INFORME DE VALORACIÓN DE LOS CRITERIOS DE ADJUDICACIÓN SUBJETIVOS SUJETOS A EVALUACIÓN PREVIA (SOBRE DOS) PARA LA CONTRATACIÓN DE LA PRESTACIÓN DE LOS SERVICIOS DE CIBERSEGURIDAD GESTIONADA DE LAS CORTES DE ARAGÓN LOTE 2. EXPTE. 30/2020.

1.- OBJETO DEL CONCURSO

El objeto del contrato consiste en la prestación de servicios de gestión y soporte de seguridad informática, en el marco de las competencias encomendadas al Servicio de Informática y Nuevas Tecnologías.

El Lote 2: Reglamento General de Protección de Datos y Delegado de Protección de Datos externo.

2.- EMPRESAS QUE HAN PRESENTADO OFERTA

Han presentado oferta las siguientes empresas:

- TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U.
- CENTRO REGIONAL DE SERVICIOS AVANZADOS, S.A.
- ECIX ARAGÓN CONSULTING, S.L.
- OESÍA NETWORKS, S.L.
- AUDIDAT 3.0, S.L.U.
- SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U.

El presupuesto base de licitación, aprobado por la Mesa de las Cortes de Aragón, para este concurso es como máximo de 19.800€ IVA excluido, (23.958 € IVA incluido), repartido en las siguientes anualidades:

EJERCICIO	**IMPORTE PRESUPUESTO BASE LICITACIÓN (IVA excluido)**	**IMPORTE PRESUPUESTO BASE LICITACIÓN (IVA incluido)**
2021 (1 julio – 31 diciembre)	4.950 €	5.989,50 €
2022 (enero a diciembre)	9.900 €	11.979 €

2023 (1 enero a 30 junio)	4.950 €	5.989,50 €
TOTAL	**19.800 €**	**23.958 €**

3.- ESTUDIO DE LAS OFERTAS PRESENTADAS

Tal y como se especifica en el Anexo XI del pliego de cláusulas administrativas particulares, los criterios de valoración de las ofertas sujetos a evaluación previa (Sobre dos) y la ponderación de puntos correspondiente son los siguientes:

LOTE 2: Reglamento General de Protección de Datos y Delegado de Protección de Datos externo.

CRITERIOS DE VALORACIÓN	**PUNTUACIÓN**
2.1.- Criterio: Servicio de Cumplimiento del Reglamento General de Protección de Datos incluyendo un Delegado de Protección de Datos externo	**Hasta 30 puntos**
Se valorará la claridad expositiva, detalle y personalización del servicio para el cumplimiento del RGPD. Deberán incluirse expresamente y en el orden indicado los siguientes aspectos: - Plan de Cumplimiento del Reglamento General de Protección de Datos: Metodología y gestión del cumplimiento normativo. Detalle y adecuación a la Administración Pública. Integración con el cumplimiento del Esquema Nacional de Seguridad. Ampliación y mejora continua de los aspectos indicados. - Plan de gestión del cumplimiento del RGPD: Planteamiento general. Herramienta que se utilizará y sus principales características. Ampliación y mejoras. - Plan de Formación RGPD: Perfil, tipología de la formación, número de cursos y contenidos. Ampliación y mejoras. - Delegado de Protección de Datos externo. La empresa licitadora deberá detallar el currículum de la persona que ejercerá las funciones de DPD responsable, indicando titulaciones adicionales, formación adicional relacionada y experiencia en trabajos similares.	

2.2.- Criterio: Plan de Soporte y mantenimiento	Hasta 5 puntos
Se valorará la claridad expositiva, detalle y personalización del Plan de Soporte y mantenimiento, obligatoriamente con la siguiente estructura: Planteamiento general. Descripción del sistema centralizado para la realización de consultas/peticiones. Servicios y prestaciones de soporte con horarios de atención y tiempos de respuesta. Procedimientos y mecanismos de gestión para la resolución de consultas/peticiones. Ampliación y mejoras de los aspectos indicados.	
2.3.- Criterio: Plan de transición y devolución del servicio	**Hasta 5 puntos**
Se valorará la claridad expositiva, detalle y personalización del plan de transición y devolución de los servicios, obligatoriamente con la siguiente estructura: Planteamiento general. Recursos dedicados a las diferentes tareas. Estimación temporal para su realización, compromiso de plazos de entrega y gestión de desviaciones. Número y sesiones de traspaso/devolución de conocimiento. Documentación que se generará para garantizar el solapamiento de actividades y la transferencia tecnológica y del conocimiento. Medidas a implantar para minimizar el impacto de dicha migración en la disponibilidad de los servicios por parte del Parlamento. Ampliación y mejoras de los aspectos indicados.	
TOTAL	**40 PUNTOS**

3.1 CRITERIO: Servicio de Cumplimiento del Reglamento General de Protección de Datos incluyendo un Delegado de Protección de Datos externo: Hasta 30 puntos

Se valorará, la claridad expositiva, detalle y personalización del servicio para el cumplimiento del RGPD. Deberán incluirse expresamente y en el orden indicado los siguientes aspectos:

- Plan de Cumplimiento del Reglamento General de Protección de Datos: Metodología y gestión del cumplimiento normativo. Detalle y adecuación a la Administración Pública. Integración con el cumplimiento del Esquema Nacional de Seguridad. Ampliación y mejora continua de los aspectos indicados.
- Plan de gestión del cumplimiento del RGPD: Planteamiento general. Herramienta que se utilizará y sus principales características. Ampliación y mejoras.
- Plan de Formación RGPD: Perfil, tipología de la formación, número de cursos y contenidos. Ampliación y mejoras.
- Delegado de Protección de Datos externo. La empresa licitadora deberá detallar el currículum de la persona que ejercerá las funciones de DPD responsable, indicando titulaciones adicionales, formación adicional relacionada y experiencia en trabajos similares.

3.1.1.- Resumen de las ofertas presentadas

1) La empresa TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U. propone, en su oferta, los siguientes planes y Delegado de Protección de Datos externo:

   - Plan de Cumplimiento del Reglamento General de Protección de Datos

   Dentro de la metodología y gestión del cumplimiento normativo, propone una estrategia de mejora continua con metodologías como PMBOK o ISO21500. Se incluye gráfico. Estará basada en cuatro

pasos: Planificar, ejecutar o hacer, controlar o verificar y actuar para mejora continua. Alineamiento con otras metodologías y sistemas de gestión, permitiendo la adopción de normativas internas que se integren dentro de un marco de cumplimiento, retención de registros y evidencias, implementación de enfoques de "diseño de protección de datos" y de "definición de protección de datos" en proyectos, documentación y registro de las acciones de cumplimiento.

Dentro del detalle y adecuación a la Administración Pública, se menciona el artículo 18.4 de la CE y el reglamento UE 2016/679 (RGPD), el concepto de dato personal y que es necesaria la asignación de recursos tanto personales como económicos.

Dentro de la integración con el cumplimiento del Esquema Nacional de Seguridad, no se propone nada específico.

Dentro de la ampliación y mejora continua de los aspectos indicados, no se propone nada específico.

- Plan de gestión del cumplimiento del RGPD

Dentro del planteamiento general, propone las siguientes actividades:

Realización de Planificación empezando con una reunión de inicio de proyecto, indicando los objetivos de la reunión. Como resultado se elaborarán los entregables: Documento de planificación de proyecto con la descripción de tareas y cronología de cada una de las tareas descritas como objeto del contrato y Acta de reunión con los acuerdos alcanzados.

Realización Documento con roles y responsabilidades.

Realización Auditoría inicial interna que permita detectar las insuficiencias del sistema y el estado de cumplimiento. Se indica metodología para el desarrollo de auditorías según lo dispuesto por la Guía CCN-STIC 802 que a su vez se remite a la norma ISO 19011, incluyendo en un gráfico los pasos. Se elaborará entregable Informe de auditoría con indicación de conformidades, no conformidades y acciones.

Realización Registro de Actividades del Tratamiento recabando la máxima información posible sobre el flujo de datos personales en la entidad, registrando las diferentes etapas por las que los datos personales transcurren durante su ciclo de vida. Se abordarán los aspectos jurídicos necesarios como revisión y documentación de la finalidad del tratamiento, responsables o corresponsables de los tratamientos, revisión de la licitud de los tratamientos, identificación de las comunicaciones de datos, revisión de las transferencias internacionales de datos, identificación y propuesta de los plazos de conservación de los datos personales para cada tratamiento. Se elaborará entregable Registro de Actividades del Tratamiento.

Realización Evaluación de Impacto en Privacidad (EIPD) con los siguientes pasos: Fase preliminar con una valoración principalmente sobre la posibilidad de "riesgo alto", fase de contexto con una valoración de su necesidad y proporcionalidad como paso previo a la realización de una EIPD, fase de gestión de riesgos mediante análisis de riesgos especializado identificando amenazas, valorándolas y evaluándolas y proponiendo controles para tratar el riesgo. Finalmente las fases de conclusión, y

validación y supervisión con seguimiento al plan de acción. Se incluye gráfico detallado con los pasos. Se elaborarán los entregables Análisis de la necesidad de EIPD e Informes completos con la EIPD.

Realización de Análisis de riesgos identificando los activos, amenazas, vulnerabilidades, impactos, necesidades de seguridad y contramedidas. Será integrable con el análisis de riesgos ENS. Una vez se obtienen los niveles de riesgo se determinarán las decisiones a tomar y las medidas de mitigación para lo que se hará uso de la plataforma Sandas GRC. Se elaborará entregable Análisis de riesgos.

Realización de Procedimientos y Normativas de seguridad revisando la estructura del marco normativo existente para verificar el adecuado cumplimiento del Esquema Nacional de Seguridad y garantizar que los principios de Protección de Datos quedan cubiertos. Se incluye gráfica explicando los tipos de medidas de los que consta el ENS.

Realización Deber de información y Cláusulas, revisando y proponiendo la relación de cláusulas de conformidad con los artículos 13 y 14 RGPD y artículo 11 de la LOPDGDD. Se revisará el procedimiento de obtención del consentimiento del titular de los datos en el caso que fuese necesario u obligatorio, de acuerdo con los artículos 7, 8, 9 y 10 del RGPD y 6, 7, 8 y 9 de la LOPDGDD con especial énfasis en los datos sensibles. Se incluye tabla modelo de cláusulas referencia de la Guía de la Agencia Española de Protección de Datos sobre el Deber de Información y el artículo 11 de la LOPDGDD. Se especifican los aspectos a tener en cuenta para el tratamiento de videovigilancia como cartel o distintivo,

información adicional, prestadores de servicios y matices según las diferentes formas de videovigilancia. Se elaborarán entregables Informe sobre el Deber de Informar con modelos de clausulados e Informe sobre el Deber de Informar en videovigilancia con protocolo y modelos.

Realización Atención de derechos, de acuerdo con los artículos 15 a 23 RGPD y de 12 a 18 LOPDGDD para la correcta atención de las solicitudes de ejercicio de derechos de acceso, rectificación, cancelación, supresión, oposición y en su caso portabilidad. Se verificará que incluya aspectos comunes a respetar como el carácter personalísimo de los derechos, necesidad de acreditación de la personalidad o representación, carácter independiente de los derechos, necesidad de carga de la prueba o cómo ejercitar los derechos. Prestarán el soporte necesario en la gestión práctica de cualquier solicitud efectuada. Se elaborará entregable Procedimiento formal de atención de derechos.

Realización Gestión y notificación de brechas de la seguridad, prestando soporte para realizar cualquier comunicación con la Agencia Española de Protección de Datos (AEPD). Plantea un proceso coordinado de gestión y notificación de incidentes según necesidades en materia de RGPD, LOPDGDD y otros criterios jurídicos como el Centro Criptológico Nacional respecto al ENS. Se plantea la integración del ciclo de gestión de brechas de seguridad establecido por la AEPD dentro del marco que da cumplimiento al ENS. Se estará atento a las novedades que se incorporen en la "Guía nacional de Gestión y Notificación de Ciberincidentes". Se elaborará entregable Procedimiento formal de gestión de brechas de seguridad.

Realización Contratos de prestadores de servicios con y sin acceso a datos, identificando los prestadores de un servicio que comporte tratamiento de datos y definición de cómo se ha de formalizar el acto jurídico de encargo de tratamiento de los datos personales. Se facilitará documentación de soporte que ayude a la entidad en la sección de un encargado con diligencia, y se propondrán en el propio modelo de contrato ciertas medidas de seguridad que requerir. Se tendrá en cuenta la Guía para la elaboración de contratos entre Responsables y Encargados de la AEPD. Cuando la prestación del servicio no represente un encargo del tratamiento y sea necesario, se redactarán cláusulas de confidencialidad con los prestadores correspondientes. Se elaborará entregable Informe sobre prestadores de servicios con y sin acceso a datos.

Realización Actividades continuas, entre las que se encuentran la supervisión continua de la legalidad, concienciación mediante un plan de concienciación continua al personal de la organización, cooperación con la Autoridad de control actuando como punto de contacto con la AEPD para resolver y tramitar cualquier cuestión.

Dentro de la herramienta que se utilizará y sus principales características, propone la herramienta Sandas GRC en modo SaaS. Dispone de opción multiusuario, visión holística del estado de avance del proceso de adecuación. Se introducirán los resultados de la ejecución de las distintas acciones. Permite la integración con PILAR e INES, dispone de un Gestor Documental, integración con otros marcos normativos, módulo para la gestión de riesgos basado en ISO 31000 y módulo de revisión para llevar a cabo tareas de auditoría, interlocución y verificación periódica del sistema de gestión.

