SERVICIO DE ASESORAMIENTO JURÍDICO-TÉCNICO PARA LA GESTIÓN, MONITORIZACIÓN DE LAS DIFERENTES BASES DE DATOS DE LA EMPRESA, INCLUYENDO REVISIÓN, EVALUACIÓN Y AUDITORIA DEL TRATAMIENTO DE DATOS AL AMPARO DE LA LEY ORGANICA 3/2018 DE 5 DE DICIEMBRE DE PROTECCIÓN DE DATOS (2024-2027).

1. NORMATIVA

PROTECCIÓN DE DATOS PERSONALES

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos –RGPD-, establece las condiciones en las que las organizaciones (incluida la Administración) pueden tratar datos personales y las garantías para las personas interesadas. Esta normativa plantea nuevos derechos, ámbitos para el tratamiento y busca una mayor implicación de los responsables de los tratamientos en la seguridad de los datos.

Por su parte, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales –LOPD_GDG- desarrolla el RGPD en varios aspectos e incluye la protección de derechos de las personas en el ámbito de Internet.

SEGURIDAD EN EL ÁMBITO DE LA ADMINISTRACIÓN ELECTRÓNICA

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, estableció la necesidad de crear un Esquema Nacional de Seguridad, desarrollado por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Una vez derogada, la posterior Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, recoge el Esquema Nacional de Seguridad en su artículo 156 apartado 2 en similares términos, con el objeto de determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos a los que se refiere la citada ley de cara a establecer la confianza de la sociedad en el desarrollo de la administración electrónica y uso de herramientas informáticas en la administración. Y más recientemente modificada por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Esta ley incorpora igualmente previsiones sobre gestión de la información, así como del acceso a la misma por parte de los entes del sector público, del que forma parte la empresa BIDEGI.

Se trata de valorar también en el marco del contrato junto con la Diputación Foral de Gipuzkoa como órgano administrativo que encarga el servicio, las posibilidades de participación de BIDEGI en este ámbito, y las características del mismo.

2. OBJETO DEL CONTRATO

El objeto del contrato es la prestación del servicio de asesoramiento jurídico-técnico para la implantación, refuerzo y gestión, así como monitorización de las bases de datos de la empresa, tanto en el ámbito BackOffice como en el ámbito Front Office, incluyendo la revisión, evaluación y auditoría de sistemas de información de la empresa y los servicios que se definen en la legislación citada en la Normativa precitada.

Las dos normas se orientan a la seguridad de la información y los servicios: en el primer caso centrándose en la protección de los datos personales como vía de proteger los derechos y libertades fundamentales de las personas, y en el segundo caso, orientada a asegurar las operaciones de la administración en el uso de medios electrónicos y, por tanto, dando confianza en su uso.

Aunque los objetos de estas normas no son totalmente coincidentes, es habitual que una gran parte de los sistemas de información que soportan servicios de la Administración traten datos personales; y que la mayor parte de los datos personales que trata la Administración lo son en el ámbito de servicios y obligaciones propias de la Administración. La coincidencia es alta.

Por otro lado, del análisis de ambas legislaciones se deduce que buena parte de las tareas necesarias para una correcta gestión de la seguridad coinciden en ambas. La identificación de tratamientos de datos personales tiene mucha relación con la identificación de servicios e información. Los roles y responsabilidades relacionadas con el tratamiento o servicios son en muchos casos coincidentes. En ambos casos es necesario regular y gestionar los riesgos asociados a la subcontratación de partes del servicio o encargos de tratamiento a terceros. Otras tareas, como la gestión de las incidencias, el control de acceso a la información, etc. son algunos de los puntos en los que hay gran coincidencia.

Es por ello que se ha considerado necesario acumular la realización de todo ello en un único proyecto.

3. TAREAS A REALIZAR

Las tareas a contratar se dividen en las siguientes:

A. **ADECUACIÓN A NORMATIVA: SERVICIO RGPD:** servicio de asesoramiento jurídico-técnico para la implantación, refuerzo y gestión, así como monitorización de las bases de datos de la empresa, tanto en el ámbito back-office como en el ámbito front-office, incluyendo la revisión, evaluación y auditoría de sistemas de información de la empresa y los servicios que se definen en la legislación citada en la Normativa precitada

B. **SERVICIO RGPD+LOPDGDD**

FINALIDAD PRINCIPAL: La entidad precisa adaptar su sistema de gestión de seguridad en materia de protección de datos personales.

