada con las líneas de trabajo estratégicas de los Centros de excelencia creados y los retos identificados por los sectores.
1.3. Dinamización de los nodos de Ciberseguridad en innovación abierta	Diseño de una línea de ayudas para realizar proyectos individuales o colaborativos I+D+i basados en ámbitos ciberseguridad y /o retos estratégicos específicos en ciberseguridad en Movilidad y Aeroespacial. Para ello se identificarán los casos de uso en los sectores de referencia, pudiendo priorizar los que usan las instalaciones creadas. El objetivo último es incrementar y potenciar el desarrollo de productos y servicios de ciberseguridad en el ámbito aeroespacial y de movilidad.

ACTUACIONES ICECYL – CASTILLA Y LEÓN

Línea de actuación 2 (WP2): Programa transversal de impulso a la Ciberseguridad donde cada CCAA, en función de su **tejido empresarial y su Estrategia de Especialización Inteligente**, pueda fortalecer el desarrollo y adopción de tecnologías de ciberseguridad en las empresas con un enfoque multiacción

2.1. Estrategias en captación, generación y atracción de talento	Desarrollo, diseño y ejecución de un programa de capacitación en ciberseguridad que garanticen la empleabilidad como palanca de retención de talento. Se define como un programa escalable en varios módulos que dé respuesta a las necesidades particulares de las empresas de la oferta y demanda.
2.2. Desarrollo de proyectos individuales/ colaborativos de Ciberseguridad	Línea de ayuda para el fortalecimiento de las capacidades empresariales en materia de ciberseguridad, así como para su protección contra amenazas y riesgos relacionados con la seguridad digital, incentivando la contratación de servicios de auditorías, demostradores “on premise” asesoramiento y asistencia técnica, implantación de soluciones y/o las inversiones en hardware y software en esta materia .

ACTUACIONES ICECYL – CASTILLA Y LEÓN

Línea de actuación 3 (WP3): Servicios de emprendimiento y aceleración en base a la especialización, apoyados en los Centros de excelencia y con componente internacional

3.1. Generación de servicios específicos - Aceleración de mercado	Generar servicios específicos ligados a la Aceleración de mercado: estudios de factibilidad, mentoring especializado, capacitación, certificación, generación de prototipos.
3.2. Fomento de la iniciativa emprendedora y llegada a mercado	Poner a disposición de los emprendedores en ciberseguridad, la verticalización de la aceleradora regional Wollaria , que ayuda en la aceleración estratégica mediante servicios especializados de aceleración: formación, coaching, management, networking, talento y financiación.
3.3. Programa de internacionalización y transferencia tecnológica	Visibilización y posicionamiento internacional, a través de redes europeas, eventos, programas, y centros de competencia complementarios. Presencia Agrupada en foros.

ACTUACIONES ICECYL – CASTILLA Y LEÓN

Línea de actuación 4 (WP4): Acciones transversales interregionales para el desarrollo del ecosistema empresarial y el potenciamiento del liderazgo nacional del sector de la ciberseguridad, esta línea pretende consolidar el funcionamiento de la Red de Nodos y la colaboración con territorios y ámbitos estratégicos como referente del sector de la ciberseguridad, tanto a nivel nacional como internacional

4.1. Mapeo de recursos y capacidades de centros de conocimiento en Ciberseguridad	Mapeo de recursos y capacidades de centros de conocimiento en materia de Ciberseguridad.
4.2. Acciones conjuntas e intercambio de conocimiento y buenas prácticas	Desarrollo de acciones conjuntas y el intercambio de conocimiento y buenas prácticas a través de grupos de trabajo especializados, por cada línea de actuación..
4.3. Sensibilización y difusión de la cultura de la ciberseguridad	Sensibilización y difusión de la cultura de la ciberseguridad.