Dentro de ampliación y mejoras, propone incorporar un Responsable de Cuenta para la consecución de los objetivos del proyecto a nivel comercial. La auditoría se llevará a cabo siguiendo metodologías reconocidas. Se revisarán textos legales web exigibles por razón de la LSSI-CE. El procedimiento de gestión de brechas se revisará/elaborará con atención a otros estándares internacionales o reconocidos. Se indica que la herramienta Sandas GRC dispone de módulos adicionales que permiten una gestión más adecuada pero no se especifican.

- Plan de Formación RGPD

Dentro del perfil, tipología de formación, número de cursos y contenidos, indican en una tabla el perfil, tipología, número de cursos y contenidos. Cumple los perfiles, número y duración mínimos exigidos en el pliego. Se añade el perfil Todo el público y la tipología uso de boletines, contenidos audiovisuales y avisos. Se realizará por docentes habituales. Se elaborará entregable Plan de Formación.

Dentro de ampliación y mejoras, proponen una circular mensual de comunicación interna y concienciación, creación de contenido audiovisual con píldoras informativas mensuales, invitaciones gratuitas para participar en ponencias y eventos, posibilidad de valorar y medir la calidad y eficacia de la formación a través de entrevistas, tests y cuestionarios según metodologías reconocidas.

- Delegado de Protección de Datos externo

Propone perfil Licenciatura en Derecho, Máster en Relaciones Internacionales y Comercio Exterior, Máster Profesional en Unión Europea especialidad en Nuevas Tecnologías, dos cursos, certificación Certified Data Privacy Professional, certificación APEP Certified Privacy, certificación Premio Nacional de Investigación Agencia Española de Protección de Datos, certificación Premio de Investigación Agencia Vasca de Protección de Datos. Experiencia de 24 años y medio.

2) La empresa CENTRO REGIONAL DE SERVICIOS AVANZADOS, S.A. propone, en su oferta, los siguientes planes y Delegado de Protección de Datos externo:

- Plan de Cumplimiento del Reglamento General de Protección de Datos

Dentro de la metodología y gestión del cumplimiento normativo, propone como metodología general del proyecto el uso de las directrices planteadas por la norma ISO 20000-1 para la ejecución de proyectos y servicios tecnológicos y los estándares incluidos en la norma ISO 27014 Gobernanza de la Seguridad de la Información así como los fundamentos ITIL. Desde el punto de vista del cumplimiento normativo emplea una metodología basada en su experiencia en clientes similares siguiendo las pautas del Reglamento General de Protección de Datos 2016/679, las Guías los Informes y Recomendaciones del Comité Europeo de Protección

de Datos y tendrá en cuenta consideraciones contenidas en otras normas como ENS y NIS, y otros estándares aplicables a la gestión de la información y la privacidad como normas ISO 27001 o 27701.

La metodología y gestión del cumplimiento normativo estará basada en normativas y estándares internacionales en materia de privacidad incluyendo las tareas de adecuación y mantenimiento dentro de un ciclo de mejora continua. Tendrá perspectiva integradora con otras normativas buscando la integración con el Esquema Nacional de Seguridad y el cumplimiento de los dictámenes de la Agencia Española de Protección de Datos aplicados a las Administraciones Públicas. Se apoyará en herramientas de gestión que darán soporte a todo el proceso de implantación y mantenimiento así como una base del conocimiento en materia de protección de datos. Realizarán un Plan de Implantación y Mantenimiento del Reglamento General de Protección de Datos y el servicio de Delegado de Protección de Datos con las siguientes líneas de trabajo: Proyecto general de implantación y mantenimiento siguiendo fases secuenciales, siendo el punto de partida una Auditoría inicial, con apoyo de la herramienta de gestión propuesta y la Oficina de GRC y teniendo como hitos de implantación el asesoramiento continuo, seguimiento en la implementación de medidas de seguridad, etc. Prestación de los servicios de Delegado de Protección de Datos con el soporte de la Oficina de Apoyo al DPD. Desarrollo de acciones formativas de concienciación en materia de privacidad, protección de datos y buenas prácticas.

Siguiendo como marco metodológico principal la doctrina de la Agencia Española de Protección de Datos aplicada a las

Administraciones Públicas, se realizará una reunión inicial y reuniones de seguimiento con los responsables de Las Cortes. Se elaborarán los entregables Actualización del Plan de Adecuación al RGPD/LOPDGDD e Informes de Actividad y Actas de las reuniones de seguimiento. Se realizará carga de información en la herramienta de gestión propuesta, conformando una base de conocimiento.

Dentro del detalle y adecuación a la Administración Pública, propone de forma detallada la Fase 1 Arranque de los Servicios de adecuación al cumplimiento de la normativa, servicios continuos del Delegado de Protección de Datos y las tareas relacionadas con la Formación y Concienciación incluyendo perfiles involucrados y entregables. Se detallan las tareas a realizar que en resumen serán: Auditoría inicial de cumplimiento siguiendo las pautas marcadas por la ISO 19011 (Auditoría de Sistemas de Gestión) para evaluar el nivel de madurez de los dominios establecidos e incluidos en un gráfico. Supervisión del cumplimiento normativo del RGPD, la LOPDGDD y normativas vinculadas al tratamiento de la información ENS, NIS, LSSI-CE. Colaboración con la Agencia Española de Protección de Datos. Supervisión y colaboración en la gestión y notificación de brechas de seguridad elaborando un procedimiento específico para la gestión de incidentes y brechas de seguridad vinculadas al tratamiento de datos personales. Supervisión del Registro de Actividades del Tratamiento mediante la herramienta de gestión propuesta y entrevistas por medios telemáticos con los responsables internos asociados a los tratamientos de datos personales, teniendo como objetivo disponer de un Registro de Actividades del Tratamiento que permita: Revisión y actualización del clausulado de protección de datos con

especial consideración para datos de categoría especial y vías de recogida de datos, Identificación de las bases de legitimación, Identificación de los encargados del tratamiento existentes y Especial consideración de los tratamientos vinculados a videovigilancia. Como última tarea proponen Asesoramiento en la creación o puesta en marcha de nuevas actividades del tratamiento, estableciendo los requisitos tanto jurídicos como técnicos y analizando los posibles riesgos en el tratamiento.

Dentro de la integración con el cumplimiento del Esquema Nacional de Seguridad, propone seguir las directrices marcadas por el Centro Criptológico Nacional, mediante identificación de los tratamientos de datos personales, integración de la valoración y riesgo de los datos personales dentro del análisis de riesgos de la seguridad, integración de la medidas de seguridad previstas en el Anexo II del ENS e integración de los procedimientos de gestión de incidentes en un procedimiento principal.

Dentro de la ampliación y mejora continua de los aspectos indicados, proponen la constante interlocución con los responsables de Las Cortes, la utilización de una herramienta de gestión y el análisis en paralelo de aquellas cuestiones que la LOPDGDD regula de forma específica en la medida en que afecten a Las Cortes.

- Plan de gestión del cumplimiento del RGPD

Dentro del planteamiento general, proponen un diagrama temporalizado en 24 meses con el desglose de una fase de adecuación de unos 11 meses y una fase de mantenimiento hasta 24 meses.

Dentro de la herramienta que se utilizará y sus principales características, propone la herramienta Global Suite en modo de servicio SaaS con licencia del módulo relativo al Reglamento General de Protección de Datos. Incluye gestor documental, modelo multiusuario con perfiles para personal de Las Cortes, Órganos de dirección y DPD, modelo participativo y colaborativo mediante módulo de encuestas, metodología MAGERIT, catálogo de riesgos, análisis de riesgos, soporta normativas como ISO 27001, 27002 y 22301, encuestas, integración de ticketing, workflow de gestión documental, workflow de tickets, Balanced Scorecard, integración con Directorio Activo de Las Cortes.

Dentro de ampliación y mejoras, indican que la herramienta incorpora identificación de procesos críticos y valoración del riesgo basada en la metodología MAGERIT, planes de adecuación o gestión del riesgo que permiten valorar el grado de avance de la implementación de los requisitos normativos, planes de auditoría de los requisitos normativos, interoperabilidad e integración Web Service y módulo de informes.

- Plan de Formación RGPD

Dentro del perfil, tipología de formación, número de cursos y contenidos, propone como entregable inicial un Plan de Formación y Concienciación anual sobre Protección de Datos. Como medios emplearán formación presencial o a través de medios telemáticos (videoconferencia), plataformas online y tareas específicas en concienciación y campañas de sensibilización en materia de privacidad (newsletters, píldoras informativas) obteniendo como entregables los materiales didácticos e informes de resultados de

las campañas. Cumple los perfiles, número y duración mínimos exigidos en el pliego.

Dentro de ampliación y mejoras, proponen utilizar la plataforma Smartfense específica para formación y concienciación de usuarios en el ámbito de la seguridad de la información. Dispone de personalización de contenidos utilizando la imagen corporativa de Las Cortes, amplio catálogo de contenidos pre-establecidos, posibilidad de llevar a cabo campañas dirigidas a determinados grupos de usuarios, obtención de estadísticas y datos sobre la eficacia de la formación, elaboración del desempeño y de los conocimiento adquiridos. Se indica un listado de cursos y contenidos complementarios al mínimo exigido. Ofrece la posibilidad de ejecutar acciones de concienciación a través del envío de newsletters, píldoras informativas, etc. indicando un listado de posibles acciones.

- Delegado de Protección de Datos externo

Propone perfil Licenciado en Derecho, formación sobre implantación de la LOPD y sobre Prevención de delitos en la Empresa/Compliance, Programa Ejecutivo Compliance Officer, ocho cursos y certificado de Auditor Interno de la norma ISO 27001. Experiencia de 8 años. Se incluye una tabla de tareas a realizar y entregables detallando el modelo de servicio.

3) La empresa ECIX ARAGÓN CONSULTING, S.L. propone, en su oferta, los siguientes planes y Delegado de Protección de Datos externo:

- Plan de Cumplimiento del Reglamento General de Protección de Datos

Dentro de la metodología y gestión del cumplimiento normativo, propone diversos servicios conforme a una metodología propia formada por Seguridad Jurídica, Inteligencia, Innovación Tecnológica, Riesgos Normativos, Matemáticas-Predicciones y Compliance/Normas vs Leyes. Se incluye gráfico. Pretende crear una cultura de cumplimiento basada en la concienciación de todos los factores humanos que intervienen en el tratamiento de datos personales. Se basa en un trabajo individualizado y ad hoc. Se partirá de una entrevista presencial con las personas que intervienen en el tratamiento de los datos tanto desde el punto de vista administrativo como técnico. El Sistema de Gestión de Protección de datos establece la estructura organizativa, las responsabilidades, los procesos y los recursos necesarios para obtener los objetivos propuestos y asegurar el cumplimiento.

Dentro del detalle y adecuación a la Administración Pública, propone la realización de una Auditoría interna revisando: Diseño de medidas técnicas y organizativas de seguridad para la protección de datos personales, según el Real Decreto 3/2010 de 8 de enero por el que se regula ENS en el ámbito de la Administración Electrónica modificado por el Real Decreto 951/2015 de 23 de octubre. Diseño de estándares de seguridad para la privacidad desde el diseño y por defecto, incluyendo algunos ejemplos. Verificación del principio de accountability con

un protocolo para bloqueo de datos en caso necesario así como la elaboración de una política de conservación de datos que garantice que no se conservan plazos superiores a los necesarios. Información y transparencia analizando cada una de las cláusulas utilizadas para facilitar la información necesaria a los interesados en los términos previstos en los artículos 13 y 14 del RGPD y se verificará el contenido legal de la web. Evaluaciones de impacto de protección de datos revisando la necesidad de haber realizado dicha evaluación y su adecuación al artículo 35 RGPD, artículo 28 LOPDGDD, "Guía para una Evaluación de Impacto en Protección de Datos Personales" y recomendaciones y guías por la AEPD. Creación del registro de actividades del tratamiento de las Cortes de Aragón, mediante identificación y análisis de las operaciones del tratamiento y su adecuación al artículo 30 del RGPD. Diseño de procedimientos para la gestión del ejercicio de derechos, por parte de los interesados verificando el cumplimiento de los plazos de respuesta y canales de comunicación. Diseño de procedimientos y mecanismos para la gestión de incidentes y violaciones de seguridad, revisando el procedimiento elaborado por Las Cortes y que contemple el catálogo de incidentes de seguridad de datos personales, los recursos que deben participar en el proceso, el protocolo de actuación, los plazos fijados por la norma y los modelos para realizar la notificación al regulador. Plan de concienciación revisando la existencia de un plan de formación y concienciación, para los empleados de Las Cortes que puedan realizar tratamiento de datos. Se elaborará Informe de auditoría con indicación de las no conformidades y se elaborará Plan de Acción para ayudar a gestionar la subsanación. Se incluye un gráfico de ejemplo.

Dentro de la integración con el cumplimiento del Esquema Nacional de Seguridad, propone revisar cada una de las fases necesarias para la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI). Se incluye gráfico con las fases. Para lograr el cumplimiento se revisará el Sistema de Gestión de Las Cortes, revisión de la implantación del Esquema Nacional de Seguridad y la detección de las posibles desviaciones.

