



Dirección General de Salud Digital  
CONSEJERÍA DE DIGITALIZACIÓN



*Este documento se ha obtenido directamente del original, que contenía todas las firmas auténticas, y se han ocultado los datos personales y los códigos que permitían acceder al original.*

**PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HAN DE REGIR PARA LA CONTRATACIÓN DEL SUMINISTRO ASOCIADO A LA MEJORA DE LOS PROCESOS DE CONSULTA A INFORMACIÓN CIENTÍFICA Y GUÍAS CLÍNICAS PARA EL SOPORTE A LA TOMA DE DECISIONES EN ATENCIÓN PRIMARIA PARA EL SERVICIO MADRILEÑO DE SALUD (SERMAS).**

## ÍNDICE

<b>1</b>	<b>INTRODUCCIÓN.....</b>	<b>3</b>
<b>2</b>	<b>OBJETO .....</b>	<b>4</b>
<b>3</b>	<b>DESCRIPCIÓN DEL SUMINISTRO .....</b>	<b>4</b>
<b>4</b>	<b>CARACTERÍSTICAS DEL PRODUCTO.....</b>	<b>5</b>
4.1	CARACTERÍSTICAS DE LA PLATAFORMA .....	5
4.2	PERIODO DE VIGENCIA Y MODALIDAD DE LICENCIAMIENTO .....	11
<b>5</b>	<b>CONDICIONES GENERALES DE ENTREGA .....</b>	<b>12</b>
5.1	SEGURIDAD .....	12
5.2	AUDITORÍAS .....	13
<b>6</b>	<b>SEGURIDAD Y CONFIDENCIALIDAD.....</b>	<b>13</b>
<b>7</b>	<b>PROPIEDAD INTELECTUAL .....</b>	<b>18</b>

## 1 INTRODUCCIÓN

Con el objetivo de seguir mejorando en los procesos y tareas administrativas asociados a la consulta de información científica y de guías clínicas en Atención Primaria, para así lograr una mayor agilidad en su ejecución y optimizar su desarrollo se quieren utilizar tecnología de automatización y de inteligencia artificial que sirvan de catalizadores para dicha mejora.

En el sector sanitario, la sobre carga de información y la necesidad de tomar decisiones rápidas y fundamentadas son desafíos diarios para los médicos y profesionales de la salud. La búsqueda de información y contenidos adecuados en herramientas, protocolos y guías supone un conjunto de procesos y trámites de carácter administrativo que son una oportunidad para su optimización y mejora. La inteligencia artificial conversacional se presenta como una solución transformadora para asistir en este entorno.

Actualmente, existen modelos como GPT-4 de OpenAI o Claude de Anthropic, que han demostrado el potencial de la IA para entablar conversación y responder preguntas complejas. Sin embargo, las versiones genéricas de estos modelos no siempre se ajustan a las exigencias del ámbito clínico, ya que pueden incurrir a errores u omisiones importantes, o no presentar las respuestas con el contexto pedagógico y clínico correcto. Por esa razón, surge la necesidad de disponer de un asistente conversacional que esté diseñado específicamente para profesionales sanitarios. Para ello es necesario combinar la potencia de los grandes modelos del lenguaje con una personalización al dominio médico local, garantizando respuestas precisas, relevantes y útiles para la práctica clínica.

La solución debe ser innovadora y que no sólo actúe como asistente, sino que también facilite mantener a los médicos al día con los últimos avances científicos y directrices de la práctica médica. Además, debe permitir crear múltiples chatbots configurables según las necesidades específicas que surjan en cada caso. Por tanto, se requiere contar con una base de conocimiento robusta y guías médicas internas, con el fin de dar un paso significativo hacia la redefinición de la eficiencia médica, asegurando que los profesionales sanitarios tengan acceso a información relevante y de calidad en todo momento y de manera ágil.

Adicionalmente, es importante que la solución técnica se despliegue en los entornos sanitarios, garantizando la seguridad y el cumplimiento normativo.

Por tanto, se debe garantizar con la adquisición del producto lo siguiente:

- El acceso a la solución por la organización.
- Disponibilidad de formación sobre su uso.
- Garantía del producto.

Con ello se quiere facilitar el cumplimiento de los objetivos marcados y se financiará con los presupuestos transferidos por el Ministerio de Sanidad. En particular, el objetivo perseguido es transformar la atención médica mediante la IA conversacional avanzada que apoye a los profesionales en su práctica diaria, mejorando la eficiencia y calidad de las decisiones clínicas.

