EXPEDIENTE Nº: AUM-ZDAT2024004

PLIEGO DE CLAUSULAS TECNICAS PARTICULARES PARA LA CONTRATACIÓN DEL SERVICIO DE ASISTENCIA EN EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS

Elexalde kalea, 49 - 48140 IGORRE (Bizkaia) * Tfnoa. 946 311 717 * Faxa 946 319 215 * e-mail: mankomunitatea.arratia@bizkaia.org * http://www.arratia.eus * IFK/CIF P4800004F

AUM-ZDAT2024004

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO DE ASISTENCIA EN EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS Y RELACIONADA PARA LA AUM Y AEHEA.

CLÁUSULA PRIMERA.- INTRODUCCIÓN

Como consecuencia de la entrada en vigor el 25 de mayo de 2018 del Reglamento (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en adelante RGPD, las Administraciones Públicas y las organizaciones tienen la obligación de establecer un mayor control sobre sus actividades de recogida y tratamiento de datos de carácter personal. El RGPD incorpora nuevos principios y desarrolla cuestiones adicionales a los ya existentes en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de desarrollo, como son el principio de licitud, lealtad y transparencia, minimización del dato, exactitud, seguridad, portabilidad, etc.

La nueva normativa incrementa el grado de información y control que los ciudadanos tienen con respecto a sus datos y a los distintos procesos de tratamiento, cesiones y finalidades de uso que recaen sobre ellos. A estos efectos, se hace necesaria la definición, desarrollo e implantación de todas las actuaciones que se precisen para cumplir con los preceptos del RGPD, para, entre otras, gestionar de forma continua los cambios, detección de los riesgos y respuesta a los mismos de cara a eliminarlos y/o mitigarlos, establecer canales y procedimientos de notificación de incidentes y quiebras de seguridad, revisión de los procesos de recogida de tratamiento de datos, elaboración de políticas de eliminación de datos, elaboración de documentación para la realización de PIAS (evaluaciones de impacto), atención al ejercicio de los derechos de los individuos, etc.

Por todo ello y al objeto de cumplir con la normativa en materia de seguridad de la información por parte de Arratiako Udalen Mankomunitatea y Arratiako Egoitza, se hace necesario tener implantados en dichas administraciones unos robustos procedimientos legales, organizativos y técnicos que aseguren la adaptación y mejora continua en cuanto al cumplimiento de la normativa de datos de carácter personal.

CLÁUSULA SEGUNDA.- ÁMBITO DE APLICACIÓN.

Las prestaciones que son objeto de este contrato irán dirigidas a Arratiako Udalen Mankomunitatea y Arratiako Egoitza.

CLÁUSULA TERCERA.- OBJETO DEL CONTRATO.

El objeto del contrato es la prestación del servicio de asistencia jurídica y técnica para la

implantación y adecuación al cumplimiento de la normativa asociada a la seguridad de la información (Protección de Datos y Esquema Nacional de Seguridad) durante toda la vigencia del contrato, y que tendrá los siguientes componentes:

- Implantación en materia de seguridad, incluido el análisis de la situación actual,
- asesoramiento y formación.
- Concienciación y formación.
- Adecuación y mantenimiento.
- Realización de Auditorías.

Todos estos componentes se describen con detalle en el apartado "Alcance del Servicio". Se entenderá incluida en el objeto de la presente contratación cualquier normativa adicional que pueda afectar con carácter general o particular la seguridad de la información tratada por Arratiako Udalen Mankomunitatea y Arratiako Egoitza en el ejercicio de sus competencias.

La presente contratación tendrá como objetivo principal conseguir la adecuación a la normativa indicada en un plazo máximo de 6 meses desde la adjudicación del mismo (considerando exclusivamente las tareas que puedan y deban ser ejecutadas por la adjudicataria) y gestionar el posterior mantenimiento de la misma durante la vigencia del contrato.

CLÁUSULA CUARTA.- ALCANCE DEL SERVICIO.

4.1 IMPLANTACIÓN EN MATERIA DE SEGURIDAD, INCLUIDO EL ANÁLISIS DE LA SITUACIÓN ACTUAL, ASESORAMIENTO Y FORMACIÓN.

La implantación en materia de seguridad conforme al Esquema Nacional de Seguridad y RGPD Incluirá al menos los siguientes servicios:

- Análisis inicial de situación de la entidad e impacto de los cambios ENS/RGPD.
- Evaluación, gestión, tratamiento y mitigación de los riesgos.
- Planificación detallada de los trabajos de adecuación a la normativa en materia de seguridad de la información y protección de datos e implantación de los mismos.
- Validación de la implantación y auditorías.
- Redacción de los textos normativos internos, propuestas, análisis de la información, atención y resolución de consultas de protección de datos y ENS, elaboración de plantillas e informes en estas materias y asesoramiento en los procesos de tratamiento de datos.
- Coordinación y ejecución de la auditoría de cumplimiento de las obligaciones en protección de datos de carácter personal.
- Resolución de consultas técnicas y/o jurídicas referentes al cumplimiento del ENS/RGPD, así como la elaboración de plantillas .

