PLIEGO DE BASES TÉCNICAS

CONTRATACIÓN DE UN SERVICIO CUYO OBJETO ES EL DESARROLLO DE UNA METODOLOGÍA PARA LA GESTIÓN DE LOS RIESGOS EN EL CUMPLIMIENTO NORMATIVO DE PROTECCIÓN DE DATOS PERSONALES PARA SU USO POR PARTE DE LA ADMINISTRACIÓN PÚBLICA DE LA CAE, INCLUYENDO EN ESA METODOLOGÍA LA REALIZACIÓN DE EVALUACIONES DE IMPACTO (EIPD)

Objeto del contrato

La oficina de la Delegada de Protección de Datos de la Administración pública de la CAE, de acuerdo con la legislación vigente, y respetando los principios de libre concurrencia y neutralidad tecnológica, pretende, mediante el presente pliego técnico, establecer las cláusulas y especificaciones técnicas para contratación de un servicio cuyo objeto es el desarrollo de una metodología para la gestión de los riesgos en el cumplimiento normativo de protección de datos personales para su uso por parte de la administración pública de la cae, incluyendo en esa metodología la realización de evaluaciones de impacto (EIPD).

Los servicios solicitados deben dar como resultado una metodología de gestión de riesgos para su uso por parte de los Departamentos y entidades del Gobierno Vasco, incluyendo en esa gestión de riesgos los tratamientos que requieran de una evaluación de impacto relativa a la protección de datos (EIPD).

Accesibilidad

Las Prescripciones Técnicas del presente contrato se han desarrollado teniendo en cuenta criterios de accesibilidad universal y de diseño universal o diseño para todas las personas.

Teniendo esto en cuenta, toda la documentación a entregar por la entidad adjudicataria, será legible por herramientas ofimáticas estándar (formato Word/Excel/PPT, o en ODF). La información estructurada podrá también entregarse en formato CSV.

Alcance de la licitación

Para el diseño de la mencionada metodología de gestión de riesgos y su implementación, deberán tenerse en cuenta y abordarse las siguientes actividades o grupos de actividades:

1. La detección de los tratamientos de alto riesgo a partir del registro de actividades de tratamiento

2. El diseño metodológico de las tareas de evaluación y tratamiento de riesgos para aquellos tratamientos que no sean de alto riesgo y que, por tanto, no requieren de una EIPD: en este caso deberá incluirse el método de cálculo del riesgo y de identificación de las medidas dirigidas a mitigar los riesgos

3. El diseño metodológico para hacer las evaluaciones de impacto relativas a la protección de datos en relación a aquellos tratamientos que sean de alto riesgo: en este caso deberá incluirse un método de trabajo que incluya como mínimo los contenidos previstos en el artículo 35.7 del RGPD

4. La propuesta de estrategia de implementación de la metodología, que deberá incluir una fase de testeo de la aplicación de la metodología diseñada a un volumen no inferior a 8 tratamientos (a definir durante la prestación del servicio), de los cuales al menos 2 deberán ser de alto riesgo, así como la revisión y mejora de la metodología en base a esos 8 tratamientos.

La metodología deberá ser propia y se valorarán positivamente los aspectos originales o novedosos que se aporten.

En la definición de la metodología deberán tenerse en cuenta las orientaciones, dictámenes y guías de las autoridades de protección de datos europeas y en particular de la Agencia Vasca de Protección de Datos, y otras autoridades de protección de datos autonómicas, así como los pronunciamientos de la Agencia Española de Protección de Datos en el ámbito de la gestión de riesgos.

El resultado de los servicios deberá ser:

a) Un entregable de dos guías separadas:

   - ☐ Un entregable en forma de manual o guía metodológica para el análisis de riesgos en materia de datos personales
   - ☐ Un entregable en forma de manual o guía metodológica para la realización de EIPD

b) Entrega de los análisis de riesgos y EIPD de los tratamientos que se han utilizados como testeo de las guías anteriormente mencionadas.

c) La entrega de los documentos de apoyo utilizados

d) La documentación resultante de la aplicación de la metodología a 8 tratamientos de datos personales

e) Un informe sobre la adecuación de la metodología a las exigencias de la normativa y de las autoridades de protección de datos

Toda la documentación deberá estar adaptada a la Administración Pública de la CAE.

Equipo de trabajo

El equipo de trabajo deberá estar formado al menos por los siguientes perfiles:

a) Persona Directora de equipo: persona con titulación en derecho (Nivel 3 del MECES, licenciatura en derecho o equivalente) con una experiencia superior a 5 años en el ámbito de la protección de datos personales, con capacidades y conocimientos en el ámbito de la gestión de riesgos de los datos personales y en evaluaciones de impacto relativas a la protección de datos, y en general en la aplicación y verificación de cumplimiento de la normativa de protección de datos; su función será la de coordinar al equipo y asegurar que los resultados estén alineados con el objeto de la licitación

   Deberá poseer, al menos, una de las siguientes certificaciones:
   - Lead Auditor 27001 - Expedida por una Entidad de Certificación.
   - Delegado de Protección de Datos - Expedida por una Entidad de Certificación acreditada por ENAC).
   - Certified Information Systems Auditor (CISA, Expedida por ISACA).