Consistirá en implantar las medidas necesarias para adecuar sus tratamientos de datos personales a los requisitos del RGPD y la LOPDGDG.

La Entidad deberá designar los interlocutores que participarán en esta fase para las tareas de coordinación con la Adjudicataria y que asumirán las tareas de planificación y seguimiento de la adecuación, así como la interlocución con los responsables de servicios, encargados de la seguridad, delegado de protección si lo tuviera y otros que consideren necesarios.

Las tareas consistirán en:

1. Planificación y control del proyecto

La adjudicataria deberá proponer y acordar con los interlocutores designados una planificación de las tareas de adecuación para la Entidad.
La planificación incluirá el cronograma con las diferentes fases a acometer, entregables en cada fase, hitos de seguimiento y cualquier otro elemento que considere adecuado.
La adjudicataria elaborará y facilitará a la Entidad informes de seguimiento en los hitos de seguimiento planificados, con los detalles del avance de la implantación.

2. **Designación de un Delegado de Protección de Datos**

Las organizaciones públicas deben incorporar un DPD.

En el supuesto en que a lo largo del contrato se designará un DPD por parte de la entidad, se valorará como mejora que la adjudicataria preste el servicio de asesoramiento externo.

La persona designada participará en cumplimiento de sus funciones en la fase de adecuación de la Entidad.

3. **Análisis de tratamientos y elaboración del Registro de actividades de tratamiento**

Partiendo de los tratamientos descritos actualmente, los Ficheros anteriormente registrados por la Entidad, así como la información que aporten los interlocutores, se identificarán y analizarán los tratamientos y flujos de datos personales de la Entidad y se elaborará el Registro adecuado a la Entidad según lo requerido.

4. **Análisis de riesgos**

La Adjudicataria analizará junto con la Entidad los riesgos en los tratamientos. Como resultado, se obtendrá información relativa a qué riesgos afectan a los tratamientos, de cara a establecer un plan de mejora o de reducción de riesgos.

En este análisis se revisarán procesos internos tales como

- El diseño de los tratamientos, de manera que se asegure la protección de los datos. Esto incluye aspectos como medios técnicos y humanos que intervienen en el tratamiento, procedimientos de trabajo, intercambios.
- Los procedimientos de ejercicio de derechos de interesados.
- Riesgos en infraestructuras TIC que soportan los tratamientos.
- Los procedimientos para detectar y gestionar incidencias de seguridad, identificar las que puedan producir fugas de información y las obligaciones al respecto.
- Las condiciones de contratación a terceros, cuando implican acceso o tratamiento de los datos personales.
- Posibles transferencias internacionales de datos y sus condiciones.
- Las medidas de seguridad existentes.

Como resultado, se obtendrá un informe detallando qué riesgos afectan a los tratamientos, de cara a establecer un plan de mejora o de reducción de riesgos.

Para la realización del análisis de riesgos, se priorizarán las adjudicatarias que dispongan de una herramienta propia para la gestión del riesgo. En todo caso, la herramienta para la realización de este análisis debe ser

compatible con las exigencias e informes tipo elaborados como modelo por la Agencia Española de Protección de Datos.

5. **Evaluaciones de Impacto**

La adjudicataria elaborará el estudio de los tratamientos para determinar si es necesario realizar la evaluación de impacto en la privacidad.

En el caso que se detecte que alguno de los tratamientos de datos personales genera un alto riesgo para los derechos y libertades de los interesados, se debe elaborar una evaluación de impacto relativa a la protección de datos para cada uno de ellos.

En caso negativo, se redactará y registrará la justificación de la no necesidad de evaluación de impacto.

En todo caso, para la realización del procedimiento de evaluación de impacto, se priorizarán las empresas que dispongan de una herramienta propia para la gestión del riesgo. En todo caso, la herramienta para la realización de este análisis debe ser compatible con las exigencias e informes tipo elaborados como modelo por la Agencia Española de Protección de Datos.

