CONDICIONES PARA LA CONTRATACIÓN DE UN SERVICIO DE EVALUACIÓN DE IMPACTO Y DOCUMENTACIÓN DE SEGURIDAD DEL BIGAN

1. Descripción de la Situación Actual

BIGAN se crea por Orden SAN/1355/2018, de 1 de Agosto de 2018 como elemento del Sistema de Información de Salud de Aragón (publicada en el BOA del 22/08/2018). BIGÁN es un proyecto que ha de entenderse como un desarrollo específico para la explotación de los sistemas de información que afectan a la Salud en Aragón, y en particular del Sistema de Información de Salud que se define en el artículo 32 de la Ley 6/2002, de 15 de abril, de Salud de Aragón.

Su misión consiste en integrar y explotar la información del conjunto de datos recogidos en el ámbito de salud de Aragón, generando así conocimiento para facilitar la evaluación en efectividad, eficiencia, calidad y sostenibilidad del Sistema de Salud de Aragón y conseguir la mejora en la toma de decisiones de planificación y gestión sanitaria, así como su utilización en programas y proyectos de investigación, desarrollo e innovación, mediante la explotación de una Plataforma de datos de base longitudinal de ciclo rápido de refresco.

Esto supone la extracción, transformación y carga de datos procedentes de distintas fuentes de información, asistenciales y no asistenciales, que, en una primera fase del proyecto, son las siguientes:

- Base de datos de Usuarios (BDU): Datos sobre población asegurada.
- Conjunto Mínimo Básico de Datos al Alta Hospitalaria (CMBD): Datos sobre episodios de hospitalización.
- Historia clínica electrónica de Atención Primaria (OMI-AP): Datos sobre consultas de atención primaria.
- PCH URGENCIAS: Datos sobre atención en servicios de urgencias hospitalarias.
- RECETA ELECTRONICA: Datos sobre prescripciones y dispensaciones de medicamentos y productos sanitarios.
- Sistema de información hospitalario (Hospital Information System/HIS): Datos sobre citaciones para consultas externas de atención especializada y cirugía programada (también conocida como lista de espera quirúrgica).
- Bases de datos de Salud Publica

Otros sistemas de información considerados para su integración en un futuro serían:

- HCE (Historia Clínica Electrónica) que incluye datos de la historia clínica de los pacientes del Servicio Aragonés de Salud.
- RIS (Radiology Information System), que incluye datos, informes e imágenes de las pruebas radiológicas.
- SIM (Sistema de Información Microbiológica), que incluye datos sobre los resultados de cultivos, antibiogramas y otras determinaciones microbiológicas).
- SENECA (Sistema de información de Emergencias Médicas de Aragón) -061.
- Farmatools (Sistema de información de Farmacia Hospitalaria).
- LIS (Laboratory Information System).
- Otros (Sanidad ambiental,…).

Desde la Unidad de Biocomputación del Instituto Aragonés de Ciencias de la Salud (en adelante, IACS), se colabora en la definición de todos los procesos de transformación, carga y anonimización de los datos, y de la definición, diseño e implementación de los procesos de análisis, minería de datos, cálculo de indicadores, y de cuantos procesos informáticos se establezcan dentro del proyecto BIGAN. Específicamente, el departamento de sanidad, a través de la participación de los órganos directivos correspondientes, será el responsable de habilitar un acceso seguro y de-identificado a sus fuentes de datos (orígenes).

Teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento que opera sobre datos, considerados de especial protección (dato sanitario), se ha previsto llevar a cabo una evaluación de impacto sobre la privacidad que se actualizará conforme sea necesario.

Asimismo, conjuntamente a la evaluación de impacto en la protección de datos personales se redactará la documentación de Seguridad a nivel de Sistema (System Level Security Policy), que describa las medidas dirigidas a evitar la potencial re-identificación de individuos a partir de los registros anonimizados; los procesos de anonimización; así como las medidas de control y auditorías necesarias para evaluar los usos de los datos y el nivel de seguridad establecido durante el transcurso del proyecto.

