ANEXO VI

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Habida cuenta de que el acceso a datos de carácter personal es necesario para la prestación del servicio y de conformidad con lo dispuesto en los artículos 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y 81.3 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley 15/1999 13 de diciembre de Proteccion de Datos de Carácter Personal, el adjudicatario debe adoptar y garantizar las medidas de seguridad correspondientes al nivel alto y que están especificadas en el Anexo de "Medidas de Seguridad Exigibles" como **Anexo VI** del presente pliego.

El adjudicatario se obliga y compromete a no tratar o utilizar dichos datos con fines distintos a los propios objeto de este contrato y a no comunicarlos, ni siquiera para su conservación, a otras personas.

Asimismo, el adjudicatario procederá una vez concluida la realización de los servicios contratados a entregar al Ayuntamiento los datos recibidos y sus correspondientes soportes, en el plazo máximo de treinta días, no pudiendo conservar, en forma alguna, copia total o parcial de dichos ficheros o datos o de cualquiera otros que hubieran podido ser generados como resultado, o a consecuencia de los trabajos encomendados.

El adjudicatario está obligado a la adopción de las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida y tratamiento o acceso no autorizado.

En el caso de que el adjudicatario destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del presente contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente, conforme a lo dispuesto en la LO 15/1999.

El Ayuntamiento de Pamplona podrá efectuar, en cualquier momento y siempre que ello no suponga distorsiones graves en el desarrollo de la actividad del adjudicatario, las auditorías de seguridad que considere oportunas, a fin de comprobar el cumplimiento, por parte del adjudicatario, de sus obligaciones y compromisos.

Si se establece la necesidad de llevar a cabo un traslado de datos entre el Ayuntamiento de Pamplona y el adjudicatario del servicio, quedará regulado de acuerdo con lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sin que ello suponga alteración alguna del precio de adjudicación del servicio.

En todo caso, corresponderá al Ayuntamiento de Pamplona, en su condición de responsable del tratamiento, observar y cumplimentar cuantas obligaciones pudieren venir impuestas por la normativa legal.

SECRETO PROFESIONAL

El adjudicatario y las personas que realicen directamente las tareas objeto del contrato, tratarán de modo confidencial cualquier información obtenida en la ejecución del contrato. La información será utilizada únicamente dentro del marco de los servicios que se describen en el pliego de prescripciones técnicas.

Para garantizar la observancia de esta cláusula, el adjudicatario deberá divulgar entre sus empleados la obligación del deber de secreto.

Asimismo el adjudicatario se compromete a tomar las medidas necesarias para la buena conservación de la información y del material de cualquier tipo suministrado o perteneciente al Ayuntamiento de Pamplona.

La obligación de secreto y confidencialidad obliga a las partes incluso una vez cumplido, terminado y resuelto el contrato.

El adjudicatario que incurra en contravención de esta obligación de secreto y confidencialidad, será responsable de todos los daños y perjuicios que su actuación pueda ocasionar al Ayuntamiento de Pamplona o a terceros.

MEDIDAS DE SEGURIDAD EXIGIBLES. - *NIVEL ALTO-.*

1. Los siguientes puntos exponen los objetivos de control establecidos en el Ayuntamiento de Pamplona, Responsable del Fichero, como garantía de cumplimiento de lo dispuesto en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley 15/1999 13 de diciembre de Proteccion de Datos de Carácter Personal, respecto a las medidas de seguridad aplicables a ficheros y tratamientos automatizados y asimismo las aplicables a ficheros y tratamientos no automatizados, exigibles para aquellos datos considerados de Nivel Alto y que deben ser adoptados por el adjudicatario en el tratamiento de los datos de los que el Ayuntamiento de Pamplona es responsable.

2. Están afectados todos los datos de carácter personal entregados por el Ayuntamiento o que el adjudicatario recoja en nombre del Ayuntamiento y todos aquellos que se obtengan como resultado del tratamiento y depositados en cualquier tipo de soporte.

3. Asimismo, están afectados todos aquellos ficheros que se creen con carácter temporal y estos, serán eliminados una vez que dejen de ser necesarios para los fines que motivaron su creación de manera que se imposibilite su recuperación posterior.

4. Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

5. El adjudicatario asume la responsabilidad de hacer pública y divulgar entre todas las personas que intervengan directa o indirectamente en el tratamiento de los datos, las medidas de seguridad, normas y procedimientos que se adopten para garantizar la seguridad de los datos, evitando su alteración, pérdida, tratamiento o acceso no autorizado. Asimismo, informará sobre el Deber de Secreto al que está obligado por Ley.

6. Las medidas de seguridad que se adopten estarán siempre de acuerdo con el sistema de información utilizado, con las características de los datos que se traten y la naturaleza del soporte donde residan. Cualquier cambio o actualización sobre la situación de partida, supondrá la adaptación de las medidas de seguridad implantadas por el adjudicatario.

Las medidas de seguridad aplicables a ficheros y tratamientos automatizados se regulan en el Título VIII, Capítulo III del Real Decreto 1720/2007 de 21 de diciembre.