b) Persona consultora jurídica: persona con una experiencia superior a 2 años en el ámbito de la protección de datos (Nivel 3 del MECES), con experiencia en proyectos y servicios que impliquen la realización de evaluaciones de impacto y diseño de metodologías de gestión de riesgos en grandes organizaciones; su función principal será la de participar en el diseño de la metodología y la posterior implementación

c) Persona consultora jurídica: persona con una experiencia superior a 2 años en el ámbito de la protección de datos personales (Nivel 3 del MECES), y con formación especializada en protección de datos y materias conectadas, con experiencia en proyectos y servicios que impliquen la realización de evaluaciones de impacto y diseño de metodologías de gestión de riesgos en grandes organizaciones; su función principal será la de participar en el diseño de la metodología y la posterior implementación

d) Persona consultora técnica: consultor o consultora de perfil técnico, ingeniero (Nivel 3 del MECES), con una experiencia superior a 2 años en tecnologías y seguridad de la información en el ámbito de la protección de datos personales, con experiencia en proyectos y servicios que impliquen la realización de evaluaciones de impacto, diseño de metodologías de gestión de riesgos y auditoria; su función principal será la de participar en el diseño de la metodología, en particular en lo que se refiere a la gestión de los riesgos para la seguridad de los datos.

Estas personas deberán quedar adscritas al contrato de manera obligatoria.

Documentación a presentar

Proyecto relativo al desarrollo de una metodología para la gestión de los riesgos en el cumplimiento normativo de protección de datos personales para

su uso por parte de la administración pública de la cae, incluyendo en esa metodología la realización de evaluaciones de impacto (EIPD)

Este proyecto se divirá èn tres partes siguiendo este orden:

- El diseño metodológico de las tareas de evaluación y tratamiento de riesgos para aquellos tratamientos que no sean de alto riesgo y que, por tanto, no requieren de una EIPD
- El diseño metodológico para hacer las evaluaciones de impacto relativas a la protección de datos en relación a aquellos tratamientos que sean de alto riesgo: en este caso deberá incluir la propuesta de un método de trabajo que incluya como mínimo los contenidos previstos en el artículo 35.7 del RGPD
- Planificación

Organización, planificación y control

Se debe detallar en la oferta el plan de trabajo del proyecto. con un nivel de detalle razonable sin perder la perspectiva de que estos planes puedan sufrir variaciones porque la Delegada de Protección de Datos de la CAE pueda priorizar otros trabajos respecto a los que ahora mismo se prevén o propongan.

Asimismo, será necesaria la elaboración de un informe con carácter mensual en el que se desglosarán los trabajos solicitados, ejecutados y estado en el que se encuentran. Los licitadores deberán proponer el modelo organizativo óptimo para la coordinación y dirección del proyecto.

Condiciones operativas

La empresa contratista asumirá respecto del personal asignado a la ejecución del contrato todo lo relacionado con la negociación y pago de retribuciones salariales, afiliaciones y cotizaciones a la Seguridad Social y pago de prestaciones, permisos, licencias, vacaciones, sustituciones, prevención de riesgos laborales, régimen disciplinario, relaciones sindicales, y todos los demás derechos y obligaciones que se deriven de los contratos de trabajos propios.

Asímismo, proporcionará a todas las personas que compongan el equipo de proyecto los medios materiales necesarios para la prestación del servicio.

Todos los gastos necesarios para la realización de los trabajos contratados, como por ejemplo, los gastos de desplazamientos, se consideran incluidos en el presupuesto del contrato.

Durante la ejecución del los trabajos objeto del contrato, la empresa contratista se compromete en todo momento, a facilitar a las personas designadas por la dirección del proyecto, la información y documentación que ésta solicite para disponer de un pleno conocimiento de los trabajos

desarrollados, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos, y herramientas utilizados para resolverlos.

Lugar de Trabajo

Las labores requeridas en el presente pliego se realizarán en las dependencias de la empresa adjudicataria, sin perjuicio de tener que acudir a cuantas reuniones se convoquen en las dependencias de la Delegada de Protección de Datos de la CAE en su oficina situada en la C/Donosti-San Sebastian, nº1, 01010, Vitoria-Gasteiz, cuando así lo solicite.

Coordinación

La empresa contratista deberá asignar al menos una persona como coordinadora técnica o responsable, perteneciente a su plantilla, que será la interlocutora con quien se relacionará con la oficina de la Delegada de Protección de Datos de la Administración Pública de la CAE y a quién corresponderá la dirección de los trabajos, así como impartir directamente las órdenes e instrucciones laborales al resto de las personas adscritas a la ejecución del contrato.

Propiedad de los trabajos objeto del contrato

Se rigen por lo establecido en la cláusula 30 del Pliego de condiciones generales.

Amaya Angulo Garzaro
Responsable del área de Asesoría Jurídica de la Delegada de Protección de Datos de la CAE

Visto Bueno

Arantza Sanabria Llaguno
Euskal Autonomia Erkidegoko Administrazio Publikoaren Datuak Babesteko Ordezkaria
Delegada de Protección de Datos de la Administración Pública de la Comunidad Autónoma de Euskadi