
EXPEDIENTE: PAS 02/22: INFORME DE VALORACIÓN DE LOS CRITERIOS SUJETOS A JUICIO DE VALOR RELATIVO AL CONTRATO DE SERVICIO DE SOPORTE Y CONSULTORÍA EN MATERIA DE PROTECCIÓN DE DATOS (RGPD Y LOPD-GDD) Y EXTERNALIZACIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS (DPO).

INFORME DE VALORACIÓN. CRITERIOS SUJETOS A JUICIO DE VALOR

El día 3 de febrero de 2023, la Comisión de Valoración relativa al contrato de servicio de soporte y consultoría en materia de protección de datos (RGPD Y LOPD-GDD) y externalización del delegado de protección de datos (DPO), se reúne a las 10:20 horas de la mañana, en la Fundación para la Investigación Biomédica del Hospital Universitario Puerta de Hierro para la apertura del sobre dos, relativo a los criterios sujetos a juicio de valor.

Ese día, se procede a abrir la documentación de los seis licitadores (6) que presentaron adecuadamente el contenido del sobre 1:

- DAC BEACHCROFT S.L.P.U.
- SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U.
- FRANCISCO JAVIER GONZÁLEZ GALÁN (PRODATEX).
- AUREN CONSULTORES SP, S.L.P.
- PONS IP S.A.
- GRUPO UNIVE SERVICIOS JURIDICOS S.L.

En la apertura del sobre dos no hay representación por parte de ningún licitador.

Tras su apertura se comprueba que, los mismos, contienen la documentación requerida en papel y en soporte electrónico.

En el presente informe se procederá a analizar las propuestas de los licitadores, las cuales deberán contener lo descrito en la cláusula 1, apartado 9.1 del Pliego de Cláusulas Administrativas. Esto es, un plan de trabajo en el que se especifique la forma de llevarlo a cabo y el seguimiento del servicio demandado que garantice la eficacia y calidad del mismo, con inclusión de una memoria descriptiva relativa a la propuesta sobre la organización del trabajo y el plan de acción propuesto para llevar a cabo el servicio, con indicación del personal interviniente, grado de dedicación y los medios a disponer para su desarrollo.

En el Pliego de Cláusulas Administrativas se indica lo siguiente:

“En relación con el criterio propuesta técnica, el licitador deberá presentar un plan de trabajo en el que se especifique la forma de llevarlo a cabo y el seguimiento del servicio demandado que garantice la eficacia y calidad del mismo, con inclusión de una memoria descriptiva relativa a la

propuesta sobre la organización del trabajo y el plan de acción propuesto para llevar a cabo el servicio, con indicación del personal interviniente, grado de dedicación y los medios a disponer para su desarrollo.

Se valorará la calidad de cada propuesta y su adaptación a las necesidades de la Fundación.

Se establece para este criterio una valoración máxima de veinte (20) puntos, dada la especial importancia de los aspectos técnicos de la prestación del servicio y habida cuenta de la complejidad del sistema empleado y de la especial sensibilidad de los datos tratados”.

Resultado de la revisión de la documentación técnica

- [REDACTED]

CRITERIOS SUJETOS A JUICIO DE VALOR (HASTA 20 PUNTOS):

PLAN DE TRABAJO.....20 puntos

El licitador comienza haciendo alusión al objeto del contrato, asegurando dentro de todas las actuaciones de la Fundación, el cumplimiento del Reglamento (UE) 2016/679 de 27 de abril de 2016, y de la Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos Personales y Garantías de Derechos Digitales.

El licitador, expone que, todas actuaciones, medidas, procedimientos y documentos dentro de las prestaciones que preste, se revisarán periódicamente cada vez que sea necesario y al menos una vez al año. En esta línea, se indica que, si fuera necesario se elaborarían nuevas medidas, procedimientos y documentos cuando se produjesen modificaciones en materia de normativas, organizativas, nuevos tratamientos, etc.

El hecho de que planteen que todos los suministros, avances de información, así como los resultados finales de los trabajos realizados con motivo de esta contratación sean propiedad exclusiva de la Fundación se valora como un aspecto positivo.

Se propone una metodología PDCA, esto es, PLAN, DO, CHECK, ACT.

Cabe destacar que, se valora muy positivamente el hecho de que la propuesta técnica esté estructurada en base al pliego de prescripciones técnicas, y parta de la estructura y pilares del mismo para explicar su eventual forma de actuación.

En primer lugar, respecto a la necesidad de asesorar en materia de protección de datos cuando así se solicite, el licitador indica que, dará respuesta con instrucciones y recomendaciones para cumplir con lo establecido en el RGPD y en la LOPDGDD o en cualquier norma que las sustituya a todas las dudas o cuestiones que le surjan a la Fundación. Incluso, se señala que, si la consulta lo requiriese, se realizaría un informe para dar respuesta a la misma.

De manera adicional, proponen un “Registro de consultoría”, lo cual aporta valor adicional a su oferta técnica. El mismo, permitiría a la Fundación, tener un grado máximo de cumplimiento

normativo y ante una denuncia o una brecha es una prueba para demostrar que a lo largo del tiempo se están realizando, todas las actuaciones necesarias para llevar u control.

El licitador también da respuesta a la necesidad de asesorar, cuando así se solicite, en la respuesta a los requerimientos de información que provengan de las autoridades de control y supervisión. Es más, el licitador no solo propone una respuesta a posteriori, si no que, proponen elaborar un procedimiento a priori con las actuaciones a realizar ante la Autoridad de Control. A este respecto proponen igualmente una mejora, que es controlar cualquier brecha de seguridad, violación o incidente a través de su registro de violaciones o brechas de seguridad, donde quedan recogidas las posibles brechas o violaciones de seguridad que se puedan producir en la Fundación.