Dentro de la ampliación y mejora continua de los aspectos indicados, propone la asistencia jurídica y técnica para la implantación del RGPD y de la LOPDGDD durante el plazo de ejecución del contrato tanto por vía telefónica como electrónica. En caso de ser necesario, un consultor se trasladaría a las instalaciones de Las Cortes para la revisión o gestión de la consulta planteada.

- Plan de gestión del cumplimiento del RGPD

Dentro del planteamiento general, propone una reunión con el Comité de Dirección para planificar, estructurar y definir las prioridades o situaciones de urgencia detectadas. Para la prestación del servicio de Delegado de Protección de Datos externo se procederá a la notificación del nombramiento a la Agencia Española de Protección de Datos en plazo de 10 días. Desde ese momento queda a disposición para cualquier consulta o solicitud a través del teléfono móvil facilitado o a través de cuenta de correo electrónico. Para la adecuación e implantación del RGPD y LOPDGDD se comenzará con la realización de entrevistas de evaluación a los distintos responsables de la entidad y revisión de la documentación. En el plazo máximo de un mes se compromete a

entregar un Informe de Auditoría inicial y un Plan de acción en el que se establezcan las actuaciones a llevar a cabo para la adaptación a la normativa vigente indicando grado de prioridad de cada una y adjuntando cuantos documentos sean necesarios para solventar la incidencia detectada que estará disponible a través de un sistema de carpetas compartidas online. Las sesiones de formación se llevarán a cabo una vez entregado el Plan de acción. En el plazo de dos meses desde la finalización de la anualidad objeto de contrato se elaborará un informe de valoración sobre el grado de implantación y adecuación a la normativa vigente en materia de protección de datos.

Dentro de la herramienta que se utilizará y sus principales características, propone para la elaboración del análisis de riesgos la herramienta ePrivacy RGPD. Permite la gestión integral 360 grados del cumplimiento del RGPD. Dispone de funcionalidades de Registro de actividad para gestión de tratamiento de datos, Data Protection Officer, Privacy by design para identificación y gestión de medidas de seguridad relacionadas en materia de protección de datos, Accountability para seguimiento de acciones en materia de protección de datos y repositorio de evidencias, Encargos de tratamiento, Evaluación de impacto e protección de datos (PIA), GAP LOPD vs RGPD para identificación y reporting del estado de situación actual frente al deseado, Ecuaciones legales con metodología de predicción de riesgos legales para valoración de impacto y gestión del cumplimiento basado en Riesgos legales calculado respecto a cada una de las normas y artículos por los que se puede iniciar un expediente y realizando el estudio del órgano sancionador, las normas de aplicación y utilizando técnicas de minería de datos. Identificación del estado de madurez de los

controles de mitigación basados en el Ciclo de Deming. Se incluye pantalla inicial del programa.

Dentro de ampliación y mejoras, propone asistencia jurídica y técnica para la implantación del RGPD y de la LOPDGDD durante el plazo de 12 meses desde la fecha de entrega del presente proyecto.

- Plan de Formación RGPD

Dentro del perfil, tipología de formación, número de cursos y contenidos, propone garantizar que todos los responsables de la entidad o la persona designada a los efectos sean conocedores de la normativa sobre protección de datos. El número de cursos es el indicado en el pliego. La formación se desarrollará de manera presencial u online. Se presenta esquema de contenidos.

Dentro de ampliación y mejoras, al finalizar la jornada formativa propone entregar un pequeño cuestionario de evaluación a todos los asistentes para analizar el grado de concienciación y conocimiento de la normativa y que sirva como evidencia de la formación suministrada y el cumplimiento del principio de Accountability.

- Delegado de Protección de Datos externo

Propone perfil licenciado en Derecho, en proceso de obtención de la Certificación como Delegado de Protección de Datos, tres jornadas y dos cursos. Experiencia de quince años.

4) La empresa OESÍA NETWORKS, S.L. propone, en su oferta, los siguientes planes y Delegado de Protección de Datos externo:

- Plan de Cumplimiento del Reglamento General de Protección de Datos

Dentro de la metodología y gestión del cumplimiento normativo, propone asesoramiento en protección de datos y seguridad de la información con el fin de realizar un seguimiento del cumplimiento de la normativa vigente aplicable en materia de protección de datos (RGPD, LOPDGDD) así como toda aquella normativa adicional aplicable. Proponen una metodología de trabajo propia por iteraciones y una hoja de ruta que se elaborará en coordinación con Las Cortes para prestar servicio de implantación, apoyo, mantenimiento y mejora en el cumplimiento de la normativa vigente y revisión de aquellos hitos de adecuación ya ejecutados realizando propuestas de mejora o actualización. Se incluye gráfico de mantenimiento operativo. La metodología estará compuesta por:

Auditoría interna de cumplimiento y adecuación al RGPD indicando en un listado los aspectos mínimos que contemplará estando basado en el análisis de las actuaciones de Las Cortes desde un punto de vista legal, técnico y organizativo con relación a las obligaciones de protección de datos así como el estudio de la documentación y políticas de protección de datos elaboradas que servirán como base.

Delegado de Protección de Datos. Se incluye tabla detallando las funciones que realizará: Punto de contacto, información y asesoramiento, soporte, supervisión, EIPD y la interlocución con AEDPD y autoridades.

Registro de Actividades de Tratamiento de Datos (RAT) asesorando con el principio de responsabilidad proactiva (Accountability) que rige el RGPD en la identificación, actualización y revisión de sus actividades de tratamientos, ponderando la optimización de la gestión de la protección de datos. Para su actualización y supervisión se tendrán en cuenta la identificación de las actividades de tratamiento de la entidad, su legitimación y los flujos de datos implicados así como las propuestas de optimización y nuevas funcionalidades. Se realizarán informes con la identificación de los tratamientos e instrucciones para la correcta publicación del RAT por medios electrónicos y su mantenimiento actualizado tal y como exige la normativa actual dando cumplimiento a lo dispuesto en la normativa de transparencia aplicable.

Revisión y adecuación de las cláusulas de información básica adicional revisando los mecanismos de recogida de datos y las cláusulas de información existentes para su actualización o para la elaboración de nuevas, al objeto de cumplir con los requisitos de transparencia e información. Se incluye tabla detallando las tareas para el cumplimiento del deber de informar.

Revisión e incorporación de textos legales de tratamientos de datos en pliegos, contratos, convenios y convocatorias (relaciones con terceros) prestando soporte y asesoramiento para la adecuación del modelo de relaciones con terceros. Se incluye tabla detallando

las tareas donde destaca que se analizarán y propondrán medidas de seguridad adicionales para mitigar los riesgos en toda relación con terceros que lo requiera y se tendrán en cuenta las medidas del ENS y la aplicación de legislación específica en el sector público como la Ley 40/2015 de 1 de octubre o la Ley 9/2017 de 8 de noviembre.

Cumplimiento RGPD en materia de videovigilancia y controles de acceso poniendo a disposición los modelos de carteles informativos y el procedimiento interno que regule el acceso, tratamiento y supervisión de las imágenes y el tiempo de conservación de las mismas. Se elaborará un protocolo de control de acceso a las instalaciones al objeto de cumplir con el deber de información como responsable del tratamiento y garantizar los principios de minimización y limitación de datos que se recaben.

Análisis de Riesgos (AARR) y Evaluación de Impacto (EIPD) aplicando una metodología adecuada a las particularidades de Las Cortes en base a las guías desarrolladas por la AEPD para la ejecución de análisis de riesgos. Se propone utilizar la herramienta GESTIONA desarrollada y publicada por la AEPD. Se priorizarán aquellas acciones que conlleven un mayor riesgo de lesionar derechos y libertades de los interesados estableciendo criterios en función de la sensibilidad de los datos, el ámbito del tratamiento y el volumen de datos tratados. Se incluye gráfico con las características del análisis de cumplimiento y fases de ejecución. Se incluye tabla detallando las evaluaciones para EIPD donde destaca el análisis de los tratamientos de datos ejecutando un procedimiento de análisis de la necesidad de realización de EIPD, en caso de detectar riesgo alto para los derechos y libertades de los interesados o que se estime recomendable se aplicará

metodología estructurada sobre seis fases basada en las guías de la AEPD y el Comité Europeo de protección de datos como parte de un proceso continuo y recurrente de evaluación, informe tras la ejecución de la EIPD con las características del tratamiento evaluado y las decisiones tomadas para mitigar o minimizar los riesgos y en su caso proceso de consulta previa a la autoridad de control.

Medidas técnicas y organizativas. Identificación e implementación de las medidas técnicas y organizativas necesarias para lograr un umbral de riesgos aceptable, basado en un enfoque de gestión continua del riesgo. Se incluye tabla detallando las acciones.

Gestión de brechas e incidentes de seguridad para el cumplimiento de las obligaciones de valoración, gestión y reporte de incidentes de Ciberseguridad. Se tendrá especial consideración la Guía nacional de notificación y gestión de incidentes (febrero 2020) publicada por el CCN así como otras recomendaciones y buenas prácticas como la Guía para la gestión y notificación de Brechas de Seguridad de Datos Personales de la AEPD. Dará apoyo para el análisis de incidentes mediante valoración de la normativa afectada por el ciberincidente si existe un "riesgo para los derechos y libertades de los interesados" y proceder a la notificación a la AEPD en plazo máximo de 72 horas así como a los afectados en caso de que el riesgo sea clasificado como "alto". Valoración de los incidentes de ciberseguridad que deben de notificarse a la autoridad. Especificaciones de las autoridades competentes y CSIRT de referencia a nivel nacional en materia de conocimiento, gestión y resolución de incidentes de ciberseguridad. Criterios para la notificación y taxonomía legal en cuanto a clasificación, peligrosidad e impacto de los incidentes. Metodología de

notificación, información a notificar y seguimiento de incidentes de ciberseguridad. Se incluye gráfico de las fases del procedimiento a alto nivel de los servicios de soporte.

Elaboración de una circular bimestral de comunicación interna y concienciación para el personal de Las Cortes sobre protección de datos y seguridad de la información.

Asesoramiento y respuesta ante el ejercicio de derechos RGPD, atención y seguimiento de consultas, y conexión con otros derechos relacionados con el acceso a información. Pondrán procedimientos que permitan atender y responder a los ejercicios de derechos en los plazos previstos por la nueva legislación. Se incluye tabla detallando las actuaciones donde destacan el procedimiento a seguir para la recepción, tramitación y resolución de las solicitudes de ejercicio de derechos, elaboración de modelos de respuesta para cada solicitud, procedimientos de conservación, bloqueo y eliminación de datos, y asesoramiento y soporte para la gestión de este derecho con otros previstos por normativa conexa como el derecho de acceso a información pública.

Asesoramiento normativo, atención de consultas y elaboración de informes. Se establecerá un canal de comunicación para la atención de todas aquellas consultas y dudas relativas a la protección de datos y seguridad de la información que puedan surgir, emitiendo las consideraciones y recomendaciones que se estimen necesarias para una correcta resolución. Se elaborarán los informes, dictámenes e instrucciones de índole jurídico-técnicas que sean requeridos por Las Cortes con recomendaciones y valoraciones así como asesoramiento y soporte para la implementación. Se proporcionará un manual de protección de

datos al objeto de establecer una metodología para el control e implantación de las actuaciones realizadas para la adecuación a lo dispuesto en el RGPD así como para disponer de un procedimiento interno. Se incluye tabla detallando los contenidos del manual. Se realizará un análisis comparativo de la normativa aplicable conexa para proporcionar una visión integral del cumplimiento de la normativa de protección de datos no sólo teniendo en cuenta el RGPD y la LOPDGDD sino también la normativa aplicable. En cumplimiento con el principio de responsabilidad proactiva (Accountability) que rige el RGPD, se realizarán verificaciones periódicas de cumplimiento de la normativa.

Dentro del detalle y adecuación a la Administración Pública, propone su experiencia en otros proyectos en el ámbito de la Administración Pública y analizar toda aquella normativa conexa aplicable al objeto de atender las especificidades propias del sector público como la Ley 39/2015 de 1 de octubre y la Ley 9/2017 de 8 de noviembre. El Plan de Cumplimiento tendrá una visión estratégica orientada a las Administraciones Públicas 360º con la experiencia y conocimiento que tiene por ser actual adjudicataria del servicio de DPD externo. Acompañará a la entidad en la adecuación de sus actividades a la nueva normativa en materia de protección de datos con el foco puesto en la garantía de los derechos y libertades de los interesados.

Dentro de la integración con el cumplimiento del Esquema Nacional de Seguridad, propone aplicar su experiencia en proyectos de convergencia entre ENS y RGPD/LOPDGDD con el objetivo de crear un modelo único y adaptado. La implementación de un Sistema de Gobierno de la privacidad acorde al RGPD/LOPDGDD puede utilizarse como base para el soporte de cumplimiento del ENS y

viceversa. El objetivo es determinar qué controles son necesarios para el cumplimento de cada norma, las medidas técnicas y organizativas de cumplimiento legal y las medidas de seguridad para los sistemas de información creando un modelo único de gestión de la seguridad de información y privacidad de los datos personales. Se incluye esquema detallado a alto nivel de la relación de los diferentes proyectos donde comprobar sinergias y complementación. En función del estado actual de cumplimiento se valorará y decidirá al inicio del servicio si proceder a una adecuación legal integrada desde el inicio o el segundo año.

Se incluye tabla con documentación entregable por procedimiento y finalidad, teniendo en cuenta los documentos y procedimientos ya desarrollados por Las Cortes con el fin de dar cumplimiento a los principios de eficacia y eficiencia.