6. **Procedimientos de ejercicio de derechos**

La adjudicataria asesorará a la Entidad en el establecimiento de mecanismos visibles, accesibles y sencillos, incluidos los medios electrónicos, para el ejercicio de derechos y en el establecimiento de procedimientos que permitan responder a los ejercicios de derechos en los plazos previstos.

7. **Plan de mejora**

La adjudicataria elaborará un Plan de mejora para la Entidad. En este Plan, deben priorizarse las medidas orientadas a mitigar riesgos en tratamientos que conlleven un mayor riesgo de lesionar derechos y las libertades de los interesados, en función de la sensibilidad de los datos, del ámbito en que se realiza el tratamiento y del volumen de datos tratados.

El Plan recogerá, al menos:

- Criterios o decisiones a adoptar por la Entidad necesarios para el Registro de tratamientos. Por ejemplo, decisiones relativas a la legitimidad de los tratamientos, identificación de la legislación que justifique el tratamiento, de los criterios o plazos de supresión; necesidades de recabar consentimientos para tratamientos donde no se haya conservado esta información, etc. Este tipo de actuaciones por parte de la Entidad se incluirán en el Plan como tareas detalladas dentro del Plan de mejora.

- Diseño de las modificaciones necesarias en los tratamientos existentes, allá donde se detecten riesgos o carencias.
- Modificaciones necesarias en los procedimientos de ejercicio de derechos, cláusulas de información, plazos o formas de ejercer derechos, notificaciones, etc.
- Modificaciones en los procedimientos de gestión de incidencias y notificación de brechas.
- Modificaciones en las condiciones de contratación de proveedores.
- Modificaciones en las condiciones para la realización de transferencias internacionales.
- Diseño de otras medidas de seguridad tanto técnicas como organizativas que eviten la pérdida de información, la destrucción involuntaria de datos o el acceso de un tercero no autorizado, y que a su vez garanticen la integridad, la disponibilidad y la inalterabilidad de los datos tratados.
- Actuaciones referidas a proveedoras de servicio encargadas de tratamiento.
- Identificar las operaciones relacionadas con los fines del tratamiento individualizando los factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados a la finalidad principal.
- Análisis de las circunstancias del tratamiento de datos ante la participación de distintos responsables y/o encargados de tratamiento de datos personales vinculados a la gestión viaria competencia de BIDEGI.
- Explotación del mapa de tránsitos de las vías competencia de Bidegi para el desarrollo e implantación de procesos de análisis del uso de las infraestructuras que permita el desarrollo e implantación de políticas públicas.
- Criterios o decisiones a adoptar por la Entidad necesarios para el Registro de tratamientos. Por ejemplo, decisiones relativas a la legitimidad de los tratamientos, identificación de la legislación que justifique el tratamiento, de los criterios o plazos de supresión; necesidades de recabar consentimientos para tratamientos donde no se haya conservado esta información, etc. Este tipo de actuaciones por parte de la Entidad se incluirán en el Plan como tareas detalladas dentro del Plan de mejora.
- Diseño de las modificaciones necesarias en los tratamientos existentes, allá donde se detecten riesgos o carencias.
- Modificaciones necesarias en los procedimientos de ejercicio de derechos, cláusulas de información, plazos o formas de ejercer derechos, notificaciones, etc
- Modificaciones en los procedimientos de gestión de incidencias y notificación de brechas.
- Modificaciones en las condiciones de contratación de proveedores. Modificaciones en las condiciones para la realización de transferencias internacionales