2. Objeto de la contratación

El IACS está interesado en la contratación de los servicios de:

- Realización de una **Evaluación de Impacto de la protección de datos** sobre el tratamiento de los datos y los servicios del BIGÁN para analizar los riesgos atinentes a la privacidad con identificación de aspectos de mejora y factibilidad de implantación de los mismos.
- Redacción de la **Documentación de Seguridad a nivel del sistema** de BIGÁN, alineado con los correspondientes documentos de Política de Seguridad del IACS, del Departamento de Sanidad, de Aragonesa de Servicios Telemáticos (AST), del Servicio Aragonés de Salud y del Gobierno de Aragón.

A tal efecto, IACS precisa de la contratación a una empresa, que deberá demostrar tener los recursos y experiencia que acrediten su capacidad para llevar a cabo estos trabajos.

3. Características de la prestación de servicios

3.1 Evaluación de impacto de la protección de datos (EIPD)

BIGÁN se concibe como un sistema modular, lo que permitirá incrementar gradualmente el cruce de la información que afecta a la salud con otras bases de datos de interés disponibles (demográficas, socio-económicas, geográficas, etc). Dicha información se introducirá en la Plataforma cumpliendo con los requisitos legales (en particular el Reglamento (UE) 2016/ 679 y la Ley Orgánica de Protección de Datos) y de calidad, para que pueda ser explotada de forma segura. Las fuentes de datos consideradas para la evaluación de impacto deberán incluir las mencionadas en el punto 1 independientemente de que a la fecha de inicio del contrato de servicios hayan sido efectivamente integradas en el BIGAN.

Contenido mínimo de la evaluación:

- Identificación de partes interesadas.
- Descripción de BIGÁN, los datos que se tratan y sus características y de los flujos de información, para una identificación clara de quién y cómo tendrá acceso y tratará los datos sensibles así como de los responsables de las distintas tareas y su duración prevista, en una descripción detallada del ciclo de vida en el tratamiento de los datos incluida la fase de servicios del BIGÁN. Incluye una descripción de buenas prácticas acreditadas en el proceso de anonimización/de-identificación de la información.
- Metodología para el análisis de riesgo y la realización de la evaluación del impacto, sistemática y reproducible y determinación del umbral de riesgo aceptable (riesgo residual).
- Identificación y valoración de los riesgos descubiertos durante la evaluación de impacto, incluida la información recabada tras el testeo sobre las probabilidades de re-identificación, incluidas estimaciones de efectividad de los procesos de re-identificación habituales mediante la adición de nuevos datos obtenidos de otras fuentes.
- Gestión de los riesgos identificados, que incluye una descripción de las medidas tanto organizativas como de seguridad lógica y física y su influencia en la disminución de la probabilidad de ocurrencia de los riesgos y las consecuencias en términos de la severidad de los impactos, asegurando que solo se tratan los datos necesarios y para las finalidades legítimas previstas y definidas.
- Análisis de las bases jurídicas que legitimen los tratamientos.
- Análisis de cumplimiento normativo.
- Informe final con recomendaciones, incluidas las eventuales propuestas de mejora del proceso de anonimización. La EIPD deberá contener, a modo de conclusión, las recomendaciones con las medidas que deben adoptarse bien sean de eliminación, mitigación, transferencia o aceptación de los riesgos para la privacidad. Dichas recomendaciones tendrán en cuenta el principio de proporcionalidad en costes, es decir, la implantación de medidas que mitiguen los riesgos de seguridad deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos.
- Verificar la correcta implantación de las medidas en relación con los objetivos establecidos para tratar los riesgos de privacidad.
- Anexo con la documentación técnica y organizativa analizada.

3.2 Redacción de la Documentación de Seguridad a nivel del Sistema

La documentación de seguridad a nivel de sistema incluirá las medidas tanto organizativas como de seguridad lógica y física en todas las capas de la infraestructura BIGÁN.

