



Anexo I de la convocatoria



Programa Ciberseguridad

Descripción del programa

MOB 2023

1. OBJETIVO

El Programa tiene como objetivo principal impulsar el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promover el progreso socio económico, así como, reactivar su actividad.

Este Programa se inscribe en el Objetivo Temático 2 “Mejorar el uso y la calidad de las tecnologías de la información y de las comunicaciones y el acceso a las mismas” del “Programa Operativo Plurirregional de España FEDER 2014 - 2020”, en el marco del título de la prioridad de inversión “Desarrollo de productos y servicios de TIC, comercio electrónico y una mayor demanda de TIC”, y contribuye a la consecución del objetivo específico OE.2.2.1. **“Desarrollar la economía digital, incluyendo el comercio electrónico, para el crecimiento, la competitividad y la internacionalización de la empresa española”.**

En este objetivo específico se persigue, en el período 2014-2020, desarrollar y mejorar las herramientas y soluciones TIC para la empresa con el fin de incrementar la oferta de servicios TIC y adaptarla a las demandas reales de los negocios, consiguiendo así mejorar el grado de equipamiento y soluciones TIC de las pymes y micropymes. Se pretende con ello, por una parte, mejorar sus procesos productivos para que puedan ganar competitividad, y que haya una significativa incorporación de las empresas al mundo del comercio electrónico, no sólo como instrumento complementario a sus formas tradicionales de venta, sino como área principal en una mayoría de ellas.

Más concretamente, el **Programa Ciberseguridad tiene como objetivos principales** los siguientes, que ayudarán a la consecución del objetivo específico antes mencionado:

- ➔ Que haya más empleados sensibilizados a través de sus empleadores mediante planes de sensibilización, que sienten las bases de la protección de la información tanto interna como de clientes, colaboradores y proveedores.
- ➔ Contribuir a la mejora de la gestión de la seguridad a través de un modelo de buenas prácticas.
- ➔ Ampliar y mejorar las capacidades de prevención, detección y corrección ante riesgos cibernéticos (ciberamenazas y ciberataques).
- ➔ Mejorar la seguridad de los servicios de las empresas en el ciberespacio
- ➔ Fomentar que las empresas dispongan de un plan de seguridad como una fuente para generar confianza.
- ➔ Fomentar que las empresas cuiden de la seguridad de su web, en particular, si disponen de tienda online y utilizan formas de pago online.
- ➔ Fomentar que las empresas tengan un plan de contingencia y continuidad.

- ➔ Promover la implantación de herramientas de ciberseguridad en el día a día de las empresas y sus operaciones y gestiones más habituales.
- ➔ Proporcionar un modelo homogéneo de la seguridad que facilite la implantación de proyectos y guie las actuaciones en materia de ciberseguridad.

Para lograr estos objetivos, el Programa Ciberseguridad ofrece a las empresas participantes un **conjunto de apoyos** en base a sus necesidades y características. Estos apoyos pueden ser en forma de **servicio de diagnóstico individualizado y/o de ayudas para el desarrollo de sus planes de implantación de soluciones innovadoras**.

Las ventajas que Ciberseguridad proporciona a las empresas participantes se resumen a continuación:

- Inversión mínima
- Mejora de la productividad y de la gestión de procesos
- Mejora del posicionamiento de la empresa
- Mejoras económicas: ahorro de costes/tiempo, reducción de cargas, aumento de ingresos...
- Mayor capacidad innovadora

2. CONTENIDO

El programa Ciberseguridad se caracteriza por su orientación hacia las demandas específicas de las PYME españolas, mediante el desarrollo de una metodología mixta de diagnóstico, apoyo en el proceso innovador y difusión del conocimiento.

El programa se materializa a través de las siguientes actuaciones:

2.1 Fase I: Diagnóstico Asistido en Ciberseguridad

El Programa consiste en la elaboración de un Diagnóstico que permite realizar un análisis exhaustivo del nivel de ciberseguridad de la pyme y sus posibilidades de mejora de la protección mediante el estudio de su dependencia de las TIC, riesgos cibernéticos a los que se expone, cultura de seguridad de la información y protocolos de actuación, que permite conocer la situación de la empresa destinataria. El análisis tendrá en cuenta aspectos técnicos, organizativos, regulatorios y normativos, entre otros.

Además, se analizará: la infraestructura tecnológica implantada en la empresa y las características particulares de su utilización, el grado de concienciación de la dirección en materia de ciberseguridad, el conocimiento y la capacitación del conjunto de la empresa, así como, la capacidad de la empresa para llevar cabo proyectos.

También se estudiará la adopción de procedimientos y soluciones tecnológicas que permitan mitigar o eliminar los riesgos asociados al uso de equipos conectados a internet, así como las metodologías

utilizadas para garantizar el cumplimiento de buenas prácticas por parte de los empleados y terceras partes involucradas en el tratamiento de información o la utilización de tecnologías de la información.

Por último, se estudian las medidas de protección en materia de ciberseguridad instauradas y se evalúa el grado de cumplimiento de la normativa y legislación vigente.

Para la ejecución de esta fase, el Programa contará con una red de Asesores Tecnológicos, pertenecientes a las Cámaras, especializados y formados en la metodología del Programa, que dinamizarán y apoyarán el desarrollo del mismo y serán el referente o soporte de las empresas destinatarias a nivel local.

Una vez concluido el diagnóstico se continuará con la elaboración, por parte del Asesor Tecnológico de la Cámara, de un Plan Director de Seguridad.

El diagnóstico es totalmente gratuito para la empresa.

2.2 Fase II: Plan Personalizado e Implantación (PPI).

En esta fase, proveedores externos a las Cámaras, realizan la implantación de las soluciones establecidas en el Diagnóstico. **El importe máximo financiable es de 4.000 €**, si bien los Planes podrán ser de mayor cantidad.

Esta fase es prefinanciada y cofinanciada por las empresas beneficiarias.

En el caso concreto de la Fase II del Programa, podrán ser beneficiarias aquellas empresas que hayan justificado documentalmente su participación previa en la Fase I del Programa en la presente convocatoria o dentro de la convocatoria correspondiente a la anualidad anterior, y que no hayan sido beneficiarias de Fase II.

También podrán optar a Fase II aquellas que acrediten haber participado en la anualidad anterior en un programa similar de Asesoramiento en materia de ciberseguridad en las pymes, de organismos de Promoción de las TIC de las Comunidades Autónomas, de organismos públicos regionales o locales o de Cámaras de Comercio, siempre que cumplan los requisitos indicados en la convocatoria.

2.3 Acciones de Sensibilización y promoción

- ➔ **De carácter territorial:** Ejecutadas localmente o a nivel autonómico por cada Cámara o alguna agrupación de Cámaras de una Comunidad Autónoma
- ➔ **Plurirregionales / transversales:** Este tipo de acciones hacen referencia a actuaciones de carácter general, ejecutadas por la Cámara de España, y cuya realización puede repercutir en la totalidad de las regiones participantes en el programa