- Diseño de otras medidas de seguridad tanto técnicas como organizativas que eviten la pérdida de información, la destrucción involuntaria de datos o el acceso de un tercero no autorizado, y que a su vez garanticen la integridad, la disponibilidad y la inalterabilidad de los datos tratados.
- Valorar si la principal encargada de tratamiento, Bidelan, en tanto proveedora principal de servicios ofrece garantías de cumplimiento de la normativa de protección de datos, por medio de la realización de una auditoría de cumplimiento normativo a los meros efectos de identificar aspectos de mejora.
- Efectuar análisis de riesgos de los tratamientos de datos personales llevados a cabo por BIDELAN. Como resultado, se obtendrá información relativa a qué riesgos afectan a los tratamientos, de cara a establecer un plan de mejora o de reducción de riesgos, así como para la revisión de las medidas de seguridad en función del análisis de riesgos realizado, obteniendo un listado de medidas y garantías que podrían adoptarse para gestionar el riesgo afrontando las peculiaridades concretas de su tratamiento.
- Identificar las operaciones relacionadas con los fines del tratamiento individualizando los factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal de la recogida de datos.
- Identificar en cada tratamiento los tipos de datos utilizados individualizando los factores de riesgo relacionados con el ámbito del tratamiento que se derivan de los datos recogidos, procesados o inferidos en el tratamiento.
- Identificar la extensión y alcance del tratamiento individualizando los factores de riesgo relacionados con el ámbito del tratamiento relativos al número de sujetos afectados, la diversidad de datos o aspectos tratados, la duración en el tiempo, el volumen de datos, la extensión geográfica, la exhaustividad sobre la persona o la frecuencia de recogida.
- Identificar las categorías de interesados individualizando los factores de riesgo relacionados con el ámbito del tratamiento relativos a la categoría de interesados, como personas usuarias de las infraestructuras o personal empleado y de subcontratas.
- Identificar los factores de riesgo que se derivan de la naturaleza del tratamiento al implementarse con determinadas características técnicas o tecnológicas.
- Identificar los factores de riesgo que se derivan en la recogida y generación de datos de la naturaleza del tratamiento al recogerse o generarse datos de forma específica. Identificar los factores de riesgo que se derivan del contexto del tratamiento al poder generarse consecuencias no contempladas en los propósitos originales previstos del tratamiento, evaluando la probabilidad de que estas amenazas se materialicen en su tratamiento y determinar el nivel de riesgo.

- Identificar los factores de riesgo que se derivan del contexto específico del sector de actividad, modelo de negocio o tipo de entidad
- Identificar factores de riesgo que se derivan del contexto en el que se realizan las comunicaciones de datos a terceros en el marco del tratamiento.
- Identificar los factores de riesgo que se derivan de la seguridad de los tratamientos y de la posible materialización de brechas de seguridad sobre los datos personales.
- Valoración del riesgo intrínseco y del riesgo residual como consecuencia de los factores de riesgo apreciados y concurrentes en la gestión de datos personales por la organización.
- Análisis para la implementación de sistemas automáticos de registro de incidencias en el tratamiento de los datos personales que se incluyen en las comunicaciones electrónicas de la empresa.
- Aplicar la gestión del riesgo a BIDEGI permitiendo su gestión con medidas de privacidad específicas para cada factor de riesgo específico identificado, medidas para la gestión de brechas de datos personales y seguridad, y medidas organizativas y políticas de protección de datos. Documentar las evaluaciones de idoneidad, necesidad y proporcionalidad, asociando una gestión de riesgo respecto de cada tratamiento de datos personales de forma individualizada.
- Identificar herramientas seguras de colaboración entre personal empleado y con clientes o personas usuarias y otras organizaciones, así como dispositivos comprometidos en la red interna.
- Elaborar un sistema de gobernanza de los datos para gestionar de forma efectiva y eficiente la información en la entidad, de modo que se gestione de forma centralizada e integrada que dé coherencia a los distintos repositorios de datos o los sistemas en los que se recogen como requisito el aseguramiento de la calidad de los datos, como resultado del análisis de las circunstancias del tratamiento de datos ante la participación de distintos responsables y/o encargados de tratamiento de datos personales vinculados a la gestión viaria competencia de BIDEGI. Este sistema permite cumplir con los principios de protección de datos (licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad y responsabilidad proactiva), garantizar que los interesados puedan ejercer sus derechos (derecho de acceso, rectificación, supresión (‘derecho al olvido’), limitación del tratamiento, notificación, portabilidad de los datos, oposición, y sobre decisiones individuales automatizadas y garantizar la protección de la protección de los datos personales desde el diseño y por defecto, mediante una gestión del riesgo para los derechos y libertades.
- Cumplir con los restantes requisitos y obligaciones legales impuestos por la normativa de protección de datos. Optimizar la información

mediante la explotación del mapa de tránsitos de personas usuarias de las vías competencia de Bidegi para el desarrollo e implantación de procesos de análisis de la acción contenida en el backoffice obteniendo mediante el análisis de estos datos una información más adaptada y actualizada en tiempo real del uso de las infraestructuras que permita el desarrollo e implantación de políticas públicas.

