Escuela de organización industrial

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES DE LA FUNDACIÓN EOI PARA LA CONTRATACIÓN DE SERVICIOS POR PROCEDIMIENTO ABIERTO

CONTRATACIÓN DEL "SERVICIO DE CONSULTORIA PARA LA APLICACIÓN DE CIBERSEGURIDAD EN PYMES" PARA LA FUNDACIÓN EOI

Número de Expediente: PA_20190730_ACTIVA CIBERSEGURIDAD.

1. INTRODUCCIÓN

Todas las empresas, incluso las de menor tamaño, están expuestas a los riesgos cibernéticos. Todas gestionan datos de carácter personal, dependen de sistemas informáticos y redes, contratan servicios a terceros y en la nube, generan y protegen su propiedad intelectual y, además, están sujetas al cumplimiento de una normativa sectorial, local, nacional y europea.

Por estas razones cualquier empresa, tenga el tamaño que tenga, debe tomar las medidas necesarias para preservar su competitividad y supervivencia frente ataques o incidentes cibernéticos.

Ante el incesante aumento de los ataques de ciberseguridad, la empresa debe determinar su nivel de seguridad actual y establecer el nivel que ha de conseguir para proteger los sistemas y la información corporativos.

La ciberseguridad se considera parte integral y necesaria de cualquier empresa. Por ello, es habitual que tomemos las medidas necesarias para mejorarla, entre otras, las destinadas a adecuarse a la normativa legal vigente, proteger los sistemas e infraestructuras de cualquier ataque o amenaza, o de forma global poner en marcha un plan estratégico para mejorar la ciberseguridad de nuestra empresa.

Pero antes de implantar cualquier medida, es fundamental conocer el nivel de seguridad de la organización. Tomaremos este nivel de seguridad como punto de partida para poder diseñar e implantar las futuras mejoras de seguridad.

Para conocer el nivel de seguridad de la empresa y reducir la probabilidad de que un ciberataque la impacte, debemos realizar auditorías de seguridad de la información. Estas consisten en un estudio crítico y detallado de toda la estructura de los sistemas de información de la organización. Su objetivo es evaluar y mejorar la seguridad, eficacia y eficiencia de los procesos productivos.

Este Proyecto es un Programa Piloto de Innovación en Ciberseguridad de la PYME. Dimensionado entre 10 y 20 horas de consultoría por empresa y con el objetivo de llegar a entre 100 y 150 PYMES.

En España hay en torno a 1.500 pequeñas y medianas empresas que tienen comprometida de alguna manera su seguridad en la red y unas 150.000 pymes presentan algún incidente relacionado con la Ciberseguridad.

El objetivo es obtener evidencias de cómo los sistemas de información de las PYMES cumplen con los requisitos de seguridad deseados y utilizar esas evidencias para llevar a cabo un proceso de mejora continua de la ciberseguridad en la PYME.

Por otra parte, concienciar a las PYMES de que deben denunciar los ataques que sufran. Si el ataque constituye una infracción a las tecnologías de la información y las comunicaciones deberá denunciarlo ante una autoridad judicial o cuerpos de

seguridad del Estado. En caso de ataque probado o, incluso, ante la simple sospecha de haber sido víctima de un ataque informático, la empresa deberá recoger pruebas informáticas mediante comprobaciones técnicas.

2. DESCRIPCIÓN DEL SERVICIO

EOI precisa contratar un servicio de consultoría para la realización de auditorías de ciberseguridad.

Dimensionado entre 10 y 20 horas de asesoramiento, según tamaño, sector y dependencia tecnológica, con el objetivo de alcanzar las 100-150 PYMES, distribuidas por todo el territorio nacional y distintos sectores de actividad.

El programa de trabajo presenta cinco actuaciones:

1. Fase 1 de Autodiagnóstico inicial: recogida de información de la empresa y su sector y análisis de la situación actual de la empresa en materia de Ciberseguridad para detectar las necesidades y posibilidades de mejora.
2. Fase 2 de Diagnóstico: Análisis de cumplimiento / auditoría de ciberseguridad.
3. Fase 3 de Implantación: Implantación de un Plan de Ciberseguridad en la empresa
4. Fase 4 de Seguimiento: Seguimiento de las medidas implantadas y valoración de otras iniciativas
5. Actuaciones de sensibilización a las Pymes sobre la importancia de integrar la CIBERSEGURIDAD en su estrategia empresarial. Difusión, Comunicación de los resultados del Proyecto, potenciar la imagen de las empresas y las actuaciones llevadas a cabo en el mismo.