Línea de actuación 5 (WP5): Información, comunicación y difusión del proyecto

SITUACIÓN ACTUAL

- **FIRMA DEL CONVENIO DE EJECUCIÓN: 30 NOVIEMBRE DE 2023**
- **APROBACIÓN DE PLAN OPERATIVO ANUAL: 20 DE FEBRERO DE 2024- Firmado Abril de 2024**
- **EN FASE DE EVALUACION ADENDA PARA INCLUIR LINEAS DE AYUDAS CON FONDOS PRTR (en progreso)**
- **DESPLIEGUE INICIAL DE ACTUACIONES EN 2024. INSTRUMENTOS PRINCIPALES: Líneas de ayuda y Licitaciones**
- **PRIMERAS ACTUACIONES A ACOMETER SEGÚN PLAN ANUAL OPERATIVO PROPUESTO**
  - **1.1 Centros de Excelencia Regional en Ciberseguridad aplicada a movilidad**

    Procedimiento de Compra Pública de Innovación

    Consulta preliminar al mercado (CPM) para la identificación de propuestas innovadoras que den respuesta a las necesidades relativas a un centro de excelencia de ciberseguridad aplicada a movilidad conectada en Castilla y León.

    CPM CIBERMOV RETECH ARGOS publicada el 31/01/2024 y cerrada el 22/02/2024 23:59.
  - **2.1. Estrategias en captación, generación y atracción de talento** (Ver detalle en siguientes slides)
  - **2.2. Línea de ayudas: Ciberseguridad aplicada a procesos, productos y servicios digitales para asegurar que la ciberseguridad llega a todos los sectores económicos** (Ver detalle en siguientes slides)
  - **3.2. Fomento de la iniciativa emprendedora y llegada a mercado.**

    Verticalización de la aceleradora regional Wollaria
  - **4. Acciones transversales**

    Sensibilización y difusión, mapeo capacidades, posicionamiento nacional e internacional,
- **5. Lanzado contrato Plan de comunicación y web**

2.1. PROGRAMA DE CAPACITACIÓN EN CIBERSEGURIDAD

Diseño y ejecución de un programa de capacitación en ciberseguridad:

- Con varios módulos adaptados a las necesidades reales de las empresas regionales
- Siguiendo perfiles de ciberseguridad ENISA y Foro Nacional Ciberseguridad
- Orientación a estudiantes y profesionales con conocimientos mínimos en el área
- 200 horas, formato mixto (no en empresa)
- Objetivo: media de 150 alumnos formados, mínimo 100 y objetivo 200

Tabla 3. Perfiles de ciberseguridad del ECSF Framework

Trabajo a desarrollar:

- Definición del Programa
- Identificación de necesidades de las empresas regionales
- Definición de los perfiles más demandados en base a las necesidades de las empresas (modular
- Captación, selección e inscripción
- Ejecución del plan formativo
- Sistema virtual de matching de perfiles activos- en evaluación sistemas actuales
- Acompañamiento y Evaluación
- Encuentro Final y Conexión del Talento

2.2. LÍNEA DE AYUDAS: CIBERSEGURIDAD APLICADA A PROCESOS, PRODUCTOS Y SERVICIOS DIGITALES

2 tipos de proyectos; Tipo A: Procesos - Tipo B: Productos y servicios de ciberseguridad

PROYECTOS TIPO A: Ciberseguridad aplicada a procesos de empresas con centro de trabajo en CYL (excluido sector TIC): Individuales o colaborativos (soluciones para cadena de valor o varias empresas con las mismas necesidades)

Gastos elegibles:

- 1 Inversión material en hardware y los equipos necesarios para la implementación de las acciones objeto del proyecto de ciberseguriddad
- 2 Inversión inmaterial en software de ciberseguridad
- 3 Colaboraciones externas necesarias para la realización de uno o varios de los siguientes conceptos:
  - Auditorías externas que evalúen la situación de seguridad de la empresa: hacking ético, auditorias anuales de seguridad, de seguimiento…
  - Consultoría para diseñar políticas de ciberseguridad y Procedimientos de gestión de incidentes
  - Consultoría para la implantación de las medidas y acciones necesarias para mejorar la ciberseguridad en la empresa y sus procesos
  - Preparación para de Certificaciones/Sellos de Seguridad
  - Obtención de Certificaciones de ciberseguridad
  - Suministro de servicios en la nube (XaaS) relacionados con ciberseguridad
  - Consultoría Especializada para el Desarrollo de Soluciones de ciberseguridad a Medida (innovación)
  - Consultoría Especializada para Integración de Tecnologías Emergentes y adaptación de proyectos de ciberseguridad (IA
  - Consultoría para concienciación, sensibilización, Formación y Capacitación
  - Consultoría para testeo, experimentación validación de las potenciales herramientas/soluciones en ciberseguridad
  - Consultoría para implantar y/o adaptar Sistemas de Monitorización para ciberseguridad
  - Consultoría para Gestión de Identidades y Accesos
  - Consultoría técnica proporcionada por asociaciones empresariales
  - Y cualquier otra consultoría necesaria para implementar la ciberseguridad de la empresa
- 4 Gastos para la tramitación de ayudas para la financiación- regional