8. **Acreditar el cumplimiento**

La adjudicataria entregará a la Entidad un expediente final que le permita demostrar que los tratamientos de datos personales se realizan cumpliendo con la normativa y se aplican las medidas técnicas y organizativas correspondientes.

El expediente deberá contener al menos los siguientes elementos:

Documentación y Procedimientos de seguridad:

- Guía general de cumplimiento normativo para la entidad:
- Anexos para acreditar el cumplimiento del principio de responsabilidad proactiva.
- Análisis de riesgos: documentación de la metodología.
- Evaluaciones de impacto sobre la privacidad: documentación de la metodología utilizada.
- Procedimientos relativos al cumplimiento de derechos
    - documentos de información al interesado,
    - modelos donde se recabe el consentimiento de los interesados, así como modelos de información en el caso de que la base de legitimación sea distinta al consentimiento.
    - procedimientos para el ejercicio de los derechos de las personas (acceso, rectificación, oposición, etc.).
- Modelos de contratos con los encargados del tratamiento aplicables en las contrataciones.
- Procedimiento de gestión de incidencias
- Procedimiento de control de acceso a la información.

Registros

- Registro de actividad del tratamiento, según normativa.
- Análisis de riesgos: resultados.
- Evaluaciones de impacto sobre la privacidad: resultados de la evaluación incluida la justificación de la no necesidad de evaluación para ciertos tratamientos.
- Documentación de posibles transferencias internacionales de datos y en su caso, modelos de legitimación de estas transferencias.
- Modelo de Registro de incidencias.
- Modelo de Registro de control de acceso a la información.

- Modelo de Registro de registro de solicitudes de ejercicio de derechos de personas interesadas.
- Documentación de apoyo a la formación en la Entidad, además de la realización de la formación específica.
    - A los roles con responsabilidad en los Servicios/Tratamientos
    - A todo el personal de la Entidad.

9. Sesión formativa

La adjudicataria llevará a cabo como mejoras, sesiones formativas dirigidas al personal de la Entidad y orientadas a la formación y concienciación en los principios del Reglamento en lo relativo al tratamiento de datos.

Se deberá proponer un programa formativo, incluyendo los contenidos formativos.

10. Asesoramiento al Responsable del Tratamiento.

En el marco del contrato, la empresa adjudicataria deberá dotar al servicio de un número mínimo anual de 20 horas de asesoramiento y elaboración de informes a demanda, en el caso de que se planteen supuestos específicos, nuevos proyectos o áreas de desarrollo de la empresa que supongan la necesidad de consulta a la empresa adjudicataria.

11. La empresa adjudicataria realizará anualmente auditorías totales o parciales de la organización, en el marco del contrato.

C. SERVICIO ASESORAMIENTO A LA PERSONA DELEGADA DE PROTECCIÓN DE DATOS INTERNA DE LA EMPRESA.

Se prevé para el supuesto de que la Entidad designe una persona como Delegada de Protección de Datos, la prestación del servicio de asesoramiento externo a esta persona.

Este servicio consistirá en prestar a la Entidad el servicio de asesoramiento a la persona Delegada de Protección de Datos, que tendrá las competencias y responsabilidades que la normativa (RGPD/LOPDGDD) asigna a este rol.

La empresa adjudicataria deberá elaborar un programa de trabajo, tareas por periodos, así como los planes de revisión / actualización que obliga la normativa.

El servicio se prestará desde el momento en que la empresa cuente con Delegado de Protección de Datos.

Para una gestión y coordinación adecuada de los datos personales de la organización, es necesaria la creación de la figura del Delegado de Protección de Datos (DPD) interno de la organización.

El DPD tiene como objetivos la información, la supervisión del cumplimiento, el asesoramiento y la cooperación respecto del cumplimiento de la normativa de protección de datos.

