Pliego de Prescripciones Técnicas

Procedimiento: Abierto, con un único criterio de adjudicación

Ampliación de las licencias de uso de Decisys y 3M GRD-MS para hospitales públicos de la Región de Murcia

Referencia:	PIAS-PPT-Abierto extension DecisysCal GRD-MS (1.2).docx
Creación:	28/09/2018
Consejería:	Hacienda
CRI:	Centro Regional de Informática
Servicio:	Servicio de Gestión Informática (Consejería de Salud)

Índice de contenido

1 Objeto

El objeto del contrato consiste en ampliar las licencias de uso del módulo Decisys-Cal® y del agrupador 3M GDR-MS actualmente contratadas para extenderlas a todos y cada uno de los hospitales públicos de la Región.

El objeto del contrato se divide en los siguientes lotes, al ser éstos susceptibles de suministro, utilización o aprovechamiento separado:

LOTE 1: Ampliación de los derechos de uso de las licencias del módulo Decisys-Cal® de la aplicación informática Decisys® para el análisis del Conjunto Mínimo Básico de Datos, extendiéndola a todos los hospitales públicos de la Región e incluyendo el derecho de uso de la base de datos Oracle requerida para su funcionamiento.

LOTE 2: Ampliación de los derechos de uso de las licencias del sistemas de agrupación de pacientes 3M GDR-MS (antes denominado 3M CGS MS), extendiéndola a todos los hospitales públicos de la Región e incluyendo:

- Actualización a las versiones y mejoras durante la vigencia del contrato.
- Disponibilidad de versiones previas.
- Instalación e integración en la aplicación de análisis actual (Decisys).

2 Valor estimado

LOTE 1

El valor estimado del lote 1 es 49.440,00 euros (sin IVA), con el siguiente desglose:

- Contrato inicial: 49.440,00 euros
- Posibles prórrogas: 0 euros
- Posibles modificaciones al alza del contrato: 0 euros

LOTE 2

El valor estimado del contrato es 62.860,00 euros (sin IVA), con el siguiente desglose:

- Contrato inicial: 62.860,00 euros
- Posibles prórrogas: 0 euros
- Posibles modificaciones al alza del contrato: 0 euros

3 Descripción técnica del suministro

3.1 Entorno funcional. Especificación de requisitos

Requisitos comunes:

1. **Interoperabilidad:** Cumpliendo con compromisos de sistemas abiertos, uso de estándares internacionales y capacidad de integración con soluciones de diferentes proveedores.
2. **Integración y personalización** a lógica de negocio, al servicio de la organización y de múltiples usuarios de distintos tipos**.**
3. **Seguridad:** máximo nivel de cumplimiento de la normativa sobre protección de datos personales, control, autorización de y parametrización de accesos, auditoria.
4. **Entorno clusterizable**. Los servicios deben poder monitorizarse, arrancarse y pararse de manera ordenada. La manera de funcionar en cluster debe ser independiente del software de cluster utilizado.
5. **Exportación de datos** a paquetes ofimáticos Open Source (LibreOffice), MSOffice.
6. **Sistemas para la autentificación del usuario**. Conexión e integración con Directorio Activo.
7. **Análisis de la casuística** de los pacientes atendidos centrada especialmente en la calidad de la asistencia prestada por los distintos servicios y hospitales, solos o agrupados, por periodos de referencia y obteniendo elementos de comparación.
8. **Actualización a las nuevas versiones** de las aplicaciones o aquellas que reemplacen a las incluidas en el objeto de este pliego que aparezcan durante el periodo de mantenimiento, que estarán a disposición de la Consejería de Salud en el momento en que aparezcan en el mercado y sin coste adicional alguno. En cualquier caso se garantizará el mantenimiento de las funcionalidades de las anteriores aplicaciones o versiones, se aportará previamente información detallada de las nuevas funcionalidades del aplicativo.
9. **Actualización de los agrupadores** empleados a las nuevas versiones que aparezcan. En caso de que alguno de estos agrupadores deje de actualizarse, la Consejería de Salud podrá mantener su uso con todas las versiones preexistentes y, a la vez, podrá optar por usar algún otro de los existentes en la cartera del fabricante.
10. **Actualización de los sistemas de Clasificación Internacional de Enfermedades** (CIE) con que trabajan las aplicaciones en el momento en que esté disponible y se decida su uso por la Consejería de Salud.
11. **Entrega de un manual** en castellano junto a cada licencia para cada centro.

