PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL PROCEDIMIENTO PARA LA CONTRATACIÓN DE LOS SERVICIOS PARA EL DESARROLLO DEL PROYECTO CIBERSEGURIDAD EN LAS EMPRESAS. PROYECTO FINANCIADO POR LA DIPUTACIÓN DE BADAJOZ.

EXPEDIENTE: PA_2025_0002

---

1. OBJETO DEL CONTRATO.

1.1. Antecedentes.

La ciberseguridad, entendida como el conjunto de prácticas, tecnologías y procesos diseñados para proteger los sistemas, redes y datos contra ataques cibernéticos, se ha convertido en un componente esencial en el panorama actual de los negocios.

La importancia de la ciberseguridad en las empresas no puede subestimarse, ya que un ataque exitoso puede tener consecuencias devastadoras, no solo en términos de pérdidas financieras, sino también en la confianza de los clientes y la reputación empresarial.

Hay que ser conscientes de que esto es particularmente relevante para las PYMES, que, aunque a menudo se perciben como objetivos menos atractivos para los cibercriminales, y hace que muchas PYMES no inviertan adecuadamente en medidas de seguridad, por lo que la realidad es que los cibercriminales tienden a atacarlas precisamente por estas debilidades: tienen menos recursos y personal especializado en comparación con las grandes empresas, y esto las hace más vulnerables a los ataques cibernéticos.

Por este motivo, es esencial promover e implementar medidas de ciberseguridad que garanticen la protección de los datos y los sistemas, fortaleciendo así la competitividad y sostenibilidad de estas organizaciones.

1.2. Contexto del proyecto.

Consciente de esta realidad, la Cámara Oficial de Comercio, Industria y Servicios de Badajoz, con la financiación de la Diputación de Badajoz ha diseñado el proyecto “Servicios para el Desarrollo del Proyecto Ciberseguridad en las Empresas”.

Este programa tiene como objetivo principal dotar a pymes y autónomos de la provincia de Badajoz de las herramientas y conocimientos necesarios para mejorar su seguridad digital.

El proyecto no solo busca la implementación de soluciones tecnológicas, sino también la sensibilización de los beneficiarios sobre la importancia de la ciberseguridad. A través de un enfoque integral, se pretende garantizar que las empresas participantes estén mejor preparadas para enfrentar los desafíos del entorno digital actual y futuro.

El contrato será licitado por la Cámara Oficial de Comercio, Industria y Servicios de Badajoz, en calidad de entidad responsable de la gestión del proyecto. Esta iniciativa cuenta con la financiación de la Diputación de Badajoz.

1.3. Objeto de la prestación.

El objeto del contrato al que se refiere el presente pliego es la contratación de los servicios externos de una entidad que desarrolle la planificación, ejecución e implantación en las empresas solicitantes de la ayuda de una serie de productos y soluciones técnicas de un catálogo predefinido de herramientas necesarias para poder hacer frente y reaccionar de

forma adecuada en caso de sufrir un ataque cibernético. Estas soluciones, con sus requisitos técnicos exigidos, son las recogidas en el **Anexo I** del presente pliego. Se emitirá un informe por cada actuación en empresa o autónomo según el contenido del documento **Anexo II** del presente pliego.

Bajo la coordinación de la Cámara de Comercio de Badajoz, el adjudicatario será el responsable de proporcionar los medios humanos y materiales para la ejecución de las soluciones técnicas requeridas, así como de la captación de los destinatarios, que serán empresas y autónomos de la provincia de Badajoz con un número de empleados de hasta 50 trabajadores y siendo al **menos un mínimo de 80 empresas o autónomos** de municipios de menos de 20.000 habitantes.

El desarrollo del plan contempla las siguientes actuaciones a ejecutar por el adjudicatario:

- Confección de documentación inicial.
- Difusión y coordinación del proyecto.
- En el caso de que desde la convocatoria que se publique no resulte como interesados el número mínimo de empresas o autónomos de 160, el adjudicatario deberá localizar e implantar soluciones hasta completar el número de mínimo de 160.
- Confección de una memoria por cada empresa o autónomo participante con las soluciones implantadas con un contenido mínimo que se recoge en el **Anexo II** del presente pliego.