Funciones:

Se deberá desarrollar el asesoramiento suficiente para el desempeño por el DPD interno de las funciones definidas en el Art. 39 del RGPD:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, de las obligaciones del RPGD y demás normativa aplicable en protección de datos.
- Supervisar el cumplimiento del RGPD y demás normativa aplicable en protección de datos, y de las políticas del responsable o encargado del tratamiento en dicha materia, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al Art. 35 del RGPD.
- Cooperar con la autoridad de control. Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa del artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.
- Participar en las decisiones relativas al diseño de los tratamientos de datos personales, en lo que al cumplimiento del Reglamento se refiere.

Resultados:

Como resultado del cumplimiento de sus funciones, el servicio de asesoramiento externo entregará a la persona Delegada de Protección de Datos interna de la Entidad:

- Por cada actuación realizada, un informe que contenga, al menos, el objeto de la actuación (consulta de la Entidad, reclamación de persona interesada, de una agencia de control, incidencia, etc.), descripción del asunto tratado, las conclusiones y su fundamento. Se adjuntará cualquier otra información relevante que se haya utilizado durante la actuación.

  Si durante la actuación, fuera necesario que la empresa externa accediera a datos de personas interesadas, una vez finalizada la actuación destruirá toda la información que le haya sido entregada (salvo referencias que

pueda haber en el informe entregado). La Entidad será responsable de conservar la información que sea necesaria.

- Mensualmente se presentará un informe sumario con las actuaciones solicitadas, finalizadas y pendientes, manteniendo en todo momento el cronograma con actuaciones planificadas, pendientes o ejecutadas actualizado y a disposición de la entidad.

Para la prestación del servicio de asesoramiento al DPD se deben dar unas condiciones mínimas que garanticen el éxito de sus funciones.

- La Entidad facilitará al servicio externo el apoyo activo en su labor desde el máximo órgano de decisión, de manera que tenga capacidad suficiente para requerir la información y para promover las acciones de corrección necesarias en el ámbito de su actuación.
- La Entidad realizará la comunicación oficial de la designación del DPD a todo el personal para garantizar que su existencia y función se conozcan dentro de la organización, siendo la empresa externa la encargada de gestionar los asuntos que lleguen al DPD, realizar los informes correspondientes y en general, llevar todos los asuntos que afecten el DPD interno en materia de gestión y tratamiento de información.

- La Entidad facilitará el acceso a las áreas o departamentos necesarios (recursos humanos, departamento jurídico, TI, seguridad, etc.) de modo que la empresa adjudicataria pueda recibir apoyo esencial, aportaciones e información de dichos servicios en el ámbito del cumplimiento de sus funciones.

- La Entidad facilitará que se formará adecuadamente al Delegado de Protección de Datos interno para que tenga capacidad de intervenir en el diseño y supervisión de los tratamientos de datos, de modo que pueda aportar sus recomendaciones orientadas a garantizar el cumplimiento.

A modo de resumen, se establecen los siguientes criterios de cumplimiento para la empresa adjudicataria.

La empresa adjudicataria deberá cumplir al menos con las siguientes horas dedicadas a cada uno de los bloques de trabajo:

Bloque A: 50 horas.
Bloque B: 275 horas.
Bloque C: 20 horas.

Total de horas anuales a dedicar al proyecto: 345 horas.

La empresa adjudicataria deberá presentar en su propuesta una planificación del reparto de tareas y dedicación horaria a cada apartado de la misma.

4. CONDICIONES GENERALES

La empresa adjudicataria dedicará a la prestación del servicio los medios humanos y materiales necesarios para su correcta ejecución de acuerdo a las especificaciones establecidas en este pliego, sin que se determine una dedicación mínima o máxima para el servicio.

En la propuesta metodológica se valorará el diseño de un esquema de adecuación general de la Entidad, aportando un cronograma de actuaciones, que abarque periodos anuales y que integre las distintas actuaciones planificadas.

La empresa adjudicataria deberá contar como mínimo con el siguiente perfil profesional, que deberá ser la persona responsable del proyecto, atendiendo en todo momento de forma directa y personal los requerimientos que se le hagan, siendo permanentemente la persona de contacto y realizando las actividades previstas en el contrato de forma personal, aun con asistencia del equipo que se considere oportuno.