Requisitos LOTE 1 (DECISYS-Cal):

1. **Información Centralizada**: Un único servidor y una sola base de datos para dar servicio a todos los centros y usuarios, permitiendo gestionar datos de distintas entidades.

   Escalable de usuario independiente a nivel hospital o regional.

   La misma aplicación y datos podrán ser compartidos por todos, independientemente del entorno o tamaño de la organización, desde la Comunidad Autónoma a sus Hospitales e incluso Servicios y profesionales, permitiendo "Drill-Down" desde el máximo nivel hasta cada episodio.

   Datos, informes y resultados de análisis estarán disponibles inmediata y automáticamente para cada usuario.

   Cada entidad podrá analizar sus propios datos al tiempo que los Servicios Centrales pueden hacerlo con todos los datos de todos los centros. Los datos de todos los centros estarán disponibles para todos los usuarios. Permitiendo la comparación inmediata entre ellos y sus unidades.

   Acceso concurrente de múltiples usuarios con información consistente para todos ellos.
2. **Soluciones Oracle** para la explotación y bases de datos.
3. **Entorno Web**
4. **Cuadros de mando** flexibles, estandarizados y centralizados generados con la herramienta Oracle Business Intelligence.
5. **Incorporación de modelos de informes estandarizados y centralizados**. Posibilidad de añadir informes configurables y filtros en cualquiera de las variables contenidas en el CMBD.
6. **Normas de comparación** propias, nacionales e internacionales, incluyendo el cálculo de puntos de corte con los criterios establecidos por el cliente. Comparación entre las diferentes unidades (Hospitales, Servicios, Médicos,…), con normas propias o externas. Parametrización del cálculo del reingreso en función de los criterios del cliente (Ministerio de Salud, CCAA, Hospital, Centro de Salud, servicio...
7. **Agrupadores 3M**. Capacidad de trabajar con diferentes familias y versiones de los sistemas de clasificación de pacientes basados en GRD seleccionados por el cliente que se gestionarán de forma automática y transparente para el usuario
8. **CIE (Clasificación Internacional de Enfermedades).** Adaptación a cualquier sistema de codificación CIE-9-MC como y CIE-10-MC/PCS ES en sus diferentes versiones y revisiones.
9. **Incorporación de indicadores** generales y sobre seguridad del paciente, ingresos evitables, de calidad en la hospitalización y de la atención pediátrica de acuerdo con las definiciones de la Agencia para la Calidad e Investigación del

cuidado de la salud (Agency for Healthcare Research and Quality - AHRQ) de Estados Unidos y del ministerio de Sanidad de España.

10. **Flexibilidad en importación, exportación, validación y depuración**: la carga de datos deberá ser rápida, cómoda y eficaz desde diferentes fuentes ofimáticas o integración con BBDD originales.
11. **Adaptación a cualquier CMBD existente** empleando procesos automatizados y parametrizables de importación y exportación, CMBD regional y nacional, diferentes fuentes ofimáticas (Archivos TXT, CSV, Excel, Access, Open Source ODF, SPSS, …) o su integración con otras BBDD. Incluye mapeos de normalización de cualquier variable.
12. **Validación/depuración de los datos** incorporados al sistema para garantizar su calidad, informando de cualquier incidencia detectada durante el proceso de validación. Incorporación de criterios de validación estándar a cada episodio y de nuevas rutinas de validación.
13. **Instalación** inicial del producto y su integración con los agrupadores adquiridos en el lote 2.