El objetivo es transformar el entorno sanitario mediante la implementación de inteligencia artificial conversacional que asista a los profesionales de la salud en la toma de decisiones rápidas y fundamentadas. Basándose en las siguientes líneas:

- **Optimizar la atención médica:** se busca mejorar la eficiencia en la atención médica mediante la implementación de un asistente avanzado respaldado por la inteligencia artificial. Adaptando la información médica al nivel de comprensión del paciente, utilizando recursos visuales para explicar aquellas situaciones clínicas complejas.
- **Mejorar la calidad del cuidado médico:** mantener a los médicos actualizados con los últimos avances científicos, estudios clínicos, tratamientos y directrices de la práctica médica.
- **Facilitar la formación continua:** Proporcionar una herramienta clave para el aprendizaje continuo de los profesionales sanitarios, ayudándoles a tomar decisiones informadas y reducir errores diagnósticos.
- **Adherencia a campañas de salud:** Permite a los médicos adherirse fácilmente a campañas programadas por la Consejería, como vacunaciones y chequeos.
- **Interfaz intuitiva:** su diseño debe ser intuitivo que permita la incorporación rápida y segura de nuevos contenidos, adaptándose a las necesidades específicas de cada centro sanitario.

En resumen, el objetivo es mejorar la calidad de la atención sanitaria, apoyar a los profesionales en su práctica diaria mediante una solución de IA avanzada y, además, facilitar el bienestar del paciente.

## 2 OBJETO

El objeto de la contratación es el suministro de licencias de usuario para el acceso a una plataforma que ofrezca una solución de asistente conversacional para consultar una base de conocimiento científico y guías clínicas y que sirva de soporte a los profesionales sanitarios de Atención Primaria.

El suministro deberá cumplir con todas las especificaciones técnicas que se describen en los siguientes puntos.

## 3 DESCRIPCIÓN DEL SUMINISTRO

Este contrato tiene como objetivo la adquisición de licencias de usuario para que los profesionales de Atención Primaria del Servicio Madrileños de Salud (SERMAS) dispongan de una plataforma de conocimiento a la que acceder y realizar consultas clínicas asistidas y de manera guiada.

Cada licencia dará derecho al acceso a la plataforma licenciada durante 30 días. Por ello, se ha estimado una población de 11.470 profesionales de Atención Primaria, que durante el próximo año necesitarán 137.640 licencias para disponer de acceso a la plataforma.

El adjudicatario proporcionará como mínimo el número de licencias de usuario indicado. Una vez adquirido el paquete de licencias, la DGSD irá activando estas según su necesidad durante doce meses.

El adjudicatario ampliará, a demanda de la Administración, el número de unidades ejecutables, hasta alcanzar el importe máximo del presupuesto base de licitación, para optimizar la cuantía asignada a este proyecto por los fondos procedentes del Plan de Acción de Atención Primaria y Comunitaria 2025-2027 como herramienta de continuidad en la implementación del Marco Estratégico para la Atención Primaria y Comunitaria (MAPyC), del Ministerio de Sanidad a favor del Servicio Madrileño de Salud y transferidos a la Dirección General de Salud Digital.

El precio unitario de licitación es el resultado de dividir el presupuesto máximo del contrato entre el número mínimo de licencias (137.640).

El número de Licencias a suministrar oscila entre un mínimo de 137.640 y un máximo resultante de la división del presupuesto máximo del contrato y el precio unitario de adjudicación. Una vez realizado el cálculo se redondeará a la baja para obtener un número entero.

## 4 CARACTERÍSTICAS DEL PRODUCTO

A continuación, se indican las características y funcionalidades que debe cumplir la plataforma para la que se suministrarán licencias de uso. Se deberán tener en cuenta los siguientes requerimientos:

### 4.1 Características de la plataforma

#### 1. Características de **Arquitectura y Seguridad técnica** que se debe cumplir:

##### Arquitectura

- Seguridad, debe garantizar que los datos manejados en la plataforma no salen del territorio de la UE
- Cloud Native: Uso de componentes *serverless*.
- Revisión constante, se debe mantener actualizada a un marco de arquitectura que garantice la adopción de las mejores prácticas.
- Cumplimiento normativo: se deben cumplir las normativas de protección de datos nacionales y europeas, asegurando que las consultas no salgan del entorno autorizado.

##### Seguridad

- Auditoría y seguimiento: Debe disponer de utilidades para su monitorización.
- Gestión de cuentas: la plataforma debe permitir la autenticación multifactor (MFA), eliminación de claves en cuentas *root* y el uso de políticas de acceso basadas en el principio de privilegio mínimo.

- Redes: La plataforma debe basarse en una segmentación de red estricta, aplicando políticas de seguridad restrictivas y el uso de listas de control de acceso.

