

*PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA  
CONTRATACIÓN DE UN SERVICIO DE EJECUCIÓN DE TAREAS  
RELATIVAS A LA SEGURIDAD DE LA INFORMACIÓN PARA EL  
HGUGM*

**CENTRO:** Hospital General Universitario Gregorio Marañón



## HOJA DE CONTROL DE CAMBIOS

Versión	Realizado / Modificado por	Fecha Modificación	Motivo del cambio
01			Creación del documento

## DISTRIBUCIÓN DEL DOCUMENTO:

Nombre	Área



## ÍNDICE

1. INTRODUCCIÓN .....	4
2. OBJETO .....	5
3. ESPECIFICACIONES TÉCNICAS DEL SERVICIO .....	6
3.1 Cumplimiento del RGPD en materia de Sistemas de Información .....	7
3.2 Realización de Análisis de aplicaciones para elaboración de Documentos de Registro de Actividades de Tratamientos. ....	7
3.3 Realización de análisis de riesgos y evaluación de impacto .....	8
3.4 Realización de tareas de documentación del comité de seguridad, Normativa de Seguridad, Diagnóstico de Seguridad y Auditoría del CPD y Procedimientos e Instrucciones Técnicas. ....	8
3.5 Respuesta al ejercicio de los derechos incluidos en el RGPD.....	8
3.6 Gestionar y resolver todas incidencias de seguridad .....	8
3.7 Relación con la OSSI en materia de seguridad .....	9
3.8 Realización de auditorías anuales para cumplimiento normativa .....	9
4. EQUIPO DE TRABAJO Y HORARIO DE SERVICIO .....	10
5. COMITÉ DE SEGUIMIENTO .....	12
6. PENALIDADES .....	13
7. CERTIFICACIONES DE EMPRESA.....	15
8. CONTENIDOS DE LAS PROPUESTAS TÉCNICAS .....	16
9. SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN .....	17
9.1 Normativa de seguridad y protección de datos .....	17
9.2 Encargado del Tratamiento. ....	17
9.3 Limitación del acceso o tratamiento. ....	17
9.4 Medidas de Seguridad. ....	18
9.5 Destino de los datos al finalizar la prestación del servicio. ....	20
9.6 Cesión o comunicación de datos a terceros.....	20
9.7 Responsabilidad en caso de incumplimiento. ....	21
9.8 Cesión del contrato. ....	21
10. COMPROMISO MEDIOAMBIENTAL .....	22
11. CONSIDERACIONES SOCIALES.....	23
12. CLÁUSULAS ADICIONALES .....	24



## 1. INTRODUCCIÓN

---

El 25 de mayo de 2016 entró en vigor el Reglamento General de Protección de Datos (RGPD), que sustituye a la normativa vigente en materia de Protección de Datos y que comenzó a aplicarse el 25 de mayo de 2018. Este periodo de dos años tiene como objetivo permitir que los Estados de la Unión Europea, las Instituciones y también las empresas y organizaciones que tratan datos de carácter personal vayan preparándose y adaptándose para el momento en que el Reglamento sea aplicable.

Con este escenario en cuanto al nuevo RGPD y junto con la necesidad del cumplimiento del Esquema Nacional de Seguridad (ENS), el Hospital General Universitario Gregorio Marañón (en adelante HGUGM), propone la contratación de un servicio y la realización de tareas necesarias como ayuda para la creación y adaptación de la documentación relativa a la seguridad, mantenimiento de las relaciones con terceras organizaciones, así como, respuesta ante la necesidad de amparar y proteger a las personas y profesionales, en el uso de los datos de carácter personal.

Por ello, se requieren los servicios de un proveedor tecnológico que incorpore un equipo especializado de seguridad que sea capaz de desarrollar los servicios y actividades contemplados en el presente pliego técnico.



