

Programa CIBERSEGURIDAD EMPRESARIAL 2025

Plazos:	Presentación de solicitudes: Desde 17/06/2025 hasta el 24/11/2025 a las 23:59 horas. Desarrollo del proyecto: Proyectos desarrollados a partir del 1 de enero de 2025 con un plazo de ejecución del proyecto, que no podrá superar el de 12 meses.
Objeto:	Impulsar acciones que contribuyan a incrementar el nivel de Ciberseguridad de las empresas de manera significativa.
Entidades Beneficiarias:	Empresas 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:	Tendrán la consideración de actuaciones subvencionables los proyectos relacionados con la ciberseguridad empresarial en empresas en las siguientes áreas: 1. 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. 2. Securitización 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. 3. Securitización de la información/datos. Auditorías y simulaciones de ataques por personas externas a la organización y auditorías sobre perfiles internos con diferentes niveles de accesos a datos de la compañía. 4. Evaluación de la ciberseguridad de dispositivos electrónicos, así como su certificación. 5. Iniciativas para la concienciación y/o capacitación de la plantilla de la empresa en el ámbito de ciberseguridad. 6. 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 industrial y de vulnerabilidad. Inventario de los diferentes elementos en un sistema crítico. Realización de un test de intrusión. Análisis de vulnerabilidades en aplicaciones web. Auditorías 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. 8. Adopción de buenas prácticas y procesos de certificación relativos a la obtención y cumplimiento de diversos estándares de Ciberseguridad (p.e.: IEC 62443, TISAX o equivalentes) u otros estándares de gestión de la Ciberseguridad (p.e.: 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), NIS2, DORA, CRA. 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. 9. 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.). 10. Monitorización de dispositivos de seguridad perimetral y de otros dispositivos (Switches, sondas, Appliances, firewalls industriales, PLCs, EDRs, etc.). 11. 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.
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.
Cuantía de las ayudas:	- El tipo de ayuda será de Subvención a fondo perdido, sujeta a los principios de publicidad, concurrencia competitiva y mínimos. - El Presupuesto global aceptado del proyecto será la suma del presupuesto aceptado en Gastos de Consultoría y/o Ingeniería, más el presupuesto aceptado en Hardware y/o Software (máximo 80%). - El Presupuesto total presentado por la entidad solicitante deberá necesariamente contemplar al menos un 20% para labores de Consultoría y/o Ingeniería. - En caso de destinarse un importe menor del 20 % del presupuesto total presentado a labores de Consultoría y/o Ingeniería, se realizará un ajuste en el resto de partidas (Hardware y Software), reduciendo el presupuesto total

	presentado, con el objetivo de que la partida para las labores de Consultoría y/o Ingeniería signifique al menos un 20 % del Presupuesto total presentado. ○ La subvención propuesta se incrementará en un 5 % adicional, sin superar el límite máximo de las ayudas, si la empresa cumple alguna de las siguientes condiciones: ▪ Disponer del Certificado de Calidad en la Gestión Lingüística Bikain como acreditación del uso, presencia y gestión del euskera en la empresa. ▪ Disponer de un Plan de Igualdad, únicamente en el caso de las empresas de 50 personas o menos de plantilla, dado que las de mayor tamaño están obligadas a tenerlo por ley. ▪ Que se trate de proyectos que implementen el uso de Software en Euskera dentro del marco de las actuaciones subvencionables de este programa. ○ La subvención máxima será de 23.000 euros por empresa/año. ○ La intensidad de las ayudas será con carácter general del 50%.
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, ni a Asociaciones o Colegios Profesionales ni formar parte de la RVCTI ni de Redes de I+D de naturaleza similar ○ No tener vinculación, vía acciones o participaciones, directa o indirectamente, con la solicitante de la ayuda.
Normativa:	RESOLUCIÓN de 29 de mayo de 2025 (BOPV Nº 112) .