#### Gestión de vulnerabilidades

- Escaneo y parcheo: La plataforma a suministrar debe hacer uso de herramientas de identificación de fallos de seguridad o vulnerabilidades tras analizar automáticamente el sistema proporcionando recomendaciones o parches y haber seguido las buenas prácticas de desarrollo seguro de OWASP (Open Web Application Security Project).
- Evaluaciones regulares: La plataforma a suministrar debe estar mantenida realizando pruebas de penetración y revisión de código.
- Actualización continua: La plataforma a suministrar deberá seguir un proceso de actualización proactiva para mitigar riesgos de seguridad.

#### Resiliencia y Restauración

- La plataforma deberá realizar copias de seguridad automáticas de datos esenciales, acompañadas de simulacros regulares de restauración para garantizar la integridad y accesibilidad de la información.
- La plataforma debe cumplir con un objetivo de RPO (Objetivo de Pérdida de Datos) inferior a 24 horas y un RTO (Objetivo de Tiempo de Recuperación) inferior a 12 horas.

#### Consideraciones

- La Plataforma debe estar optimizada para soportar alta demanda y con capacidad de escalabilidad automática.
- Se debe garantizar el compromiso de no utilizar los datos para fines distintos de los que se autoricen de manera específica.
- Que la solución implementa buenas prácticas como la realización de revisiones técnicas formales (FTR), en el diseño y la operación de la solución.
- Debe ser prioritario en la plataforma la confidencialidad, integridad y disponibilidad de la información.

## 2. Características de la **Protección de la información** que se debe cumplir:

#### Condiciones de la plataforma

- Se debe garantizar la integridad y seguridad de un entorno cerrado, tanto de trabajo, de los contenidos, como de la propia plataforma.
- Se abstendrá de reproducir, distribuir, modificar o utilizar los contenidos sin el consentimiento expreso y por escrito. Así mismo, se compromete a que ningún tercero acceda al entorno cerrado, salvo autorización y por escrito de la DGSD.
- Debe haber compromiso de vectorizar los contenidos para que ningún tercero pueda hacer uso de estos.

- El acceso al entorno cerrado en la nube pública estará restringido exclusivamente a personas autorizadas por la DGSD.
- Las copias de seguridad deben realizarse diariamente.
- Los contenidos proporcionados cargados en la plataforma suministrada sólo serán usados para los modelos de IA específicos y nunca se emplearán en el entrenamiento de otros modelos sin consentimiento previo explícito ni para ningún otro fin que no haya sido autorizado de manera explícita y por escrito.

#### Anonimización de información

- Se debe anonimizar automáticamente la información sensible, como datos personales, DNI, direcciones u otros identificadores, en cada consulta que se realice. Esta opción podrá ser configurable y dependerá su activación por parte de la DGSD.
- No se almacenan ningún dato personal que no se proporcione como parte de una consulta.
- Se deben aplicar técnicas de anonimización y enmascaramiento para garantizar la privacidad y que la información no pueda ser reconstruida ni se pueda asociar a una persona física.
- Se deben cumplir los principios de privacidad por diseño y por defecto, alineados con el RGPD y otras normas vigentes.
- Esta capa de seguridad adicional permite trabajar con confianza en entornos sensibles, sabiendo que los datos están protegidos en todo momento y que el sistema está diseñado para minimizar riesgos desde el origen.
- Se podrá configurar en la plataforma el filtrado de consultas para evitar la carga de datos personales en la realización de consultas.

### 3. Características de **Gestión y Contenido** que se debe cumplir:

#### Base de contenidos

- La plataforma debe disponer ya de más de 1TB de información médica actualizada y contrastada.
- Debe permitir la incorporación protocolos clínicos como guías de práctica clínica locales en su base de conocimiento.
- La información base de la plataforma debe actualizarse periódicamente a poder ser semanalmente con nuevas evidencias médicas y normativas, garantizando que las respuestas se basen en la información sanitaria más reciente y relevante.
- El listado de contenidos base que debe disponer la plataforma para cubrir todo el ámbito de la medicina en España, son:
  - Alergología.
  - Anestesiología y Reanimación.

- Cardiología.
- Cuidados Paliativos.
- Dermatología.
- Endocrinología y Nutrición.
- Enfermedades infecciosas.
- Epidemiología.
- Estadística.
- Farmacología.
- Gastroenterología.
- Genética.
- Geriatria.
- Ginecología y Obstetricia.
- Hematología.
- Inmunología.
- Medicina Legal y Bioética.
- Nefrología.
- Neumología.
- Neurología.
- Oftalmología.
- Oncología Médica.
- ORL.
- Pediatría.
- Planificación y Gestión Sanitaria.
- Psiquiatría.
- Radiología-Urgencias.
- Reumatología.
- Traumatología.
- Urología

Estos contenidos son de carácter dinámico y evolutivo, y deben ampliarse de forma continua en la plataforma suministrada.