La persona responsable de la empresa adjudicataria deberá contar con al menos siete años de experiencia en la materia, habiendo sido responsable directo de auditorías en el sector público vasco, debiendo acreditar al menos 10 proyectos de características similares al objeto de este contrato. Se valorará conocer específicamente el ámbito de la Administración Electrónica. Las empresas que liciten a este contrato deberán contar con dos personas en su plantilla que cubran estos requisitos, debiendo acreditarlo en el momento en que se les solicite, y mantenerlos adscritos al proyecto a lo largo de la duración del mismo.

Servicios a demanda.

La Entidad podrá solicitar y se encontrarán dentro de la ejecución del contrato, asesoramientos a demanda en áreas vinculadas al contrato, en todo momento, debiendo realizarse este asesoramiento en un plazo no superior a 72 horas. En el caso de que sea preciso un tiempo superior, deberá ponerse en conocimiento de la Entidad este extremo, para que sea autorizado por la Entidad.

El servicio se prestará desde las instalaciones de la empresa adjudicataria, salvo cuando deban hacerse entrevistas con las personas relacionadas, tareas de campo orientadas a analizar la situación de las entidades, entrevistas con el personal de las entidades o reuniones o presentaciones a las sedes de las entidades. La empresa adjudicataria deberá realizar al menos el 30 % de las horas asignadas en la sede de la Entidad, en su sede de Zarauz.

El material escrito a entregar deberá estar redactado en euskera y castellano. Se facilitará al menos una copia en papel y una copia electrónica en formato electrónico y editable.

Cuando la naturaleza del contenido lo permita (inventarios y registros, listados...) se entregarán formatos estructurados (hoja de cálculo, base de datos, …) en lugar de documentos de texto, de cara a facilitar su manejo e integración con otras aplicaciones.

El personal a cargo de las tareas de Adecuación y de prestar el servicio de Delegado de Protección de Datos deberá tener capacidad de comunicarse en euskera y castellano.

Se constituirá una Comisión de Seguimiento del Proyecto, compuesta por personal técnico de la empresa y los socios de la empresa adjudicataria asignados al proyecto, con las siguientes tareas:

- Control y seguimiento de la planificación del proyecto con la adjudicataria.
- Control y seguimiento de la ejecución de las tareas y de los materiales entregados.
- Control y seguimiento de las consultas realizadas y su resolución.
- Elaborar informes y estadísticas generales, orientadas a dar a conocer el grado de implantación de la normativa en la empresa.

5. MEJORAS QUE SE VALORARÁN EN LA ADJUDICACIÓN DEL CONTRATO.

1. Tiempo de respuesta.

En el caso de que surja alguna necesidad urgente (incidencia u otras) por parte de la empresa, se valorará favorablemente que el socio adscrito al proyecto pueda personarse en las instalaciones de BIDEGI en Zarauz en un plazo máximo de treinta minutos con la finalidad de coordinar su resolución.

2. Formación del personal:

Se valorará haber participado o dirigido publicaciones y / o investigaciones del sector que acrediten conocimiento específico de la materia. SE valorará igualmente la participación en proyectos universitarios docentes, así como la experiencia docente específica en niveles universitarios.

6. PRECIO.

Valoración del contrato: 25.000,00 euros anuales; 100.000,00 euros en valoración total.

Horas de socio senior: 90 euros por hora, 121 horas: 10.890,00 euros
Horas de técnico: 60 euros por hora, 210 horas: 12.600,00 euros
Horas de personal administrativo: 30 euros por hora, 50 horas: 1500,00 euros

Valor total del contrato anual: 25.000,00 €.

Las empresas licitadoras que opten al contrato deberán justificar su precio por hora, debiéndose computar el precio total ofertado a los efectos de la adjudicación del contrato.

Gipuzkoako Azpiegituren Agentzia
Agencia Guipuzcoana de Infraestructuras
IFK: A-20783023
Asti auzoa, 631 - A- 20800 Zarautz

JUAN PABLO MEDRANO OLMEÑO
2023/12/19

Responsable Asesoría Jurídica de Bidegi, S.A.