La Cámara de Comercio de Badajoz publicará una convocatoria pública de acceso a las ayudas para las empresas y autónomos que deseen beneficiarse de la misma.

Todas estas actuaciones se desarrollarán bajo las indicaciones y pautas recibidas por la entidad contratante y conforme a lo indicado en el Pliego de Prescripciones Técnicas, si bien, dicho contrato se ejecutará a libre riesgo y ventura de la entidad adjudicataria siendo responsable éste técnica y legalmente del desarrollo de las mismas.

El número mínimo de empresas y autónomos a implantar soluciones es de **160**.

1.4. Necesidades a satisfacer mediante el contrato.

Con la implementación en las empresas de estas herramientas se pretende en las mismas los siguientes objetivos genéricos:

- La preservación de los datos propiedad intelectual e ideas.
- Autentificar la disponibilidad de sus servicios, sin interrupciones.
- Proteger los accesos a la información.
- Proteger la operatividad de los sistemas.
- Mejora la competitividad en el mercado y nos prepara ante los cambios de la transformación digital.
- Proteger los datos de posibles manipulaciones.
- Desarrollo de nuevos modelos de negocio.
- Evitar que puedan suplantar o tomar el control de datos y sistemas de la empresa.
- Evitar el robo de información, datos, imágenes, etc.

- Asegura la digitalización de los procesos y su blindaje.
- Proteger los dispositivos personales.

Estos objetivos generales ayudarán a la consecución de los siguientes objetivos específicos:

1. Fortalecimiento de la ciberseguridad: permitirá a la pyme mejorar sus capacidades en ciberseguridad, protegiendo sus activos digitales y datos sensibles de posibles ciberataques.

2. Fomento de la transformación digital: contribuirá a impulsar la transformación digital de las pymes, promoviendo su adaptación a entornos digitales seguros y preparados para los desafíos actuales.

3. Acceso a asesoramiento especializado: las pymes beneficiarias recibirán asesoramiento especializado en ciberseguridad, lo que les permitirá identificar vulnerabilidades, implementar medidas preventivas y fortalecer sus sistemas de protección.

4. Mejora la competitividad: al fortalecer la ciberseguridad, las pymes mejorarán su competitividad al garantizar la continuidad de sus operaciones y la confianza de sus clientes en un entorno digital seguro.

5. Apoyo a la resiliencia empresarial: la subvención contribuirá a aumentar la resiliencia empresarial frente a posibles amenazas cibernéticas, asegurando la continuidad del negocio y la protección de la información sensible.

2. ALCANCE DEL CONTRATO.

El alcance del contrato se define por las actividades, servicios y soluciones que la empresa adjudicataria deberá ejecutar para garantizar el cumplimiento de los objetivos del proyecto. Este alcance incluye las siguientes áreas clave:

2.1. Empresas Beneficiarias

El proyecto está dirigido a pymes y autónomos de la provincia de Badajoz que cumplan con los siguientes requisitos para ser considerados beneficiarios:

- No contar previamente con medidas de ciberseguridad implantadas en sus sistemas.
- Ser una pequeña o mediana empresa (pyme) o autónomo con actividad económica registrada en la provincia de Badajoz.
- Presentar la documentación administrativa pertinente requerida en la convocatoria para formalizar su participación.
- No encontrarse en situación de prohibición para contratar según lo establecido en la legislación vigente.

La empresa adjudicataria deberá identificar, seleccionar e implementar las soluciones de ciberseguridad en al menos 160 empresas y/o autónomos, de hasta 50 trabajadores, siendo al **menos un mínimo de 80 empresas o autónomos** de municipios de menos de 20.000 habitantes, garantizando que cumplan con los requisitos establecidos en el proyecto.