Carga de Nuevos contenidos



- La plataforma debe permitir fácilmente la incorporación de nuevos contenidos, permitiendo a los equipos de usuarios actualizar la información de forma rápida, intuitiva y segura.
- En la plataforma debe existir diferentes maneras de realizar la carga de nuevos contenidos:
  - o Se debe contar con una interfaz de usuario optimizada para arrastrar y soltar archivos directamente en la plataforma para que la carga sea inmediata.
  - o Debe poder realizarse subidas en batch, automatizando la incorporación de grandes volúmenes de documentos de una manera eficiente.
- Ya sea para añadir nuevas guías clínicas, protocolos, informes u otro tipo de documentos, el proceso siempre debe ser ágil, escalable y accesible, incluso para perfiles NO técnicos.

#### Referencias a fuentes

- Cada respuesta generada por la plataforma debe incluir la referencia directa a las fuentes originales de donde proviene el contenido, consiguiendo transparencia, trazabilidad y confianza en la información.
- Esta funcionalidad debe permitir a los usuarios:
  - o Acceder fácilmente al contenido fuente desde la propia respuesta.
  - o Validar la calidad y fiabilidad de la información consultada.
  - o Contrastar y profundizar en los temas de interés con total autonomía.
  - o Fomentar un uso responsable del conocimiento, basado en evidencias y no en interpretaciones aisladas.
- Ya sea un documento técnico, una guía clínica o un protocolo interno, la plataforma debe enlazar al contenido original, asegurando cada dato esté sustentado en su contexto real.
- Cada respuesta no debe ser útil, sino también verificable y confiable.

#### Tendencia de temáticas

- La plataforma debe incorporar una funcionalidad avanzada de análisis de tendencias, diseñada para identificar y mostrar los temas más consultados por los médicos a lo largo del tiempo.
- Gracias esta funcionalidad, el comité de Gobierno del dato y otros perfiles estratégicos pueden:
  - o Detectar áreas de interés o demandados por la organización.
  - o Anticipar necesidades formativas o informativas en base a la demanda real.
  - o Ajustar la oferta de contenidos y recursos, en función del comportamiento de búsqueda.
  - o Visualizar la evolución de estos temas.

- De tal manera, que el uso cotidiano de la plataforma será una fuente valiosa de inteligencia operativa, alineando la gestión del conocimiento con las prioridades reales de los usuarios.

#### 4. Características de **Gobernanza y Estrategia** que se debe cumplir:

La plataforma deberá poder dar soporte y facilitará la Gobernanza y estrategia según esta estructura de gobierno.

#### Comité para el Gobierno de los Datos

- Apoyo en la creación, estructuración y optimización del comité, aportando experiencia como partner estratégico en consultoría, por el fabricante de la solución en caso de ser requerido.
- El gobierno se basa en 3 pilares clave:
  - Gobierno del conjunto de contenidos: mediante definición de políticas, roles y responsabilidades con el fin de garantizar que los datos estén correctamente clasificados, gestionados y accesibles según las necesidades del negocio.
  - Análisis de la información: la plataforma debe proporcionar herramientas y metodologías para que el comité pueda interpretar los datos de forma eficaz, alineando la toma de decisiones con los objetivos estratégicos de la organización.
  - Consultoría: El fabricante de la plataforma debe estar dispuesto a trabajar codo con codo con el equipo, aportando conocimiento experto para resolver retos concretos, implementar buenas prácticas y asegurar la evolución continua del comité.

#### 5. Características de **Integración y personalizaciones** que debe cumplir la plataforma:

- La plataforma debe ofrecer integraciones y personalizaciones adaptables a las necesidades específicas, permitiendo abordar despliegues con solvencia técnica y visión estratégica. Entre las que destaca:
  - Autenticación con Single Sign On (SSO):
    - Facilitar la integración con sistemas de autenticación unificada para asegurar la identidad del usuario y simplificar el acceso a las plataformas de gobierno del dato; por ejemplo, utilizando el estándar abierto JSON Web Token.
    - Disponer de otras opciones a consensuar con la DGSD.
  - Registro de la actividad (Logs):
    - Debe existir trazabilidad completa de las acciones realizadas por los usuarios. De tal manera que estos registros permitan generar indicadores que puedan ser integrados en el cuadro de mando para realizar seguimiento o ser de interés en las auditorías.