Dentro de la ampliación y mejora continua de los aspectos indicados, propone la revisión periódica de la estructura documental desarrollada, con la finalidad de ir afinando y mejorando la misma con respecto a las nuevas necesidades en materia de protección de datos para mejora continua. Se incluye tabla con controles marco para garantizar la mejora continua. Se incluye tabla con mejoras en materia de ciberseguridad y protección de datos mencionando recomendaciones relacionadas con el uso de plataformas audiovisuales, políticas de movilidad y teletrabajo, procedimientos para la anonimización de los datos, buenas prácticas, protocolos Covid-19 respecto al tratamiento de datos, procedimiento automatizado propio para la gestión de brechas e incidentes y gestión de alertas.

- Plan de gestión del cumplimiento del RGPD

Dentro del planteamiento general, propone un modelo basado en cuatro pilares que actuarán como guía en las actividades de coordinación con Las Cortes y en la definición y difusión de la documentación con objetivo de crear y ejecutar un servicio competitivo, flexible y atractivo. Los pilares son: Modelo estratégico, modelo de servicios, modelo organizativo y modelo técnico con la metodología de gestión del servicio, normativas, buenas prácticas, estándares y procedimientos e identificación de herramientas de apoyo.

Dentro de la herramienta que se utilizará y sus principales características, propone la herramienta Risk4all, una solución GRC con soporte para evaluación del cumplimiento de regulaciones de privacidad, gestión de riesgos, gestión de incidentes, plan de acción y revisiones, gestión de documentación, indicadores y objetivos y gestión de alertas. Funciones multientidad, Evaluación de Impacto sobre la Privacidad, evaluaciones privacidad, gestión de derechos, evaluación de riesgos y gestión de documentación.

Dentro de ampliación y mejoras, propone para la sinergia entre RGPD/LOPDGDD y ENS un grupo de trabajo mensual y establecer los indicadores necesarios para medir el avance y la correcta gestión de los controles a implementar. Incluirá un módulo de cuadro de mando en la herramienta. Pondrán a disposición de Las Cortes una herramienta diseñada para: Gestión y categorización de nivel de riesgo ante un incidente de seguridad, valoración de una posible comunicación a la AEPD, etc., y un registro centralizado de incidencias de seguridad de los datos de carácter personal para el cumplimiento a lo establecido en los artículos 33 y 34 del RGPD.

- Plan de Formación RGPD

Dentro del perfil, tipología de formación, número de cursos y contenidos, propone formación a todos los niveles: Funcional, organizacional y tecnológico basado tanto en el nivel jerárquico de las funciones o puestos desempeñados como en la tipología y sensibilidad de información tratada y del riesgo que el desempeño de tareas lleva implícito. El plan de formación consiste en el análisis, diseño, ejecución, seguimiento y control de todas las actividades y acciones relacionadas con la formación en temas de protección de datos y seguridad de la información. Se incluye tabla con perfiles, tipo y objetivo de formación. Cumple los perfiles, número y duración mínimos exigidos en el pliego. Podrá realizarse de forma presencial o mediante webinars o formaciones telemáticas. Se elaborará un Decálogo de Protección de Datos y un Manual que describa las obligaciones y responsabilidades en el tratamiento de datos personales. El contenido de los cursos estará basado en los temarios establecidos para cada segmentación de perfil, profundizando en temas de interés de acuerdo a los riesgos y amenazas. Se incluye tabla con perfil, tipo de formación y título del curso.

Dentro de ampliación y mejoras, propone un curso específico de perfil político para los diputados de las Cortes de Aragón donde se asesorará en aspectos relacionados con protección de datos y seguridad de la información propios de su actividad política, haciendo hincapié en materias que pueden entrar en colisión con la protección de datos personales, como las obligaciones de transparencia o la normativa de procedimiento administrativo.

Incluyen 4 talleres formativos de 2 horas de duración, uno por cada perfil específico indicando en una tabla los objetivos de los talleres. Ofrecen actividades de concienciación adicional como Píldoras formativas, Activaciones con todas las iniciativas de concienciación para los sitios e intraweb de Las Cortes tales como ventanas pop-up, fondos de pantalla, fondos para la intranet con información clave sobre seguridad, puntos de contacto y canales de comunicación para apoyo sobre temas de seguridad, y Últimas noticias con casos reales que puedan afectar a la plantilla de Las Cortes.

- Delegado de Protección de Datos externo

Propone perfil Licenciatura en derecho, Master en Derecho de las Nuevas Tecnologías y tres certificaciones/cursos. Experiencia 15 años y medio.

5) La empresa AUDIDAT 3.0, S.L.U. propone, en su oferta, los siguientes planes y Delegado de Protección de Datos externo:

- Plan de Cumplimiento del Reglamento General de Protección de Datos

Dentro de la metodología y gestión del cumplimiento normativo, propone asistencia técnico-jurídica permanente con la resolución jurídica de las cuestiones relativas a protección de datos incluidos los procedimientos administrativos del propio responsable del

tratamiento así como los proyectos de investigación. Prestará asesoramiento jurídico hasta agotar la vía administrativa haciéndose cargo de los procedimientos de solicitud de información, inspectores y sancionadores de la Agencia Española de Protección de Datos.

Auditoría interna inicial, con un control interno de cumplimiento de la normativa de protección de datos respecto a medidas técnicas y organizativas, para garantizar la seguridad del tratamiento en base a los principios de protección de datos de carácter personal recogidos en el Reglamento (UE) 2016/679 y la legislación nacional aplicable. Se analizará qué medidas técnicas y organizativas son las más apropiadas para garantizar un nivel de seguridad adecuado al riesgo añadiendo aquellas que en el momento de inicio de los trabajos no fuesen tomadas en consideración. Se comprobará que todos los usuarios autorizados para tratar información de carácter personal únicamente puedan tratar tales datos. Se supervisará que la entidad ha llevado a cabo una atribución clara de los roles y las responsabilidades.

Análisis de riesgo que permitirá asignar un nivel de riesgo específico y diferenciado a cada una de sus actividades de tratamiento, proponiendo una serie de actuaciones tendentes a la gestión constante del riesgo en el normal desarrollo de la actividad propia de la entidad tal y como exige el art. 32.1 RGPD. Se generará un sistema de protección de datos desde el diseño y protección de datos por defecto, quedando revestida cualquier actuación del principio de responsabilidad proactiva del art. 5.2 RGPD. Si se detectan tratamiento de datos personales que impliquen un alto riesgo para los derechos y libertades de los interesados, se valorará la necesidad e idoneidad de realizar una

evaluación de impacto de la protección de datos personales (PIA) teniendo en cuenta lo dispuesto en el art. 35 RGPD.

Registro de las actividades de tratamiento, detallando la información que contendrá el registro. Modificarán y/o actualizarán el registro de las actividades de tratamiento del responsable del tratamiento para dar cumplimiento a lo establecido en el art. 30 RGPD previa emisión de un informe sobre el estado del responsable del tratamiento.

Concienciación del personal y Manual de Protección de Datos elaborando mensualmente una circular con información sobre protección de datos personales según lo indicado en el pliego y que deberá ser difundida entre el personal con acceso a datos personales del responsable del tratamiento. Se prestará atención a cómo afectan las novedades legislativas, jurisprudenciales e interpretativas en materia de protección de datos personales al normal desenvolvimiento de la actividad propia del responsable. Se redactará una circular para el personal implicado. Se elaborará progresivamente un Manual de Protección de Datos específico para Las Cortes que permita su constante actualización. Modificará y/o actualizará el registro de las actividades de tratamiento del responsable del tratamiento con la finalidad de dar cumplimiento a lo establecido en el art. 30 RGPD.

Legitimación del tratamiento y consentimiento revisando y adecuando en su caso los criterios de legitimación de cada tratamiento de datos personales desarrollado por el responsable del tratamiento y elaborando al efecto las cláusulas pertinentes a fin de verificar el cumplimiento de lo establecido en el RGPD

además de analizar los criterios de legitimación del tratamiento de datos en cada caso concreto.

Información adoptando todas las medidas necesarias para facilitar al interesado la información relativa al tratamiento de sus datos. El nivel de precisión que requiere la normativa exige poder adaptar la totalidad de documentos y formularios de los que dispone la entidad por lo que se revisará y adecuará en su caso las cláusulas informativas del tratamiento utilizadas por el responsable del tratamiento.

Seguridad del tratamiento según el art. 32 RGPD asesorando al responsable del tratamiento en relación a los aspectos: Valoración y gestión del riesgo para los derechos y libertades de los interesados, Asesoramiento sobre la implantación de las medidas de seguridad adecuadas a los riegos y naturaleza de las actividades de tratamiento, Establecimiento de mecanismos de verificación, evaluación y valoración regulares de las medidas técnicas y organizativas para garantizar la seguridad de los datos personales.

Violaciones de seguridad de los datos personales, asesorarán al responsable del tratamiento en relación con la notificación de los supuestos de violación de la seguridad de los datos personales con la finalidad de dar cumplimiento a lo establecido en el art. 33 RGPD. Se proporcionará un procedimiento de gestión de brechas de seguridad y una fórmula matemática que permitirá valorar el riesgo que presentan las incidencias detectadas. Se realizarán simulacros de brechas de seguridad para comprobar que los protocolos y procedimiento establecidos son efectivos y se adaptan a la realidad y circunstancias.

Relación entre responsables y encargados del tratamiento, proponen revisar y adecuar en su caso los contratos de tratamiento existentes y los que se vayan a suscribir en un futuro prestando especial atención a los modelos comúnmente utilizados como los pliegos o contratos de prestación de servicios. Implantará un protocolo que permita examinar y auditar a todos los encargados de tratamiento, ya sea previamente o durante el normal desenvolvimiento de la relación entre las partes, analizando si ofrecen las garantías adecuadas que exige la normativa en la materia.

Videovigilancia y controles de acceso, asesorará en relación a las obligaciones específicas en materia de videovigilancia y las garantías que deben preservarse respecto a empleados y ciudadanos en los locales del responsable del tratamiento y en la vía pública. Se prestará atención a la proporcionalidad de la instalación del sistema de videovigilancia y al enfoque de las cámaras. Se analizarán los controles de acceso implantados y utilizados por el responsable del tratamiento, garantizando que presenten un encaje legal válido, que se trata de medidas útiles y adecuadas y que se respetan todas las exigencias documentales y administrativas.

Evaluaciones de impacto, deberá analizarse si en el normal desenvolvimiento de la actividad propia de la entidad surge algún tratamiento de datos personales que revista las características referidas en el art. 35 RGPD. Se comprobará si surge algún tratamiento de datos personales que cumpla con dos o más criterios entre los estipulados por la Agencia Española de Protección de Datos. Asesorarán al responsable en lo referente al

desarrollo, contenido y encaje jurídico y técnico de las evaluaciones de impacto.

Derechos del interesado, asesorará al responsable del tratamiento en relación con los mecanismos de recepción y gestión de las solicitudes de ejercicio de los derechos de los interesados recogidos en el Capítulo III del RGPD.

Desarrollo de funciones de delegado de protección de datos, desarrollará a través de profesionales cualificados conforme al esquema de certificación de delegados de protección de datos de la Agencia Española de Protección de Datos (AEPD-DPD) las labores de Delegado de Protección de Datos en base a las letras a), b), c) y e) del art. 39.1 RGPD.

Dentro del detalle y adecuación a la Administración Pública, se nombran algunas entidades.

Dentro de la integración con el cumplimiento del Esquema Nacional de Seguridad, no se propone nada específico.

Dentro de la ampliación y mejora continua de los aspectos indicados, no se propone nada específico.