Para la identificación y selección de las empresas participantes, la entidad adjudicataria podrá emplear los medios que considere más adecuados para la difusión de la convocatoria y la captación de participantes. Los costes asociados a estas actividades, como campañas publicitarias, eventos informativos, visitas comerciales u otras acciones, deberán ser asumidos por la propia adjudicataria dentro del marco del contrato.

La empresa adjudicataria será responsable de verificar el cumplimiento de estos requisitos al momento de seleccionar las empresas participantes, asegurando que el proceso sea transparente y conforme a los criterios establecidos.

2.2. Servicios Incluidos.

Los servicios que deberá prestar la empresa adjudicataria incluyen:

- Búsqueda de las empresas participantes: Difusión de la convocatoria y selección de las empresas beneficiarias, asegurando que cumplan con los criterios establecidos para participar en el proyecto.
- Diagnóstico Inicial: Evaluación del estado de ciberseguridad de las empresas participantes, identificando vulnerabilidades y áreas de mejora.
- Instalación de Soluciones de Ciberseguridad: Implementación de herramientas y medidas específicas, como antivirus, firewalls, autenticación multifactor (MFA) y copias de seguridad en la nube. Estas soluciones expresamente señaladas son las que se consideran mínimas para este proyecto, si bien se pueden implantar otras soluciones que se consideren adecuadas en cada caso.
- Formación y sensibilización: Capacitación de los responsables y empleados de las empresas participantes en buenas prácticas de ciberseguridad.
- Diagnóstico final: Realización de una evaluación posterior a la instalación para validar las mejoras implementadas y elaborar un informe de resultados, con el mínimo establecido en el documento **Anexo II** del presente pliego.
- Difusión de resultados: Comunicación de los resultados obtenidos durante la ejecución del proyecto, tanto a nivel individual para las empresas participantes como de manera global para los interesados, asegurando la promoción de las buenas prácticas implementadas y el impacto positivo del proyecto. La adjudicataria podrá emplear medios como informes públicos, presentaciones, eventos o publicaciones digitales para esta tarea.

2.3. Límites y exclusiones.

El alcance del contrato no incluye:

- La implantación de medidas de ciberseguridad en empresas que ya dispongan de sistemas similares.
- Soluciones o servicios que excedan las especificaciones técnicas indicadas en el proyecto.
- Costes asociados a la adquisición de hardware o licencias que no estén directamente relacionados con las medidas descritas en este pliego.

Asimismo, se priorizará la implantación de las medidas más relevantes del Decálogo de Ciberseguridad del INCIBE.

3. DURACIÓN.

El contrato tendrá un plazo de ejecución máxima desde el día siguiente al de la firma del documento en el que se formalice el mismo, **hasta el 30 de septiembre de 2025**, incluyendo el período de justificación, sin perjuicio de ampliación eventualmente, para el caso de que se concediera ampliación en el plazo de ejecución por parte del organismo concedente de la subvención, para la conclusión de los objetivos del Programa, sin que ello suponga superar el valor del contrato inicial.

4. ESPECIFICACIONES TÉCNICAS.

La entidad adjudicataria deberá desarrollar la planificación, ejecución e implantación en las empresas solicitantes de la ayuda de una serie de productos y soluciones técnicas de un catálogo predefinido de herramientas necesarias para poder hacer frente y reaccionar de forma adecuada en caso de sufrir un ataque cibernético. Estas soluciones, con sus requisitos técnicos exigidos, son las recogidas en el **Anexo I** del presente pliego. Se emitirá un informe por cada actuación en empresa o autónomo según el contenido del documento **Anexo II** del presente pliego.

Bajo la coordinación de la Cámara de Comercio de Badajoz, el adjudicatario será el responsable de proporcionar los medios humanos y materiales para la ejecución de las soluciones técnicas requeridas, así como de la captación de los destinatarios, que serán empresas y autónomos de la provincia de Badajoz con un número de empleados de hasta 50 trabajadores y siendo al **menos un mínimo de 80 empresas o autónomos** de municipios de menos de 20.000 habitantes.