## 2. OBJETO

Constituye el objeto del contrato, la contratación del servicio para la **ejecución correcta de tareas en tiempo y forma** relativas a los siguientes objetivos:

- En caso de que el nuevo RGPD deba incluir nuevos documentos y acciones a realizar, se realizarán por parte del adjudicatario para el cumplimiento de la normativa vigente.
- Realización del análisis de todas las aplicaciones instaladas en el HGUGM para su posterior inclusión o realización de Documentos para los Registros de Actividades de Tratamiento, categorización de las aplicaciones y análisis de viabilidad de los aplicativos.
- Realización de las tareas relativas a la constitución, modificación y mejoras de la Normativa de Seguridad, los Procedimientos e Instrucciones Técnicas y todo aquello que se considere necesario de manera adicional por parte del HGUGM. Además de la preparación de documentación para el comité de seguridad. Se adaptará toda esta documentación al nuevo RGPD.
- Elaboración y mantenimiento actualizados de los documentos de Registros de Actividades de Tratamiento, categorización de las aplicaciones y análisis de viabilidad de los aplicativos y de la organización administrativa del HGUGM bajo requerimientos de sus órganos superiores.
- Respuesta al ejercicio de los derechos de Supresión, Oposición, Portabilidad, Limitación, Acceso y Rectificación incluidas en el nuevo RGPD, incluyéndolas, tramitándolas y resolviéndolas, con las herramientas que determine en cada momento el HGUGM en tiempo y forma, y de manera correcta.
- Gestionar y resolver todas las incidencias de seguridad en tiempo y forma, acorde con las necesidades del HGUGM, incluyendo el análisis, valoración técnica y funcional así como elaboración de las respuestas a los incidentes de seguridad relativos a los CISEM recibidos en la Subdirección de Sistemas de Información.
- Llevar la relación con la OSSSI (Oficina de Seguridad de Sistemas de Información) de la Dirección General de Sistemas de Información del Servicio Madrileño de Salud en materia de seguridad, contestando a los requerimientos, peticiones y necesidades de manera correcta y verificada por el HGUGM en tiempo y forma.
- Realización de toda la documentación de análisis de riesgos y evaluación de impacto relativa al HGUGM en la herramienta PILAR o la que en cada momento determine el HGUGM, para adecuación al RGPD.
- Realización de auditorías legales en el HGUGM en base a la normativa y legislación vigente tanto del ENS y del RGPD, para la revisión de la adaptación de protocolos internos y exposición de puntos de mejora sobre la auditoría.  
Gestión de documentación para la interconexión de las VPN, así como validación de la misma. Interlocución con terceros para cumplimentación de documentación de seguridad.



### 3. ESPECIFICACIONES TÉCNICAS DEL SERVICIO

---

Como condición general para todos los puntos expuestos en este apartado, el visado de la correcta ejecución de las tareas y de la documentación elaborada, será realizado por el interlocutor del servicio nombrado por parte del HGUGM.

Si se determina por parte del HGUGM que una tarea o documento, política, proceso, protocolo o entregable no es correcto, el adjudicatario tendrá 3 días naturales para subsanar los mismos. En caso de que, tras la nueva entrega por parte del adjudicatario, se determine por parte del HGUGM que sigue sin estar correcto, será motivo de aplicación de las penalidades correspondientes. Será motivo de rescisión de contrato la reiterada baja calidad de la documentación o tareas entregadas.

En caso del incumplimiento de las entregas por parte del adjudicatario, será motivo de la aplicación de las penalidades correspondientes.

La entrega de documentos, políticas, protocolos, procesos y procedimientos por parte del HGUGM al adjudicatario se realizará en formato electrónico o formato papel, recibiendo acuse de recibo en las siguientes 24 horas por parte del adjudicatario. En caso de no recibir dicho acuse de recibo y justificar el HGUGM su entrega mediante correos electrónicos, se considera entregado a efectos de contabilización de tiempos de realización de las tareas encomendadas.

Toda la documentación generada por el adjudicatario será en formato electrónico bajo los parámetros y ajustes definidos por el HGUGM al inicio del contrato.

Todo el material, entregables, documentación generados durante la duración del contrato será propiedad del HGUGM, y no podrá ser utilizado por el adjudicatario para otros fines que no sean la prestación del servicio objeto de este contrato.

Si fuera necesario dar acceso a herramientas corporativas, el HGUGM será el encargado de facilitarlo al adjudicatario.