El licitador también se compromete a modificar o realizar documentación nueva o procedimientos cada vez que se produzcan cambios operativos, estructurales, o porque se necesite por necesidades del servicio. En relación con esto, se propone como mejora realizar informes trimestrales y anuales de todo lo acontecido en su aplicación, remitirán un informe en el que se definirá los trabajos realizados y los cometidos de cada persona. En su oferta indican todos los indicadores y parámetros de control que dicho informe contendrá. Algunos de estos, son: Agenda (todas las actividades a modo informativo que se realizan con la Fundación), Registro de solicitud de derechos (Registro fechado y con el plazo para contestar a derechos que hayan sido requeridos por los interesados), Registro de formación (El RGPD y la LOPDGDD da bastante importancia a la concienciación y formación que se decida hacer en protección de datos), Registro de auditorías, Registro de evaluación de impacto, etc.

Todos estos indicadores y parámetros de control que se plantean también aportan valor adicional a la oferta técnica de [REDACTED]

Igualmente, el licitador determina que velará por el cumplimiento del artículo 31.2 de la Ley Orgánica 3/2018, de 5 diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, por el cual, las administraciones públicas deberán de publicar un inventario de actividades de tratamiento que será accesible por medios electrónicos. En este sentido, se indican que apartados se revisarán. [REDACTED] también propone incorporar una mejora a este servicio.

Se determina que existirá un respaldo cuando se produzcan transferencias de datos personales, a un tercer país o una organización internacional, así como, cuando sea necesario redactar las cláusulas informativas a incluir en los modelos. Además, se valora positivamente que en su oferta se indique que, [REDACTED] no solo se compromete a cumplir lo prevenido por el Reglamento Europeo de Protección de Datos sino también con los criterios de máxima simplificación que reclama la vigente Ley Orgánica 3/2018, de 5 de diciembre, indicando en este sentido, la información básica que deberá contener. Su oferta también mejora los mínimos exigidos ofreciendo soporte en el CANAL ÉTICO de la entidad para mejorar la información permitiendo el acceso a la política de privacidad de la entidad, así como la elaboración de una propuesta de respuesta a los interesados para la Fundación.

Respecto a la revisión de las medidas de responsabilidad proactiva, el licitador indica que la misma dependerá de si la Fundación actualmente dispone de un DPD o no. En caso de no disponer, establecen que se realizará el nombramiento del mismo. Aportando el valor de ser [REDACTED] quien se encargue de hacer la gestión de comunicar a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos.

También, se valora de forma positiva el hecho de que, en caso de existir un comité de seguridad de la información, apoyen y den soporte al mismo para cumplir con cuantas necesidades tengan (en caso de no existir y que se quiera realizar, asesorarán sobre las personas más idóneas para asumir los roles). También encontramos muy interesante lo que indican respecto a las reuniones del comité de seguridad. Establecen que, de estas, se suelen realizar informes, a modo de acta, y, si la Fundación diese autorización para esto, solicitarían una copia del mismo para emitir su propio informe, lo cual sería de gran ayuda. También, ponen a disposición de la Fundación a un auditor interno y de una auditora Jefa, para asesorarla en estos campos.

Se explica de forma lógica y detallada como se llevaría a cabo la revisión y actualización de la política de protección de datos de carácter personal, proponiendo, además, la confección de aquellos documentos que no existan, la revisión de los existentes o la ampliación de servicios como el de detectar aquellos encargos del tratamiento en los que la Fundación no resulte ser el Responsable del Tratamiento, etc.

Proponen, no solo cumplir con la asesoría en materia de protección de datos personales para dar respuesta a los nuevos acontecimientos o prácticas de relevancia, si no también, dar respuesta a las consultas directas u on-line que pudieran surgir en un plazo máximo de 8 horas, proponiendo un sistema que registre las mismas.

Proponen que las reuniones de seguimiento (sin perjuicio de los mínimos requeridos) se podrán hacer tantas como sean necesarias de manera online, a través de programas de videoconferencia, programas de control remoto e incluso telefónicamente, esto supone un aspecto importante para la Fundación. Y, también, indican que, comunicarán todos aquellos documentos, novedades, informes jurídicos que sean de interés para la Fundación a través de una función de su aplicación, que permite enviar al DPD los mails que estime necesario quedando así registrado.

Por último, respecto al Servicio de externalización del Delegado de Protección de Datos, la oferta cumple con todas las actuaciones necesarias para el cumplimiento de sus fines. Y, como valor añadido se proponen acciones y mejoras como las siguientes:

- Elaboración de un procedimiento con las actuaciones a realizar ante la Autoridad de Control por parte de la Fundación en cuanto a las notificaciones establecidas en el RGPD, y en su caso a los interesados.
- Poder acceder a la aplicación, propiedad de [REDACTED], dando de alta en la misma a las personas interesadas (se entregará un manual de 4 páginas). Esta propuesta nos resulta muy útil para poder llevar un mejor control.

- Emisión de informes acerca si la empresa o colaborador designado es adecuado conforme al cumplimiento normativo.
- Asesorar, cuando así se solicite, sobre la realización de una Evaluación de Impacto relativa a la Protección de Datos, así como supervisar la aplicación de las medidas técnicas y organizativas resultantes de la misma.
- Comunicar a la Fundación cualquier vulneración relevante en materia de protección de datos.
- Actuar como punto de contacto e interlocutor entre la de la Fundación y los interesados en cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos atendiendo y gestionando sus reclamaciones.
- Etc.

CONCLUSIONES:

Un aspecto adicional que valorar es la transparencia a la que el licitador se compromete, ya que propone que dar acceso a su software a aquellas personas que sean necesarias para controlar su trabajo o para colaborar en las funciones que se requieran.

Dentro de la oferta de [REDACTED], se valoran muy positivamente dos aspectos. El primero, es que su propuesta sigue toda la estructura descrita en el pliego de prescripciones técnicas y a partir de ella habla sobre su metodología. Y, el segundo, es el hecho de que sobre todos y cada uno de los mínimos exigidos en el pliego de prescripciones técnicas se aporten mejoras pesadas por el licitador expresamente en relación con cada servicio, hacen de esta oferta técnica un trabajo muy elaborado, y, en consecuencia, la misma debe ser valorada de forma muy positiva.

Además, para la Fundación, supone una gran ayuda que el licitador en su oferta indique que de toda la formación realizada se entregará un material en formato PDF, así como que, elabore un cronograma orientativo que recoja una formación sobre cursos relacionados con la protección de datos.

