CAV 20.24 PROGRAMA CIBERSEGURIDAD INDUSTRIAL 2020

21 de Abril de 2020
La SPRI ha hecho público el Programa Ciberseguridad Industrial 2020. El objetivo es 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) en empresas industriales.

Plazo presentación de solicitudes
Hasta el 27 de noviembre de 2020 o hasta el agotamiento de los recursos.

Beneficiarios
Pymes y grandes empresas

Actuaciones subvencionables
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 industriales.
2.– 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.
3.– 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.
4.– Evaluación de la ciberseguridad del software industrial en las plantas productivas y mejora del mismo.
5.– Iniciativas para la concienciación de la plantilla de la empresa industrial en el ámbito de ciberseguridad.
6.– Diagnóstico de situación actual de la industria manufacturera 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. Auditorías de las comunicaciones inalámbricas industriales.
7.– Adaptación a estándares de Ciberseguridad industrial (p.e. IEC 62443 o equivalentes). Gestión de la Ciberseguridad (p.e. ISO 27001 o equivalentes). Cumplimiento del Esquema Nacional de Seguridad, PIC, mejora continua del proceso de ciberseguridad y similares.
8.– 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 (cifrado del almacenamiento, control de acceso, control de distribución de copias, borrado seguro, etc.)
9.– Monitorización de dispositivos de seguridad perimetral y de otros dispositivos industriales (Switches, sondas, Appliances, firewalls industriales, PLCs, etc.).
10.– Otros proyectos que incrementen de manera significativa el nivel de ciberseguridad de las empresas industriales manufactureras y reduzcan el riesgo y la vulnerabilidad ante los diferentes tipos de ataques existentes.

Gastos elegibles
Consultoría, ingeniería,hardware y software y que cumplan los siguientes requisitos:
a) Devengados o facturados a partir de la presentación de la Solicitud de Ayuda en SPRI y durante los 12 meses siguientes a dicha fecha. Se admitirán gastos devengados o facturados antes de la presentación de la Solicitud de Ayuda de proyectos iniciados a partir del 1 de enero de 2020, siempre que estas solicitudes sean presentadas dentro de los dos meses contados a partir de la fecha de la publicación de la convocatoria en el BOPV.
b) Realizados por empresas expertas externas.

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.

Modalidad y cuantía de las ayudas
- Las ayudas se instrumentarán en forma de **subvenciones a fondo perdido.**
A efectos del cálculo de la subvención se tendrán en cuenta lo siguiente:
- 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.
- El **"presupuesto máximo aceptado",** base para la aplicación de los porcentajes y cálculo de la subvención, será la suma de los dos conceptos descritos (Gastos de Consultoría y/o Ingeniería, Hardware y Software), siendo el máximo permitido para los gastos de Hardware y Software el 80% del "presupuesto máximo aceptado".
- El Presupuesto total presentado por la entidad solicitante deberá necesariamente contemplar al menos un **20% para labores de Consultoría y/o Ingeniería.**
- Aquellas empresas que presenten el Certificado de Calidad en la Gestión Lingüística Bikain como acreditación del uso, presencia y gestión del euskera en la empresa, obtendrán una subvención adicional del 5%, así como la disposición de un Plan de Igualdad.
- El porcentaje de subvención será del 50% de los gastos e inversiones elegibles aprobados, con un límite de **subvención máxima anual de 18.000 euros por empresa beneficiaria.**

Las ayudas concedidas en aplicación de este Programa tienen la consideración de ayudas de menor importancia o de mínimis.

AFM Cluster ofrece el servicio de gestionar todas estas ayudas, desde el encaje de proyectos en los programas idóneos de financiación y redacción de memorias, hasta la tramitación administrativa de los expedientes, por lo que no duden en contactar con nosotros en caso de estar interesados en recibir este apoyo.

Para más información, no duden en ponerse en contacto con nosotros (Tlf.: 943 30 90 09 **-** invema@invema.es**)**