El adjudicatario utilizará el gestor documental y resto de herramientas informáticas que en cada momento indique el HGUGM, siendo responsable el adjudicatario de la gestión de la parte correspondiente a seguridad.

Independientemente de los plazos marcados en cada apartado del presente pliego, como cláusula más restrictiva será, que el adjudicatario garantizará por encima de todo, que el HGUGM, pueda cumplir los plazos establecidos en la normativa vigente y en la que se pudiera desarrollar durante la duración del contrato.



### **3.1 Cumplimiento del RGPD en materia de Sistemas de Información**

El adjudicatario realizará la creación y revisión de todos los nuevos documentos, políticas, protocolos, procesos y procedimientos existentes en el HGUGM sobre el nuevo RGPD en materia de Sistemas de Información.

Se tomará especial atención a acciones de proactividad como recoge el nuevo RGPD, que se deben realizar para cumplimiento normativo para todas las nuevas aplicaciones que vayan incluyéndose en el Hospital, y para las que, habiéndose instalado previamente, no dispongan de toda la documentación pertinente.

El plazo para toda la generación de documentación y entregables, es de 30 días naturales desde la entrega de cada documento, política, protocolo, proceso o procedimiento, a excepción de los casos particulares de los Documentos de Registro de Actividad de Tratamiento y el Análisis de Riesgos y la evaluación del impacto que se ceñirán a los tiempos establecidos en sus apartados correspondientes.

### **3.2 Realización de Análisis de aplicaciones para elaboración de Documentos de Registro de Actividades de Tratamientos.**

Se realizará un análisis pormenorizado de todas las aplicaciones en funcionamiento en el Hospital y sus parámetros, particularidades, características técnicas y funcionales y análisis de riesgos con la finalidad de obtener los Documentos de Registro de Actividades de Tratamientos.

Se estiman 10 aplicaciones en total entre sanitarias, de gestión y control que actualmente no disponen de la documentación necesaria. Se deben analizar tanto parámetros técnicos, como de gestión de usuarios, como todo lo relacionado para el cumplimiento de Registro de Actividades de Tratamientos de la RGPD.

El plazo para toda la generación de documentación y entregables de este análisis, es de 30 días naturales desde la firma del contrato.

Además, el adjudicatario, diseñará y pondrá en marcha los procesos y procedimientos necesarios para mantener actualizados los documentos, basados en las particularidades e idiosincrasia del HGUGM. El plazo de entrega de la documentación de estos procesos y procedimientos es de 10 días naturales tras la obtención de los Documentos de Registro de Actividades de Tratamientos.

Toda acción o necesidad de documentación, de tramitación, de entrega, actualización relativa a los Registros de Actividades de Tratamientos, incluyendo la inclusión de nuevas aplicaciones durante la duración del contrato, quedará cubierta por el adjudicatario mediante el presente pliego, contando con 7 días laborables para la entrega tras su notificación por parte del HGUGM.



### **3.3 Realización de análisis de riesgos y evaluación de impacto**

El adjudicatario será el encargado de la realización de toda la documentación de análisis de riesgos y evaluación de impacto relativa al HGUGM y la incluirá en las herramientas que decida en cada momento el HGUGM sobre aplicaciones que se incorporen nuevas durante la duración del contrato, el adjudicatario tendrá 30 días naturales.

### **3.4 Realización de tareas de documentación del comité de seguridad, Normativa de Seguridad, Diagnóstico de Seguridad y Auditoría del CPD y Procedimientos e Instrucciones Técnicas.**

Realización de las tareas relativas a la constitución, modificación y mejoras de la Normativa de Seguridad, Diagnóstico de Seguridad y Auditoría del CPD, los Procedimientos e Instrucciones Técnicas y todo aquello que se considere necesario de manera adicional por parte del HGUGM. Además de la preparación de la documentación para el comité de seguridad. Se mantendrá adaptada toda esta documentación al RGPD.

Colaboración y participación activa con los proyectos de seguridad de la información que se generen desde el ámbito corporativo del SERMAS.

El plazo para la modificación de la documentación y entregables de este apartado, es de 90 días naturales desde la firma del contrato.