- Cuadro de mando:
  - Ofrecer un cuadro de mandos que permita visualizar de una manera clara y personalizada la actividad, uso de datos y KPIs relevantes para el equipo del Servicio Madrileño de Salud.
  - El cuadro de mando propio de la plataforma debe ser accesible directamente desde ésta y debe permitir monitorizar y visualizar la información clave de forma clara, ágil y centralizada.
  - Se debe poder personalizar el cuadro de mando desde la plataforma y este debe estar alimentado de manera continua por datos reales y actualizados.
- Todas las integraciones y personalizaciones deben estar disponibles para ser flexibles, escalables y seguras, garantizando una implantación exitosa y siempre alineada con la estrategia tecnológica de la DGSD.

## 4.2 Periodo de vigencia y modalidad de licenciamiento

El suministro de licencias de las que se beneficiará la Consejería de Digitalización y el Servicio Madrileño de Salud para disponer de una plataforma de acceso a información clínica para Atención Primaria debe cumplir con los requisitos indicados en este documento, la licencia dará derecho al acompañamiento del fabricante de la plataforma durante el periodo de vigencia de las licencias de usuario.

Los usuarios tendrán necesariamente que pertenecer a la Consejería de Digitalización o a la Consejería de Sanidad, incluidos terceros que puedan dar apoyo al Servicio Madrileño de Salud.

Cada licencia de usuario tendrá una vigencia de 30 días.

Las características del licenciamiento son:

- Derecho de uso: por usuario de alta en la plataforma.
- Derecho de actualización: de parches de seguridad, versiones menores, versiones mayores, documentación científica de base, otros...
- Derecho de acceso a documentación: Guías de usuario, contenidos formativos para los diferentes tipos de usuarios que existan, manuales de instalación, configuración, seguridad, etc.
- Derecho de consulta al fabricante (soporte del fabricante):
  - Horario: de lunes a viernes de 09:00 a 17:00 y en los meses de julio y agosto de 09:00 a 15:00.
  - Tiempo de respuesta: máximo 2 días laborables
  - Disponibilidad de un canal de Q&A para la resolución de las dudas más frecuentes. Y facilitar una guía para el soporte de nivel 1 desde otros canales de atención al usuario de la Consejería de Digitalización o del SERMAS.

- Derecho al soporte para la carga y extracción de contenidos en la plataforma, garantizando la exclusividad de su uso a los estrictamente autorizados.
- Derecho a la configuración y parametrización de la plataforma según las necesidades de la DGSD y el SERMAS, proveyendo el fabricante soporte para la realización de estas tareas.

Para el disfrute de la plataforma por parte de los usuarios de la organización se dará un plazo de 10 días para la configuración del entorno cerrado y exclusivo en el que trabajarán estos usuarios dentro de la plataforma suministrada.

## 5 CONDICIONES GENERALES DE ENTREGA

### 5.1 Seguridad

En materia de seguridad de la información, es fundamental que el adjudicatario alcance entre otros, los siguientes objetivos en la plataforma suministrada:

- Garantizar un adecuado nivel de seguridad de la configuración de la herramienta suministrada. El adjudicatario tendrá que contemplar la seguridad en los diferentes momentos del ciclo de vida de la herramienta. Estas actuaciones permitirán gestionar los riesgos de seguridad en todo momento, y tomar las decisiones que se consideren oportunas.
- Garantizar la correcta implantación del modelo de seguridad en herramienta suministrada, marcado por el Servicio de Seguridad de Sistemas de Información de la DGSD y por la Agencia de Ciberseguridad de la Comunidad de Madrid, involucrando a los equipos de seguridad desde el inicio de los trabajos de disponibilidad y configuración de la herramienta, haciendo las pruebas que sean necesarias, garantizando en todo caso las medidas de ciberseguridad y seguir las pautas marcadas en general.
- Cumplir con todos los requerimientos que sean de aplicación de acuerdo en el marco normativo de seguridad vigente de la Comunidad de Madrid y de todas las actualizaciones posteriores que se produzcan, así como en todo el marco legal en materia de ciberseguridad que sea de aplicación. Entre otros, destaca el Reglamento General de Protección de Datos y el Esquema Nacional de Seguridad.
- Disponer de los recursos adecuados para llevar a cabo la ejecución de las tareas que le correspondan en el modelo de cumplimiento, dando respuesta en los plazos marcados por el Servicio de Seguridad de Sistemas de Información.
- Dar cumplimiento como encargado de tratamiento a aquello establecido en el Reglamento General de Protección de Datos. Por lo que hace la seguridad en el tratamiento de estas, el adjudicatario implementará las medidas de seguridad establecidas por el Servicio de Seguridad de Sistemas de Información y la Agencia de Ciberseguridad de la Comunidad de Madrid en el marco de Ciberseguridad para la Protección de Datos. Esta implementación y nivel de cumplimiento serán incorporados al modelo de cumplimiento normativo de la Comunidad de Madrid.