7. La adjudicataria asume la responsabilidad de garantizar que todas aquellas personas que intervengan en el tratamiento de los datos durante la ejecución del contrato conocen los objetivos y alcance sus funciones, así como las obligaciones que se derivan, las normas que deben cumplir y las consecuencias de su incumplimiento.

8. La adjudicataria establecerá un sistema de Registro de Incidencias en el que se debe hacer constar:

- Fecha y hora en la que se produjo la incidencia
- Tipo de incidencia
- Datos identificativos de que realiza la notificación
- Efectos que se deriven de la incidencia.

9. Cualquier anomalía o mal funcionamiento que se produzca y que afecte o que pudiera llegar a afectar a la seguridad de los datos de carácter personal, será notificada inmediatamente al Ayuntamiento de Pamplona.

10. La adjudicataria adoptará las medidas preventivas y/o correctivas necesarias para garantizar la resolución del incidente y eliminar o minimizar los efectos sobre la seguridad de los datos y la probabilidad de que se repita la incidencia. La persona Responsable del Fichero será informada sobre las características de las medidas adoptadas y podrá desestimarlas si no se consideran adecuadas.

11. Sólo aquellas personas cuya intervención sea necesaria en alguna de las fases del tratamiento que configura el contrato tendrán acceso a los datos de carácter personal, ficheros y recursos afectados. La Responsable del Fichero podrá solicitar de la Encargada del Tratamiento un listado completo de las personas con acceso a los recursos protegidos (cualquier parte integrante del sistema de información).

12. La adjudicataria mantendrá un mapa de personas que especifique quiénes tienen acceso a qué recursos protegidos y el tipo de acceso permitido. Los permisos de acceso se establecerán exclusivamente basándose en las necesidades derivadas de las funciones asignadas a estas personas de manera que se garantice la restricción de acceso a los datos y recursos. La Responsable del Fichero podrá solicitar a la adjudicataria una descripción de las asignaciones que se realicen.

13. La adjudicataria implantará un mecanismo de autenticación de personas con acceso a los sistemas que permitan comprobar de forma segura su identidad con el fin de evitar suplantaciones de identidad y accesos no autorizados.

14. La adjudicataria adoptará las medidas de seguridad necesarias que permitan garantizar que los procesos de autenticación son seguros. Se adoptarán normas de seguridad y control específicas para preservar la calidad de las contraseñas de uso y controlar su asignación, distribución y almacenamiento de forma segura. La Responsable del Fichero podrá invalidar las medidas de seguridad adoptadas por la adjudicataria si entiende que éstas son insuficientes con respecto a la política de seguridad implantada en el Ayuntamiento de Pamplona.

15. La adjudicataria implantará un mecanismo de control de acceso a los recursos que asegure la restricción de acceso de las personas a los recursos autorizados y con los permisos establecidos. Identificará a quienes sean responsables de la administración del control de acceso lógico y sólo las personas designadas podrán conceder, alterar o anular el acceso sobre los datos y recursos y siempre conforme a los criterios de seguridad establecidos.

16. Todos los soportes que contengan datos de carácter personal, tanto los datos base como los resultantes de los procesos que conforman el contrato, estarán inventariados e identificados físicamente de manera que siempre pueda conocerse:

- Su ubicación física
- Su contenido
- El grado de sensibilidad y confidencialidad de la información que contiene

17. La adjudicataria adoptará las medidas de seguridad físicas necesarias que permitan garantizar:

□□ La protección al soporte y su contenido, asegurando su disponibilidad

□□ El control de acceso a los soportes y en consecuencia a los datos que contienen.

18. El intercambio de soportes que contengan datos de carácter personal entre la Responsable del Fichero y la adjudicataria se realizará adoptando las medidas de seguridad necesarias para proteger la integridad del soporte y de la información que contienen así como la confidencialidad de los datos, durante los traslados que se prevea. La Responsable del Fichero especificará en cada caso las condiciones en que se efectuará el traslado.

19. La adjudicataria es responsable de controlar que los soportes que se encuentran bajo su tutela no sean trasladados en ningún caso fuera de las instalaciones designadas para el tratamiento o almacenamiento de los mismos, sin el conocimiento y la autorización de la Responsable del Fichero.

20. Todas y cada una de las medidas de seguridad, normas y procedimiento de actuación y control adoptados por la Encargada del Tratamiento, serán acordes con el contenido del Documento de Seguridad elaborado por la Responsable del Fichero donde se especifica la normativa de seguridad de obligado cumplimiento para toda persona con acceso a los datos de carácter personal en cualquier tipo de soporte y a los sistemas de información donde residen o que los trata.

21. La adjudicataria únicamente tratará los datos conforme a las instrucciones de la Responsable del Fichero, que no los aplicará o utilizará con un fin distinto al que figura en el contrato. No los comunicará ni siquiera para su conservación a otras personas.

22. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al Ayuntamiento de Pamplona, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. En el caso de que la adjudicataria destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerada, también, Responsable del Tratamiento, respondiendo de la infracción en que hubiera incurrido persona.