El desarrollo del plan contempla las siguientes actuaciones a ejecutar por el adjudicatario:

- Confección de documentación inicial.
- Difusión y coordinación del proyecto.
- En el caso de que desde la convocatoria que se publique no resulte como interesados el número mínimo de empresas o autónomos de 160, el adjudicatario deberá localizar e implantar soluciones hasta completar el número de mínimo de 160.
- Confección de una memoria por cada empresa o autónomo participante con las soluciones implantadas con un contenido mínimo que se recoge en el **Anexo II** del presente pliego.

En definitiva, la empresa adjudicataria deberá garantizar que los servicios prestados cumplan con los estándares técnicos y operativos establecidos en este pliego.

A continuación, se detallan las especificaciones de cada uno de los servicios incluidos.

4.1. Diagnóstico Inicial.

El diagnóstico inicial tiene como objetivo evaluar el estado actual de la ciberseguridad en las empresas participantes, identificando vulnerabilidades, riesgos y áreas de mejora.

Así, se deberá realizar en cada empresa participante un análisis detallado del estado actual de ciberseguridad de las empresas participantes.

Este análisis será fundamental para diseñar e implementar las medidas necesarias que permitan mejorar la seguridad de los sistemas y datos de las empresas.

Con todo ello, se procederá a la identificación de vulnerabilidades, amenazas y riesgos asociados a sus sistemas de información y comunicaciones.

Finalmente, se elaborará un informe diagnóstico que contemple las medidas necesarias para mitigar los riesgos detectados.

La adjudicataria deberá utilizar herramientas especializadas de análisis de vulnerabilidades y generar reportes automáticos y manuales que permitan identificar amenazas activas. Además, se deberá realizar una entrevista inicial con los responsables de la empresa para complementar la información técnica con el contexto específico de la organización.

4.2. Instalación de Soluciones de Ciberseguridad.

La implementación deberá incluir las siguientes herramientas y medidas:

- Antivirus: Instalación de software de protección contra malware en todos los equipos de las empresas participantes.
- Firewall: Implantación de dispositivos físicos o soluciones software para proteger las redes corporativas.
- Autenticación Multifactor (MFA): Configuración de métodos de autenticación adicionales a las contraseñas, como códigos únicos o aplicaciones móviles.
- Copias de Seguridad Cloud: Configuración de soluciones de respaldo en la nube para garantizar la recuperación de datos en caso de incidentes.
  Las soluciones deberán cumplir con las especificaciones detalladas en este pliego técnico y estar alineadas con los principios del Esquema Nacional de Seguridad.

Estas medidas son las que se consideran mínimas, si bien deberán implementarse las siguientes medidas adicionales cuando se considere:

- Análisis de riesgos. Se deberá realizar un análisis de riesgos para identificar amenazas a las que está expuesta la empresa, evaluar el estado de ciberseguridad de la empresa y fortalecer los aspectos que necesiten mejora.
- Plan director de seguridad. Es necesario elaborar un plan director de seguridad que debe definir los objetivos de seguridad de la empresa, los recursos necesarios para alcanzarlos y los responsables de su ejecución.
- Plan de continuidad de negocio. En caso de sufrir un incidente de seguridad, es importante tener un plan de contingencia, que debe definir los pasos a seguir para dar una respuesta planificada ante cualquier suceso para minimizar su impacto y restaurar la actividad normal de la empresa lo antes posible.

4.3. Formación y Sensibilización.

La seguridad de la empresa depende del compromiso y conocimiento de todos. Por este motivo, hay que formar y sensibilizar a los empleados para que tengan buenas prácticas; reconozcan amenazas, como correos maliciosos, y utilicen contraseñas robustas.

Para ello, se desarrollarán al menos las siguientes actividades.