3. ESPECIFICACIONES TÉCNICAS

Acciones de captación y selección de empresas participantes en el proyecto.

Se realizará un estudio de aquellos sectores que se quieran integrar en el Proyecto Piloto, justificando su importancia e interés.

Será necesario identificar, al mismo tiempo, las Pymes que serán las posibles beneficiarias y sobre las que se implementarán las actuaciones innovadoras recogidas en el Proyecto.

El adjudicatario será el responsable de la difusión, evaluación y selección de las empresas participantes en el Proyecto, de acuerdo con los criterios establecidos por EOI.

El adjudicatario se compromete a captar y evaluar un mínimo de 100 candidatos que cumplan con los requisitos de la convocatoria pública que se llevará a cabo conforme a lo establecido en el Plan de Captación establecida por el adjudicatario.

Para poner en marcha las acciones de captación y selección de beneficiarios participantes, el adjudicatario deberá responsabilizarse de diseñar y ejecutar un Plan de Captación y Selección de empresas interesadas orientado a activar, animar y captar empresas interesadas que participen en el proyecto; dicho plan deberá haberse presentado antes de los primeros siete días naturales desde la firma del contrato. En el

Plan de captación de deberán priorizar pymes que estén teniendo o hayan tenido recientemente ciberataques, para lo que se deberá contar, en todo caso, con información facilitada por INCIBE.

A estos efectos, las acciones irán encaminadas a captar empresas participantes para las actividades de consultoría:

- Animación y participación en el proceso de captación de empresas para participar en el Proyecto.

  El adjudicatario se compromete a captar y evaluar un mínimo de 100 candidatos que cumplan con los requisitos de la convocatoria pública.

  El adjudicatario identificará, propondrá y se pondrá en contacto con posibles agentes interesados en participar, difundir y colaborar con el proyecto.

  Se entenderá que un candidato ha sido "captado" cuando haya realizado la solicitud correspondiente, habiéndose aceptado por parte de la Dirección del Proyecto como válida la documentación solicitada, de acuerdo con los criterios de la convocatoria.

  Estas actuaciones de captación deberán desarrollarse fundamentalmente en las dos primeras semanas desde la aceptación del Plan de captación y selección, debiendo haberse concluido en las tres primeras semanas.

  Para el desarrollo de actuaciones de captación, el adjudicatario deberá contar con todos los medios materiales para el normal desarrollo de la actividad, debiendo ser validados y aprobados previamente por EOI. Para las actuaciones de captación se podrá contar con la colaboración de otras instituciones.

  El licitador deberá proponer en su Oferta Técnica un Plan de Captación y Selección de empresas participantes suficientemente detallado. En el Plan de captación de deberán priorizar pymes que estén teniendo o hayan tenido recientemente ciberataques

- Revisión y valoración de solicitudes. El adjudicatario se responsabilizará de la revisión y valoración de todas las solicitudes de los beneficiarios, así como la elaboración de los correspondientes informes de selección de cada una de las empresas solicitantes de acuerdo a los criterios establecidos por EOI. Además, deberá elaborar un informe final con una lista priorizada de los solicitantes de acuerdo a los criterios establecidos por EOI.
- Formalización de las peticiones de participación. El adjudicatario se responsabilizará de que las empresas solicitantes de las consultorías formalicen correctamente la petición de participación en el proyecto, en especial toda la documentación administrativa que le permita participar en el mismo, de acuerdo con los criterios de la convocatoria pública y EOI. Igualmente, el adjudicatario se responsabilizará de la recogida y custodia documental necesaria para la correcta prestación del servicio.
- Seguimiento. Finalmente, el adjudicatario se responsabilizará del seguimiento de las empresas participantes en las consultorías con el fin de lograr su

mantenimiento durante toda la iniciativa, de forma que si alguna empresa decidiera abandonar el servicio de consultoría antes de concluirlo, el adjudicatario proveerá una nueva que cumpla los requisitos de la convocatoria.

