PRESUPUESTO DE LA CONVOCATORIA	FECHA PRESENTACIÓN SOLICITUDES
3.500.000 €	Desde 25/02/2022 hasta las 15:00h del 14/11/2022
PERIODO FINANCIABLE	**TIPO DE AYUDA**
12 meses (a partir de presentación de la solicitud) (o partir del 01/01/2022 si la solicitud se hace antes del 23/04/2022)	Subvención

OBJETIVO

Impulsar la Ciberseguridad Industrial, especialmente proyectos que aborden la convergencia e integración de los sistemas de protección ante ciberataques para entornos IT/OT (Information Technology/Operational Technology).

BENEFICIARIOS Y CONDICIONES

Empresas industriales y de servicios conexos ligados al producto-proceso industrial, así como las empresas matrices de los grupos industriales y de servicios conexos ligados al producto-proceso industrial ubicados en la Comunidad Autónoma del País Vasco. Las entidades beneficiarias deberán cumplir:

- Disponer de un centro de actividad industrial y realizar la actuación subvencionable en la CAPV.
- Acreditar estar de alta en el correspondiente epígrafe industrial del I.A.E. del País Vasco.

CARACTERÍSTICAS DE LA FINANCIACIÓN

Los gastos de Hardware y Software no podrán ser superiores al 80% del presupuesto máximo aceptado, siendo por tanto obligatorio dedicar al menos un 20% del presupuesto a los gastos de Consultoría y/o Ingeniería.

Modalidad y cuantía de las ayudas:

- 50 % subvención sobre el presupuesto máximo aceptado para el proyecto por cada uno de los conceptos financiables.
- Aquellas empresas que presenten el Certificado de Calidad en la Gestión Lingüística Bikain, un plan de igualdad (empresas de 50 personas o menos de plantilla) o que se trate de proyectos que implementen el uso de Software en Euskera obtendrán una subvención adicional del 5%.
- La subvención máxima anual por empresa será de 18.000 euros para la realización de una o más actuaciones subvencionables.

CONCEPTOS FINANCIABLES

Tendrán la consideración de **actuaciones subvencionables** los proyectos relacionados con la Ciberseguridad Industrial:

- Convergencia e integración de los sistemas de protección ante ciberataques para entornos IT/OT**.** Diseño y ejecución de arquitecturas seguras y en su caso materialización de la segmentación de redes industriales.
- Securización de los accesos remotos OT a los equipos industriales de la planta productiva requeridos para el mantenimiento de equipo, control y operación de los mismos, tareas realizadas cada vez con más frecuencia de manera remota.

- Securización de la información/datos industriales. Auditorías y simulaciones de ataques por personas externas a la organización y auditorias sobre perfiles internos con diferentes niveles de accesos a datos de la compañía.
- Evaluación de la ciberseguridad del software industrial en las plantas productivas y mejora del mismo.
- Iniciativas para la concienciación de la plantilla de la empresa industrial en el ámbito de ciberseguridad.
- Diagnóstico de situación actual de la industria en materia de ciberseguridad industrial y elaboración de su plan de acción para la mejora de la Ciberseguridad. Análisis de riesgo industrial y de vulnerabilidad industrial. Inventario de los diferentes elementos en un sistema crítico industrial. Realización de un test de intrusión industrial. Análisis de vulnerabilidades en aplicaciones web. Auditorias de las comunicaciones inalámbricas industriales.
- Adopción de buenas prácticas recogidas en estándares de Ciberseguridad industrial u otros estándares de gestión de la Ciberseguridad ampliamente reconocidos. Adaptación al cumplimiento del Esquema Nacional de Seguridad, Reglamento PIC. Mejora continua del proceso de gestión de ciberseguridad mediante el despliegue de medidas específicas o evolución de las mismas a niveles de madurez superiores a los preexistentes.
- Medidas de protección de información estratégica o sensible como puedan ser la propiedad intelectual, estrategias de I+D+i, planos de edificios o de diseño de productos, información afectada por el RGPD o cualquiera otra directamente relacionada con la competitividad y sostenibilidad del negocio.
- Monitorización de dispositivos de seguridad perimetral y de otros dispositivos industriales.
- Otros proyectos que incrementen de manera significativa el nivel de ciberseguridad de las empresas industriales y reduzcan el riesgo y la vulnerabilidad.

Tendrán la consideración **de gastos y/o inversiones elegibles** los de consultoría, ingeniería, hardware y software y que cumplan los siguientes requisitos:

- Devengados o facturados a partir de la presentación de la solicitud de ayuda en SPRI y durante el plazo establecido para la ejecución del proyecto.
- Realizados por empresas expertas externas que cumplan las siguientes condiciones:
  - No tener la consideración de Sociedades Públicas, Entidades de Derecho Público, Asociaciones o Colegios Profesionales ni formar parte de la RVCTI.
  - No tener vinculación directa o indirectamente con la solicitante de la ayuda.

OTRAS CONSIDERACIONES

- Ayuda en régimen de evaluación individualizada conforme al orden de presentación de las solicitudes.
- Ayudas compatibles con cualesquiera otras asignadas para el mismo objeto.
- Ayuda sujeta a régimen de minimis.