- Desarrollo de sesiones formativas dirigidas a responsables y empleados de las empresas participantes.
- Contenidos enfocados en buenas prácticas de ciberseguridad, detección de amenazas y uso adecuado de las herramientas implementadas.
- Entrega de materiales de formación en formato digital para consulta posterior.

4.4. Diagnóstico final.

Este apartado incluye:

- Realización de un análisis posterior a la instalación para evaluar la efectividad de las medidas implementadas.
- Validación de las mejoras logradas en la seguridad de los sistemas y datos.
- Elaboración de un informe de resultados para cada empresa participante y uno global para el proyecto.

El diagnóstico final tiene como objetivo evaluar la efectividad de las soluciones de ciberseguridad implementadas y validar las mejoras logradas en la protección de los sistemas y datos de las empresas participantes. Este diagnóstico permitirá demostrar el impacto del proyecto y proporcionar información clave para garantizar la sostenibilidad de las medidas adoptadas.

El diagnóstico final deberá realizarse mediante:

- Análisis de resultados cuantitativos: Utilizando herramientas de monitoreo y reportes generados por las soluciones implementadas.
- Auditoría: Verificación del estado de los sistemas y las prácticas de ciberseguridad de la empresa.
- Entrevistas finales: Reuniones con los responsables de las empresas para recabar información cualitativa sobre la percepción de las mejoras y la efectividad de las medidas adoptadas.

El diagnóstico final debe entregarse en formato digital y ser comprensible tanto para técnicos como para responsables no especializados en ciberseguridad y conforme al documento **Anexo II** del presente pliego.

4.5. Difusión de Resultados.

La difusión de los resultados es un componente esencial del proyecto, ya que permite comunicar los logros alcanzados, sensibilizar a más empresas sobre la importancia de la ciberseguridad y promover las buenas prácticas implementadas.

Este proceso contribuye a generar un impacto positivo más allá de las empresas beneficiarias directas, fomentando una mayor concienciación y fortaleciendo la cultura de la ciberseguridad en el tejido empresarial de la provincia.

La importancia de esta fase radica en los siguientes aspectos:

1. Transparencia y rendición de cuentas: La comunicación de los resultados garantiza que los interesados, incluidos los organismos financiadores y las empresas participantes, conozcan los beneficios obtenidos a través del proyecto.
2. Sensibilización de nuevas empresas: Al visibilizar los logros, se motiva a otras empresas y autónomos a adoptar medidas similares de ciberseguridad, ampliando el impacto del proyecto.
3. Posicionamiento regional: La difusión refuerza la imagen de la provincia de Badajoz como un referente en la promoción de la ciberseguridad entre pymes y autónomos.
4. Promoción de Buenas Prácticas: Compartir casos de éxito y lecciones aprendidas facilita la replicabilidad del modelo en otros contextos y sectores.

La difusión deberá realizarse en coordinación con la Cámara Oficial de Comercio, Industria y Servicios de Badajoz para garantizar la coherencia con los objetivos estratégicos del proyecto y asegurar el alcance a los públicos objetivo.

Teniendo en cuenta todo lo anterior, la difusión de resultados deberá incluir:

- Comunicación de los resultados obtenidos durante la ejecución del proyecto.
- Elaboración de materiales como informes públicos, presentaciones, artículos o notas de prensa, según las necesidades del proyecto.
- Organización de eventos informativos para dar a conocer el impacto del proyecto en la región.

5. ABONO DE LOS SERVICIOS.

Con carácter general la facturación de los servicios se realizará, previa remisión de las correspondientes facturas y aceptación de los trabajos realizados por la Cámara de Badajoz, de acuerdo al siguiente plan de facturación y relación de hitos establecidos:

La entidad adjudicataria recibirá un primer pago tras la firma del contrato correspondiente al 10% del importe de adjudicación, en base a los trabajos previos necesarios y preparatorios de la ejecución del contrato.