- Plan de gestión del cumplimiento del RGPD

Dentro del planteamiento general, propone unos Objetivos e hitos que constan de: Fase 1 Inicio de los trabajos, reunión con los interlocutores principales del responsable del tratamiento. Fase 2 Rutina de reuniones, proponiendo un calendario de reuniones periódicas con los interlocutores principales del responsable del

tratamiento, mínimo una reunión al mes con cada interlocutor y semanales con determinados responsables de área cuyo tratamiento de datos implique un alto riesgo para los derechos y libertades de los ciudadanos, estableciendo pequeños objetivos. Fase 3 Toma de datos inicial, con cada área o sección del responsable del tratamiento para conocer el nivel de cumplimiento, comenzar los trabajos de adaptación y el desarrollo de documentación necesaria para cumplimiento de las obligaciones en el Reglamento (UE) 2016/679, nivel de riesgo para cada actividad. Fase 4 Entrega de documentación, documento de política de protección de datos. Fase 5 Explicación y aplicación de la plataforma y de la documentación, la documentación elaborada se volcará en la plataforma digital elaborada por AUDIDAT para el responsable del tratamiento. Se mostrarán las opciones y funcionalidades de la plataforma a los responsables de sección. Fase 6 Elaboración de un registro de actividades de tratamiento, en un lenguaje y formato que permita su automática publicación en el apartado de transparencia de la página web. Se establecerá un sistema de comunicación que permita modificar de una manera ágil el registro de tratamiento interno. Fase 7 Formación, en jornada de trabajo prestando atención a los cambios introducidos por la normativa europea y a las innovaciones legislativas y jurisprudenciales. Fase 8 Encargados de tratamiento, se revisarán y adecuarán los contratos de tratamiento de datos por cuenta de terceros ya suscritos por la entidad y modelos de contrato de tratamiento de datos que permitan regular la relación del responsable del tratamiento con los distintos encargados. Se auditarán y examinarán todos los encargados de tratamiento para comprobar si ofrecen las garantías adecuadas que exige la normativa. Se generará un registro centralizado de encargados de

tratamiento de la entidad, actualizando de manera constante el listado de empresas profesionales que prestan servicios a favor del responsable del tratamiento y regular la relación con los mismos. Fase 9 Análisis de la página web, para comprobar que cuenta con los avisos, políticas y textos legales en materia de protección de datos personales, política de cookies, política de privacidad, política de protección de datos, registro de actividades de tratamiento y el respeto al principio de minimización de datos. Fase 10 Protocolo de acceso a la documentación (ciudadanos), documentando unas instrucciones básicas que puedan servir para solucionar aquellas cuestiones en las que un ciudadano solicite acceso a la información que contenga datos de carácter personal. Fase 11 Protocolo de acceso a la documentación (personal) con instrucciones básicas para solucionar cuestiones en las que los usuarios del sistema soliciten acceso a información que contenga datos de carácter personal. Fase 12 Valoración de resultados. Fase 13 Evaluación de las medidas técnicas, comprobando que los datos personales, atendiendo a su naturaleza y finalidad, están protegidos por unas medidas de seguridad adecuadas y analizando qué medidas técnicas y organizativas son las más apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Fase 14 Verificación de protocolos y procedimientos, donde también se determinará qué operaciones de tratamiento requieren de un mayor tiempo, dedicación y recursos para adaptarse a los requisitos legales existentes. Fase 15 Protocolo de violaciones de seguridad, a través de simulacros en los que se compromete la confidencialidad, integridad, disponibilidad o resiliencia de la información personal documentando los resultados y valorando la eficacia. Fase 16 Protocolo de atención a los derechos de los interesados, a través de simulacros en los que se plantean situaciones ficticias,

documentando los resultados y valorando la eficacia. Fase 17 Valoración de resultados, en jornada de trabajo. Fase 18 Nuevos objetivos y preparación de la auditoría de medidas de seguridad y el control periódico del cumplimiento. Se identificarán posibles deficiencias y medidas correctoras o complementarias. Se incluye tabla con planificación temporal de las fases. Se incluye cronograma de desarrollo de funciones durante el primer y segundo año.

Dentro de la herramienta que se utilizará y sus principales características, propone plataformas digitales de gestión. Software de gestión propio elaborados por el personal técnico de AUDIDAT. Su personal utilizara un software para facilitar la gestión de su actividad y el desarrollo de las labores, que cuenta con un procedimiento de validación derivado de la ISO 9001 que analiza la idoneidad, necesidad, legalidad y utilidad de cualquier documento o escrito, credenciales y permisos independientes. Otro software de gestión se pondrá a disposición del responsable del tratamiento será una plataforma digital elaborada por AUDIDAT para: Gestionar, descargar y modificar toda la información relativa a la organización en materia de protección de datos personales en diversos formatos, permitir la gestión de los sistemas de información utilizados para tratar los datos personales, gestionar el personal autorizado y los procedimientos y medidas de seguridad que deben implantarse, contactar directamente con cualquier departamento de AUDIDAT o con el consultor asignado al desarrollo de las tareas, disponibilidad plena y constante de cualquier documento o informe, subida de documentos, programa de cumplimiento "Audidat Cumple". Se encargarán de incluir la

información de manera continua permitiendo que ambos softwares contengan la totalidad de los datos en formatos ofimáticos.

Dentro de ampliación y mejoras, no se propone nada específico.

- Plan de Formación RGPD

Dentro del perfil, tipología de formación, número de cursos y contenidos, propone formación al personal implicado en el tratamiento de datos personales desarrollando las jornadas formativas necesarias para recibir un mínimo de formación en la materia según lo indicado en el pliego. Se incluye un índice del contenido de las jornadas formativas adaptado al perfil de los alumnos.

Dentro de ampliación y mejoras, no se propone nada específico.

- Delegado de Protección de Datos externo

Propone perfil Licenciatura en Derecho, Máster en Asesoría Jurídica de Empresas, Perito Judicial Protección de Datos, seis cursos. Experiencia ocho años.

6) La empresa SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U. propone, en su oferta, los siguientes planes y Delegado de Protección de Datos externo:

- Plan de Cumplimiento del Reglamento General de Protección de Datos

Dentro de la metodología y gestión del cumplimiento normativo, propone el detalle de las funciones y actividades que debe asumir el DPD según el RGPD y la AEPD.

Auditoría interna inicial, con objeto de conocer el estado actual de cumplimiento y las necesidades de adecuación. Se detectarán posibles desviaciones en el cumplimiento de la norma y se identificarán mejoras. Se incluye gráfico con la metodología del auditor. Se realizará informe de auditoría con carácter confidencial en el que se reflejará el grado de adecuación a la legislación vigente. Se incluye el índice que contendrá el informe.

Se desarrollarán las actividades contenidas en el Sistema de Gestión de Protección de Datos en fases del ciclo de mejora continua. Fase PLAN: Política de protección de datos donde se actualizará/realizará de forma conjunta con el cliente la Política de Protección de Datos Personales. Actualización del Registro de Actividades de Tratamiento (RAT). Actualización del Diagnóstico de situación, realizando una actualización del GAP Análisis para revisar el nivel de madurez y el nivel de medidas técnicas de seguridad existentes destinadas a proteger los datos de carácter personal. Revisión de roles y responsabilidades, con la definición de un marco de gobierno y gestión de protección de datos que se requiere de una organización de seguridad y que garantice que las tareas a realizar se ejecuten correctamente, y se actualizará o definirá documento de designación de roles y responsabilidades tomando como referencia la guía 801 del CCN. Actualización del análisis de evaluación de impacto de protección de datos. Análisis

de riesgos a partir de marcos reconocidos internacionalmente como ISO 27001, MAGERIT v3.0, ISO 31000 e ISO 27005 proponiendo el uso de la herramienta PILAR y entregando un informe con el nivel de riesgo actual y recomendaciones de las medidas que se han de implementar para mitigar el riesgo.

Fase DO: Actualización del marco documental SGPD conformado por una Política de Privacidad actualizada, Actualización de la evaluación de impacto EIPDs sobre tratamientos con nivel de riesgo alto o muy alto, Actualización del procedimiento de ejercicio de los derechos ARSOPL, Procedimiento de notificación de violaciones de seguridad de los datos personales a la Agencia Española de Protección de Datos, Actualización de las cláusulas de cumplimiento de la LOPD que se adaptarán a la página web, contratos con encargados de tratamiento y formularios tipo, Actualización de la obtención del consentimiento de la LOPD a los requerimientos del RGPD, Actualización del procedimiento en relación con la revisión de los contratos de Encargados de Tratamiento, Revisión del Manual del Sistema de Gestión de Protección de Datos, Modelo de Responsabilidad Proactiva, Cuadro de mando de cumplimiento RGPD basado en el Modelo de Responsabilidad Proactiva, Revisión de todos los procesos en los que se recabe consentimiento para garantizar que cumple con los requisitos legales, Revisión de los Modelos de cláusulas con actualización de todas las cláusulas de información y/o contractuales y análisis de los contratos de prestación de servicios actuales, Inventariado de todas las relaciones con proveedores y terceros que impliquen o puedan implicar el tratamiento y procesamiento de datos personales, Revisión de los tratamientos realizados a través de sistemas de videovigilancia así como la

adecuación de los avisos de privacidad. Dentro de esta fase también se incluye: Implantación y actualización del plan de tratamiento de Riesgos. Cuadros de mando basado en la Responsabilidad proactiva y el grado de avance del mantenimiento RGPD, con actualización continua en función de los controles que se puedan ir implantando en el tiempo y periódicamente se realizará una revisión general. Incluye gráfico de ejemplo de cuadro de mando. Formación.

Fase CHECK: Se realizará una auditoría por un equipo distinto al equipo de la Adecuación con objeto de cumplir el principio de independencia y evitar conflicto de intereses así como detectar posibles desviaciones en el cumplimiento de la norma e identificar mejoras. Se incluye gráfico con la metodología que el auditor aplicará. Soporte a incidentes de seguridad y escalado incluyendo el aprendizaje de intereses para reducir que se repitan. En caso de incidentes de seguridad con impacto considerable y que sea necesaria la notificación al CNN CERT / AEPD, darán soporte de personal experto.

Fase ACT: Revisión del Sistema de gestión y seguimiento de las acciones correctivas y de mejora. Planes de mejora base para la detección de mejoras, control y seguimiento de acciones a desarrollar y la incorporación de acciones correctoras ante posibles contingencias no previstas. Soporte a la implantación de mecanismos técnicos para asegurar el ejercicio de derechos conteniendo el art. 12 RGPD y LOPD-GDD algunas reglas comunes. Soporte para atender cualquier solicitud de información por parte de las autoridades de control, atender solicitudes que provengan de organismos y entidades externas o comunicar incidentes de seguridad.

Dentro del detalle y adecuación a la Administración Pública, se nombra el Delegado de Protección de Datos en las AAPP y adaptación al RGPD con diversos enlaces externos.

Dentro de la integración con el cumplimiento del Esquema Nacional de Seguridad, propone que las tareas se ejecuten con una visión transversal de gestión, de forma que una actividad en la medida de lo posible sirva para el máximo de esquemas de certificación o buenas prácticas de cumplimiento. Incluyen gráfico con esquema transversal de gestión incluyendo ENS, ISO 27001/27011, ISO 22301 e ISO 27701/RGPD.

Dentro de la ampliación y mejora continua de los aspectos indicados, propone de forma detalla la planificación de las actividades de la metodología y gestión a veinticuatro meses.

- Plan de gestión del cumplimiento del RGPD

Dentro del planteamiento general, propone realizar un Análisis de Riesgos para verificar el nivel de riesgo y en caso de riesgo alto, realización de una Evaluación de Impacto relativa a la Protección de Datos (EIPD).

Dentro de la herramienta que se utilizará y sus principales características, propone el uso de PILAR para análisis de riesgos en varias dimensiones: Confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (accountability). Permite realizar análisis cuantitativos y cualitativos; y Análisis de Impacto de Continuidad de Operaciones. También propone INES-AR

herramienta de Análisis de Riesgos basada en PILAR e integrada en INES.

Dentro de ampliación y mejoras, propone la herramienta INES, colaborando con Las Cortes para la carga de información y posterior comunicación del estado de seguridad.

- Plan de Formación RGPD

Dentro del perfil, tipología de formación, número de cursos y contenidos, propone el mínimo indicado en el pliego. Se detallan los contenidos orientativos por unidades y objetivos.

Dentro de ampliación y mejoras, propone la herramienta Microsoft Teams como espacio de trabajo para mejorar la comunicación y colaboración de los equipos de trabajo. En el desarrollo de las sesiones formativas se utilizará la técnica de gamificación para fomentar la intervención y participación activa de los asistentes mediante la herramienta Kahoot, servicio web de educación social y gamificada.

- Delegado de Protección de Datos externo

Propone perfil Licenciado en Derecho, Licenciado en Administración y Dirección de Empresas, Máster en Propiedad Industrial, Intelectual y Nuevas Tecnologías. Experiencia de seis años.

3.1.2.- Valoración de las ofertas presentadas

Según lo expuesto anteriormente, en lo relativo al Servicio de Cumplimiento del Reglamento General de Protección de Datos incluyendo un Delegado de Protección de Datos externo:

La oferta más completa es la presentada por la empresa CENTRO REGIONAL DE SERVICIOS AVANZADOS S.A.

Respecto al plan de cumplimiento del Reglamento General de Protección de Datos (RGPD) presenta alto nivel de detalle y personalización en metodología y gestión, integrando diversas metodologías reconocidas. Alto nivel de detalle y personalización en adecuación a la Administración Pública indicando las fases y tareas a realizar. Adecuada integración con el cumplimiento del ENS mediante directrices marcadas por el Centro Criptológico Nacional.

El plan de gestión del cumplimiento del RGPD propone la herramienta comercial Global Suite específicamente diseñada para la gestión de normas ISO y GRC (Gobierno, Riesgo y Cumplimiento) funcionando en modo SaaS con módulo RGPD, Gestor Documental, módulo encuestas, metodología MAGERIT, catálogo y análisis de riesgos, ticketing, Balanced Scorecard e integración con Directorio Activo.

Respecto al plan de formación presenta alto nivel de detalle y personalización con un listado de cursos y contenidos complementarios al mínimo exigido, propone como mejora la herramienta Smartfense, específica para formación y concienciación de usuarios en el ámbito de la seguridad informática.

Y con respecto al DPD proponen a un especialista adecuadamente formado con ocho años de experiencia en RGPD.

Por ello se le otorga una puntuación de 20 puntos.

A continuación destaca la oferta presentada por la empresa OESÍA NETWORKS, S.L.

Respecto al plan de cumplimiento del Reglamento General de Protección de Datos (RGPD) presenta alto nivel de detalle y personalización en metodología y gestión con una metodología propia muy detallada. Bajo nivel de detalle y personalización en adecuación a la Administración Pública. Presenta una integración adecuada en el cumplimiento del ENS.

Para el plan de gestión del cumplimiento del RGPD propone la herramienta Risk4all específicamente diseñada para la gestión de GRC (Gobierno, Riesgo y Cumplimiento) con soporte para evaluación de las regulaciones de privacidad, gestión de riesgos, gestión de incidentes, plan de acción y revisiones, gestión de documentación, indicadores y objetivos y gestión de alertas.

Respecto al plan de formación presenta bajo nivel de detalle, ajustado a los mínimos exigidos, propone como mejora con un curso específico de perfil político.