El licitador deberá proponer en su Oferta Técnica un Cronograma de Trabajo

El adjudicatario deberá elaborar un documento compartido con los responsables del Proyecto en EOI en el que se vaya mostrando la evolución de:

- Empresas participantes
- Distribución de las PYMES por:
  - Sectores
  - Tamaño
  - Provincia
- Número de horas de consultoría que serán necesarios por cada empresa

El adjudicatario deberá elaborar una memoria final que incluya:

- Detalle de las empresas participantes
- Distribución de las PYMES por:
  - Sectores
  - Tamaño
  - Provincia
- Motivación del detalle del número de horas de consultoría hechas por cada empresa, en función de:
  - Sector
  - Tamaño
  - Dependencia Tecnológica

Actuaciones de consultoría a las Pymes participantes en el proyecto

Mediante diagnósticos individualizados a Pymes se estudiarán y definirán las necesidades de mejora y eficiencia que deben abordar en materia de CIBERSEGURIDAD, así como las necesidades de cumplimiento normativo y legal.

Para ello, se pondrá a disposición de las Pymes participantes al equipo de consultores, que den cobertura a todo el territorio nacional y con disponibilidad suficiente para ejecutar los trabajos de consultoría en el tiempo indicado.

Se debe ofrecer asesoramiento a un número estimado de 100 Pymes mediante sesiones presenciales y en remoto.

Cada empresa recibirá un mínimo de 10 horas/empresa y un máximo de 20 horas/empresa que han de incluir:

- Un mínimo de 8 horas de sesiones individuales presenciales y un máximo de 16 horas, repartidas en al menos 3 visitas o reuniones con la empresa, preferentemente en la sede de la empresa. Correspondientes a las fases 1 (autodiagnóstico inicial), 2 (diagnóstico) y 3 (implantación)
- Seguimiento remoto, un mínimo de 2 horas de seguimiento remoto individualizado y un máximo de 4 horas para cada empresa correspondiente a la fase 4 (seguimiento). Para ello el licitador deberá indicar el tipo de seguimiento remoto que empleará para desarrollar esta modalidad.

La propuesta técnica deberá presentar un modelo o patrón básico que recoja todos los aspectos notorios de cada sesión en remoto. El asesoramiento remoto podrá ser telefónico, videoconferencia y/o correo electrónico.

De esta manera, el adjudicatario realizará la prestación a EOI del servicio de un máximo de 1.700 horas de Consultoría de CIBERSEGURIDAD Individualizada que se irá distribuyendo hasta agotarse, en función de las necesidades de cada empresa. El número de horas por empresa será determinado por el adjudicatario según unos criterios objetivos que deberá establecer claramente en función del tamaño, sector y dependencia tecnológica de la PYME

El licitador deberá proponer en su Oferta Técnica los criterios para estimar el número de horas de consultoría a la pyme en función del tamaño, sector y dependencia tecnológica suficientemente detallado.

- **Diseño y Desarrollo de las Actuaciones de la Fase 1 de Autodiagnóstico inicial**

  El adjudicatario llevará a cabo el diseño y desarrollo de un procedimiento de Autodiagnóstico de CIBERSEGURIDAD de las Pymes participantes en el proyecto.

  Durante dos horas, el consultor hará la recogida de información de la empresa y análisis de la situación actual de la pyme en materia de Ciberseguridad para detectar las necesidades y posibilidades de mejora.

  Para ello el consultor usará con el empresario, o empleado que este designe, la herramienta de diagnóstico del Instituto Nacional de Ciberseguridad (INCIBE) alojada en https://www.incibe.es/protege-tu-empresa/conoces-tus-riesgos.

  Para ayudar a las empresas a evaluar su estado de ciberseguridad y a avanzar hacia mayores niveles de protección, el kit de autodiagnóstico de INCIBE especialmente diseñado para este fin, determina el estado en seguridad de la información, qué riesgos amenazan el funcionamiento de la empresa y qué aspectos debe mejorar.

  Para cada Pyme se realizará un informe en el cual se recogerán los resultados de esta fase y las primeras observaciones a tener en cuenta en la Fase 2.

  Realizando esta fase de autodiagnóstico con el empresario, se persigue que las Pymes hagan una primera reflexión de los riesgos de seguridad de sus negocios en función de cómo utilizan la tecnología: correo electrónico, página web, tabletas, smartphones, etc.