El resto de pagos se realizarán en función del número de soluciones implantadas, de conformidad con los siguientes hitos:

- HITO 1: El segundo pago, que se corresponderá con el 30% del precio de adjudicación, se realizará cuando se haya acreditado la implantación de soluciones en empresas o autónomos de, al menos, un número de 54.

- HITO 2: El tercer pago, que se corresponderá con el 30% del precio de adjudicación, se realizará cuando se haya acreditado la implantación de soluciones en empresas o autónomos de, al menos, un número de 108.

- HITO 3: El cuarto y último pago, que se corresponderá con el 30% restante del precio de adjudicación, se realizará cuando se haya acreditado la implantación de soluciones en empresas o autónomos de, al menos, un número de 160. En todo caso, este hito deberá estar cumplido antes del 30 de septiembre de 2025.

Con carácter general, el pago de los servicios objeto del presente contrato se realizará en el plazo de 30 días a contar desde la fecha de aprobación de la factura, mediante transferencia bancaria a la cuenta que la empresa comunique a la Cámara de Comercio de Badajoz al efecto.

6. OBLIGACIONES DE LA ENTIDAD ADJUDICATARIA.

La entidad adjudicataria será responsable de la correcta ejecución del proyecto, garantizando que los servicios y soluciones proporcionados cumplan con los requisitos establecidos en este pliego, siendo las siguientes las principales obligaciones.

6.1. Equipo de Trabajo.

La Cámara de Badajoz exigirá a la empresa adjudicataria la asignación de medios y organización necesarios para la correcta prestación del servicio.

Corresponde al adjudicatario la selección de los recursos humanos más adecuados para el cumplimiento del servicio y la disposición de un número suficiente para poder atender las necesidades del servicio, considerándose que el equipo mínimo el siguiente:

- Responsable del Proyecto:
    - o Experiencia demostrada de al menos 5 años en la gestión de proyectos similares relacionados con ciberseguridad.
    - o Habilidades de coordinación y comunicación para actuar como enlace principal con la Cámara de Comercio.
- Técnicos Especialistas en Ciberseguridad:
    - o Formación específica en ciberseguridad, redes y sistemas de información.
    - o Experiencia de al menos 5 años en la implementación de soluciones como antivirus, firewalls, autenticación multifactor y copias de seguridad en la nube.
- Formadores en Ciberseguridad:
    - o Capacitados para impartir formación a pymes y autónomos en buenas prácticas de ciberseguridad.
    - o Experiencia de al menos 5 años en la preparación de materiales didácticos y adaptados al nivel técnico del público objetivo.

- Soporte Técnico:
    - o Personal dedicado a resolver incidencias técnicas relacionadas con la implementación de las soluciones.
    - o Capacidad para realizar configuraciones avanzadas y ajustes personalizados en las herramientas instaladas.

Una misma persona puede ocupar distintos roles dentro del equipo.

En caso de que el personal fuera insuficiente para el cumplimiento de las prestaciones objeto del contrato, el adjudicatario deberá aumentarlo en número suficiente para dar la atención debida al servicio.

En caso de enfermedad, vacaciones y bajas de los trabajadores, la empresa adjudicataria estará obligada a garantizar el correcto cumplimiento de las obligaciones contempladas en el pliego, debiendo proceder a la correspondiente sustitución con personal que reúna los perfiles exigidos.

Las entidades licitadoras deberán presentar en su oferta técnica una descripción completa del equipo de trabajo propuesto.

El adjudicatario no podrá sustituir el personal adscrito a la realización de los trabajos sin la autorización expresa del encargado del contrato.

6.2. Búsqueda y selección de empresas participantes.

- Difundir la convocatoria utilizando los medios más efectivos, asumiendo los costes asociados.
- Verificar que las empresas participantes cumplen con los requisitos establecidos.
- Gestionar la documentación administrativa necesaria para formalizar la inscripción de las empresas beneficiarias.