La documentación de seguridad a nivel de sistema deberá cumplir, y en su caso ampliar o detallar los procedimientos generales de seguridad y control establecidos en la Políticas de Seguridad del IACS, del Departamento de Sanidad, del Servicio Aragonés de Salud y la del Gobierno de Aragón, y en lo que se refiera a infraestructura de sistemas y comunicaciones, los requisitos establecidos a tal efecto por la entidad pública Aragonesa de Servicios Telemáticos.

Contenido mínimo de la documentación de seguridad a nivel de sistema:

- Descripción del Sistema.
- Gobernanza del sistema: definición del equipo de trabajo, segregación de perfiles y medidas organizativas.
- Procedimientos de seguridad durante el ciclo de vida en el tratamiento de los datos incluida la fase de servicios del BIGÁN: políticas de seguridad, personal de seguridad, medidas físicas, medidas tecnológicas, etc. Hacer especial hincapié en el procedimiento de extracción y uso de datos para investigación.
- Plan de Contingencia que contendrá procedimientos de notificación, gestión y respuestas ante las incidencias.

La documentación de seguridad y el documento de evaluación de impacto serán documentos interrelacionados, dado que el objetivo de seguridad está basado en resultados, no en medios (eg. Hardware, software, etc) ya que estos cambian constantemente.

4. Presupuesto máximo

Máximo de 14.800 euros de base imponible.

5. Plazo de ejecución

Hasta el 31 de Diciembre de 2018.

6. Hitos

1. Entregable con descripción y análisis preliminar del BIGAN, estableciendo la metodología y cronograma para la evaluación de impacto.
2. Entregable identificación y gestión de los riesgos.
3. Entregable análisis de cumplimiento normativo.
4. Entregable Informe final Evaluación de impacto, con toda la documentación relativa a lo indicado en el apartado 3.1 (incluyendo entregables de hitos 2 y 3, formando un todo), y cumpliendo con los mínimos exigidos por el art. 35.7 del RGPD
5. Entregable Documentación de Seguridad a nivel del sistema.

La facturación de los hitos será:

- Para el Hito 1: 10%

- Para Hitos 2 y 3: 40%

- Para Hito 4: 30%

-Para Hito 5: 20%

Los hitos serán sucesivos cronológicamente.

7. Criterios de solvencia exigidos

Será necesario cumplir con los siguientes criterios de solvencia para que pueda ser valorada su oferta.

Deberá acreditar mediante declaración que dispone de personal para la prestación directa del servicio que tenga, al menos, 3 años de experiencia en la prestación de servicios similares.

8. Plazo para presentar ofertas

Catorce días naturales desde el día siguiente a la recepción de la solicitud.

9. Contenido de las ofertas

El licitador deberá detallar las actividades a realizar mediante una propuesta que incluya:

- Un modelo organizativo y de gestión del proyecto
- Metodología a utilizar para el desarrollo de los trabajos

Asimismo deberá justificar los criterios de solvencia técnica exigidos y presentar la oferta económica con el importe de los servicios, desglosando la base imponible y los impuestos aplicables.

10. Criterios para la valoración de la licitación

1. CRITERIOS QUE DEPENDEN DE UN JUICIO DE VALOR (de 0 a 45 puntos):

Calidad de la oferta técnica:

La valoración y ponderación de este criterio de adjudicación (calidad de la oferta técnica) se realizará atendiendo a los siguientes aspectos (subcriterios de valoración):

1.1. Modelo organizativo y de gestión del proyecto (máximo 22,5 puntos):

1.1.1. Se tendrá en cuenta la adecuación y organización del equipo de trabajo

1.2. Metodología utilizada para el desarrollo de los trabajos (máximo 22,5 puntos):

1.2.1 Se tendrá en cuenta el enfoque propuesto, la estructuración de las tareas a realizar y la viabilidad del plan de trabajo dentro del calendario propuesto para la consecución de los distintos entregables previstos.

2. CRITERIOS QUE NO DEPENDEN DE UN JUICIO DE VALOR (de 0 a 55 puntos):

Valoración económica (máximo 55 puntos)

Se concederán 55 puntos a la oferta más económica y se disminuirá proporcionalmente el resto de las ofertas según la fórmula:

Puntos = 55 * (Oferta más económica / Oferta)