23. Los ficheros que contengan datos de carácter personal que por la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información, deban reunir las medidas de seguridad de nivel medio, deberán además reunir las medidas de nivel básico.

24. La adjudicataria designará a una o a varias personas responsables de seguridad encargadas de coordinar y controlar las medidas de seguridad, normas y procedimiento que se adopten para garantizar la seguridad de los datos, evitando su alteración, pérdida, tratamiento o acceso no autorizado.

25. La designación de una o varias responsables de seguridad por parte de la Encargada de Tratamiento en ningún caso supone una delegación de la responsabilidad adquirida en el contrato, que corresponde a la Encargada del Tratamiento.

26. Los sistemas de información e instalaciones de tratamiento de datos utilizados para la realización de los tratamientos objeto del presente contrato, se someterán a una auditoria al menos cada dos años, que verifique el cumplimiento de los procedimientos y normas en materia de seguridad de datos conforme a la instrucción de la Responsable del Fichero.

27. Los informes de auditoria serán analizados por la Responsable del Fichero que propondrá las medidas correctoras que deberá adoptar la Responsable del Tratamiento para la adecuación de los sistemas de información y las instalaciones de tratamiento de datos, acorde a las instrucciones de la Responsable del Fichero.

28. La adjudicataria establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de toda persona que intente acceder al sistema de información y la verificación de que está autorizada. Deberá limitar la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. La Responsable del Fichero podrá invalidar las medidas de seguridad adoptadas por la Encargada del Tratamiento si entiende que éstas son insuficientes con respecto a la política de seguridad implantada en el Ayuntamiento de Pamplona.

29. La adjudicataria identificará a las personas con autorización para acceder a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal e implantará un mecanismo de control de acceso físico a los mismos conforme a los criterios de seguridad establecidos.

30. La adjudicataria establecerá un sistema de Registro de Entrada de soportes informáticos que permita, directa o indirectamente conocer:

- El tipo de soporte.
- La fecha y hora de entrada.
- La Persona emisora del soporte.

- El número de soportes.
- El tipo de información que contienen.
- La forma de envío.
- La persona responsable de la recepción, que deberá estar debidamente autorizada.

31.La adjudicataria establecerá un sistema de Registro de Salida de soportes informáticos que permita, directa o indirectamente, conocer:

- El tipo de soporte.
- La fecha y hora de salida
- La destinataria del soporte
- El número de soportes.
- El tipo de información que contienen.
- La forma de envío.
- La persona responsable de la entrega, que deberá estar debidamente autorizada.

32. La adjudicataria adoptará las medidas necesarias para impedir, cuando un soporte vaya a ser desechado o reutilizado, cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

33. La adjudicataria adoptará las medidas necesarias para impedir cualquier recuperación indebida, de la información almacenada en ellos, cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento.

34. La adjudicataria notificará inmediatamente al Ayuntamiento de Pamplona, cualquier anomalía o mal funcionamiento que se produzca y que afecte o que pudiera llegar a afectar a la seguridad de los datos de carácter personal. Será necesaria la autorización por escrito de la Responsable del Fichero para la ejecución de los procedimientos de recuperación de los datos.

35.La adjudicataria establecerá que en el Registro de Incidencia del Nivel medio, además de los señalados en el punto anterior, se deberá consignar:

- Procedimientos realizados de recuperación de datos.
- Persona que ejecutó el proceso de recuperación.
- Datos restaurados.
- Si ha lugar, qué datos han sido necesarios grabar manualmente en el proceso de recuperación.

36. La adjudicataria adoptará las medidas necesarias para que las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizaren con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

37. Los ficheros que contengan datos de carácter personal que por la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información, deban reunir las medidas de seguridad de nivel alto, deberán además reunir las medidas de nivel medio y básico.

38. La adjudicataria, establecerá las medidas necesarias para garantizar que la distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada

durante su transporte. La Encargada del Tratamiento deberá cifrar los datos de carácter personal o bien, utilizar cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceras personas, en el caso de que dichos datos sean transmitidos a través de redes de telecomunicaciones.

39. La adjudicataria establecerá un mecanismo que permita guardar de cada acceso, como mínimo, la identificación de quien ha accedido, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

40. Los mecanismos que permiten el registro de los datos detallados en el punto anterior estarán bajo el control directo de la persona responsable de seguridad que designe la encargada del tratamiento sin que se deba permitir en ningún caso, la desactivación de los mismos. La responsable de seguridad competente se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados. El período mínimo de conservación de los datos registrados será de dos años.

41.La adjudicataria adoptará las medidas necesarias para conservar una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en el Real Decreto.

Asimismo deberán ser aplicadas las medidas de seguridad de nivel alto aplicables a ficheros y tratamientos no automatizados, reguladas en el Título VIII, Capítulo IV (artículos 105-114) del

Real Decreto. (Los ficheros que contengan datos de carácter personal que por la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información, deban reunir las medidas de seguridad de nivel alto, deberán además reunir las medidas de nivel medio y básico.)