6.3. Prestación de Servicios de Ciberseguridad.

- Realizar el diagnóstico inicial para identificar vulnerabilidades y necesidades.
- Implantar las soluciones de ciberseguridad especificadas, asegurando su correcto funcionamiento.
- Proporcionar formación y sensibilización a los responsables y empleados de las empresas beneficiarias.
- Realizar el diagnóstico final para evaluar los resultados e impacto del proyecto.

6.4. Cumplimiento del Decálogo de Ciberseguridad del INCIBE.

Garantizar que las medidas implementadas cumplen con las recomendaciones del Decálogo de Ciberseguridad, priorizando las más relevantes.

6.5. Generación de Informes.

- Elaborar y entregar informes en cada fase del proyecto:
    - o Informes de diagnóstico inicial.
    - o Documentación de las soluciones instaladas.

o Informes de diagnóstico final y evaluación de resultados, conforme al documento Anexo II del presente pliego.

6.6. Comunicación y coordinación.

- Participar en reuniones periódicas de seguimiento y supervisión con la Cámara de Comercio.
- Designar un responsable que actúe como enlace principal.
- Informar de cualquier incidencia o desviación en la ejecución del proyecto.

6.7. Difusión de resultados.

- Comunicar los logros alcanzados mediante informes públicos, eventos y publicaciones digitales.
- Coordinar las actividades de difusión con la Cámara de Comercio para garantizar coherencia y alcance.

7. RESOLUCIÓN DE INCIDENCIAS.

La entidad adjudicataria deberá garantizar un procedimiento claro y eficiente para la gestión y resolución de incidencias que puedan surgir durante la ejecución del proyecto. Este procedimiento tiene como objetivo minimizar los impactos negativos en la calidad del servicio, garantizar la continuidad de las actividades y mantener la confianza de las empresas participantes.

Se considerará una incidencia cualquier situación que impida o dificulte el desarrollo normal de las actividades relacionadas con el proyecto. Esto incluye, pero no se limita a:

- Fallos técnicos en las soluciones implementadas.
- Retrasos en la ejecución de actividades según los plazos establecidos.
- Problemas en la comunicación o coordinación con las empresas participantes o con la Cámara de Comercio.
- Dudas o reclamaciones de las empresas beneficiarias relacionadas con el servicio prestado.

Las entidades licitadoras deberán presentar en su oferta técnica una descripción completa del procedimiento para la resolución de incidencias.

La entidad adjudicataria será responsable de garantizar la resolución efectiva de todas las incidencias dentro de los plazos establecidos.

El responsable del proyecto designado por la adjudicataria actuará como punto de contacto principal para la gestión de incidencias.

8. CONTROL Y SEGUIMIENTO.

Para el control y seguimiento de los servicios contratados, la Cámara de Badajoz podrá establecer las instrucciones y orientaciones que estime pertinentes para la correcta

realización del objeto del contrato, y convocar cuantas reuniones técnicas y de seguimiento sean necesarias para su correcto desarrollo.

A tales efectos la Cámara de Badajoz designará a un responsable del contrato encargado, entre otras cosas, de velar por la ejecución de los servicios solicitados y ofertados por el adjudicatario en su totalidad, así como por la calidad de los mismos.

El adjudicatario designará un responsable del servicio como principal interlocutor de la Cámara de Badajoz para el seguimiento, control y evaluación continua de los servicios prestados, y con competencias para la resolución de cualquier tipo de disputa o discrepancia en la prestación del servicio.

El responsable del servicio por parte del adjudicatario asistirá a cuantas reuniones puedan ser fijadas por la Cámara de Badajoz para el seguimiento, control y evaluación de los servicios prestados.

9. CONFIDENCIALIDAD Y DEBER DE SIGILO. DATOS DE CARÁCTER PERSONAL.

La entidad adjudicataria y el personal encargado de la realización de tareas propias de la adjudicación, guardarán secreto profesional sobre todas las informaciones, documentos y asuntos a los que tenga acceso o conocimiento durante la vigencia del contrato, estando obligados a no hacer públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo contractual.