  El licitador deberá proponer en su Oferta Técnica los modelos de reseña de tutoría a utilizar, así como el modelo de informe a entregar a la empresa participante.

El adjudicatario deberá elaborar una memoria final que incluya:

- Detalle de los resultados individuales de esta fase por cada una de las empresas participantes.
- Información agregada y consolidada de los resultados por sector de actividad.
- Información agregada y consolidada de los resultados por el total de las empresas participantes.
- Propuestas de mejora en esta fase para posteriores ediciones del Proyecto.

- **Diseño y Desarrollo de las Actuaciones de la Fase 2 de Diagnóstico**

El adjudicatario llevará a cabo una evaluación de las necesidades de cumplimiento legal, con recomendaciones para su implementación, y necesidades de auditoría de CIBERSEGURIDAD de las Pymes participantes en el proyecto.

La duración de esta fase será entre 2 y 8 horas, en función del tamaño, sector y dependencia tecnológica y según el número de horas de consultoría que se haya diseñado previamente para cada empresa.

El objetivo de esta fase es conocer el nivel de seguridad de la pyme y tomar este nivel de seguridad como punto de partida para poder diseñar e implantar las futuras mejoras de seguridad.

Para conocer el nivel de seguridad de la empresa y reducir la probabilidad de que un ciberataque comprometa a la pyme, debemos solicitar o realizar periódicamente auditorías de seguridad de la información. Estas consisten en un estudio crítico y detallado de toda la estructura de los sistemas de información de la organización.

Estos son los aspectos mínimos que deben considerarse en esta fase:

- protección antimalware (ransomware, troyanos, etc)
- protección antispam, prevención del fraude y de filtrado de contenidos
- administración de permisos de usuarios y accesos a servicios
- seguridad de los dispositivos móviles
- gestión automatizada de actualizaciones y parches
- monitorización del uso de los recursos informáticos y de red
- evaluación de las necesidades de cumplimiento legal

En función de los resultados de la pyme analizada, se recomendará a la PYME algún tipo de las siguientes auditorías, que quedan fuera de esta actuación:

- Test de penetración. Es un tipo de auditoría técnica que consiste en un conjunto de pruebas a las que se somete a una aplicación, servicio o sistema, con el objetivo de encontrar huecos o fallos a través de los cuales sería posible conseguir acceso no autorizado a información de la empresa.

- Auditoría de red. Permiten analizar la red de la empresa en busca de puertos abiertos, recursos compartidos, servicios o electrónica de red (router, switch, etc.). Además, en estas auditorías se emplean herramientas que permiten realizar la catalogación de las infraestructuras conectadas a la red o incluso detectar versiones de dispositivos inseguros, versiones de software o la necesidad de instalar actualizaciones o parches.
- Auditoría de seguridad perimetral. Se trata de un proceso destinado a determinar el nivel de seguridad de las barreras que protegen la red de comunicaciones de una organización de los riesgos que provienen del exterior y del interior. Podríamos englobarla dentro de la auditoría de red, aunque está más especializada en detectar fallos de seguridad desde el punto de vista de exterior.
- Auditoría web. Analiza los fallos de seguridad o vulnerabilidades que afectan al funcionamiento de una página web.

Para cada Pyme se realizará un informe en el cual se recogerán los resultados de esta fase, con recomendaciones concretas, y las observaciones a tener en cuenta en la Fase 3.

Realizando esta fase de diagnóstico se persigue que las Pymes conozcan si protegen adecuadamente la información y si disponen de las medidas de seguridad adecuadas para protegerla. Obtener evidencias, agregadas y anónimas de que cómo los sistemas de información de la pyme cumplen con los requisitos de seguridad deseados y utilizar estas evidencias para llevar a cabo un proceso de mejora continua de la ciberseguridad.

El licitador deberá proponer en su Oferta Técnica un checklist de los aspectos a considerar en cada pyme en función de su sector de actividad y su tamaño, los modelos de reseña de tutoría a utilizar, así como el modelo de informe a entregar a la empresa participante. Deberán utilizarse, en la medida de los posible, recursos diseñados por INCIBE y de uso gratuito para las PYMES.

El adjudicatario deberá elaborar una memoria final que incluya:

- Detalle de los resultados individuales de esta fase por cada una de las empresas participantes.
- Información agregada y consolidada de los resultados por sector de actividad.
- Información agregada y consolidada de los resultados por el total de las empresas participantes.
- Propuestas de mejora en esta fase para posteriores ediciones del Proyecto.