Y con respecto al DPD proponen a un especialista adecuadamente formado con quince años y medio de experiencia en RGPD.

Por ello se le otorga una puntuación de 18 puntos.

En tercer lugar la oferta presentada por la empresa TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U.

Respecto al plan de cumplimiento del Reglamento General de Protección de Datos (RGPD) presenta bajo nivel de detalle y personalización en metodología y gestión. Bajo nivel de detalle y personalización en adecuación a la Administración Pública. Sin propuesta específica para integración con el cumplimiento del ENS.

El plan de gestión del cumplimiento del RGPD propone la herramienta Sandas GRC específicamente diseñada para la gestión de GRC (Gobierno,

Riesgo y Cumplimiento) en modo SaaS que permite integración con PILAR e INES, dispone de gestor documental, módulo de gestión de riesgos y revisión para auditoría.
Respecto al plan de formación presenta bajo nivel de detalle, ajustado a los mínimos exigidos.
Y con respecto al DPD proponen a un especialista adecuadamente formado con veinticuatro años y medio de experiencia.
Por ello la puntuación obtenida es de 15 puntos.

En cuarto lugar la oferta presentada por la empresa SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U.
Respecto al plan de cumplimiento del Reglamento General de Protección de Datos (RGPD) presenta alto nivel de detalle y personalización en metodología y gestión con una metodología propia y metodologías reconocidas para el análisis de riesgos. Bajo nivel de detalle y personalización en adecuación a la Administración Pública, y una suficiente integración con respecto al cumplimiento del ENS.
El plan de gestión del cumplimiento del RGPD propone las herramientas PILAR e INES-AR gratuitas provistas por el Centro Criptológico Nacional ajustadas a los mínimos exigidos.
Respecto al plan de formación presenta bajo nivel de detalle, ajustado a los mínimos exigidos, propone como mejora la herramienta Kahoot de gamificación para fomentar la intervención y participación activa de los asistentes.
Y con respecto al DPD proponen a un especialista adecuadamente formado con seis años de experiencia en RGPD.
Por ello se le otorga una puntuación de 11 puntos.

En quinto lugar la oferta presentada por la empresa AUDIDAT 3.0, S.L.U. Esta oferta no se ajusta a la estructura incluida en el pliego.

Respecto al plan de cumplimiento del Reglamento General de Protección de Datos (RGPD) presenta alto nivel de detalle y personalización en metodología y gestión con una metodología propia. Bajo nivel de detalle y personalización en adecuación a la Administración Pública. Sin propuesta específica para integración con el cumplimiento del ENS.

Para el plan de gestión del cumplimiento del RGPD propone una herramienta de gestión propia con procedimiento de validación derivado de la ISO 9001 y otra herramienta/plataforma para el responsable del tratamiento.

Respecto al plan de formación presenta bajo nivel de detalle, ajustado a los mínimos exigidos.

Y con respecto al DPD proponen a un especialista adecuadamente formado con ocho años de experiencia en RGPD.

Por ello se le otorga una puntuación de 10 puntos.

En último lugar la oferta presentada por la empresa ECIX ARAGÓN CONSULTING, S.L.

Respecto al plan de cumplimiento del Reglamento General de Protección de Datos (RGPD) presenta bajo nivel de detalle y personalización en metodología y gestión. Alto nivel de detalle y personalización en adecuación a la Administración Pública, y una suficiente integración con respecto al cumplimiento del ENS.

Para el plan de gestión del cumplimiento del RGPD propone la herramienta ePrivacy RGPD, con Registro de actividad, Data Protection Officer, Privacy by design Accountability, Encargos de tratamiento, Evaluación de impacto de protección de datos, GAP LOPD vs RGPD, Ecuaciones legales.

Respecto al plan de formación presenta bajo nivel de detalle, ajustado a los mínimos exigidos.

Y con respecto al DPD proponen a un especialista con Licenciatura en Derecho, en proceso de obtención de la Certificación como Delegado de Protección de Datos, tres jornadas, dos cursos y quince años de experiencia en RGPD.

Por ello se le otorga una puntuación de 7 puntos.

3.2 CRITERIO: Plan de Soporte y mantenimiento: Hasta 5 puntos

Se valorará la claridad expositiva, detalle y personalización del Plan de Soporte y mantenimiento, obligatoriamente con la siguiente estructura: Planteamiento general. Descripción del sistema centralizado para la realización de consultas/peticiones. Servicios y prestaciones de soporte con horarios de atención y tiempos de respuesta. Procedimientos y mecanismos de gestión para la resolución de consultas/peticiones. Ampliación y mejoras de los aspectos indicados.

3.2.1.- Resumen de las ofertas presentadas

1) La empresa TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U. propone, en su oferta, el siguiente Plan de Soporte y mantenimiento:

   Dentro del planteamiento general, propone un soporte especial de backoffice de más de 30 consultores especialistas para atender a las consultas planteadas por Las Cortes, aportar conocimientos específicos para resolución de alguna tarea y asegurar el servicio en períodos como las vacaciones, fines de semana o festivos.

Dentro de la descripción del sistema centralizado para la realización de consultas/peticiones, propone un buzón a través de su herramienta propuesta o de correo electrónico, donde registrar las peticiones o consultas. Las consultas pasarán siempre un filtro previo por parte del equipo principal del proyecto con el objetivo de organizarlas y resolverlas rápidamente si se hubieran planteado con anterioridad. Las respuestas atenderán siempre una formalidad oportuna. La atención se procurará en idioma castellano.

Dentro de los servicios y prestaciones de soporte con horarios de atención y tiempos de respuesta, propone un horario habitual de oficina de 8:00 a 19:00 horas de lunes a viernes. Se proporcionará soporte en días festivos y fines de semana siempre que la cuestión sea urgente y deba ser atendida con brevedad. Se garantizará tiempo de respuesta de 48 horas, reduciéndose a 24 horas en caso de cuestiones críticas.

Dentro de los procedimientos y mecanismos de gestión para la resolución de consultas/peticiones, propone el correo electrónico o su herramienta. Se analizarán en primera instancia por parte del equipo principal y si no pudieran ofrecer una respuesta se remitirá a la oficina de soporte, al interlocutor más adecuado.

Dentro de ampliación y mejoras de los aspectos indicados, propone ampliación de personas de la Oficina de Soporte a 30 personas, herramienta para gestionar las consultas si Las Cortes lo considera oportuno, tiempo de respuesta a 24 horas para situaciones críticas, soporte en otros idiomas si fuera necesario, ampliación del horario de soporte a fines de semana y festivos.

2) La empresa CENTRO REGIONAL DE SERVICIOS AVANZADOS, S.A. propone, en su oferta, el siguiente Plan de Soporte y mantenimiento:

Dentro del planteamiento general, propone la Fase 2 Mantenimiento del cumplimiento del RGPD/LOPDGDD con los objetivos prestar asesoramiento jurídico y técnico especializado para la mejora continua de la gestión de la privacidad y llevar a cabo las tareas previstas en el Plan de Adecuación/Implantación y Planes de Tratamiento del Riesgo. Se incluyen los perfiles involucrados. Las tareas previstas serán: Atención de derechos y conexión con otro tipo de normativa como transparencia, acceso a información pública, etc. Asesoramiento cambios normativos que puedan afectar al sistema de gestión, desde cambios sobre el RGPD y la LOPDGDD como cambios relacionados con la seguridad de la información, aplicación de la normativa de archivo y clasificación de información de titularidad pública. Soporte a la implementación de medidas de seguridad técnicas y organizativas, en línea de lo indicado por el RD 3/2010 y las contenidas por el RGPD. Desarrollo de procedimientos necesarios en el ámbito de protección de datos, elaboración de políticas vinculadas a tratamientos concretos como videovigilancia, geolocalización, teletrabajo, datos biométricos, etc. Se elaborarán entregables.

Dentro de la descripción del sistema centralizado para la realización de consultas/peticiones, propone la creación de una dirección correo electrónico o vía telefónica a través de la cual se gestione la demanda de consultas de acuerdo a una escala de importancia y tiempos de respuesta. Se incluye tabla indicativa con

cuatro prioridades. El tiempo de resolución de consultas para prioridad 1 uno-dos días hábiles, prioridad 2 dos-tres días hábiles, prioridad 3 cuatro-seis días hábiles y prioridad 4 siete-nueve días hábiles.

Dentro de los servicios y prestaciones de soporte con horarios de atención y tiempos de respuesta, proponen un horario de atención de 8:00h a 18:00h de lunes a viernes.

Dentro de los procedimientos y mecanismos de gestión para la resolución de consultas/peticiones, proponen como vías correo electrónico y telefónica.

Dentro de ampliación y mejoras de los aspectos indicados, propone la realización de un informe final de servicio o informe GAP que analizará el grado de cumplimiento alcanzado y que servirá como base para posteriores servicios o la continuación del mismo.

3) La empresa ECIX ARAGÓN CONSULTING, S.L. propone, en su oferta, el siguiente Plan de Soporte y mantenimiento:

Dentro del planteamiento general, propone un servicio de consultoría continuo consistente en la resolución de cualquier duda planteada en la materia, análisis de cualquier nuevo tratamiento de datos que se pretenda realizar así como en la remisión de nuevas instrucciones o directrices dictadas por la Agencia Española de Protección de Datos y otras Autoridades de control europeas.

Dentro de la descripción del sistema centralizado para la realización de consultas/peticiones, propone un número de teléfono directo del Delegado de Protección de datos quien dispondrá de un plazo de dos días para emitir la respuesta que considere oportuna. Quedará a disposición de Las Cortes un correo electrónico donde también se podrán realizar las consultas oportunas.

Dentro de los servicios y prestaciones de soporte con horarios de atención y tiempos de respuesta, propone el horario de recepción de consultas será de lunes a viernes de 8:00 a 19:00 horas.

Dentro de los procedimientos y mecanismos de gestión para la resolución de consultas/peticiones, propone un número de teléfono y un correo electrónico.

Dentro de ampliación y mejoras de los aspectos indicados, no se propone nada específico.

4) La empresa OESÍA NETWORKS, S.L. propone, en su oferta, el siguiente Plan de Soporte y mantenimiento:

Dentro del planteamiento general, propone servicios de asesoramiento y soporte en materia de protección de datos y seguridad de la información en coordinación con la oficina de apoyo al DPD. Asesorará a los Responsables de Seguridad y otros implicados en las directrices para el cumplimiento de las obligaciones de valoración, gestión y reporte de incidentes de Ciberseguridad. Propone listado de tareas de asesoramiento legal y técnico con elaboración y revisión de informes, procedimientos de

cumplimiento, supervisión de cumplimiento de encargados de tratamientos, gestión de la privacidad por diseño y por defecto, determinación e implementación de medidas de seguridad adicionales en base al ENS y mantenimiento de documentos de seguridad que los soportan, soporte en la gestión de relaciones con las autoridades de control así como solicitudes de información por parte de unidades internas, ejercicio de derecho y soporte en el cumplimiento de novedades LOPDGDD.

Dentro de la descripción del sistema centralizado para la realización de consultas/peticiones, propone un servicio continuo de atención de peticiones de soporte por diferentes canales: Buzón de correo electrónico, atención telefónica, asistencia personal y otros mecanismos ya implementados en Las Cortes.

Dentro de los servicios y prestaciones de soporte con horarios de atención y tiempos de respuesta, propone el uso de un buzón de correos atendido de 8:00 a 19:00h de lunes a viernes.

Dentro de los procedimientos y mecanismos de gestión para la resolución de consultas/peticiones, propone que el servicio de soporte legal podrá apoyarse en las herramientas, modelos y plantillas propias de la empresa basadas en las metodologías y recomendaciones de las Autoridades Competentes o adecuarlas a las propias de Las Cortes. Se incluye gráfico a alto nivel de las fases.

Dentro de ampliación y mejoras de los aspectos indicados, propone acciones de soporte legal para valoración, notificación y gestión de incidentes. Se tendrá en especial consideración la Guía nacional de notificación y gestión de incidentes (febrero 2020) publicada por el CCN, INCIBE y CNPIC así como otras recomendaciones y buenas

prácticas como la Guía para la gestión y notificación de Brechas de Seguridad de Datos Personales. Dará apoyo a la valoración de la normativa afectada, valoración expresa de los incidentes de ciberseguridad que deben notificarse a la autoridad competente indicando los canales definidos, especificaciones de las autoridades competentes y CSIRT, criterios para la notificación y taxonomía legal en cuanto a clasificación, peligrosidad e impacto de los incidentes de ciberseguridad, metodología de notificación, información a notificar y seguimiento de incidentes. Un perfil legal de ciberseguridad estará a disposición de Las Cortes para involucrarse en un plazo máximo de una hora en caso de incidentes detectados en horario de oficina 8x5.

5) La empresa AUDIDAT 3.0, S.L.U. propone, en su oferta, el siguiente Plan de Soporte y mantenimiento:

   Dentro del planteamiento general, no se propone nada específico.

   Dentro de la descripción del sistema centralizado para la realización de consultas/peticiones, propone realizarlo a través de vía telefónica y correo electrónico.

   Dentro de los servicios y prestaciones de soporte con horarios de atención y tiempos de respuesta, propone contactar directamente con el Departamento Técnico-Jurídico por vía telefónica y a través de correo electrónico de lunes a viernes en horario de 8:00 a 14:00 y de 16:00 a 19:00. El tiempo máximo de respuesta será 24 horas a contar desde la recepción de la consulta.