- Asesoramiento jurídico y acompañamiento en procesos de inspección llevados a cabo por la Agencia Española de Protección de Datos.
- Formación en materia de seguridad a los empleados de la entidad.

Para la prestación del servicio de asesoramiento, se deberán contemplar, al menos los siguientes canales, con horario de atención mínimo de 8:00 a 16:00 horas en días laborables:

- ✓ Presencial, al menos, una vez al mes durante una jornada laboral completa.
- ✓ Telefónico: deberá incluir exclusivamente numeración que no sea de tarificación
- ✓ especial y/o adicional.
- ✓ Correo electrónico.

4.2 CONCIENCIACIÓN Y FORMACIÓN.

En relación con la fase quinta de la ejecución se realizarán por parte de la empresa adjudicataria, como mínimo, las siguientes actividades:

- 1 jornadas de formación presencial de 5 horas de duración, para poner en conocimiento de los/as trabajadores/as afectados/as la actividad a realizar y con las siguientes características:
  - Contenidos: Cursos con diferentes niveles de profundidad sobre la normativa asociada a la seguridad de la información, en concreto el ENS y RGPD. Cualquier otro curso que mejore las capacidades en cuanto al conocimiento de las normas internas, ciberseguridad, legislación, etc.
  - Destinatarios: Personal que se designe desde Arratiako Udalen mankomunitatea y Arratiako Egoitza.
- Una píldora audiovisual sobre aspectos de concienciación y formación en seguridad, y en un formato audiovisual adecuado para captar la atención y transmitir las ideas de una forma sencilla y eficiente.

4.3 ADECUACIÓN Y MANTENIMIENTO.

Deberá incluir las tareas necesarias para la implantación, gestión y ejecución de la adecuación normativa inicial y el mantenimiento posterior de la misma. La ejecución se llevará a cabo a través de las distintas fases que se relacionan en el apartado quinto del presente pliego.

4.4 REALIZACIÓN DE AUDITORÍAS.

Relacionado con la fase sexta de la ejecución se realizarán tareas permanentes y rutinarias de control, revisión y auditoría de eventos asociados a la seguridad de la información como el uso de otras aplicaciones o herramientas internas o de terceros que requiera una auditoría periódica sobre el acceso y uso de la misma. Además se redactarán proyectos de auditoría formales para el ENS y RGPD que se repetirán cíclicamente a lo largo de la ejecución del contrato.

4.5 IMPLANTACIÓN DE FUNCIONES DE DPD DE AUM Y AHEA

La empresa adjudicataria indicará, explicará y modelizará en el caso que sea posible al Delegado de Protección de Datos (DPD) de la Entidad correspondiente conforme a lo dispuesto en el artículo 37.1 del RGPD. A tal efecto asumirá las siguientes tareas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
- Identificación de las bases jurídicas de los tratamientos.
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Determinación de la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específico distintas de las establecidas por la normativa general de protección de datos.
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- Redacción de los contratos de encargados de tratamiento.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
- Diseño e implantación de políticas de protección de datos.
- Auditoría de protección de datos.
- Establecimiento y gestión de los registros de actividades de tratamiento.
- Análisis de riesgo de los tratamientos realizados.
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
- Realización de evaluaciones de impacto sobre la protección de datos.
- Relaciones con las autoridades de supervisión.
- Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

El DPD de las entidades desempeñará sus funciones y la empresa adjudicataria prestará la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento. Para ello deberá ser capaz de:

- Recabar información para determinar las actividades de tratamiento.
- Analizar y comprobar la conformidad de las actividades de tratamiento.
- Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
- Recabar información para supervisar el registro de las operaciones de tratamiento.

- Asesorar en la aplicación del principio de la protección de datos por diseño y por defecto.
- Asesorar sobre:
  - Si se debe llevar a cabo o no una evaluación de impacto de la protección de datos.
  - Qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos.
  - Si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o con contratación externa.
  - Qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos e intereses de los afectados.
  - Si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y,
  - Si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardasaplicar) son conformes con el Reglamento.
- Priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos.
- Asesorar al responsable del tratamiento sobre:
  - Qué metodología emplear al llevar a cabo una evaluación de impacto de la protección de datos.
  - Qué áreas deben someterse a auditoría de protección de datos interna o externa.
  - Qué actividades de formación internas proporcionar al personal responsable de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos.