- **Diseño y Desarrollo de las Actuaciones de la Fase 3 de Implantación**

  El adjudicatario llevará a cabo el diseño de un Plan Director de Ciberseguridad de las Pymes participantes en el proyecto con identificación de recursos necesarios,

inversiones, responsables y planificación temporal, para ser desarrollado e implantado por el empresario.

La duración de esta fase será entre 4 y 6 horas, en función del tamaño, sector y dependencia tecnológica y según el número de horas de consultoría que se haya diseñado previamente para cada empresa.

Para cada Pyme se realizará un informe en el cual se recogerán las soluciones propuestas, detallando los beneficios previstos en el caso de aplicación de dichas soluciones.

El objetivo de esta fase es que el empresario desarrolle el Plan Director de Seguridad. Cuando decidimos abordar la ciberseguridad es importante tener una planificación de las actividades a realizar que cuente con el compromiso de la dirección. Este plan va a marcar las prioridades, los responsables y los recursos que se van a emplear para mejorar el nivel seguridad de la pyme en el mundo digital.

Contendrá los proyectos que vamos a abordar tanto técnicos como de contenido legal y organizativos. Así, habrá proyectos de instalación de productos o de contratación de servicios, pero otros serán para cumplir con las leyes de privacidad y comercio electrónico, formar a los empleados o para poner en marcha procedimientos y políticas internas.

El resultado de la Fase 2 será el punto de partida para que la pyme se fije el objetivo de dónde quiere estar. Este objetivo y los proyectos a aplicar siempre tendrán que estar alineados con las estrategias de negocio. Qué vamos a proteger, cómo haremos la prevención, qué incidentes podríamos tener, cómo nos preparamos para reaccionar, etc.

Tendrá en cuenta, al menos, lo siguiente:

- Definición de proyectos e iniciativas a implementar (como ejemplo)
  - Plan Director de Seguridad
  - Plan de Contingencia y Continuidad de Negocio
  - Cumplimiento Legal
  - Desarrollo de cultura en seguridad
  - Necesidad o no de contratación de servicios
  - Protección de la web
  - Protección de la información
  - Protección del puesto de trabajo
  - Protección en movilidad y conexiones inalámbricas
  - Protección de los Clientes
  - Fraude y Gestión de la Identidad Online

- Clasificación y priorización de iniciativas
  - Corto plazo
  - Medio plazo

- Largo plazo

- Implantación
  - Asignación de responsables y recursos
  - Creación de un comité de gestión
  - Revisión continua

Para cada Pyme se realizará un informe en el cual se recogerán los resultados de esta fase, con recomendaciones concretas, y las observaciones a tener en cuenta en la Fase 4.

Debe quedar claro en el informe final qué debe hacer la pyme en caso de sufrir un ciberataque y con quién debe ponerse en contacto en caso de sufrir un incidente o ataque, así como la obligación de denunciarlo.

El licitador deberá proponer en su Oferta Técnica los aspectos a considerar en cada pyme en función de su sector de actividad y su tamaño los modelos de reseña de tutoría a utilizar, así como el modelo de informe a entregar a la empresa participante. Deberán utilizarse, en la medida de los posible, recursos diseñados por INCIBE y de uso gratuito para las PYMES.

El adjudicatario deberá elaborar una memoria final que incluya:

- Detalle de los resultados individuales de esta fase por cada una de las empresas participantes
- Información agregada y consolidada de los resultados por sector de actividad.
- Información agregada y consolidada de los resultados por el total de las empresas participantes
- Propuestas de mejora en esta fase para posteriores ediciones del Proyecto

- **Diseño y Desarrollo de las Actuaciones de la Fase 4 de Seguimiento**

  El adjudicatario llevará a cabo el seguimiento de la Implantación de la Fase 3 en la pyme.

  La duración de esta fase será entre 2 y 4 horas, en función del tamaño, sector y dependencia tecnológica y según el número de horas de consultoría que se haya diseñado previamente para cada empresa.

  Para cada Pyme se realizará un informe en el cual se recogerán las medidas implantadas y valoración de otras iniciativas que puedan recomendarse poner en marcha

  El objetivo de esta fase es que el empresario tenga la opción de reportar al consultor cualquier dificultad que haya tenido en la fase de implantación y que el consultor pueda hacer un balance de las medidas que finalmente se están implantando en la pyme y las dificultades que pudieran surgir.