Dentro de los procedimientos y mecanismos de gestión para la resolución de consultas/peticiones, propone que todas las cuestiones recibirán formato de informe firmado por el Administrador Único y Director Técnico-Jurídico y se incluirán en una base de datos disponible de manera continua.

Dentro de ampliación y mejoras de los aspectos indicados, no se propone nada específico.

6) La empresa SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U. propone, en su oferta, el siguiente Plan de Soporte y mantenimiento:

Dentro del planteamiento general, propone basarse en el Modelo de Calidad Total. La Gestión mantiene la visión holística focalizada en lo que aporta valor y la evolución del servicio alineada con el negocio, asegurando la calidad entregada y la aplicación de la metodología. La Entrega del Servicio ejecuta los servicios en base a la calidad comprometida y los objetivos que se desean obtener. La metodología se basa en las principales normas y buenas prácticas universales. Utilizarán herramientas de automatización y propuestas innovadoras del servicio. El modelo de calidad total se concreta en el plan de calidad y de mejora continua a través del modelo de relación, compartiendo el estado del servicio, mejoras propuestas, iniciativas de innovación y sus riesgos. El modelo organizativo a nivel de ejecución del servicio se compone de dos niveles, Supervisión y gestión y Ejecución: Oficina del DPD. Se incluye diagrama de estructura. Se incluye gráfico detallado con modelo de seguimiento a nivel estratégico, táctico y operativo.

Dentro de la descripción del sistema centralizado para la realización de consultas/peticiones, propone 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. Como características tiene: Recopilación datos de contacto usuario final, priorización a partir Urgencia e Impacto, notificaciones automáticas vía email, relación con problemas para investigar la causa raíz de las incidencias y agilizar la resolución, relación con Cambios.

Dentro de los servicios y prestaciones de soporte con horarios de atención y tiempos de respuesta, propone atención telefónica, email o en las propias herramientas del servicio, en horario de atención de 8:00h a 18:00h de lunes a viernes. Para solicitudes según la prioridad, el tiempo de repuesta será: Crítica menor de 24 horas naturales, Alta menor de 48 horas naturales, Media y Baja menor de 72 horas naturales.

Dentro de los procedimientos y mecanismos de gestión para la resolución de consultas/peticiones, propone tras recibir una petición de servicio, proceder a su dimensionamiento tras la aprobación y planificar las actividades y tareas necesarias. El procedimiento será Alta y definición de la petición, Estimación de los trabajos en base al esfuerzo en horas que requiere la solicitud, Validación de la estimación por parte de Las Cortes, Planificación y priorización de los trabajos, Ejecución de los trabajos por la Oficina Técnica y Validación de los trabajos por parte de Las Cortes.

Dentro de ampliación y mejoras de los aspectos indicados, propone una herramienta de seguimiento del servicio basada en Power BI

para asegurar el correcto cumplimiento del objeto del servicio y de los niveles de servicio.

3.2.2.- Valoración de las ofertas presentadas

Según lo expuesto anteriormente, en lo relativo al Plan de Soporte y mantenimiento:

Las ofertas más completas son las presentadas por las empresas OESÍA NETWORKS, S.L. y SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U.

La oferta de la empresa OESÍA NETWORKS, S.L. presenta alto nivel de detalle y personalización. Propone sistema centralizado para la realización de consultas/peticiones a través de atención telefónica, email y asistencia personal. Propone soporte con horario de 8:00 a 19:00h de lunes a viernes. No se incluye información específica respecto al tiempo de respuesta. Propone como mejora valorable acciones de soporte legal para incidentes y un perfil legal de ciberseguridad a disposición de las Cortes de Aragón en un plazo máximo de una hora en caso de incidentes detectados en horario de oficina 8x5.
Por ello se le otorga una puntuación de 4 puntos.

La oferta de la empresa SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U. presenta alto nivel de detalle y personalización. Propone sistema centralizado para la realización de consultas/peticiones a través de atención telefónica, email y herramienta de gestión de servicios Service Desk Plus.

Propone soporte con horario de 8:00h a 18:00h de lunes a viernes. Tiempo de respuesta: De 24 a 72 horas naturales. Propone como mejora herramienta de seguimiento del servicio basada en Power BI.
Por ello se le otorga una puntuación de 4 puntos.

En segundo lugar están las ofertas presentadas por las empresas CENTRO REGIONAL DE SERVICIOS AVANZADOS, S.A. y TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U.

La oferta de la empresa CENTRO REGIONAL DE SERVICIOS AVANZADOS, S.A. presenta un nivel medio de detalle y personalización. Propone sistema centralizado para la realización de consultas/peticiones a través de atención telefónica, email. Propone soporte con horario de 8:00h a 18:00h de lunes a viernes. Tiempo de respuesta: De uno-dos días hábiles a siete-nueve días hábiles en función de la gravedad del incidente.
Por ello se le otorga una puntuación de 3 puntos.

La oferta de la empresa TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U. presenta bajo nivel de detalle y personalización. Propone sistema centralizado para la realización de consultas/peticiones a través email y herramienta para gestión. Propone soporte con horario habitual de oficina de 8:00 a 19:00 h de lunes a viernes y en días festivos y fines de semana para cuestiones urgentes. Tiempo de respuesta: 48 horas, reduciéndose a 24 horas en caso de cuestiones críticas. Propone como mejoras ampliación de personas de la Oficina de Soporte a treinta personas, soporte en otros idiomas si fuera necesario.
Por ello se le otorga una puntuación de 3 puntos.

Y por último las ofertas presentadas por las empresas ECIX ARAGÓN CONSULTING, S.L. y AUDIDAT 3.0, S.L.U.

La oferta de la empresa ECIX ARAGÓN CONSULTING, S.L. presenta bajo nivel de detalle y personalización. Propone sistema centralizado para la realización de consultas/peticiones a través de número de teléfono directo del Delegado de Protección de Datos, email. Propone soporte con horario de lunes a viernes de 8:00 a 19:00h. Tiempo de respuesta: Dos días.
Por ello se le otorga una puntuación de 2 puntos.

La oferta de la empresa AUDIDAT 3.0, S.L.U. no se ajusta a la estructura incluida en el pliego, presenta bajo nivel de detalle y personalización. Propone sistema centralizado para la realización de consultas/peticiones a través de atención telefónica, email. Propone soporte con horario de lunes a viernes en horario de 8:00 a 14:00 y de 16:00 a 19:00. Tiempo de respuesta: 24h.
Por ello la puntuación obtenida es de 2 puntos.

3.3 CRITERIO: Plan de transición y devolución del servicio: Hasta 5 puntos

Se valorará la claridad expositiva, detalle y personalización del plan de transición y devolución de los servicios, obligatoriamente con la siguiente estructura: Planteamiento general. Recursos dedicados a las diferentes tareas. Estimación temporal para su realización, compromiso de plazos de entrega y gestión de desviaciones. Número y sesiones de traspaso/devolución de conocimiento. Documentación que se generará para

garantizar el solapamiento de actividades y la transferencia tecnológica y del conocimiento. Medidas a implantar para minimizar el impacto de dicha migración en la disponibilidad de los servicios por parte del Parlamento. Ampliación y mejoras de los aspectos indicados.

3.3.1.- Resumen de las ofertas presentadas

1) La empresa TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U. propone, en su oferta, el siguiente Plan de transición y devolución del servicio:

   Dentro del planteamiento general, propone el último mes de contrato la realización de actividades de transferencia de conocimiento y retorno de la documentación generada y todos los registros de actividad del servicio y configuraciones almacenados en medios digitales. Destruirán toda la información una vez haya sido transferida a las Cortes de Aragón. Garantizará la adecuada continuidad del servicio hasta el momento en que su prestación sea asumida por el nuevo proveedor.

   Dentro de los recursos dedicados a las diferentes tareas, proponen el equipo principal del proyecto, la Oficina de Soporte y el Responsable de Cuenta.

   Dentro la estimación temporal para su realización, compromiso de plazos de entrega y gestión de desviaciones, propone que sea durante el último mes de contrato.

   Dentro del número y sesiones de traspaso/devolución de conocimiento, propone la devolución del servicio en unas 22 sesiones de trabajo. Se realizará garantizando el conocimiento de los responsables de la entidad, cerrando situaciones abiertas para

evitar posibles impactos en la organización, transferencia tecnológica integrando la aplicación Sandas GRC con Pilar o descargando su información, garantizando la formalización del cambio de titularidad del servicio.

Dentro de la documentación que se generará para garantizar el solapamiento de actividades y la transferencia tecnológica y del conocimiento, propone recuperar todos los entregables comprometidos y la creación de cuantos informes sean necesarios. Se podrán extraer los informes que surjan de los cuadros de mando de la herramienta Sandas GRC.

Dentro las medidas a implantar para minimizar el impacto de dicha migración en la disponibilidad de los servicios por parte del Parlamento, proponen la revisión por expertos tecnológicos sobre migración de datos de la herramienta, revisión jurídico-organizativa sobre todos los aspectos abiertos y propuesta de cierre, mantenimiento de precios de mercado para la prestación de servicios considerados de interés prioritario durante los próximos doce meses a la finalización del contrato.

Dentro de ampliación y mejoras de los aspectos indicados, propone la aportación de un perfil Responsable de la Cuenta que velará por las cuestiones comerciales y organizativas del proyecto. Realizará un seguimiento semanal sobre el avance del proyecto y mensual donde se tratarán cuestiones de gestión de proyecto analizando desviaciones o problemas. Se propone la utilización de herramientas de gestión de proyectos como O365 Planner para la coordinación a lo largo del servicio.

2) La empresa CENTRO REGIONAL DE SERVICIOS AVANZADOS, S.A. propone, en su oferta, el siguiente Plan de transición y devolución del servicio:

Dentro del planteamiento general, propone dos meses antes de la fecha de terminación del contrato un Plan de Devolución con una planificación definitiva consensuada con Las Cortes, seguimiento periódico para garantizar el cumplimiento y viabilidad, plan de riesgos asociados al proceso de devolución de cada uno de los servicios y un plan de acción en caso de materialización de los riesgos identificados, así como colaboración total. Se creará una lista de reuniones y se consensuará el calendario de formación y de transferencia del servicio. Se utilizará un Plan de Retorno creado durante la fase inicial de prestación de servicios que será consensuado antes de la fase de devolución. Se indica listado de entregables.

Dentro de los recursos dedicados a las diferentes tareas, propone la participación de los principales niveles de gestión que hayan gobernado la prestación del servicio durante el contrato, los recursos claves y todos aquellos recursos no contemplados pero que a juicio de Las Cortes aporten valor a esta fase. Para el seguimiento del Plan de Devolución se creará un comité de seguimiento de la devolución. Se incluye tabla con los participantes, planificación y funciones. Se plantea un rol de "Gestor de la Devolución".

Dentro la estimación temporal para su realización, compromiso de plazos de entrega y gestión de desviaciones, propone un plan

estructurado en cuatro fases desplegadas a través de dos meses y con las actividades detalladas en un esquema ilustrativo.

Dentro del número y sesiones de traspaso/devolución de conocimiento, propone elaborar un plan de formación a partir del documento del Plan de Devolución consensuado. Entregarán una plantilla a Las Cortes y al proveedor entrante con el detalle del calendario de reuniones.

Dentro de la documentación que se generará para garantizar el solapamiento de actividades y la transferencia tecnológica y del conocimiento, propone entregar Procedimientos operativos de los diferentes servicios prestados así como sus relaciones y dependencias, Metodología, estándares y recomendaciones, Base de datos de conocimiento. Se realizará entrega de toda la documentación realizada u obtenida durante el período de prestación de los servicios y la concerniente a la gestión y administración de los mismos.

Dentro las medidas a implantar para minimizar el impacto de dicha migración en la disponibilidad de los servicios por parte del Parlamento, propone un período de análisis de modo que sea comprendida y aceptada por parte del receptor en su totalidad. Se revisará y planificará con el adjudicatario entrante las posibles actividades y trabajos pendientes, colaborando en la finalización de los mismos aunque se extiendan más allá del contrato.

Dentro de ampliación y mejoras de los aspectos indicados, propone el compromiso de proveer soporte remoto al nuevo proveedor durante un mes después del contrato y la incorporación a la formación prevista de elementos relacionados con el manejo y

operación de las herramientas de gestión utilizadas (Global Suite y Smartfense).

3) La empresa ECIX ARAGÓN CONSULTING, S.L. propone, en su oferta, el siguiente Plan de transición y devolución del servicio:

Dentro del planteamiento general, propone entregar la documentación generada en soporte automatizado a la finalización del servicio. En caso de que las consultas se hayan resuelto por teléfono o sin necesidad de emitir informe o dictamen, se elaborará un resumen con las consultas planteadas mensualmente.

Dentro de los recursos dedicados a las diferentes tareas, no se propone nada específico.

Dentro la estimación temporal para su realización, compromiso de plazos de entrega y gestión de desviaciones, propone que la entrega de toda la documentación generada se realizará dentro del plazo de dos meses desde la finalización del contrato. Será remitida al correo electrónico de la persona designada por Las Cortes. La carpeta de uso compartido permanecerá a disposición de Las Cortes durante el período de dos meses.

Dentro del número y sesiones de traspaso/devolución de conocimiento, no se propone nada específico.

Dentro de la documentación que se generará para garantizar el solapamiento de actividades y la transferencia tecnológica y del conocimiento, no se propone nada específico.