PERFILES PROFESIONES

Los perfiles mínimos necesarios para la prestación del servicio base serán:

• Un Auditor.

◦ **Funciones**: supervisión de todo el proceso de auditoría, y la exactitud de los hallazgos y recomendaciones mencionados en el informe, así como preservar las evidencias de la auditoría.

◦ **Formación básica**: acreditar al menos 150 horas de formación o, por otro lado, experiencia profesional acreditada en materia de seguridad de la información durante al menos cuatro años. Tanto la formación como la experiencia deberán versar sobre:

- Auditoría de sistemas de información.
- Seguridad y gestión de riesgos de seguridad.
- Requisitos del ENS y LOPD.

◦ **Experiencia**:

- Experiencia verificable y evidenciada de al menos 2 años, en auditoría de tecnologías de la información.
- Experiencia probada de al menos 2 años en estos elementos en seguridad y gestión de riesgos de seguridad con alguna metodología reconocida

• Un Consultor.

◦ **Funciones**: cualquier tarea técnica y/o jurídica especializada que sea necesaria para el cumplimiento del objeto del contrato.

◦ **Formación básica**: acreditar al menos:

- 150 horas de formación en sistemas y comunicaciones.
- 150 horas de formación en normativa ENS y LOPD.

◦ **Experiencia:**

- Experiencia verificable y evidenciada de al menos 3 años en consultoría de sistemas y comunicaciones.
- Experiencia verificable y evidenciada de al menos 3 años en consultoría de normativa ENS y LOPD

CLÁUSULA QUINTA. FASES DE LA EJECUCIÓN

5.1 FASE 1. METODOLOGÍA PROPUESTA PARA LA IMPLANTACIÓN DEL RGPD EN AUM Y AHEA QUE CONFORMAN EL ÁMBITO DE APLICACIÓN

5.1.1 Objetivos

La finalidad de esta primera fase consiste en definir el modelo que se va a utilizar para lograr la adaptación de AUM y AHEA al cumplimiento de la normativa de Protección de Datos, incluyendo su contenido y funciones a desarrollar por el mismo de forma que se garantice al finalizar el contrato la implantación, el cumplimiento y la formación.

5.1.2 Alcance

En esta parte del proyecto, el/la adjudicatario/a definirá el proceso de implantación del RGPD, conteniendo los siguientes hitos:

- Política de implantación para el cumplimiento de protección de datos.
- Determinación de las funciones, responsabilidades, competencias que configuran la nueva normativa dentro de las entidades del ámbito de aplicación y su correspondiente soporte documental.
- Información documentada que recoja no solo los documentos referidos a las obligaciones del nuevo RGPD sino todos aquellos documentos, cláusulas, procesos, documentación que sea necesario analizar para poder ejecutar e implantar con un alto nivel de cumplimiento del RGPD y normativa. En este sentido, se debe colaborar para que cada corporación cuente con un sistema de cumplimiento de protección de datos, por defecto y desde el diseño. Se deberá alinear en todo momento con el principio de responsabilidad proactiva.
- Definición y documentación de procedimientos de supervisión y control.

Se acometerá además la elaboración de un modelo de cumplimiento de la normativa de protección de datos, para cumplir lo dispuesto en el RGPD, considerando asimismo las orientaciones, dictámenes, informes, recomendaciones de órganos consultivos independientes,directivas europeas, buenas prácticas, certificaciones, informes y recomendaciones de la Agencia Española de Protección de Datos (AEPD), etc.

5.1.3 Plazo

Un mes a contar desde la fecha de formalización del contrato.

5.1.4 Entregables.

La empresa adjudicataria deberá proporcionar al responsable del contrato la siguiente documentación:

• Modelo de implantación del RGPD.

• Planificación y calendario establecido para la implantación y cumplimiento de la normativa en materia de protección de datos de carácter personal.

5.2 FASE 2.- ANÁLISIS INICIAL DE SITUACIÓN DE LAS ENTIDADES E IMPACTO DE LOS CAMBIOS ENS/RGPD. EVALUACIÓN Y GESTIÓN DEL RIESGO.

5.2.1 Objetivo

Esta fase tiene como objetivo valorar la situación actual de implantación ENS/RGPD así como el impacto que suponen los cambios normativos Además, se realizará un evaluación y gestión del riesgo, ya que es una de las nuevas obligaciones recogidas en el RGPD, relacionándose con la responsabilidad proactiva y siendo el punto de partida para la determinación de la necesidad de llevar a cabo una evaluación de impacto.

5.2.2 Alcance

• ENS: Aplicando las guías CCN correspondientes:

- Revisión y clasificación de los sistemas de información.
- Revisión y elaboración de un informe de adecuación.
- Revisión del estado del plan de adecuación.

