Telf. 943 316430
itec@itecconsultoria.com
Web: www.itecconsultoria.com

Programa CIBERSEGURIDAD EMPRESARIAL 2026

Plazos:	**Presentación de solicitudes:** Desde **19/05/2026** hasta **el 23/11/2026 a las 23:59 horas.** **Desarrollo del proyecto:** Proyectos desarrollados a partir del 1 de enero de 2026 con un plazo de ejecución del proyecto, que no podrá superar el de 12 meses.
Objeto:	Impulsar acciones que contribuyan a **incrementar** de manera significativa **la protección, la ciberseguridad y la resiliencia operativa de las empresas de la CAE** y de sus **productos,** promoviendo la **mejora de sus sistemas de gestión** de ciberseguridad.
Entidades Beneficiarias:	**Empresas industriales o de servicios conexos** ligados al producto-proceso industrial, ubicadas en la CAPV 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. Y que figuren de alta en el Impuesto de Actividades Económicas del País Vasco.
Hecho subvencionable:	Los proyectos deberán encuadrarse en alguna de las fases relacionadas con los procesos habituales de adecuación y certificación a normativas o estándares en ciberseguridad que se detallan a continuación: **1. Ciberseguridad en la empresa:** ○ *Diagnóstico inicial*: ▪ Evaluación de controles y políticas existentes ▪ **Auditorías de Ciberseguridad** de empresas o producto. ▪ **Medición del nivel** de capacitación y concienciación de la plantilla. ▪ Otros proyectos para **analizar la situación actua**l de la empresa en ciberseguridad ○ *Estrategia y Planes de Acción*: ▪ PDS – Planes de Acción ▪ Desarrollo de planes de acción para la mejora de la ciberseguridad ▪ Otros proyectos para **definir y desarrollar la estrategia en ciberseguridad** ○ *Implementación de soluciones y medidas*: ▪ ***Identificar*:** Generación y mantenimiento de un inventariado de activos; Definición de políticas y procedimientos; Evaluación de amenazas y riesgos; Evaluación de cumplimiento normativo y otros. ▪ ***Gobernar*:** Definición y aprobación de una política global de ciberseguridad alineada con los riesgos y objetivos del negocio; Elaboración e implantación de un procedimiento de gestión de crisis; Estrategia para el cumplimiento normativo, así como herramientas para su seguimiento (GRC); Otros proyectos dirigidos a garantizar el gobierno de la ciberseguridad en las empresas. ▪ ***Proteger*:** Securización de los accesos remotos OT, control de accesos IT y gestión de identidades; Iniciativas de concienciación y capacitación en ciberseguridad; Segmentación de redes y arquitecturas seguras; Implantación de herramientas y tecnologías de protección (Firewalls, IDS/IPS, EDR, XDR, MDM, ZTNA, VPN, SASE, WAF, CASB, y equivalentes); Gestión vulnerabilidades y realización de tests de penetración; Cifrado de datos (incluido PQC, Quantum, y equivalentes) y securización de la información y Otros proyectos que contribuyan a elevar el nivel de protección de las empresas. ▪ ***Detectar*:** Servicios de seguridad gestionados (MSSP); Contratación de servicio de SOC; Monitorización de dispositivos de seguridad; Otros proyectos dirigidos a integrar capacidades de detección en las empresas. ▪ ***Responder*:** Planes de Respuesta ante Incidentes (ICP) y Planes de Continuidad de Negocio (BCP) y Simulacros de incidentes de Ciberseguridad. ▪ ***Recuperar*:** Planes Disaster Recovery; Copias de Seguridad y BRS (Business Recovery Systems); Replicación de CPDs relacionados con Planes Disaster Recovery y Otros proyectos dirigidos a integrar capacidades de recuperación en las empresas. ○ *Evaluación, Auditoría y Certificación*: ▪ Proceso de evaluación y conformidad sobre marcos normativos orientados a la ciberseguridad. ▪ Procesos de auditoría sobre marcos normativos orientados a la ciberseguridad. ▪ Procesos de certificación sobre marcos normativos orientados a la ciberseguridad. ○ *Mejora continua*: ▪ **Procesos de revisión, renovación y/o adecuación** sobre marcos normativo orientados a la ciberseguridad **2. Ciberseguridad de Producto:** ○ **Implantación de un marco organizativo y de proceso** que asegure la ciberseguridad durante todo el ciclo de vida del producto. ○ **Proyectos de consultoría para ayudar en el diseño y desarrollo seguro de productos**. Integrar controles de seguridad desde el diseño, incluyendo análisis de amenazas, revisión de código y validación de arquitectura segura. ○ **Proyectos de Implementación de cifrado de datos** (incluido PQC, Quantum, y equivalentes) ○ en tránsito y reposo, autenticación mutua y gestión segura de claves. ○ **Implantación de soluciones dirigidas a la gestión activa de vulnerabilidades**. ○ **Evaluación y Certificación de Ciberseguridad del Producto**: pruebas de conformidad relativa a los productos. ○ Otros proyectos vinculados a la ciberseguridad de producto.

Telf. 943 316430
itec@itecconsultoria.com
Web: www.itecconsultoria.com

Gastos subvencionables:	○ Gastos de **consultoría, ingeniería, hardware y software.** ○ Para **proyectos** que contemplen la **implantación** de aplicaciones de gestión en formato **tipo SAAS**, también podrá ser considerado como gasto elegible el coste imputable a este tipo de servicio, durante un plazo máximo de 12 meses, siempre que cumplan con las condiciones indicadas en las bases.

Cuantía de las ayudas:	○ El tipo de ayuda será de **Subvención a fondo perdido**, sujeta a los principios de publicidad, concurrencia competitiva y mínimis. ○ El **Presupuesto máximo aceptado** del proyecto será la suma del presupuesto aceptado en Gastos de Consultoría y/o Ingeniería, más el presupuesto aceptado en Hardware y/o licencias de Software. ○ Los **gastos de consultoría y/o ingeniería** deberán representar **al menos el 20% de la base elegible** del proyecto. Esta obligación no se aplicará a los proyectos destinados a implementar productos o soluciones desarrolladas y proporcionadas por empresas que cuenten con el sello <<Cybersecurity Made in Europe>> de ECSO. ○ La **subvención máxima** será de **100.000€** para la realización **de una o más actuaciones elegibles/proyectos.** ○ La **intensidad de las ayudas será con carácter general del 60%**.

Requisitos específicos:	Las **empresas externas** expertas deben cumplir las siguientes condiciones: ○ No pertenecer o formar parte de alguno de los sectores públicos, conforme a las normas de clasificación institucional que resulten de aplicación.

Normativa:	RESOLUCIÓN de 27 de abril de 2026 (BOPV Nº 90) .