- Asumir la corrección de todas aquellas vulnerabilidades de seguridad para cumplir con los umbrales solicitados por el Servicio de Seguridad de Sistemas de Información, a partir de los cuales la herramienta podrá ser utilizada.
- Asumir la corrección de todas aquellas vulnerabilidades de seguridad detectadas en los análisis de seguridad. El Servicio de Seguridad de Sistemas de Información podrá ejecutar en cualquier momento los análisis de seguridad que considere oportunos.
- Garantizar el despliegue efectivo de la estrategia de ciberseguridad determinada por el Servicio de Seguridad de Sistemas de Información, velando por la implementación efectiva de los diferentes servicios, procesos y tecnologías que la componen.

## 5.2 Auditorías

La Agencia de Ciberseguridad de la Comunidad de Madrid, el Servicio de Seguridad de Sistemas de Información (OSSI) o cualquier organismo competente de la Comunidad de Madrid podrán revisar o auditar la correcta ejecución de los procesos de seguridad con la periodicidad que consideren necesaria.

En todos aquellos casos en que se decida la realización de una auditoría, el adjudicatario tendrá que garantizar el acceso total, incondicional e irrevocable a los documentos y herramientas existentes que estén relacionadas con el suministro del producto.

El adjudicatario proporcionará la asistencia y la información que requieran las auditorías, sin cargo adicional para la Consejería de Digitalización. La información se proporcionará en la forma y tiempos requeridos.

La realización de la auditoría en ningún momento eximirá al adjudicatario del cumplimiento de los compromisos derivados de la licitación.

En la finalización de la auditoría las partes revisarán las desviaciones y/u observaciones detectadas, elaborando un plan de acción. El conjunto del resultado será firmado por ambas partes.

El adjudicatario, de acuerdo con el calendario establecido en el plan de acción, se compromete a informar del estado y a llevar a cabo las actividades establecidas en el plan de acción. La DGSD podrá verificar que el plan de acción se ha implementado correctamente.

## 6 SEGURIDAD Y CONFIDENCIALIDAD

En el caso de que el adjudicatario, en el ejercicio del contrato, tuviera que tratar con datos personales del Servicio Madrileño de Salud, cumplirá con la legislación vigente en materia de protección de datos personales que resulte de aplicación, en concreto *con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)*, y el *Reglamento (UE) 2016/679 del Parlamento Europeo 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (RGPD)*; o cualesquiera otras

aplicables en materia de Protección de Datos que se encuentren en vigor a la adjudicación de este contrato o que puedan estarlo durante su vigencia.

Así, y a los efectos de este contrato, el Servicio Madrileño de Salud y/o la DGSD tendrá la consideración de responsable del tratamiento y el adjudicatario tendrá la consideración de Encargado del Tratamiento conforme a lo establecido en los artículos 28 y 29 del RGPD, así como en el artículo 33 de la LOPDGDD.

Adicionalmente, el adjudicatario deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio. Dicho POC de seguridad será el propio responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma.

**Encargado del Tratamiento:** El adjudicatario, se compromete a cumplir las medidas y requisitos de seguridad exigidos por el responsable del tratamiento.

El tratamiento de datos personales por el adjudicatario se regirá por un contrato, Pliego o acto jurídico análogo, donde se establezca el objeto, la duración, la naturaleza y finalidad del tratamiento, así como el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

Las obligaciones derivadas de esta responsabilidad asumida por el adjudicatario serán recogidas en un documento específico que será firmado por la Entidad contratante y el adjudicatario de forma previa al inicio de los trabajos.

**Limitación del acceso o tratamiento:** El adjudicatario limitará el acceso o tratamiento de datos personales pertenecientes al responsable del tratamiento, limitándose a realizar el citado acceso o tratamiento cuando se requiera imprescindiblemente para la prestación del servicio y/o de las obligaciones contraídas, y en todo caso limitándose a los datos que resulten estrictamente necesarios.

**Instrucciones de Tratamiento:** Toda la información que se entregue al adjudicatario para el desarrollo de los trabajos tendrá el carácter de confidencial.

A los efectos de la ejecución del contrato, en su calidad de Encargado del Tratamiento quedará obligado, a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento o realización de los trabajos objeto de este pliego, especialmente los personales o empresariales, que no podrá copiar o utilizar con fin distinto al que figura en este pliego, ni tampoco ceder a otros ni siquiera a efectos de conservación.