• RGPD:

- Revisión de puntos para la adaptación al nuevo RGPD.
- Análisis de las medidas de seguridad existentes para los datos de carácter personal.
- Adecuación de las reglas, normas y principios que inspiran el principio de responsabilidad proactiva y el enfoque del riesgo así como los protocolos internos existentes orientados a garantizar los mismos.
- Determinar las medidas técnicas y organizativas adecuadas al riesgo que conlleva el tratamiento a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD. A tal efecto se analizarán los datos que son objeto del tratamiento, con qué finalidades se hace y qué tipo de operaciones de tratamiento se llevan a cabo. A partir de este conocimiento se concretarán de forma explícita la forma en que se aplicarán las medidas que el RGPD prevé, asegurándose de que son las adecuadas para cumplir con el mismo.
- Llevar a cabo un análisis de los riesgos asociados a todos los tratamientos de datos de carácter personal. Se entiende este análisis como medida previa a la implantación de medidas de seguridad y control específicas. Primero se debe determinar si las operaciones de tratamiento de datos suponen un riesgo para los derechos y libertades del interesado, el nivel de riesgo asociado a las mismas, y en base a ello proceder a definir las medidas a adoptar para garantizar esos derechos y libertades, y en

su caso, realizar evaluaciones de impacto (EIPD o PIA por sus siglas en inglés). Por lo tanto, este análisis previo será la base para dar cumplimiento a la obligación de realizar evaluaciones de impacto.

Previamente a evaluar y analizar los riesgos será necesario componer la imagen completa del tratamiento que se está llevando a cabo. En este sentido, se deberá obtener la siguiente información:

- Identificación del tratamiento.
- Identificación de cada área o departamento relacionado con el tratamiento.
- Tipología de datos que se pretenden tratar (datos identificativos, datos económicos y financieros, datos de salud, biométricos, de geolocalización, etc.).
- Descripción de la categoría de interesados.
- Tratamiento de datos de Menores o de Titulares Vulnerables.
- Finalidades del tratamiento
- Plazos de conservación de los datos asociados as las distintas finalidades de tratamiento
- Origen de los datos (el propio interesado, fuentes accesibles al público, etc.).
- Destinatarios de los datos (internos, externos, encargados de tratamiento y cesiones de datos efectuadas)
- Movimientos y transferencias internacionales de datos.
- Tecnologías utilizadas.
- Toda esta información deberá ser recogida a través de un inventario o de un registro de actividades de tratamiento.

Una vez se haya obtenido información suficiente relativa al tratamiento de datos personales, se deberán identificar las amenazas o potenciales escenarios de riesgo asociados al tratamiento de datos. El proceso de gestión de los riesgos se divide en tres etapas:

- Identificación de amenazas, entendidas como cualquier incidente que pueda afectar a la privacidad y que acarree un perjuicio o impacto negativo determinado tanto para losderechos y libertades del interesado como para quien trate los datos. El primer paso en la gestión del riesgo será el de analizar toda la información relativa a los tratamientos de datos que se realicen para, de esta manera, detectar las amenazas y los riesgos asociados. Una vez detectados los riesgos se evaluarán, valorando la probabilidad de que sucedan, así como el nivel de impacto en la privacidad que tendría su materialización, pudiendo ser desde irrelevante, leve, grave, significativamente grave o extremadamente grave en función del tipo de amenaza identificada.
- Evaluación de riesgos asociados al tratamiento, entendiéndose éstos como aquella situación en que existe la probabilidad de que una amenaza concreta se materialice, aprovechando una vulnerabilidad en la forma en que dicho tratamiento se realiza.

Deberán tenerse en cuenta como situaciones de riesgo las siguientes:

  - Privación de derechos y libertades de los interesados
  - Ocasión de daños y perjuicios físicos, materiales o inmateriales a las personas interesadas.
  - Revelación de categorías especiales de datos personales.
  - Creación o utilización de perfiles personales.
  - Tratamiento de datos de colectivos vulnerables.
  - Tratamientos de datos a gran escala.

- Tratamiento y mitigación de los riesgos. Cuando ya estén las amenazas identificadas y los riesgos evaluados, el siguiente paso para gestionarlos es tratarlos, de manera que se mitigue su nivel de exposición con medidas de control que reduzcan bien su probabilidad bien su impacto (o ambos). Este tratamiento del riesgo puede consistir bien en eliminarlo, mitigarlo, modificar su probabilidad, compartirlo, o transferirlo. Para los procesos clave del tratamiento que pueden reducir la probabilidad de que se materialicen las amenazas detectadas o reducir su gravedad si efectivamente se producen. Estas medidas se dividirán en preventivas, cuando estén orientadas a la reducción de la probabilidad o en reactivas o de recuperación cuando estén dirigidas a minimizar el impacto o gravedad.