Requisitos LOTE 2 (Agrupador 3M™ Core Grouping System GRD-MS):

1. **Agrupador 3M™ Core Grouping System GRD-MS** (antes denominado 3M™ CGS MS), versiones v20.0, v22.0, v24.0, v26.0, v28.0, v30.0, v33.0, v34.0 y v35.0 y posteriores durante la vigencia del contrato
2. **Editor de estructuras de entrada y salida** del software para su adaptación a las definidas por el usuario
3. **Agrupamiento interactivo** con devolución de valores CDM, GRD, los códigos de retorno del agrupador y los indicadores de validación.
4. **Procesamiento Batch** ejecutable desde interfaz de Windows o desde la línea de comandos.
5. **Planificador de versiones** creadas por el usuario para agrupar registros
6. Disponibilidad de las **diferentes versiones de codificación CIE10,** así como las que en el futuro aparezcan futuras y de futuras ampliaciones
7. **Instalación** inicial del producto y su integración con la aplicación adquirida en el lote 1**.**
8. **Disponibilidad de las diferentes versiones de codificación CIE 10**
9. **Otros:**
   - Actualización a nuevas familias y clasificaciones que surjan durante la vigencia del contrato o que se indiquen por el Ministerio de Sanidad

- Actualización de las licencias a las versiones sucesivas, las mejoras que se añadan y la disponibilidad de versiones anteriores, durante la vigencia del contrato.
- Integración con las soluciones de análisis, visualización datos y codificación de casos de la Consejería de Salud y del Servicio Murciano de Salud.

3.2 Entorno tecnológico

Requisitos LOTE 1 (DECISYS-Cal):

- Servidor con sistema operativo Windows Server 2012 R2 o superior
- Servidor web Apache 1.3 o superior
- Base de datos Oracle 11g R2 o superior
- Oracle Business Intelligence Standard Edition One 10.1.3.4.2 o superior
- Integración con 3M™ Core Grouping Software

El sistema centralizado deberá poder instalarse en un entorno virtualizado con VMWare.

Requisitos LOTE 2 (Agrupador 3M™ Core Grouping System GRD-MS):

Funcionamiento en estaciones de trabajo tipo PC, con las siguientes características:

- Sistema operativo Windows 8.1 Enterprise o Windows 10 Enterprise
- CPU: 1.2 GHz o superior
- RAM: 2 Gb o superior
- Monitor: resolución 1024x768 o superior

4 Cumplimiento normativo en materia de seguridad

4.1 Reglamento General de Protección de datos de Carácter Personal (RGPD)

Objeto del encargo del tratamiento

El adjudicatario del contrato ejercerá como encargado del tratamiento de datos de carácter personal necesario para prestar el servicio contratado. El alcance de dichos tratamientos se refiere exclusivamente a la consulta y modificación de datos del CMBD albergados en la aplicación objeto del contrato.

El Responsable del Tratamiento (RT) de dichos datos es la, Dirección General de Planificación, Investigación, Farmacia y Atención al Ciudadano (DGPIFAC), de la Consejería de Salud.

Obligaciones del encargado del tratamiento

El encargado del tratamiento y todo su personal se obliga a:

a) Utilizar los datos personales objeto de tratamiento, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b) No descargar datos personales de la aplicación objeto del contrato salvo que sea imprescindible y previa autorización de la DGPIFAC como responsable del tratamiento.

c) Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.

   Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al DPD.

d) Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

   1. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.
   2. Las categorías de tratamientos efectuados por cuenta de cada responsable.
   3. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:
      a) La seudoanimización y el cifrado de datos personales.
      b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
      c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
      d) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

e) No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa de la DG de Planificación, Investigación, Farmacia y Atención al Ciudadano (DGPIFAC) como responsable de tratamiento de los datos en los supuestos legalmente admisibles.