El adjudicatario quedará obligado además de por el deber de confidencialidad, por el deber de seguridad de los datos personales, en todas aquellas previsiones que estén contempladas en las actividades que formen parte del contrato adjudicado, en especial:

- El adjudicatario y el personal encargado de la realización de las tareas guardarán y asegurarán la confidencialidad, disponibilidad e integridad sobre todas las informaciones, documentos y asuntos a los que tengan acceso o conocimiento durante la vigencia del contrato, no revelando, transfiriendo o cediendo, ya sea verbalmente o por escrito, a



cuantos datos conozcan como consecuencia de la ejecución del contrato, sin límite temporal alguno.

- El adjudicatario, mediante la suscripción del contrato de adjudicación, asumirá el cumplimiento de lo previsto en las presentes cláusulas, atendiendo en especial, a los artículos 28, 29, 30 y 32 del RGPD, así como los artículos 28 y 31 de la LOPDGDD.
- El adjudicatario utilizará los datos personales única y exclusivamente, en el marco y para las finalidades determinadas en el objeto del contrato adjudicado y del presente documento, y bajo las instrucciones del responsable del Tratamiento, para aquellos aspectos relacionados con sus competencias.
- Accederá a los datos personales responsabilidad del responsable del Tratamiento únicamente cuando sea imprescindible para el buen desarrollo del contrato.
- En caso de que el tratamiento incluya la recogida de datos personales en nombre y por cuenta del responsable del Tratamiento, el Adjudicatario deberá seguir los procedimientos e instrucciones que reciba del responsable del Tratamiento, especialmente, en lo relativo al deber de información y, en su caso, la obtención del consentimiento de los afectados.
- Si el adjudicatario considera que alguna de las instrucciones del responsable del Tratamiento infringe el RGPD, la LOPDGDD, o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, informará inmediatamente al responsable del Tratamiento.
- En caso de estar obligado a ello por el artículo 30 del RGPD y 31 de la LOPDGDD, el adjudicatario mantendrá un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable del Tratamiento, que contenga la información exigida por el artículo 30.2 del RGPD.
- Dará apoyo al responsable del Tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.
- Dará apoyo al responsable del Tratamiento en la realización de las consultas previas a la Autoridad de Control, cuando proceda.
- Pondrá a disposición del responsable del Tratamiento toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen al responsable del Tratamiento u otro auditor autorizado por este.
- En caso de estar obligado a ello por el artículo 37.1 del RGPD y por el artículo 34 de la LOPDGDD, designará un delegado de protección de datos y comunicará su identidad y datos de contacto al responsable del Tratamiento, cumpliendo con todo lo dispuesto en los artículos 37, 38 y 39 del RGPD y 35 a 37 de la LOPDGDD.
- En caso de que el adjudicatario deba transferir o permitir acceso a datos personales responsabilidad del responsable del Tratamiento a un tercero en virtud del Derecho de la

Unión o de los Estados miembros que le sea aplicable, informará al responsable del Tratamiento de esa exigencia legal de manera previa, salvo que estuviese prohibido por razones de interés público.

- Se prohíbe el tratamiento de datos por terceras entidades que se encuentren en terceros países sin un nivel de protección equiparable al otorgado por la normativa de protección de datos personales vigente en España, salvo que se obtenga la preceptiva autorización de la Agencia Española de Protección de Datos para transferencias internacionales de datos, de conformidad con los artículos 44, 45, 46, 47, 48, y 49 del RGPD y los artículos 40, 41, 42 y 43 de la LOPDGDD.
- El adjudicatario comunicará y hará cumplir a sus empleados, y a cualquier persona con acceso a los datos personales, las obligaciones establecidas en los apartados anteriores, especialmente las relativas al deber de secreto y medidas de seguridad.
- El adjudicatario no podrá realizar copias, volcados o cualesquiera otras operaciones de conservación de datos, con finalidades distintas de las establecidas en el servicio adjudicado, sobre los datos personales a los que pueda tener acceso en su condición de adjudicatario, salvo autorización expresa y por escrito del responsable del Tratamiento.
- Adoptar y aplicar las medidas de seguridad estipuladas en el presente contrato, conforme lo previsto en el artículo 32 del RGPD, y el Esquema Nacional de Seguridad que resulte de aplicación, que garanticen la seguridad de los datos personales responsabilidad del Responsable del Tratamiento y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.
- El adjudicatario se compromete a formar e informar a su personal en las obligaciones que de tales normas dimanen, para lo cual programará las acciones formativas necesarias, incluida la formación en protección de datos y seguridad. Asimismo, el Adjudicatario y su personal tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- El adjudicatario comunicará al responsable del Tratamiento, para aquellos aspectos relacionados con sus competencias, de forma inmediata, cualquier incidencia en los sistemas de tratamiento y gestión de la información que haya tenido o pueda tener como consecuencia la alteración, la pérdida o el acceso a datos personales, o la puesta en conocimiento por parte de terceros no autorizados de información confidencial obtenida durante la prestación del servicio.
- El adjudicatario estará sujeto a las mismas condiciones y obligaciones descritas previamente en el presente documento, con respecto al acceso y tratamiento de cualesquiera documentos, datos, normas y procedimientos pertenecientes al responsable del Tratamiento a los que pueda tener acceso en el transcurso de la ejecución del contrato.