Dentro las medidas a implantar para minimizar el impacto de dicha migración en la disponibilidad de los servicios por parte del Parlamento, propone que el Delegado de Protección de Datos quedará a disposición de Las Cortes para llevar a cabo una reunión de cierre y traspaso de funciones al nuevo adjudicatario. Esta reunión deberá realizarse dentro del plazo de dos meses desde la finalización del contrato, debiendo convocarse con una antelación mínima de 7 días a fin de que el Delegado de Protección de Datos disponga de tiempo para organizarla.

Dentro de ampliación y mejoras de los aspectos indicados, no se propone nada específico.

4) La empresa OESÍA NETWORKS, S.L. propone, en su oferta, el siguiente Plan de transición y devolución del servicio:

Dentro del planteamiento general, propone centralizar las capacidades basándose en tres pilares: Modelo organizativo, Equipo de trabajo y Gestión de las contingencias y garantía de continuidad del servicio. Se definirá y establecerá un modelo de comunicación y seguimiento del servicio a través de comités permanentes. En las sesiones de devolución del conocimiento, se elaborará un Plan de devolución que incluye las acciones: Elaboración de un Plan de Transferencia, puesta en marcha de la transferencia, presentaciones y formación relativas a la transferencia del conocimiento, medición y evaluación de la transferencia, informes periódicos de resultado de la transferencia tecnológica, recopilación, revisión, actualización y entrega de la

documentación elaborada, devolución de los medios técnicos y lógicos.

Dentro de los recursos dedicados a las diferentes tareas, propone el Jefe de proyecto, equipo propuesto y la oficina de apoyo al DPD con disponibilidad del cien por ciento para Las Cortes. Propone comité de adaptación que se reunirá semanalmente incluyendo tabla de funciones y composición. Propone comité de seguimiento de devolución del servicio semanal y entregables.

Dentro la estimación temporal para su realización, compromiso de plazos de entrega y gestión de desviaciones, se propone que con una antelación de un mes a la finalización se pondrá en marcha el plan de devolución que durará un mes.

Dentro del número y sesiones de traspaso/devolución de conocimiento, propone sesiones de adquisición del conocimiento ejecutando todas las acciones necesarias para garantizar el arranque óptimo de los servicios. Se incluye tabla de desarrollo del plan de transición. Se proponen tres sesiones: Situación de partida donde se creará un Comité de Adaptación. Diagnóstico inicial y consolidación de la transición donde se desarrollará un Plan de Transición y un Plan de contingencia. Puesta en marcha del plan de transición y consolidación del mismo revisando y aprobando tiempos de respuesta, necesidades y mejoras que se quieran implementar en el servicio, intervenciones, recursos y carga de trabajo así como la formalización del Plan de Trabajo y Calendario para el Servicio Regular. Se incluyen los entregables que se generarán. El Plan de devolución de duración un mes, asegurará la finalización de todas las tareas, actualización de históricos y

lecciones aprendidas. De manera complementaria se elaborará un plan de comunicación del cambio.

Dentro de la documentación que se generará para garantizar el solapamiento de actividades y la transferencia tecnológica y del conocimiento, se incluye tabla con los tipos de actividades de la fase de asunción incluyendo la documentación de actividades que conlleva. Se incluye tabla detalle con la documentación generada de las sesiones de traspaso/devolución del servicio que incluye presentaciones y material de formación, documentación requerida para cada workshop, presentaciones y material de formación relativas al seminario impartido y material de apoyo que se utilice en cada taller.

Dentro las medidas a implantar para minimizar el impacto de dicha migración en la disponibilidad de los servicios por parte del Parlamento, propone la utilización de su propia Oficina de Calidad y Productividad dando apoyo al equipo de trabajo durante la fase de devolución. Se incluye tabla de riesgos y acciones de mitigación.

Dentro de ampliación y mejoras de los aspectos indicados, propone contar con el apoyo de la Oficina de Calidad y Productividad que aportará de manera complementaria otras competencias de mejora para el servicio. Se incluye tabla con competencias para: Gestión de Contingencias y Continuidad del Servicio, disponiendo de un Plan de Continuidad, estando el Jefe de proyecto a disposición y contacto permanente mediante correo electrónico o teléfono y ofreciendo y aplicando su plan de gestión de incidencias de proyecto en tiempos predefinidos y elaborando un catálogo de estrategias de recuperación o cambio. Plan de Cobertura de Recursos Humanos para garantizar la continuidad del servicio

gestionando bajas del personal, planificadas o sobrevenidas, temporales o permanentes, indicando plazos de incorporación de recursos. Centros de competencia de soporte y garantía formado por más de 100 profesionales en el ámbito de ciberseguridad, proporcionarán recursos adicionales de soporte y/o sustitución inmediata en casos de contingencia. Formación continua del equipo de trabajo del personal de Oesía.

5) La empresa AUDIDAT 3.0, S.L.U. propone, en su oferta, el siguiente Plan de transición y devolución del servicio:

   Dentro del planteamiento general, no se propone nada específico.

   Dentro de los recursos dedicados a las diferentes tareas, no se propone nada específico.

   Dentro la estimación temporal para su realización, compromiso de plazos de entrega y gestión de desviaciones, no se propone nada específico.

   Dentro del número y sesiones de traspaso/devolución de conocimiento, no se propone nada específico.

   Dentro de la documentación que se generará para garantizar el solapamiento de actividades y la transferencia tecnológica y del conocimiento, propone que permitirá al responsable del tratamiento continuar con su adaptación constante a la normativa de protección de datos a pesar de que finalice su relación con

AUDIDAT pues tendrá la posibilidad de descargar cualquier documento en formato editable.

Dentro las medidas a implantar para minimizar el impacto de dicha migración en la disponibilidad de los servicios por parte del Parlamento, no se propone nada específico.

Dentro de ampliación y mejoras de los aspectos indicados, no se propone nada específico.

6) La empresa SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U. propone, en su oferta, el siguiente Plan de transición y devolución del servicio:

Dentro del planteamiento general, propone una metodología general con Fase de Transición de salida y Fase de cierre. Se incluye gráfica de despliegue del servicio.

Dentro de los recursos dedicados a las diferentes tareas, propone de forma muy detalla las competencias y adecuación de los recursos a través de una matriz RACI (Responsable, Aprobador, Consultado, Informado) con los perfiles Gestor de Cliente, DPD as a Service y Responsable del Servicio, Consultor legal de Protección de datos y privacidad, Consultor Auditor y Consultor especialista en Seguridad Informática.

Dentro la estimación temporal para su realización, compromiso de plazos de entrega y gestión de desviaciones, propone de forma

muy detallada las actividades a realizar temporizadas en cuatro semanas.

Dentro del número y sesiones de traspaso/devolución de conocimiento, proponen 10 sesiones totales distribuidas en Definición del Plan de Salida, Lanzamiento del plan de Salida, Reunión de revisión de documentación, Formación Modelo de gestión al equipo de la Oficina del DPD, Transferencia Funcional y Técnica, Seguimiento de la devolución.

Dentro de la documentación que se generará para garantizar el solapamiento de actividades y la transferencia tecnológica y del conocimiento, propone de forma detallada la documentación que se genera en cada una de las actividades planificadas en cuatro semanas.

Dentro las medidas a implantar para minimizar el impacto de dicha migración en la disponibilidad de los servicios por parte del Parlamento, propone el seguimiento con el Comité del Plan de Salida, la identificación de Riesgos y Plan de Mitigación/Contingencia.

Dentro de ampliación y mejoras de los aspectos indicados, propone un inventario de los riesgos asociados en la fase de devolución acompañado de un plan de mitigación. Se incluye ejemplo para el riesgo Transición sin colaboración activa del proveedor actual.

3.3.2.- Valoración de las ofertas presentadas

Según lo expuesto anteriormente, en lo relativo al Plan de transición y devolución del servicio:

Las ofertas más completas son las presentadas por las empresas OESÍA NETWORKS, S.L. y SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U.

La oferta de la empresa OESÍA NETWORKS, S.L. presenta alto nivel de detalle y personalización. Los recursos dedicados a las diferentes tareas serán el Jefe de proyecto, un equipo de trabajo y la oficina de apoyo al DPD con disponibilidad total para Las Cortes. La estimación temporal será un mes. Número de sesiones de traspaso/devolución de conocimiento: 3 sesiones. Las medidas a implantar para minimizar el impacto serán la utilización de su propia Oficina de Calidad y Productividad dando apoyo al equipo de trabajo durante la fase de devolución. Propone como mejora contacto permanente mediante correo electrónico o teléfono.
Por ello la puntuación obtenida es de 4 puntos.

La oferta de la empresa SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U. presenta alto nivel de detalle y personalización. Los recursos dedicados a las diferentes tareas serán los perfiles Gestor de Cliente, DPD as a Service y Responsable del Servicio, Consultor legal de Protección de datos y privacidad, Consultor Auditor y Consultor especialista en Seguridad Informática. La estimación temporal será de un mes. Número de sesiones de traspaso/devolución de conocimiento: 10 sesiones. Las medidas a implantar para minimizar el impacto serán el seguimiento con el Comité del Plan de Salida, la identificación de Riesgos y Plan de Mitigación/Contingencia. Propone como mejora un inventario de los riesgos asociados en la fase de devolución acompañado de un plan de mitigación.
Por ello la puntuación obtenida es de 4 puntos.

A continuación está la oferta de la empresa CENTRO REGIONAL DE SERVICIOS AVANZADOS, S.A. Presenta un nivel medio de detalle y personalización. Los recursos dedicados a las diferentes tareas serán la participación de los principales niveles de gestión que hayan gobernado la prestación del servicio durante el contrato. La estimación temporal será dos meses. Número de sesiones de traspaso/devolución de conocimiento: Según documento del Plan de Devolución consensuado. Las medidas a implantar para minimizar el impacto serán un período de análisis de modo que sea comprendida y aceptada por parte del receptor en su totalidad, se revisará y planificará con el adjudicatario entrante las posibles actividades y trabajos pendientes, colaborando en la finalización de los mismos aunque se extiendan más allá del contrato. Propone como mejora proveer soporte remoto al nuevo proveedor durante un mes después del contrato.
Por ello la puntuación obtenida es de 3 puntos.

Seguidamente la oferta de la empresa TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U. Presenta bajo nivel de detalle y personalización. Los recursos dedicados a las diferentes tareas serán el equipo principal del proyecto, la Oficina de Soporte y el Responsable de Cuenta. La estimación temporal será un mes. Número de sesiones de traspaso/devolución de conocimiento: 22 sesiones. Las medidas a implantar para minimizar el impacto serán la revisión por expertos tecnológicos sobre migración de datos.
Por ello la puntuación obtenida es de 2 puntos.

En quinto lugar la oferta de la empresa ECIX ARAGÓN CONSULTING, S.L. Presenta bajo nivel de detalle y personalización. Dentro de los recursos dedicados a las diferentes tareas no se propone nada específico. La

estimación temporal será dos meses. Respecto al número y sesiones de traspaso/devolución de conocimiento no se propone nada específico. Las medidas a implantar para minimizar el impacto serán que el Delegado de Protección de Datos quedará a disposición de Las Cortes para llevar a cabo una reunión de cierre y traspaso de funciones al nuevo adjudicatario.
Por ello la puntuación obtenida es de 1 punto.

En sexto y último lugar está la oferta de la empresa AUDIDAT 3.0, S.L.U. Esta oferta no se ajusta a la estructura incluida en el pliego. Presenta bajo nivel de detalle y personalización. Dentro de los recursos dedicados a las diferentes tareas no se propone nada específico. Dentro la estimación temporal para su realización no se propone nada específico. Respecto al número y sesiones de traspaso/devolución de conocimiento no se propone nada específico.
Dentro las medidas a implantar para minimizar el impacto de dicha migración en la disponibilidad de los servicios por parte del Parlamento no se propone nada específico.
Por ello la puntuación obtenida es de 0,5 puntos.

4.- VALORACIÓN FINAL DE LAS OFERTAS ATENDIENDO A LOS CRITERIOS SUJETOS A EVALUACIÓN PREVIA

De acuerdo a lo expuesto en el apartado 3 del presente informe, el cuadro resumen de la valoración de los criterios sujetos a evaluación previa de las ofertas presentadas por los licitadores para la contratación del expediente 30/2020, es el siguiente:

Criterio de valoración SOBRE 2	Puntuación máxima 40 puntos	TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U.	CENTRO REGIONAL DE SERVICIOS AVANZADOS, S.A.	ECIX ARAGÓN CONSULTING, S.L.	OESÍA NETWORKS, S.L.	AUDIDAT 3.0, S.L.U.	SOTHIS SERVICIOS TECNOLÓGICOS, S.L.U.
2.1. Servicio de Cumplimiento del Reglamento General de Protección de Datos incluyendo un Delegado de Protección de Datos externo	**30**	***15***	***20***	***7***	***18***	***10***	***11***
2.2. Plan de Soporte y mantenimiento	**5**	***3***	***3***	***2***	***4***	***2***	***4***
2.3. Plan de transición y devolución del servicio	**5**	***2***	***3***	***1***	***4***	***0,5***	***4***
Totales	***40***	***20***	***26***	***10***	***26***	***12,5***	***19***

Zaragoza, a 16 de abril de 2021

POCINO LANA FRANCISCO JAVIER - DNI 25182347S

Firmado digitalmente por POCINO LANA FRANCISCO JAVIER - DNI 25182347S
Fecha: 2021.04.16 11:26:22 +02'00'

Fdo.: Francisco Javier Pocino Lana