   El encargado puede comunicar los datos a otros subencargados del tratamiento del mismo responsable, de acuerdo con las instrucciones de la DGPIFAC . En este caso la DGPIFAC identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

f) Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

g) Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

h) Mantener a disposición de la DGPIFAC la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i) Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j) Notificación de violaciones de la seguridad de los datos

El encargado del tratamiento notificará al responsable de tratamiento (DGPIFAC), DPD y la DGIPyT, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas, y comunicar las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

1. Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
2. Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
3. Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

k) Colaborar con la DGPIFAC en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

l) Colaborar con la DGPIFAC en la realización de las consultas previas a la autoridad de control, cuando proceda.

m) Poner disposición de la DGPIFAC toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por aquella.

n) Medidas de Seguridad:

En todo caso, deberá implantar mecanismos para:

1. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
2. Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
3. Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
4. Seudonimizar y cifrar los datos personales.

o) Designar un Delegado de Protección de Datos y comunicar su identidad y datos de contacto a la DGPIFAC.

p) Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado a la DGPIFAC.

4.2 Esquema Nacional de Seguridad (ENS)

El adjudicatario asumirá el cumplimiento de lo establecido en el Real Decreto 3/2010, de 8 de enero, modificado por Real Decreto 951/2015, de 23 de octubre, sobre el Esquema Nacional de Seguridad (ENS) en este sentido y para los servicios objeto del contrato dispondrá o se comprometerá a disponer en el plazo de 12 meses a partir del inicio del contrato, de la Certificación de Conformidad con el ENS aplicable a sistemas de información de categoría **ALTA.**

El nivel exigible por la Dirección Técnica en la implantación de las medidas de seguridad en los entregables correspondientes a los servicios contratados para cada uno de los sistemas de información vendrá determinado por la categorización del sistema de información objeto de este contrato y son los siguientes:

Sistema de Información	Dimensión Disponibilidad	Dimensión Integridad	Dimensión Confidencialidad	Dimensión Autenticidad	Dimensión Trazabilidad
CMBD	A	A	A	A	A

4.3 Política de seguridad

El adjudicatario, al inicio del contrato y siempre que varíe el personal relacionado con el servicio contratado, recabará y entregará al Director Técnico una declaración responsable individual del personal a su servicio en relación con el objeto del contrato en la que:

- El firmante asume que toda la información que conozca en relación con el contrato será considerada confidencial a los efectos contemplados en la Política de Seguridad de la CARM, cuerpo documental que se desarrolle en aplicación de su Artículo 20 y Manual de Uso de los Medios Electrónicos.
- Bajo la premisa anterior se obliga como persona usuaria a las condiciones fijadas por dicha normativa.

Mantener a disposición de la DGPIFAC y la DGIPyT la documentación acreditativa del cumplimiento de las obligaciones establecidas para el cumplimiento normativo en materia de seguridad.

La Administración se reserva el derecho de auditar en cualquier momento el nivel de cumplimiento de las medidas de seguridad.

El adjudicatario deberá facilitar el acceso a los recursos que solicite la Administración para la correcta realización de la auditoría.

El adjudicatario deberá, en un plazo no superior a 3 meses, solventar sin coste para la Administración, aquellas deficiencias detectadas en dicha auditoría cuando los recursos o servicios afectados sean de su competencia o estén incluidos en la prestación de los servicios que realiza.

El incumplimiento de condiciones y compromisos puede conllevar, además de la responsabilidad civil y judicial, las correspondientes penalizaciones.

Murcia, (documento firmado electrónicamente al margen)

Jefe de Servicio de Planificación y Financiación Sanitaria
Fdo.: Joaquín Palomar Rodríguez

Jefe de Servicio de Gestión Informática
Fdo.: Manuel Agüera Pardo

EL SECRETARIO DE LA COMISIÓN TÉCNICA DE COORDINACIÓN INFORMÁTICA.
Certifica que el presente documento ha sido informado favorablemente por la Comisión celebrada el 17/10/2018
Fdo.: José Arturo Botí Espinosa