PUNTACIÓN: 19 PUNTOS.

- [REDACTED]

CRITERIOS SUJETOS A JUICIO DE VALOR (HASTA 20 PUNTOS):

PLAN DE TRABAJO.....20 puntos

Lo primero que hay que resaltar de la oferta de [REDACTED] es que la misma, no sigue la estructura descrita en el pliego de prescripciones técnicas. Esto dificulta la valoración de la propuesta ya que no se expone de una manera clara el cumplimiento de los mínimos exigidos con las acciones y metodologías propuestas.

La propuesta de [REDACTED] comienza enumerando la normativa aplicable. A continuación, encontramos que [REDACTED] propone incluir valores y principios, sin costes adicional, dentro de estos se valoran positivamente algunos de ellos, como, por ejemplo:

- Incorporación de herramienta de gestión del servicio Service Desk Plus con el objetivo de centralizar todas las peticiones y solicitudes en un único punto
- Propuesta de implantación de un Comité de Dirección de Protección de Datos
- Puesta a disposición de la Oficina de Calidad de Proyectos y Servicios – OCPS de [REDACTED]

[REDACTED] divide su oferta. Por un lado, establece diferentes fases, indicando en cada una de ellas, las actuaciones a desarrollar, los hitos y los entregables. Y, por otro lado, desarrolla la memoria descriptiva y otros aspectos.

Dentro de la memoria descriptiva, hay diferentes actuaciones.

Lo primero que se establece es que [REDACTED] pone a disposición del servicio un amplio equipo de trabajo que permita cubrir las necesidades del cliente, se valora positivamente que, al inicio del proyecto, el equipo de trabajo de [REDACTED] realice una fase de adquisición de conocimientos del cliente, solicitando la entrega de documentación revisándola para la adecuación RGPD.

Se indica que el equipo de trabajo asumirá funciones como:

- Informar y asesorar a la Fundación y a los empleados que se ocupen del tratamiento de las obligaciones que les incumban en virtud del Reglamento,
- supervisar el cumplimiento de lo dispuesto en el Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas de la Fundación en materia de protección de datos personales,
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35
- Asistencia presencial a las instalaciones de la Fundación con carácter trimestral, para la realización del Comité de Protección de Datos
- Etc.

Se valoran positivamente estas propuestas, así como otras no enumeradas que sí podemos encontrar en su oferta. Sin embargo, no se detallan mejoras propuestas por el licitador que aporten un valor añadido a los requisitos mínimos exigidos en el pliego de prescripciones técnicas (por ejemplo, no proponen más reuniones que las mínimas requeridas).

Sobre la adecuación y mantenimiento RGPD / LOPDGDD, se valoran puntos como que llevará a cabo una revisión continua de los tratamientos y sus riesgos asociados, o que se basarán en la metodología de mejora continua PDCA (Plan-Do-Check-Act).

Sí que se valora muy positivamente, debido a la importancia que tiene para la Fundación, que [REDACTED] haya desarrollado unas sesiones formativas para impartir en materia de protección de datos, a las distintas áreas de trabajo del cliente, para reforzar la cultura de cumplimiento y resolver todas aquellas dudas que puedan surgir día a día.

[REDACTED], propone un modelo de equipo, compuesto por: Responsable del servicio, DPD as a service (sus funciones son explicadas en un punto a parte. La explicación sobre sus funciones es exhaustiva y clara), Equipo táctico y operativo (perfil jurídico RGPD LOPGD y Perfil técnico Seguridad) y un Pool de especialistas. Es útil, descriptivo y funcional, que se describan las funciones de todos y cada uno de ellos, así como que se adjunte un cuadro con la dedicación de cada uno de ellos al presente concurso.

[REDACTED] también propone, sin coste alguno, el uso de la herramienta de gestión de servicios Service Desk Plus, con el objetivo de centralizar todas las peticiones y solicitudes en un único punto y poder emitir informes de gestión del servicio de forma rápida y automatizada. Esto supone una gran propuesta para la Fundación ya que dicha herramienta facilita la recopilación de todas las cuestiones necesarias. [REDACTED] explica y enumera las funciones de la herramienta.

También se valora positivamente que [REDACTED] proponga definir un Comité de Protección de Datos que se reúna con una periodicidad trimestral y aborde tareas como, el análisis de incidentes de seguridad, el análisis de ejercicio de derechos por parte de los interesados, promueva la formación y concienciación en materia de protección de datos.

Además, propone el establecimiento de un segundo Comité de Seguimiento del servicio, a nivel táctico y operativo, que se reúna con una periodicidad mensual, y con funciones como informar acerca de la gestión de recursos, asignación y liberación de personas para la realización de los objetivos del servicio, presentar la información sobre la gestión de los Acuerdos de Nivel de Servicio: procedimientos, herramientas, informes, presentar y gestionar los riesgos, problemas e incidencias del servicio, y hacer un seguimiento hasta el cierre de estos, etc.

Incluso, propone la estructura que podrían tener los comités. La idea de crear estos Comités es muy atractiva.

El licitador, propone una implantación dividida en las fases. Destaca que en cada una de ellas encontramos un cronograma y una planificación general de actividades relacionadas con la

gestión del servicio. Además, en cada una de ellas, también se detallan las fases, tareas y entregables que deberán desarrollarse o tener lugar en cada una.

Destaca de este desarrollo, la fase de Pleno Servicio, en ella se indica que [REDACTED] ha diseñado una hoja de ruta para facilitar el cumplimiento del RGPD por parte de las organizaciones a partir de la implementación de un Sistema de Gestión de Protección de Datos.

[REDACTED], en esta fase, también propone la elaboración de un Registro de Actividades de Tratamiento que cumpla con la obligación del Reglamento General de Protección de Datos de mantener un registro de operaciones de tratamiento.

Otra propuesta destacable es la revisión del estado general de controles de seguridad de la FUNDACIÓN y su madurez (tomarán como referente el modelo de madurez definido en la Fundación, bien sea en base a la ISO27000, ENS o el que tenga definido), evaluarán las evidencias recopiladas durante las entrevistas y posteriormente, indican, a partir de los resultados obtenidos, entregarán un informe a la organización con los puntos fuertes identificados y las oportunidades mejora.