Cuando estén determinados los potenciales escenarios de riesgos asociados a cada tratamiento, así como las medidas adoptadas para su mitigación, atendiendo a la información que se ha recabará al inicio del proceso, se deberá valorar el nivel de riesgo que supone llevar a cabo el tratamiento para cada entidad, pudiendo ser aquel: muy bajo, bajo, medio, alto o muy alto).

En función del nivel de los riesgo resultantes, la empresa adjudicataria propondrá a las distintas entidades estrategias a seguir para enfrentarlos, las cuales deberán tener como finalidades evitar el riesgo, reducirlo, asumirlo o transferirlo a un tercero según los casos. Si el riesgo es de nivel alto o muy alto, se trata de un riesgo no tolerable que ha de ser reducido, si arroja un nivel medio, estaremos ante un riesgo tolerable que será conveniente supervisar para que el mismo no se vea incrementado y si el riesgo resulta ser bajo o muy bajo, se tratará de un riesgo asumible el cual deberá ser supervisado y controlado para garantizar que mantiene en dicho nivel.

Una vez se hayan adoptado dichas medidas técnicas organizativas con el objetivo de mitigar el riesgo, deberá verificarse que cumplen su función mediante un nuevo análisis y evaluación de los riesgos. De esta manera se llegará al riesgo residual que supone el tratamiento analizado, el cual será ya irreducible y para el que únicamente cabe la posibilidad de aceptarlo, asumirlo o transferirlo.

Es en base al nivel de este riesgo remanente que la empresa adjudicataria determinará si nos encontramos ante un tratamiento que supone un riesgo alto o muy alto que haría necesaria la realización de una evaluación de impacto EIPD o PIA.

Por lo tanto, si del análisis de riesgo se concluye que existe un alto riesgo para los derechos y libertades de los interesados, se llevarán a cabo a cabo una Evaluación de impacto (EIPD o PIA), a fin de estar en condiciones de poder adoptar las medidas adecuadas para adecuar esos tratamientos a las exigencias del RGPD. La EIPD recogerá el contenido previsto en el RGPD.

En los casos en que las EIPD hayan identificado un alto riesgo que a juicio del responsable, previa motivación de la empresa contratista, no pueda mitigarse por medios razonables en términos de la tecnología disponible y costes de aplicación, la empresa formulará la consulta que AUM Y AHEA, en su caso, realizará a la autoridad de protección de datos competente. La consulta debe ir acompañada de la documentación que prevé el RGPD, incluyendo la propia Evaluación de Impacto.

5.2.3 Plazo

Tres meses a contar desde la fecha de formalización del contrato.

5.2.4 Entregables

La empresa adjudicataria deberá proporcionar al responsable del contrato la siguiente documentación:

- Documento de análisis de situación e impacto de cambios normativos.
- Inventario de ficheros LOPD (Ley Orgánica de Protección de datos).
- Inventario o registro de actividades de tratamiento.
- Análisis de Riesgos del RGPD, y en caso de que fuera necesario, Evaluación de Impacto de Protección de Datos (EIPD o PIA).
- Formación: actualización normativa ENS/RGPD.

5.3 FASE 3.- PLANIFICACIÓN DETALLADA DE LOS TRABAJOS A REALIZAR PARA LOGRAR LA ADECUACIÓN ENS/RGPD.

5.3.1 Objetivos:

Definir un plan de adecuación, y, ejecutarlo, para lograr un pleno cumplimiento normativo en 6 meses como máximo a contar desde la fecha de formalización del contrato.

El fin para el ámbito del ENS es la obtención futura, para todas las entidades, del Certificado de Conformidad, pero no es objeto de este pliego la auditoría para dicha certificación.

5.3.2 Alcance:

- ENS:
    - Seguimiento de todos los puntos de control definidos en la Guía CCN-STIC 806.
        - ✓ Identificación y valoración de información y sistemas:
    - Revisión y actualización inventario de activos.
    - Revisión y valoración de activos.
        - ✓ Categorías del sistema
    - Valoración de niveles.
    - Identificación de medidas.
    - Valoración de fragmentar sistemas.
        - ✓ Análisis de riesgos:
    - ▪ Identificación y asociación de amenazas.
    - ▪ Análisis de riesgos
    - ▪ Riesgo residual, frecuencia e impacto.
    - ▪ Establecer la metodología de análisis de riesgo y proceder a su implantación.
        - ✓ Declaración de aplicabilidad.
        - ✓ Análisis de las medidas de seguridad exigidas en base a la categorización de los sistemas.
        - ✓ Ejecución del plan de adecuación.
- RGPD:
    - Elaboración de plan de adecuación para conseguir una plena implantación.