- Régimen de minimis y porcentaje de subvención superior al 50%

2.2. LÍNEA DE AYUDAS: CIBERSEGURIDAD APLICADA A PROCESOS, PRODUCTOS Y SERVICIOS DIGITALES

PROYECTOS TIPO B: Ciberseguridad aplicada a productos y servicios de empresas con centro de trabajo en CYL (incluido sector TIC): Individuales o colaborativos (soluciones para cadena de valor o varias empresas con las mismas necesidades)

Gastos elegibles:

- 1 Inversión material en hardware y los equipos necesarios para la implementación de la solución o soluciones objeto del proyecto
- 2 Inversión inmaterial en software de seguridad
- 3 Gastos de personal para la realización de uno o varios de los siguientes conceptos de innovación
    - Evaluación de Riesgos desde el Diseño
    - Herramientas y Plataformas de Desarrollo Seguro
    - Seguridad en la Arquitectura
    - Pruebas de Seguridad Integradas
    - Diseño Centrado en la Privacidad
    - Primera Validación de productos/servicios en cliente: producto en TRL altos, que puedan validar y adecuar a mercado - Innovacion:
    - Preparación y adecuación NIS2
    - Preparación y adecuación CRA
    - Preparación, adecuación y obtención de sellos/reconocimiento para cualquier de los Estándares y normativa de ciberseguridad
- 4 Colaboraciones externas necesarios

    - Régimen de minimis y porcentaje de subvención superior al 50%

IMPACTO CYL

Línea de actuación 1 (WP1): Creación y fomento de una Red de Centros de excelencia en ciberseguridad y su oferta de servicios especializados por ámbitos estratégicos	1.1: Diseño funcional y operativo de los Servicios de los Centros de Excelencia Regionales en Ciberseguridad, así como de la operativa de transferencia de buenas prácticas e iniciativas.	2 Labs, 4 casos de uso/servicios 10 agentes activos por cada ámbito
	1.2: Construcción y fomento de nodos de formación y generación de conocimiento experto en ciberseguridad en las áreas de Especialización Territorial foco en la competitividad de la oferta.	60 profesionales
	1.3: Dinamización de los nodos de Ciberseguridad en innovación abierta	15 casos de uso/productos/servicios
Línea de actuación 2 (WP2): Programa transversal de impulso a la Ciberseguridad donde cada CCAA, en función de su **tejido empresarial y su Estrategia de Especialización Inteligente**	2.1: Desarrollo, diseño y ejecución de estrategias en captación, generación y atracción de talento.	50 entidades receptoras: entre 1-10 alumnos y 200 alumnos formados con acceso a empleabilidad
	2.2: Apoyo para el desarrollo de proyectos individuales/colaborativos de Ciberseguridad en cada ámbito de especialización.	120 beneficiarios
Línea de actuación 3 (WP3): Servicios de emprendimiento y aceleración en base a la especialización,	3.1: Generación de servicios específicos ligados a la Aceleración de mercado.	15 empresas
	3.2: Fomento de la iniciativa emprendedora y llegada a mercado.	15 emprendedres
	3.3: Programa de internacionalización y transferencia tecnológica	3 beneficiairios
Línea de actuación 4 (WP4): Acciones transversales interregionales para el desarrollo del ecosistema empresarial y el potenciamiento del liderazgo Nacional del sector de la ciberseguridad	4.1: Mapeo de recursos y capacidades de centros de conocimiento en materia de Ciberseguridad.	1 con taxonimia común
	4.2: Desarrollo de acciones conjuntas y el intercambio de conocimiento y buenas prácticas a través de grupos de trabajo especializados, por cada línea de actuación.	10 acciones conjuntas
	4.3: Sensibilización y difusión de la cultura de la ciberseguridad	10.000 empresas /profesionales sensibilizados

GRACIAS

@empresasjcyl.es

RETECH CIBERSEGURIDAD

INSTITUTO PARA LA COMPETITIVIDAD EMPRESARIAL DE CASTILLA Y LEÓN