En la oferta también existe la “gestión de riesgos”, que según [REDACTED] consistirá en la identificación y análisis de los riesgos a los cuales están expuestos los activos de información, para identificar y seleccionar los controles apropiados de seguridad. En este sentido, el licitador define lo que sería el alcance y el contexto del riesgo y cuáles serían los criterios a tener en cuenta para poder aceptar una cantidad de riesgo mínima. Es correcta para la Fundación esta idea de [REDACTED] en cuanto a la importancia de identificar cuáles son los activos esenciales de la Fundación involucrados en el alcance del análisis de riesgos que se han de proteger y sobre los que por tanto se han de aplicar medidas de seguridad que traten los posibles riesgos a los que están expuestos. El licitador indica, en relación con esto, que también seleccionará una opción de tratamiento para aquellos riesgos identificados que estén por encima del nivel de riesgo aceptable definido (propone diferentes opciones de tratamiento).

Se valoran todas las acciones propuestas por [REDACTED] muy positivamente, si bien en cierto, que habría sido interesante que el servicio hubiera incluido la implantación de medias técnicas (se indica en la oferta que no está incluido). Dentro de las acciones que sí se llevarían a cabo dentro de la Fase DO, destaca, la definición e implantación de indicadores de protección de datos: KPi, Revisión del estado de controles, etc.

La oferta del licitador continúa definiendo el plan de formación y, en concreto, se debe destacar que el licitador se compromete en cuanto a flexibilidad de horarios para adecuarlo de la mejor manera posible a los horarios del personal de la Fundación. Además, se debe resaltar positivamente los contenidos propuestos, la flexibilidad que presentan y el diseño de como abordarían y desarrollarían dichas sesiones formativas.

Por último, hay que resaltar de la oferta de [REDACTED], tres aspectos. El primero es su propuesta de Auditoría de Cumplimiento. Antes de realizarla, proponen acciones para la obtención de evidencias, con las cuales se auditarán los aspectos señalados en la ley. Además, también proponen, comprobar el nivel de madurez de la Fundación a nivel de medidas técnicas de seguridad existentes con el fin de realizar un informe de auditoría en el que se refleje el grado de adecuación a la legislación vigente de protección de datos de carácter personal de las medidas de seguridad existentes en la Fundación.

El segundo aspecto es su propuesta de revisión de los incidentes de seguridad registrados en la FUNDACIÓN con el objetivo de poder detectar deficiencias de controles de seguridad, mejoras a realizar y, en definitiva, realizar el aprendizaje de incidentes, incluso hacen una clasificación en detalle en función de la tipología del incidente.

El último aspecto que se debe destacar es su voluntad de realizar planes de mejoras que integren la decisión estratégica sobre cuáles son los cambios que deben incorporarse.

CONCLUSIONES:

La oferta de [REDACTED] no sigue la estructura descrita en el pliego de prescripciones técnicas, y, en consecuencia, su estructura no es valorada de forma positiva. Sin embargo, se valoran positivamente otros aspectos como que se describan las funciones de todos y cada uno de los miembros del equipo de trabajo, o que se desarrollen unas sesiones formativas para impartir en materia de protección de datos.

También supone un gran punto a favor de [REDACTED] el hecho de que pongan a disposición de la Fundación el uso de la herramienta de gestión de servicios Service Desk Plus, con el objetivo de centralizar todas las peticiones y solicitudes en un único punto.

Se valora muy positivamente la planificación por fases que encontramos en la oferta técnica, ya que nos ofrece una visión real de cómo se desarrollaría el servicio a lo largo de la ejecución del contrato junto a [REDACTED].

El plan de formación propuesto se ajusta a las necesidades de la Fundación, y se valora muy positivamente: 1) el hecho de que las mismas sean presenciales, 2) En el caso de nuevas incorporaciones, [REDACTED] pondrá a disposición medios para que el nuevo personal que se está formando pueda realizar consultas, y 3) la realización de un seguimiento de los talleres a través de cuestionarios de satisfacción que permitan mejorar la calidad de los talleres.

Dentro de la gran propuesta realizada por [REDACTED], hubiera sido interesante que la misma hubiese recogido todas las propuestas y acciones a realizar de un modo más esquemático y personalizado para la Fundación.

PUNTUACIÓN: 17 PUNTOS.

- [REDACTED]

CRITERIOS SUJETOS A JUICIO DE VALOR (HASTA 20 PUNTOS):

PLAN DE TRABAJO.....20 puntos

La propuesta de [REDACTED] comienza indicando que, en el supuesto de que resultase adjudicatario, el personal adscrito al contrato de [REDACTED] mantendría una reunión con los responsables del proyecto para realizar la planificación del mismo. Proponen una reunión inicial, y una posterior toma de datos para conocer su funcionamiento. Igualmente, es positivo que se comprometan a analizar toda la documentación obrante en la Fundación, relacionada con su adecuación al RGPD y medidas de seguridad adoptadas en materia de protección de datos, con el fin de realizar una auditoría inicial de nivel de cumplimiento.

Establecen que, a partir de lo descrito, elaborarán la documentación necesaria (memorias, informes, procedimientos o cualquier documento que la Fundación requiera) y definirán las medidas jurídico-organizativas y técnicas a actualizar o implantar por la Fundación. Este, es un correcto punto de partida.

También es muy interesante su flexibilidad respecto a las comunicaciones, facilitarían una cuenta de correo electrónico para atender incidencias, consultas y cualquier solicitud de actuación, además, es muy valorable que no establezcan límites en cuanto al número de consultas a realizar.

[REDACTED] divide su plan de trabajo principalmente en, una fase inicial de revisión y otra segunda fase de adaptación, lo cual es adecuado ya que el pliego de prescripciones técnicas también divide las acciones necesarias en estos dos puntos.

Dentro de la primera fase, se vuelve a indicar que se realizará una evaluación inicial del estado de cumplimiento de la normativa aplicable en materia de protección de datos personales mediante análisis de la documentación existente.