- Actualización y adaptación de la información y documentos específicos necesarios a raíz del RGPD y, en su caso, a la norma estatal de transposición, y confección de cualesquiera otros documentos que la empresa proponga elaborar de cara a informar, asesorar y sensibilizar a los usuarios que tratan DCP:
- Información y consentimiento: adecuación para los usuarios con acceso a datos de carácter personal (automatizado y no automatizado) con sus respectivas cláusulas y formularios, contemplando los cambios operados a nivel de categorías de datos, en el deber de información, en el consentimiento, en las transferencias internacionales de datos, bases de legitimación para el tratamiento de datos, cesiones de datos o encargos de tratamientos, principios inspiradores de la protección de datos etc.
- Derechos de los interesados: adaptación a las nuevas exigencias del RGPD para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición incorporando los nuevos derechos: derecho al olvido, derecho a la limitación del tratamiento y derecho a la portabilidad. Así mismo entra en el alcance del contrato la actualización y /o confección de los formularios pertinentes.
- Encargos de tratamientos y cesión de datos: adecuación de las cláusulas de encargo de tratamiento que se recojan en los contratos, de forma que se reflejen los nuevos contenidos adicionales: el objeto y la duración del encargo; la naturaleza del tratamiento; el tipo de datos personales; las categorías de interesados; las obligaciones y los derechos del responsable; la previsión de que las personas que deberán tratar los datos se han comprometido a mantener la confidencialidad; la asistencia del encargado al responsable para que pueda atender las solicitudes de ejercicio de derechos; la supresión o la devolución de los datos al finalizar el encargo; la obligación de poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones del encargado del tratamiento y para permitir y contribuir a la realización de auditorías e inspecciones por parte del responsable o de otro auditor autorizado por el responsable. A tal efecto se tendrán en cuenta la Directrices dadas por la AEPD para la redacción de estos contratos. De igual manera se hará expresa mención a las nuevas obligaciones expresamente dirigidas a los encargados del tratamiento, tales como la obligación de mantener un registro de actividades de tratamiento, o el deber de determinar las medidas de seguridad aplicables a los tratamientos que realizan o el de designar a un Delegado de Protección de Datos en los casos que prevé el RGPD.
- Adecuación web y redes sociales: adecuación LOPD-LSSI y RGPD para todos los servicios que se prestan vía electrónica por medio de la web, correo electrónico, SMS.etc

5.3.3 Plazo

Seis meses a contar desde la fecha de formalización del contrato.

5.3.4 Entregables:

En el plazo de seis meses señalados con anterioridad y para acreditar el cumplimiento de los señalado en esta fase del contrato, el adjudicatario deberá entregar al responsable del contrato:

• Informes de adecuación. En concreto, por cada Sistema de Información afectado se entregará:

◦ El resultado del análisis efectuado.

◦ Las insuficiencias que se observen con ocasión del análisis y propuesta de medidas correctoras.

◦ Las recomendaciones que se efectúen.

◦ La opinión o conclusiones de los consultores acerca del grado de cumplimiento de la normativa legal contrastada.

• Análisis del cumplimiento normativo de las regulaciones de protección de datos y documentación generada del alcance anteriormente previsto.

• Actualización de la documentación al ENS, en el caso de que haya existente, y elaboración de la misma, para los casos en que no la hubiera.

5.4 FASE 4.- ASISTENCIA Y PUESTA EN MARCHA DE LA IMPLANTACIÓN.

La empresa adjudicataria, en base a su experiencia y al conocimiento adquirido en las fases anteriores asesorarán a las entidades comprendidas dentro del ámbito de aplicación para elaborar la documentación, implantar la política y procedimientos del RGPD y resto de normativa aplicable, buenas prácticas, recomendaciones de las autoridades nacionales de control conforme a la propuesta elevada a la finalización de la Fase 1, aprobada en su caso, y que deberá contener entre otros aspectos, los siguientes:

- Establecimiento de un protocolo de comunicación, si ello fueraposible, al objeto de implantar el principio de responsabilidad proactiva, privacidad desde el diseño y por defecto, etc.
- Elaboración de protocolos de actuación y gestión de incidentes, ejercicio de derechosde los interesados, gestión de cesiones de datos, procedimientos ante solicitudes de Fuerzas y Cuerpos de Seguridad del Estado, Tribunales, etc, basados en normativa de transparencia.
- Establecimiento de protocolos de revisión continúa del grado de cumplimiento del RGPD y adaptación continua a la normativa.
- Establecimiento personalizado de cláusulas y registros del check-list para cada uno de los canales de entrada de datos en función de las finalidades del tratamiento de los datos (página web, fax, teléfono, oficinas presenciales...)
- Establecimiento de medidas de seguridad adecuadas.
- Establecimiento de protocolos y metodología para realización de EIPD o PIAS y documentos similares.
- Elaboración de un protocolo de notificación de incidencias que afecten a datos de carácter personal.
- Establecimiento de protocolos para el borrado de datos y documentos dentro de cada entidad.

