CONVOCATORIA: **CIBERSEGURIDAD EMPRESARIAL 2024 –**

SPRI - AGENCIA VASCA DE DESARROLLO EMPRESARIAL

PRESUPUESTO DE LA CONVOCATORIA	FECHA PRESENTACIÓN SOLICITUDES
3.500.000 euros	Desde 03/05/2024 hasta el 08/11/2024
PERIODO FINANCIABLE	**TIPO DE AYUDA**
12 meses (a partir de presentación de la solicitud) (o partir del 01/01/2024 si la solicitud se hace antes del 31/07/2023)	Subvención

OBJETIVO

El objeto del Programa es impulsar aquellos proyectos que contribuyan a incrementar el nivel de ciberseguridad de las empresas de manera significativa.

BENEFICIARIOS Y CONDICIONES

Empresas ubicadas en la Comunidad Autónoma del País Vasco, siempre que:

- Dispongan de un centro de actividad en la Comunidad Autónoma de Euskadi, centro en el que el proyecto presentado deberá tener impacto y en el que se realizará la actividad subvencionable.
- Figuren de alta en el Impuesto de Actividades económicas del País Vasco

CARACTERÍSTICAS DE LA FINANCIACIÓN

Tendrán la consideración de actuaciones subvencionables los proyectos relacionados con la ciberseguridad empresarial en empresas en las siguientes áreas:

a) Convergencia e integración de los sistemas de protección ante ciberataques para entornos IT/OT (Information Technology / Operational Technology). Diseño y ejecución de arquitecturas seguras y en su caso materialización de la segmentación de redes empresariales.
b) Securización de los accesos remotos OT a los equipos de las plantas productivas requeridos para el mantenimiento de equipos, controles y operaciones de los mismos, tareas realizadas cada vez con más frecuencia de manera remota.
c) Securización de la información/datos. 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.
d) Evaluación de la ciberseguridad de dispositivos electrónicos, así como su certificación.
e) Iniciativas para la concienciación y/o capacitación de la plantilla de la empresa en el ámbito de ciberseguridad.
f) Diagnóstico de situación actual de la industria en materia de ciberseguridad y elaboración de su plan de acción para la mejora de la ciberseguridad. Análisis de riesgo y de vulnerabilidad. Inventario de los diferentes elementos en un sistema crítico. Realización de un test de intrusión. Análisis de vulnerabilidades en aplicaciones web. Auditorias de las comunicaciones inalámbricas 7.– Replicación de CPDs dirigidos a la adopción de políticas de ciberseguridad relacionadas con Planes de Disaster Recovery o de contingencia, así como a escenarios de alta disponibilidad dirigidos a garantizar la continuidad de negocio en cualquier empresa.
g) Adopción de buenas prácticas y procesos de certificación relativos a la obtención y cumplimiento de diversos estándares de ciberseguridad (por ejemplo: IEC 62443, TISAX, UNECE/R155 o

equivalentes) u otros estándares de gestión de la ciberseguridad (por ejemplo: ISO 27001, CAB o equivalentes) ampliamente reconocidos, así como reglamento o leyes en vigor de obligado cumplimiento. Adaptación al cumplimiento del Esquema Nacional de Seguridad (Real Decreto 3/2010), Reglamento PIC (Real Decreto 704/2011). 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.

h) 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 (ejemplo de medidas: cifrado del almacenamiento, control de acceso, control de distribución de copias, borrado seguro, etc.)

i) Monitorización de dispositivos de seguridad perimetral y de otros dispositivos (Switches, sondas, Appliances, firewalls, PLCs, EDRs, etc.).

j) Otros proyectos que incrementen de manera significativa el nivel de ciberseguridad de las empresas y reduzcan el riesgo y la vulnerabilidad ante los diferentes tipos de ataques existentes

CONCEPTOS FINANCIABLES

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.
- **Es obligatorio cumplir con la Ley 18/2022, de 28 de septiembre, de creación y crecimiento de empresas, que, entre otras, modifica en su artículo 11 la Ley 38/2003, de 17 de noviembre, General de Subvenciones, de forma que una empresa no podrá ser beneficiaria de una ayuda superior a 30.000 €, si no cumple los plazos de pago estipulados en la Ley 3/2004 de lucha contra la morosidad (60 días).**
- **La ficha es meramente informativa y, por tanto, no recoge la información completa. Es imprescindible remitirse a la normativa reguladora.**