Respecto al registro de actividades de tratamiento, establecen que, si se requiere su actualización, [REDACTED] se pondrá en contacto con los responsables de las áreas de cada una de las actividades del tratamiento que existieran en la Fundación y fijará una reunión para poder ir actualizando como se precisa. Por su parte, en relación con el análisis objetivo de riesgos inherentes a cada uno de los tratamientos de la Fundación, proponen revisar las medidas de seguridad implantadas y en su caso se determinar las medidas que fueran necesarias implantar y la necesidad de llevar a cabo una evaluación de impacto. También realizarán evaluaciones de impacto en la protección de los datos personales, en la Fundación, para determinar las salvaguardas necesarias para garantizar la privacidad y seguridad de los datos personales.

También revisarán las medidas de seguridad aplicadas en los tratamientos realizados en soporte papel y los formularios y modelos utilizados por la Fundación u otros soportes de recogida en los

que se recaban datos personales, con el fin de analizar la inclusión de cláusulas informativas y consentimientos informados. Estas medidas parecen correctas y adecuadas, y se valora positivamente.

La propuesta de [REDACTED] continúa mencionando otras acciones a realizar/información a solicitar, sin embargo, no existe una explicación de cómo se llevarían a cabo estas acciones o porque es importante recabar la información. El licitador se limita a nombrar (Transferencias internacionales de datos, Procedimiento de gestión y notificación de brechas de seguridad, Procedimiento de privacidad desde el diseño y por defecto).

Por ejemplo, respecto al procedimiento de conservación y destrucción de datos personales, solo se indica que se determinarán los mecanismos de destrucción segura, pero no se explican que criterios, o como se procedería a su determinación.

En la segunda fase, [REDACTED] indica que procederá a la adaptación de la normativa realizando actuaciones como el análisis y entrega de cláusulas informativas adaptadas a cada tratamiento y categoría de interesados.

Establecen que determinarán un procedimiento de solicitudes de ejercicio de derechos en el que se definirá la actuación a llevar por la Fundación ante la recepción de ejercicios. En este punto sí que se indica cómo se debería actuar. Respecto a la realización de un documento de análisis objetivo de riesgos, establecen la necesidad de llevar a cabo una evaluación de impacto. En este sentido, sí que fijan importantes parámetros y definen una metodología para la realización de las evaluaciones de impacto en materia de protección de datos personales.

Una mejora respecto a los requisitos mínimos que parece muy conveniente es la adaptación de Aviso legal, política de privacidad y política de cookies en el sitio web de la Fundación.

La oferta del licitador continúa mencionando acciones como la realización de auditorías de protección de datos, la remisión de boletines jurídicos periódicamente respecto a las novedades en materia de protección de datos, la asistencia al órgano que asume las competencias de Delegado de Protección de Datos o el asesoramiento y resolución de las consultas sobre protección de datos realizadas desde otros organismos como Comisión Delegada.

Respecto al asesoramiento en cuestiones de seguridad de la información, sí que se debe destacar que se establezca una explicación mayor de, por ejemplo, cuales serían los controles de cumplimiento periódico.

Por otra parte, respecto a las Funciones de Delegado de Protección de Datos, la oferta del licitador indica que existirá una comunicación constante, y un seguimiento de los proyectos determinados de cara a optimizar el cumplimiento de las diferentes normas objeto de la prestación de los servicios. En este punto se mencionan funciones básicas mencionadas en el pliego de

prescripciones técnicas. Algunas de estas acciones únicamente son mencionadas, sin embargo, sí que se deben destacar otras funciones de las que proponen.

Por ejemplo, en el asesoramiento en la realización de evaluaciones de impacto y preparación de la consulta previa, es valorado muy positivamente que el licitador proponga asesorar sobre la idoneidad o no de llevar a cabo una evaluación de impacto determinada. Además, indican que realizarían una consulta previa a la Agencia Española de Protección de datos si de esa evaluación de impacto entrañara un alto riesgo.

También es interesante su propuesta de evaluación, y en su caso, notificación de las brechas de seguridad o vulneraciones relevantes que pudieran producirse en la Fundación.

Por último, en la oferta del licitador encontramos adjunto un cronograma de trabajo bien diseñado y un cuadro con el equipo técnico que estaría adscrito al contrato. También, se mencionan los medios materiales disponibles, aspecto valorado positivamente; y las herramientas innovadoras en la prestación del servicio, dentro de las que destacan:

- La Plataforma de gestión de protección de datos, que asegura garantizar un intercambio de archivos, expedientes y datos de forma eficaz, seguro y práctico [REDACTED] cuenta con una plataforma de implementación propia llamada "Intranet"). Este aspecto nos resulta muy útil y es valorado positivamente debido al grado de pragmatismo que ofrece.
- La herramienta Gestor Digital de Expedientes: Offionline. Se indica que esta, sirve de guía, carpeta documental y seguimiento de cada uno de los expedientes. El responsable del contrato designado por la Fundación podrá acceder en cualquier momento a su documentación en materia de protección de datos, mediante el usuario y contraseña que le serán facilitados. Esta propuesta es igualmente muy práctica y aporta un valor adicional a la oferta del licitador.

CONCLUSIONES:

La oferta de [REDACTED] sigue la estructura descrita en el pliego de prescripciones técnicas, sin embargo, existen algunas acciones necesarias que no encontramos descritas en su oferta, en consecuencia, estas actuaciones con carácter mínimo y enunciativo para el cumplimiento de los fines que no se encuentran desarrolladas. Además, se considera que la oferta de [REDACTED] es demasiado general y no se encuentran puntos personalizados para la Fundación en ciertos aspectos que son importantes para el presente concurso.

Existen aspectos de la oferta en los que el licitador se limita a mencionar acciones, sin establecer medidas o acciones a llevar a cabo para alcanzar resultados. Por ejemplo, cuando se habla sobre el diseño e implantación de medidas de seguridad o cuando simplemente se menciona el plan de formación sin entrar a determinar un plan de ejecución del mismo.

Si bien es cierto, que a pesar de lo expuesto se valoran positivamente otros aspectos.