Esta fase se desarrollará durante todo el periodo de vigencia del contrato.

5.5 FASE 5.- PLAN DE FORMACIÓN Y COMUNICACIÓN.

La adjudicataria deberá celebrar una jornada para poner en conocimiento el objeto del contrato la actividad a desarrollar, así como, la documentación o actividad que de estas requerirá. Con tal fin, la adjudicataria destinará a la celebración de esta jornada el tiempo indispensable para ello, aportando los locales y medios necesarios para su celebración. A tal efecto, la empresa deberá elaborar un Plan de Comunicación y Sensibilización que de a conocer la política de protección de datos, así como un plan de formación.

Esta fase se desarrollará durante todo el periodo de vigencia del contrato.

5.6 FASE 6.- VALIDACIÓN DE LA IMPLANTACIÓN Y AUDITORÍAS.

5.6.1 Auditoría ENS

Objetivos:

Cumplimiento del artículo 34 y Anexo III del Real Decreto 951/2015, y por lo tanto, verificar el cumplimiento de los requisitos establecidos por el Real Decreto 951/2015 en los capítulos II y III y en los Anexos I y II con el objeto de auditar el cumplimiento del Esquema Nacional de Seguridad.

Emitir una opinión independiente y objetiva, basada en los principios de integridad, presentación imparcial, debido cuidado profesional, confidencialidad, independencia y enfoque basado en la evidencia, sobre este cumplimiento de tal forma que permita a los responsables correspondientes, tomar las medidas oportunas para subsanar las deficiencias identificadas, si las hubiera.

Alcance:

- Auditoría de cumplimiento ENS, que deberá usar una metodología basada en:
  1. Auditoría de verificación de cumplimiento del ENS según las pautas establecidas en las guías CCNSTIC 802 y 808, siguiendo el itinerario, y los puntos de registro establecidos, con el objetivo de encauzar de una forma homogénea la realización de la auditoría con las premisas mínimas ya establecidas para su ejecución.
  2. La evaluación global de los resultados de la auditoría en relación al objetivo y alcance definidos y a los requisitos del RD 3/2010.
  3. Seguimiento de estándares de calidad para auditorías definidos en la ISO 19011.
- Se emitirá un pre-informe de Auditoría, identificando incumplimientos detectados y posibles acciones correctivas a corto, medio y largo plazo.
- Se ejecutará una fase de adecuación para las acciones a corto plazo.
- Se emitirá un informe de Auditoría con las acciones a medio-largo plazo.
- Actualización de Plan de acción con mejoras con más impacto.

Entregables:

Se llevará a cabo una auditoria entre los meses 10º y 12º a partir de la fecha de firma del contrato, que incluirá al menos:

• Preinforme e informe con el siguiente contenido (cumplimiento de las guías CCN-STIC 802 y 808):

- El resultado del análisis efectuado.
- Las no conformidades que se observen con ocasión del análisis y propuesta de medidas correctoras, indicando las prioritarias.
- Las recomendaciones que se efectúen.
- La opinión o conclusiones de los auditores acerca del grado de cumplimiento de la normativa legal contrastada.

• Resumen ejecutivo con las acciones que les correspondan.

• Resumen ejecutivo global para la presentación del resumen de la auditoría.

5.6.2 Auditoría LOPD/RGPD (Repetición cíclica)

Objetivo:

Auditoría obligatoria en protección de datos de carácter personal (de conformidad con los artículos 96 y 110 RDLOPD) y auditoría de aspectos jurídicos.

Alcance:

• Auditoría de cumplimiento de la LOPD, que deberá usar una metodología basada en:

- Los criterios establecidos en el marco normativo LOPD-RDLOPD
- Los estándares de calidad para auditorías definidos en la ISO 19011

• Se emitirá un pre-informe de Auditoría, identificando incumplimientos detectados y posibles acciones correctivas a corto, medio y largo plazo.

• Se ejecutará una fase de adecuación para las acciones a corto plazo.

• Se emitirá un informe de Auditoría con las acciones a medio-largo plazo.