### **Destino de los datos al finalizar la vigencia de las licencias suministradas**

Una vez cumplida o resuelta la relación contractual acordada entre el responsable del Tratamiento y el adjudicatario, el adjudicatario deberá solicitar al responsable del Tratamiento instrucciones precisas sobre el destino de los datos personales de su responsabilidad, pudiendo elegir éste último entre su devolución, remisión o destrucción íntegra, siempre que no exista previsión legal que exija la conservación de los datos, en cuyo caso no podrá procederse a su destrucción. La devolución o destrucción de la información no eximirá al adjudicatario del cumplimiento de confidencialidad aquí reflejada.

Así mismo, el responsable del Tratamiento tendrá derecho a exigir en cualquier momento que la información confidencial, proporcionada al adjudicatario, sea destruida o devuelta, ya sea antes, durante o después de la celebración.

### **Cesión o comunicación de datos a terceros.**

El adjudicatario no comunicará los datos accedidos o tratados a terceros, ni siquiera para su conservación. Así, el adjudicatario no podrá subcontratar ninguna de las prestaciones que formen parte del objeto del pliego y que comporten el tratamiento de datos personales, salvo servicios auxiliares necesarios para la normal ejecución del contrato.

- En caso de que el adjudicatario necesitara subcontratar todo o parte de los trabajos contratados por el responsable del Tratamiento en los que intervenga el tratamiento de datos personales, deberá comunicarlo previamente y por escrito al responsable del Tratamiento, con una antelación de 1 mes, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subencargada, así como sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable del Tratamiento no manifiesta su oposición en el plazo establecido.
- El subencargado, también está obligado a cumplir las obligaciones establecidas en este documento para el adjudicatario y las instrucciones que dicte el responsable del Tratamiento.
- Corresponde al adjudicatario exigir por contrato al subencargado el cumplimiento de las mismas obligaciones asumidas por él a través del presente documento.
- El adjudicatario seguirá siendo plenamente responsable ante el responsable del Tratamiento en lo referente al cumplimiento de las obligaciones.

### **Responsabilidad en caso de incumplimiento.**

En el caso de que el adjudicatario destinase los datos a otra finalidad, los comunicase o bien, los utilizase incumpliendo las estipulaciones contenidas en el presente pliego, o en general, los utilice de forma irregular, así como cuando no adoptase las medidas correspondientes para el almacenamiento y custodia de estos, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente. A tal efecto, se obliga a indemnizar al responsable del Tratamiento, por cualesquiera daños y perjuicios que sufra directamente, o por toda reclamación, acción o procedimiento, que traiga su causa de un

incumplimiento o cumplimiento defectuoso por parte del adjudicatario de lo dispuesto tanto en los Pliegos, como en el Contrato, como en lo dispuesto en la normativa reguladora de la protección de datos personales.

## 7 PROPIEDAD INTELECTUAL

El contratista acepta expresamente que todos los derechos de propiedad intelectual sobre las configuraciones, parametrizaciones, adaptaciones, implementaciones complementarias, estudios, documentos, productos, subproductos, etc., generados al amparo del presente contrato, corresponden únicamente a la DGSD, con exclusividad y a todos los efectos, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el contratista autor material de los trabajos.

Así, podrán ser reutilizados sin coste en cualquier otra implantación en el ámbito del SERMAS o del SNS.

No se incluye en el anterior apartado los derechos de uso sobre los productos protegidos con propiedad intelectual y que se adquieran en esta contratación.

El adjudicatario renuncia expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del contrato pudieran corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de la DGSD.

Madrid,

**LA DIRECTORA GENERAL DE SALUD DIGITAL**

Firmado digitalmente por: RUIZ HOMBREBUENO NURIA  
Fecha: 2025.11.19 14:46