El primer punto destacable es su plan de atención y comunicación, tanto en situaciones ordinarias como extraordinarias, indica que la respuesta, podrá ser de forma verbal (telefónica), por correo electrónico o bien por medio de emisión de informe en función de la complejidad de la consulta. Incluso, se adjunta un cuadro en el que se determina: Tipo de consulta, el tiempo estimado de resolución y el funcionamiento de resolución. También, una mejora que parece muy conveniente e innovadora es la adaptación de Aviso legal, política de privacidad y política de cookies en el sitio web de la Fundación.

La propuesta sobre las herramientas innovadoras en la prestación del servicio es valorada muy positivamente debido al grado de pragmatismo que ofrece.

PUNTUACIÓN: 13 PUNTOS

- [REDACTED]

CRITERIOS SUJETOS A JUICIO DE VALOR (HASTA 20 PUNTOS):

PLAN DE TRABAJO.....20 puntos

[REDACTED] comienza exponiendo en su oferta técnica las funciones que desarrollará cada miembro del personal interviniente.

Respecto al plan de trabajo, se propone en primer lugar, crear una dirección de correo específica para centrar todas las consultas y correspondencia entre la Fundación y [REDACTED]. Esta idea resulta conveniente.

La oferta del licitador continúa indicando que la misma, se divide en dos fases (ambas se corresponden con la estructura planteado en el pliego de prescripciones técnicas).

En la primera fase (Análisis previo y resolución de consultas), se propone que el Equipo de [REDACTED] conozca y comprenda en profundidad los tratamientos de datos de la Fundación, para ello proponen un plan de acción muy completo y que cubre todas las necesidades de la Fundación. Estará basado en el estudio de toda la documentación que se aporte (RAT, análisis de riesgos, evaluaciones de impacto, procedimientos internos, tipología de contratos relevantes, etcétera), mientras que, al mismo tiempo, se procederá a entrevistar a las personas implicadas de forma más recurrente y relevante en el tratamiento de datos de carácter personal. Incluso aportan un cronograma con todas las tareas necesarias a desarrollar en el que se especifican en que semana se comenzará con cada una de ellas.

Respecto a la segunda fase, es destacable lo que indican respecto a las reuniones. Proponen la realización de una reunión mensual para tratar los asuntos de protección de datos, y también indican que el equipo de trabajo estará disponible para asistir telemáticamente a otras reuniones que precise la Fundación.

Resumen su servicio en esta fase en dos ámbitos. El primero de ellos es el relativo al soporte y consultoría en materia de protección de datos, en este punto el licitador se limita a mencionar las actuaciones necesarias para el cumplimiento de los fines con carácter mínimo y enunciativo. Se echa en falta un detalle de cómo se procedería a actuar en cada una, o, al menos, en las que el licitador considerase más relevantes.

Lo mismo ocurre con la segunda parte relativa al servicio de externalización del DPD.

A pesar de no aportar un plan de actuación, el licitador sí que ofrece medidas para asegurar la calidad de los trabajos divididas en medios materiales, seguridad y confidencialidad. De ellas, nos gustaría resaltar su Sistema de Gestión integrado de Calidad y el compromiso de cumplir con los requisitos establecidos por las normas internacionales.

También se valora positivamente las medidas dispuestas por [REDACTED] para vigilar y garantizar el adecuado cumplimiento del contrato.

A pesar de todo lo expuesto, en la oferta de [REDACTED] no se establece ningún plan respecto a la formación del personal de la Fundación, aspecto que se hubiera valorado muy positivamente.

CONCLUSIONES:

En primer lugar, se ha de resaltar que la oferta de [REDACTED], a pesar de ser esquemática, recoge todos los mínimos exigidos en el pliego de prescripciones técnicas. Nos parece muy eficiente la forma en la que exponen cuando procederían a dar lugar a cada acción.

Si bien es cierto, que, a pesar de esta buena valoración, hubiera sido interesante encontrar un plan de cómo se llevarían a cabo las actuaciones necesarias para el cumplimiento de los fines, así como propuestas de mejora sobre alguna de ellas.

PUNTUACIÓN: 13 PUNTOS

- [REDACTED]

CRITERIOS SUJETOS A JUICIO DE VALOR (HASTA 20 PUNTOS):

PLAN DE TRABAJO.....20 puntos

El licitador comienza su propuesta con el desarrollo de una memoria técnica en la que se recogen todas y cada una de las actuaciones mínimas recogidas en el pliego de prescripciones técnicas, tanto para el Soporte y consultoría RGPD y LOPD-GDD, como para el Servicio de externalización del Delegado de Protección de Datos.

Es destacable, que, en todas estas acciones necesarias, indique y describa detalladamente cómo procedería a su ejecución.

De todas las actuaciones descritas respecto al Soporte y consultoría RGPD y LOPD-GDD, destacan algunas como lo planteado respecto al asesoramiento en materia de protección de datos cuando así se solicite por la Fundación, [REDACTED] indica que realizará esta acción desarrollando procedimientos ad-hoc que describan la implicación que tiene la normativa de protección en el desarrollo de la actividad profesional. Además, algo que aporta un valor adicional es que también realizarían labores de información y asesoramiento a aquellas entidades externas que tengan implicación en los tratamientos de datos llevados a cabo, informándoles de las implicaciones en materia de protección de datos. También indican en este punto un canal de comunicación directo por vía electrónica y telefónica para la atención y resolución de las consultas planteadas.

Igualmente, en relación con el asesoramiento en la respuesta a los requerimientos de información que provengan de las autoridades de control y supervisión, [REDACTED] establece que dará soporte a la Fundación en aquellos requerimientos de información, en eventuales inspecciones y procedimientos administrativos. Asimismo, indican, redactará las consultas previas pertinentes que la Fundación haya de presentar ante la Agencia Española de Protección de Datos (AEPD) atendiendo al artículo 36 RGPD y en el caso de la recepción de reclamaciones ante la AEPD, [REDACTED] enumera las actuaciones a realizar. Todas estas propuestas se valoran muy positivamente.