Entregables:

Se llevará a cabo una auditoria entre los meses 10º y 12º a partir de la fecha de firma del contrato, que incluirá al menos:

• Preinforme e informe de auditoría con el siguiente contenido mínimo:

- Resultado del análisis efectuado. Se incluirán indicadores de cumplimiento en base a estándares de la ISO/IEC 27001.
- Deficiencias que, en su caso, fueren encontradas y propuesta de medidas correctoras o complementarias.
- Recomendaciones que, en su caso, se pudieren efectuar.
- Opinión o conclusiones de los auditores acerca del grado de cumplimiento de la normativa legal.

• Resumen ejecutivo por Áreas con las acciones que les correspondan.

• Resumen ejecutivo global para la presentación del resumen de la auditoría.

6. PROPIEDAD INTELECTUAL.

AUM Y AHEA podrán requerir al adjudicatario para que realice la carga de todo el conocimiento y documentación generada.

El contratista acepta expresamente que los derechos de explotación de cualquier trabajo desarrollado y documentación generada al amparo del presente contrato corresponden únicamente a AUM Y AHEA, con exclusividad y a todos los efectos.

La empresa adjudicataria no podrá hacer uso de los mismos, ya sea como referencia o como base de futuros trabajos, salvo que cuente con autorización expresa, escrita y registrada de AUM Y AHEA.

7. TRANSFERENCIA DE CONOCIMIENTO. RETORNO DEL SERVICIO.

Durante la ejecución del objeto del contrato, el adjudicatario se compromete, en todo momento, a facilitar al personal que determine AUM Y AHEA la información y documentación que se solicite para disponer de un pleno conocimiento de las circunstancias en que se desarrolla el mismo, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizadas para resolverlos.

Con el objetivo de asegurar el mantenimiento del servicio una vez finalizado el contrato, la empresa adjudicataria proporcionará en su oferta técnica un plan de reversión o retorno del servicio, que permitirá transferir a AUM Y AHEA el servicio de forma ordenada y sin interrupciones. Esta transferencia incluirá todo el material, documentación, datos, procedimientos elaborados, informes del seguimiento y cualquier otro material relacionado.

Además, para tal fin, el adjudicatario se compromete durante un periodo de tres meses y con un mínimo de 20 horas al mes, a realizar la transferencia de conocimiento a la nueva adjudicataria o al personal que determine AUM Y AHEA.

8. ACUERDO DE NIVEL DE SERVICIOS (ANS).

AUM Y AHEA podrá ponerse en contacto con la empresa adjudicataria siempre que lo considere necesario a fin de recabar información sobre la marcha general del Servicio.

Asimismo podrá comprobar la materialización y calidad de los servicios prestados mediante los medios que considere oportunos. La revisión del cumplimiento del ANS especificado en este apartado, se realizará coincidiendo con la facturación del contrato, para lo que se deberá aportar, de forma anexa a la factura, el informe detallado correspondiente. La regularización por penalizaciones se aplicará en la facturación de alguno de los meses siguientes al de la revisión.

Los indicadores, y sus valores objetivos, que como mínimo se tratarán para el control de

la calidad de los servicios serán los siguientes:

- Consultas:

◦ Tiempo de respuesta a consultas: tiempo entre el escalado de una consulta y el contacto inicial de un técnico para iniciar la resolución de la misma.

◦ Tiempo de solución consultas: tiempo entre el escalado de una consulta y su resolución.

• Formación: Incumplimiento de los hitos de concienciación y formación: incumplimiento en la forma y/o plazo de los entregables asociados.

• Auditorías y otros proyectos previstos:

◦ Incumplimiento de los plazos de adecuación: incumplimiento del plazo establecido para la adecuación normativa (seis meses, o un valor inferior ofertado como mejora).

◦ Incumplimientos en proyectos: incumplimiento en la forma y/o plazo de los proyectos.

• Seguimiento y adecuación / DPD: Incumplimiento de los requisitos establecidos en los pliegos.

A continuación se indican los valores objetivos establecidos para estos indicadores. En el supuesto de que la adjudicataria no cumpla con alguno de los valores objetivos fijados para el contrato en el ANS establecido, por causas imputables a la misma, AUM Y AHEA tendrá derecho a exigir una compensación cuantificada según se indica en las siguientes tablas:

CONTENIDO DE LAS PROPUESTAS TÉCNICAS.

Las propuestas técnicas incluirán los apartados que se indican a continuación, los cuales vienen detallados en la cláusula 19 del pliego de prescripciones técnicas particulares:

1. Introducción y puntos generales.

2. Diseño y metodología propuesta para la implantación del ENS/RGPD en las entidades del ámbito de aplicación.

3. Análisis de situación, evaluación de impacto y del riesgo, formación y planificación de los trabajos.

4. Asistencia y puesta en marcha de la implantación.

ARRATIAKO UDALEN MANKOMUNITATEA