  El licitador deberá proponer en su Oferta los modelos de reseña de tutoría a utilizar, así como el modelo de informe a entregar a la empresa participante.

  El adjudicatario deberá elaborar una memoria final que incluya:

- Detalle de los resultados individuales de esta fase por cada una de las empresas participantes
- Información agregada y consolidada de los resultados por sector de actividad.
- Información agregada y consolidada de los resultados por el total de las empresas participantes
- Propuestas de mejora en esta fase para posteriores ediciones del Proyecto
- **Identificación de opciones de mejora de la implantación de la CIBERSEGURIDAD en las pymes y desarrollo de un catálogo genérico de buenas prácticas.** Apoyándose en los datos recogidos se identificarán los puntos críticos de las Pymes participantes y se propondrán las correspondientes opciones de mejora. Se desarrollará además un catálogo de buenas prácticas que recoja ejemplos de PYME Cibersegura por cada uno de los sectores participantes.

- **Diseño y Desarrollo de las Actuaciones de sensibilización a las pymes sobre la importancia de integrar la CIBERSEGURIDAD en su estrategia empresarial.** Difusión de la iniciativa, comunicación de los resultados del Proyecto, potenciar la imagen de las empresas y las actuaciones llevadas a cabo en el mismo.

  A través de esta fase se pretende difundir todos los resultados, parciales y finales, del proyecto.

  El adjudicatario deberá generar al menos 3 contenidos de media a la semana relativos a las actividades del proyecto para ser difundidos por las redes sociales de EOI, hasta la finalización del contrato.

El adjudicatario realizará una Memoria final justificativa del servicio prestado donde se incorporen los asesoramientos realizados y los resultados obtenidos.

4. PLANIFICACIÓN TEMPORAL

La duración será desde la firma del contrato hasta la finalización del Proyecto que se prevé para el 20 de diciembre de 2019. El Proyecto deberá ser presentado por los licitadores con una planificación de acuerdo a esta duración.

Las actuaciones se desarrollarán en todo el territorio nacional, para lo cual el adjudicatario deberá tener plena disponibilidad para estar permanentemente vinculado al lugar de realización de los trabajos durante la ejecución del Proyecto.

Además, tendrá disponibilidad para viajar a la sede de EOI en Madrid cuando fuese requerido (máximo una vez por semana durante todo el Proyecto).

El adjudicatario deberá estar presente en todas las actividades y eventos que se organicen.

5. EQUIPO DE TRABAJO

De conformidad con lo establecido en el artículo 76.2 de la LCSP, los licitadores se comprometerán a adscribir a la ejecución del contrato los medios personales o

materiales suficientes para ello. A este compromiso se le atribuye el carácter de obligación esencial a los efectos previstos en el artículo 211 de la LCSP.

El adjudicatario deberá llevar a cabo sus tareas mediante un equipo multidisciplinar, estable, con amplia experiencia en la realización de Proyectos similares al ofertado. El equipo de trabajo estará dirigido por un **Director de Proyecto**, designado por el adjudicatario, que actuará como único interlocutor ante EOI, quien actuará como responsable de la elaboración y entrega de los trabajos, estará integrado en su propia plantilla y tendrá entre sus obligaciones las siguientes:

- Actuar como interlocutor del adjudicatario frente a EOI, canalizando la comunicación entre la empresa y el personal integrante del equipo adscrito al contrato, de un lado, y EOI, de otro lado, en todo lo relativo a las cuestiones derivadas del a ejecución del contrato.
- Apoyar a la EOI en la promoción del Proyecto y captación de las empresas beneficiarias.
- Distribuir el trabajo entre el personal encargado de la ejecución del contrato, e impartir a dichos trabajadores las órdenes e instrucciones de trabajo que sean necesarias en relación con la prestación del servicio contratado.
- Supervisar el correcto desempeño por parte del personal integrante del equipo de trabajo de las funciones que tiene encomendadas, así como controlar la asistencia del dicho personal al puesto de trabajo.
- Incorporar al equipo de trabajo a las personas que estime necesarias para verificar y evaluar todas las actuaciones a su cargo.
- Organizar el régimen de vacaciones del personal adscrito a la ejecución del contrato, debiendo a tal efecto coordinarse adecuadamente el adjudicatario con EOI, a efectos de no alterar el buen funcionamiento del servicio.
- Informar a EOI del grado de cumplimiento y evolución del Proyecto, garantizando el cumplimiento de plazos y requisitos de servicio.
- Informar a EOI acerca de las variaciones, ocasionales o permanentes, en la composición del equipo de trabajo adscrito a la ejecución del contrato, así como de cualquier incidencia que afecte o pueda afectar al Proyecto, proponiendo las medidas para su corrección o las medidas preventivas que correspondan.
- Emisión de informes y mejora continua de la calidad del servicio.
- Emisión de un informe indicando las medidas de control impuestas y las acciones a llevar a cabo que sean necesarias cuando las desviaciones del Proyecto así lo requieran.
- Velar por el cumplimiento de las medidas de protección de datos personales, confidencialidad, custodia de la documentación y de cualquier otra normativa de aplicación al Proyecto.
- Convocar las reuniones y comités de seguimiento necesarias para la buena marcha del Proyecto o con el fin de determinar, analizar y valorar las incidencias que, en su caso, se produzcan durante su ejecución.
- Asistir a las reuniones y Comités de seguimiento necesarios convocados por EOI para la buena marcha del Proyecto o con el fin de determinar, analizar y valorar las incidencias que, en su caso, se produzcan durante su ejecución.

- Emitir las certificaciones parciales de recepción de los trabajos a realizar.
- Todas aquellas correspondientes a la buena marcha del servicio.

El equipo de consultoría debe presentar una dotación mínima de nueve personas, incluyendo un Director de Proyecto cuyas funciones y responsabilidades son las anteriormente descritas, y un mínimo de 8 consultores.

Deberán cumplir como mínimo los siguientes requisitos de cualificación y experiencia, que se califican de esencial:

- Perfil director del proyecto:
    - Titulación superior.
    - Responsable de la dirección y organización de servicios similares al objeto del contrato o con una experiencia suficiente y demostrada referida especialmente a los trabajos relativos al objeto del contrato.
    - Experiencia, de al menos 5 años, en gestión de proyectos similares al objeto del contrato; y en gestión de proyectos en el sector público.
    - Experiencia, de al menos 5 años, en gestión de proyectos con PYMES, de temas relacionados con el objeto del contrato.
- Perfil equipo de consultores:
    - Un mínimo de 8 consultores, con titulación superior y con experiencia, de al menos 3 años, en servicios similares al objeto del contrato o con una experiencia suficiente y demostrada referida especialmente a los trabajos relativos al objeto del contrato.

El licitador que haya sido propuesto como adjudicatario, conforme a lo establecido en el apartado 7 del Pliego de Cláusulas Administrativas Particulares, deberá poner a disposición la mesa de contratación, en el plazo para presentar la garantía definitiva, los currículum vitae de los medios personales que se compromete a adscribir para la prestación del Servicio objeto del contrato, al objeto de verificar el cumplimiento de los requisitos de cualificación anteriormente indicados. En los currículum se deberá incluir el detalle de los Proyectos y tipos de servicios prestados similares a los descritos en los pliegos.

6. GESTIÓN Y SEGUIMIENTO DEL PROYECTO - SISTEMAS DE CONTROL Y CALIDAD DE SERVICIO

El adjudicatario deberá indicar cómo se realizará la gestión y seguimiento del Proyecto (estructura de gestión, responsables técnicos y administrativos, flujos de información, etc.). Deben estar muy bien definidos los flujos de información que se establecerán durante el desarrollo del Proyecto (informes de progreso y seguimiento o cualquier otro entregable). Esta propuesta de gestión y seguimiento del proyecto será aprobada por EOI, siendo obligatoria para el adjudicatario.