El resultado de las tareas realizadas a lo largo del contrato, así como el soporte utilizado (papel, fichas, etc.) serán propiedad de la Cámara.

La información y documentación obtenidas por la entidad adjudicataria con ocasión de la ejecución del contrato, que son propiedad de la Cámara, deberán ser diligentemente conservadas por la entidad adjudicataria desde que las reciba y sólo podrán ser utilizadas a los meros efectos del cumplimiento del contrato, quedando prohibidos cualquier otro uso, la conservación de copias y la cesión, total o parcial, a terceros.

Si la entidad adjudicataria aporta equipos informáticos una vez finalizadas las tareas y antes de retirar dichos equipos, deberá borrar toda información utilizada, o derivada de la ejecución del contrato. De la misma manera, deberá borrar la información de los equipos utilizados para la ejecución del contrato. La destrucción, en su caso, de la documentación de apoyo que no se considere indispensable se realizará en máquina destructora de papel o cualquier otro medio que garantice su ilegibilidad, en el lugar donde se realicen los trabajos.

La entidad adjudicataria se compromete a no dar información y datos proporcionados por la Cámara para cualquier uso no previsto en el presente pliego. En particular, no proporcionará sin autorización expresa de Cámara, copia de los documentos o datos a terceros.

La entidad adjudicataria seleccionada declarará documentalmente que se responsabiliza de que el tratamiento de datos de carácter personal que se pueda realizar se hará con absoluto respeto de las normas de seguridad, de acuerdo con lo establecido en el Reglamento 2016/679 (UE) general de protección de datos personales, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y demás normativa de aplicación en vigor en materia de protección de datos y será, asimismo, de

aplicación la Disposición adicional vigésimo quinta de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público. En caso de incumplimiento de lo estipulado, la entidad contratante y el personal asignado al proyecto serán responsables de las infracciones que deriven de él.

Los datos personales que la persona licitante o la persona adjudicataria facilite para la participación en el presente procedimiento de contratación y, en su caso, para el adecuado desarrollo del contrato, serán tratados, en su condición de responsable, por la persona titular de la Cámara.

La legitimación para el tratamiento de los datos es el cumplimiento de una misión realizada en interés público o en el ejercicio de poder públicos conferidos al responsable del tratamiento, y conforme a la LCSP.

Los datos personales proporcionados por el licitante o adjudicatario serán tratados con la finalidad de llevar a cabo la tramitación general de la contratación y el desarrollo de las prestaciones derivadas de la misma, por lo que se conservarán mientras sean necesarios para dichas finalidades y, en todo caso, durante los plazos establecidos por la legislación vigente.

10. PROPIEDAD INTELECTUAL E INDUSTRIAL.

Todos los datos e información manejados por el adjudicatario a causa del desarrollo de su actividad, incluyendo los soportes físicos o digitales que utilice y en los que deposite la información relacionada con los servicios objeto del presente contrato, serán propiedad del órgano contratante, sin que el adjudicatario pueda conservar copia o utilizarlos con fin distinto al que figura en el presente contrato. La Cámara se reserva todas las facultades inherentes a este derecho, pudiendo reproducirlos, publicarlos o divulgarlos parcialmente o en su totalidad, en la medida que le sea conveniente y adecuado, sin que pueda oponerse por ello la empresa adjudicataria alegando derechos de autor.

El adjudicatario no podrá hacer uso del nombre, marca o logotipos facilitados por la administración contratante fuera del cumplimiento de las obligaciones dimanantes del presente contrato, ni de las circunstancias y para los fines expresamente pactados en este, ni una vez terminada la vigencia del contrato.

En Badajoz, a 21 de enero de 2025.

08820610H FRUCTUOSO DELGADO (C:Q0673001D)

Firmado digitalmente por 08820610H FRUCTUOSO DELGADO (C:Q0673001D)
Fecha: 2025.01.21 11:14:24 +01'00'

Fdo.: Fructuoso Delgado Viñals
Secretario General