Con el fin de cumplir con los controles periódicos de cumplimiento, durante los tres primeros meses de ejecución del contrato (y durante toda la vida del contrato), [REDACTED] realizará una revisión del sistema documental y procedimental de protección de datos de la Fundación, emitiendo un informe que reflejará aquellas recomendaciones de mejora. Y, adicionalmente elaborarán de informes y documentos de diversa índole que, en función de las necesidades que vayan surgiendo en cada momento, podrán ser reclamadas por las distintas áreas funcionales de la Fundación, lo cual resulta muy conveniente para las necesidades de la Fundación.

En general, también destacan propuestas como: 1) revisiones del Registro de Actividades del Tratamiento, nuevos proyectos que impliquen un nuevo tratamiento de datos personales; 2) supervisión de la adecuación de los tratamientos de la Fundación cuya base de legitimación sea el consentimiento desde una visión legal y técnica; 3) Llevar a cabo un proceso de revisión tanto

de los procedimientos realizados determinantes de cuestiones como, brechas de seguridad o ejercicio de derechos y revisar el Registro de Actividades de Tratamiento, el análisis de riesgos y evaluaciones de impacto, implementando medidas de seguridad para poder asegurarse de que las mismas mitigan los riesgos detectados; 4) Emisión por parte del delegado de Protección de Datos de un Informe en el que quedarán patentes todas las acciones llevadas a cabo a lo largo del año; 5) Establecimiento de reuniones de seguimiento mensuales (entre el personal del equipo y los responsables de cada Área o Departamento o cualquier otra persona integrante del área que pueda tener dudas); 6) Comunicación de novedades legislativas a través de píldoras informativas que compilarán las novedades o criterios en materia de protección de datos dados por la Agencia Española de Protección de Datos y que tengan relevancia o afecten a la actividad o tratamientos llevados a cabo por la Fundación.

De todas las actuaciones descritas en relación con el Servicio de externalización del delegado de Protección de Datos destacamos que establezcan una primera fase de organización en la que se mantendrán las primeras reuniones con el fin de conocer el organigrama de la Fundación y la puesta a disposición de [REDACTED] de cada una de las políticas y procedimientos que conforman el sistema de protección de datos de la organización.

Además, en su oferta, [REDACTED] incluye acciones como, emitir informes y procedimientos relativos a las cuestiones o tratamientos que conlleven una especial atención bien por las categorías o volumen de datos tratados, o bien por qué se valore por parte del DPD. También, indican que se revisará la formación y acciones de concienciación realizadas en la Fundación con el objetivo de, en su caso, mejorarlas o modificarlas para adaptarlas a las necesidades formativas de los empleados. El DPD también se mantendrá al tanto del desarrollo de las auditorías realizadas en la Fundación de forma que conozca las condiciones en las que se desarrollan las mismas y si estas examinan las cuestiones determinantes de acuerdo con la normativa vigente.

Por otra parte, [REDACTED] establece de una serie de mecanismos con el fin de asegurar la calidad en la ejecución de todas las fases del proyecto (Mecanismos de coordinación e interlocución del equipo de [REDACTED] con los responsables de cada una de las áreas/departamentos, mecanismos de supervisión y seguimiento del proyecto y mecanismos para la identificación y prevención de riesgos asociados al desarrollo del proyecto) y enumera una serie de acciones para asegurar la calidad durante el desarrollo del proyecto. Ambas propuestas son muy bien valoradas.

Como valor añadido también proponen un “Plan de seguimiento del proyecto” que se articulará mediante una serie de planes de acción y se apoyará en los datos proporcionados por el sistema, así como en los medios existentes. Para el seguimiento del proyecto [REDACTED] se apoyará en la Herramienta, [REDACTED] para la gestión y realización de las labores de asesoramiento y supervisión en el cumplimiento de la normativa, dicha herramienta también permitiría realizar un seguimiento de las deficiencias detectadas y hacer un seguimiento del Plan de Acción de establecido, dando la posibilidad, asimismo, de llevar un control de las evidencias que mitiguen tales deficiencias. En su propuesta, se establece incluso que, si fuera se implantarían nuevas medidas técnicas y organizativas y se desarrollarían nuevos procedimientos.

La oferta de [REDACTED] incorpora además un plan de acción a modo de tabla organizativa, en la que se ilustran el servicio o acción a desarrollar, el plazo en el que los mismos se llevarán a cabo y el personal interviniente en cada uno, así como su dedicación. Por ejemplo, en la asesoría en materia de protección de datos personales, para dar respuesta a los nuevos acontecimientos o prácticas de relevancia para la observancia del RGDP, se indica que las consultas se responderán en máximo 8 horas, que las consultas calificadas por la Fundación como No urgentes, se contestarán en máximo de 24 horas, y que estas consultas se harán bien por medios electrónicos o por llamada telefónica o de forma presencial. También señalan que, el responsable máximo del servicio tendrá dedicación plena en cuestiones urgentes, y que los demás miembros del equipo darán soporte al responsable y tendrán dedicación parcial en consultas urgentes de complejidad elevada, mientras que en consultas no urgentes de complejidad media-baja tendrán dedicación plena.

El hecho de que hayan elaborado este cuadro tan ilustrativo y práctica aporta un gran valor a la oferta del licitador, y es valorado muy positivamente.

Por último, [REDACTED] menciona a los medios humanos adscritos, especificando las funciones asignadas a cada uno de los miembros del equipo de forma clara.

CONCLUSIONES:

Lo primero que se debe destacar de la propuesta de [REDACTED] es que la misma está desarrollada a partir de la estructura descrita en el pliego de prescripciones técnicas y a partir de ella desarrolla la metodología a aplicar en cada actuación.

Además, existe en su oferta un hecho muy destacable y valorado, ya que su elaboración de un cuadrante en el que se expongan todos los plazos y las personas responsable e implicadas en cada actuación, hace de esta oferta técnica un trabajo muy elaborado y claro y, en consecuencia, se valora su oferta técnica de forma muy positiva.

El único punto que no encontramos en la oferta de [REDACTED] y hubiera aportado valor a la oferta es el relativo a la formación del personal de la Fundación en materia de protección de datos.