En todo caso, el adjudicatario deberá:

- Reportar el avance de los trabajos semanalmente y poner en común siguientes pasos y puntos críticos o de decisión con la Dirección del proyecto.
- Generar un informe final sobre el servicio prestado (memoria descriptiva de actuaciones)
- Elaborar una memoria final del proyecto sobre el servicio prestado

El adjudicatario deberá garantizar además:

- Participación en las comisiones de seguimiento a petición de la dirección del proyecto de EOI. La empresa adjudicataria deberá garantizar la asistencia del responsable del servicio a las reuniones de la comisión de seguimiento a requerimiento de la dirección del proyecto de EOI.
- Garantía de calidad y soporte documental. El adjudicatario deberá garantizar la calidad de los trabajos y la consecución de objetivos en tiempo y forma así como por la satisfacción de las Pymes beneficiarias; completar y custodiar debidamente toda la documentación necesaria para acreditar el correcto desarrollo de las actividades.

En la oferta se deberá incluir el Plan de Calidad propuesto y Plan de Contingencia ante situaciones extraordinarias, incluyendo un Acuerdo de Calidad de Servicio propuesto, que contenga valores concretos de:

- Tiempos de solución de incidencias.
- Controles de calidad.
- Indicadores propuestos para la consecución de los objetivos de EOI.

EOI designará un responsable del contrato. Las funciones de éste serán, con carácter general, las derivadas de la dirección, comprobación, informe y vigilancia de la correcta realización de los trabajos y, en especial, las que le asigne EOI, tales como:

- Actuar como interlocutor principal frente al adjudicatario en todo lo relativo a las cuestiones derivadas del a ejecución del contrato.
- Supervisar el correcto desempeño por parte del personal integrante del equipo de trabajo de las funciones que tiene encomendadas, así como controlar la ejecución del contrato.
- Convocar las reuniones y Comités de seguimiento necesarios para la buena marcha del Proyecto o con el fin de determinar, analizar y valorar las incidencias que, en su caso, se produzcan durante su ejecución.
- Velar por el cumplimiento de los trabajos a realizar.
- Incorporar al equipo de trabajo a las personas que estime necesarias para verificar y evaluar todas las actuaciones a su cargo.
- Emitir las certificaciones parciales de recepción de los trabajos a realizar.

Asimismo, EOI se reserva el derecho a realizar todos aquellos controles e inspecciones que crea oportuno con el fin de garantizar el cumplimiento del contrato.

El adjudicatario, durante la ejecución del contrato, deberá entregar informes periódicos recogiendo los principales datos sobre su actividad.

7. OFERTA TÉCNICA

La Oferta técnica deberá acreditar un dominio conceptual, metodológico y técnico adecuado para la ejecución del contrato y reflejar capacidad técnica probada para dar servicio en el desarrollo del objeto previsto y para la consecución de los objetivos marcados.

La Oferta Técnica deberá incluir la información necesaria para la completa descripción técnica del Proyecto, incluyendo:

Descripción del Proyecto relacionándolo directamente con los objetivos y con los criterios de valoración, detallados en el punto 1 del Pliego de Cláusulas Administrativas Particulares:

Calidad técnica. En cuanto a calidad técnica de la oferta se valorará la respuesta a los requisitos establecidos, entendiendo que estos requisitos constituyen un nivel mínimo de cumplimiento, por lo que la oferta deberá incluir cualesquiera otras prestaciones que faciliten la satisfacción de la necesidad de EOI.

- Metodología de desarrollo del Proyecto y, especialmente:
  - La metodología de desarrollo del proyecto propuesta necesariamente incluirá un cuadro de mando con asignación de recursos, indicadores, sistema de evaluación y seguimiento de acuerdo a las tareas descritas.
  - Plan de captación de empresas en todo el territorio nacional, de diverso tamaño y de diversos sectores
  - Enfoque propuesto para las sesiones de la consultoría de CIBERSEGURIDAD. Incluyendo la metodología de trabajo, el tiempo y el calendario de las sesiones, así como características del informe que recibirá cada Pyme.
  - Informe y servicios que prestará para:
    - Fase 1 de Autodiagnóstico inicial
    - Fase 2 de Diagnóstico: Análisis de cumplimiento y auditoría de Ciberseguridad
    - Fase 3 de Implantación
    - Fase 4 de Seguimiento
    - Extrapolación y difusión de los resultados del proyecto.

Acuerdos de calidad de servicio:

- Tiempos de respuesta a requerimientos de EOI.
- Tempos de solución de incidencias.

Además, La Oferta se debe presentar de acuerdo a lo indicado en el punto 5 b. (SOBRE 2, CRITERIOS QUE DEPENDEN DE UN JUICIO DE VALOR) del Pliego de Cláusulas Administrativas Particulares.