PUNTUACIÓN: 17 PUNTOS

- [REDACTED]

CRITERIOS SUJETOS A JUICIO DE VALOR (HASTA 20 PUNTOS):

PLAN DE TRABAJO.....20 puntos

El licitador comienza su propuesta con el desarrollo de una memoria técnica en la que se recogen las diferentes actuaciones a desarrollar. Las mismas, están fraccionadas en fases. En la Fase I se realizará una evaluación de riesgos inicial de los sistemas de tratamiento de datos personales dispuestos por la fundación y se elaborará de un informe de conclusiones provisionales, en el que se analizará el cumplimiento de las obligaciones básicas recogidas por la normativa de aplicación en protección de datos (derecho de información, consentimientos, etc.) así como aquellas medidas técnicas necesarias para la seguridad de la información tratada).

También proponen realizar una revisión y actualización en su caso, del registro de actividades de tratamiento de datos (ART. 30 RGPD) articulado por la Fundación, donde queden delimitadas las distintas finalidades de la información personal a la que la Fundación accede y trata. Resulta correcta la explicación que realiza el licitar sobre este aspecto.

Adicionalmente, en relación con los datos de salud, se llevará a cabo una evaluación de impacto concreta sobre los riesgos que un uso desprotegido de los mismos, pueda implicar para los derechos asistenciales de los pacientes o participantes en estudios de investigación. En este aspecto serán analizadas las distintas transferencias internacionales de datos a EE. UU. en las que se encuentre participando la Fundación, y se confeccionará un protocolo de regularización y adaptación a los nuevos escenarios. Esta propuesta al no ser un mínimo, aporta valor a la oferta del licitador.

Otras propuestas interesantes son: 1) La revisión y actualización (o en su caso confección) de un manual de medidas técnicas y organizativas que garantice un tratamiento seguro de la información por parte de la Fundación; 2) Revisión, o en su caso confección, del protocolo de gestión de violaciones de seguridad; 3) Actualización de las cláusulas informativas relativas a la obtención de datos de carácter personal de los distintos usuarios de la Fundación en sus diferentes soportes; 4) Revisión, o en su caso confección, de los modelos contractuales para la contratación de servicios profesionales por parte de la fundación.

Respecto a la asunción del cargo de Delegado De Protección De Datos de la Fundación, [REDACTED] asegura que cumplirá con las funciones recogidas tanto en el pliego de prescripciones técnicas como en el RGPD, además señalan que, se articulará una dirección de correo electrónico, donde además de ser notificada a la Agencia Española de Protección de Datos (AEPD), será atendida de forma regular por el equipo mencionado por el licitador en su oferta.

Se valora positivamente la propuesta relativa a la formación al personal de la Fundación.

La oferta de [REDACTED] continúa estableciendo un plan de acción, el mismo recoge que, tras haber desarrollado el trabajo de revisión y verificación de todos los registros documentales y electrónicos descritos en la memoria, en esta segunda fase se procederá a la ejecución material de todas aquellas recomendaciones, actualizaciones y/o solución de incidencias que se hayan advertido.

A continuación, en la oferta del licitador se recoge, en una tercera fase un plan de soporte y formación, el cual está perfectamente planteado y supone un aspecto muy positivo. Respecto al soporte, indican que, se llevará a cabo de forma presencial y de forma telemática, de tal modo que las consultas de la Fundación se trasladarán vía email y serán atendidas dentro de las 48 horas siguientes a su recepción. En cuanto a la formación, se propone un programa formativo (4 cursos: 8 horas en total) al personal de la Fundación. Adjuntan un índice completo de contenidos para cada curso.

[REDACTED] menciona en su propuesta algo innovador. Debido a que la Fundación es titular de un Biobanco hospitalario proponen, atendiendo a los documentos cuya confección está prevista tanto por la Ley 14/2007, de Investigación Biomédica como por el Real Decreto 1716/2011, de 18 de noviembre, por el que se establecen los requisitos básicos de autorización y funcionamiento de los biobancos con fines de investigación biomédica y del tratamiento de las muestras biológicas de origen humano, revisar: 1) Reglamento Interno del Biobanco; 2) Memoria descriptiva; 3) Acuerdo de cesión de muestras, etc.

Por último, el licitador en su oferta adjunta a estructura de medios propuesta para dar soporte directo a la Fundación en la asunción de los servicios objeto de la presente propuesta, estará compuesta de forma directa por 3 profesionales.

CONCLUSIONES:

La oferta de [REDACTED] no sigue la estructura descrita en el pliego de prescripciones técnicas, y, en consecuencia, la estructura no es valorada de forma positiva. Sin embargo, a pesar de no mencionar muchas de las actuaciones mínimas recogidas (hay puntos donde sí se mencionan, pero se asegura su cumplimiento de forma generalizada), la oferta sí que contiene otras propuestas adicionales que se valoran positivamente. Por ejemplo, que se mencione a las personas responsables e implicadas en las actuaciones, que propongan la revisión o confección de los modelos contractuales, etc.

Se destaca de la presente oferta la propuesta respecto al Biobanco hospitalario.

PUNTUACIÓN: 16 PUNTOS

A continuación, se presenta un cuadro resumen con la valoración de las ofertas

CRITERIOS SUJETOS A JUICIO DE VALOR (HASTA 20 PUNTOS):	Puntuación						
LICITADOR	AUREN	DACBEACHCROFT	PONS	PRODATEX	SOTHIS	UNIVE ABOGADOS	PLIEGOS
Plan de trabajo: Forma de llevarlo a cabo y el seguimiento del servicio demandado que garantice la eficacia y calidad del mismo, con inclusión de una memoria descriptiva relativa a la propuesta sobre la organización del trabajo y el plan de acción propuesto para llevar a cabo el servicio, con indicación del personal interviniente, grado de dedicación y los medios a disponer para su desarrollo.	17	16	13	19	17	13	20

Madrid, 14 de febrero de 2023

Dña. María Elena Lérica Tejada.

D. Jose Ignacio Anaya Campos

Dña. Begoña Saenz de Tejada Madina

Dña. Olaitz Berástegui Lizarraga