El plazo para toda la generación de documentación y entregables de nuevas necesidades en este apartado, es de 14 días naturales desde la solicitud.

El plazo para la entrega de toda la documentación y entregables generados de necesidades para el Comité de Seguridad, será 96 horas antes de la fecha del siguiente Comité.

### **3.5 Respuesta al ejercicio de los derechos incluidos en el RGPD**

El adjudicatario realizará la respuesta al ejercicio de los derechos Supresión, Oposición, Portabilidad, Limitación, Acceso y Rectificación incluidas en el nuevo RGPD, incluyéndolas, tramitándolas y resolviéndolas, en las herramientas que determine en cada momento el HGUGM en tiempo y forma, y de manera correcta.

Con el fin de poder realizar la revisión pertinente por parte del personal del HGUGM, el adjudicatario se compromete a realizar de manera correcta la respuesta o acciones necesarias en 7 días naturales tras la recepción del documento y la entregará a quien designe el HGUGM.

### **3.6 Gestionar y resolver todas incidencias de seguridad**





En el HGUGM se reciben incidencias de seguridad desde varios servicios, ubicaciones y aplicaciones de manera simultánea.

Es tarea del adjudicatario, asesorar, gestionar y resolver todas las incidencias de seguridad en tiempo y forma, acorde con las necesidades del HGUGM.

Algunas de las aplicaciones sobre las que se reciben incidencias de seguridad son Service Desk, CISEM...etc.

Además, las incidencias e incidentes de seguridad más comunes a resolver son las que proceden de atención al paciente,

Se estima un total de 50 incidencias de seguridad anuales, principalmente CISEM. Es importante recalcar que estas incidencias tienen una componente técnica y funcional significativa.

Con el fin de poder realizar la revisión pertinente por parte del personal del HGUGM, el adjudicatario se compromete a realizar de manera correcta la respuesta o acciones necesarias en 7 días naturales tras la recepción del documento y la entregará a quien designe el HGUGM.

### **3.7 Relación con la OSSI en materia de seguridad**

El adjudicatario será el encargado de asesorar y en los casos que designe el HGUGM relacionarse con la OSSI (Oficina de Seguridad de Sistemas de Información) de la Dirección General de Sistemas de Información del Servicio Madrileño de Salud en materia de seguridad, contestando a los requerimientos, peticiones y necesidades de manera correcta y verificada por el HGUGM en tiempo y forma.

Los plazos serán los designados por la propia OSSI, siendo corroborados por el HGUGM en cada momento.

### **3.8 Realización de auditorías anuales para cumplimiento normativa**

Realización de auditorías anuales en el HGUGM en base a la normativa y legislación vigente tanto del ENS como del RGPD. Revisión de la adaptación de protocolos internos a normativa vigente y exposición de puntos de mejora sobre la auditoría realizada.

El plazo para toda la generación de documentación y entregables de este análisis, es de 60 días naturales desde la petición por parte del HGUGM.



## 4. EQUIPO DE TRABAJO Y HORARIO DE SERVICIO

El presente pliego se expone como un servicio, que se prestará en horario de 8.00 a 18.00 y, para ello, el adjudicatario presentará el equipo de trabajo que cumpla al menos con los siguientes puntos:

- Cada una de la persona o personas que trabajen prestando el servicio cumplirán al menos con 1 Titulación y 2 Certificaciones y 1 curso de formación de las que se exponen a continuación:
  - Titulaciones:
    - Titulado Superior o Grado en Informática o Telecomunicaciones.
    - Titulado Superior o Grado en Derecho.
  - Certificaciones:
    - Auditor ISO 27001
    - CISA (Certified Information Systems Auditor)
    - CISM (Certified Information Security Management)
    - CISSP (Certified Security Systems Security Professional)
    - Delegado de Protección de Datos según RGPD
  - Formación:
    - Curso de formación de al menos 100 horas en Delegado de Protección de Datos
    - Curso de formación de al menos 40 horas en ENS
    - Curso de Formación de al menos 40 horas en RGPD
    - Experto Universitario en Inglés Jurídico

No serán valorados los cursos de formación expedidos por el licitador sobre los empleados que presenta al concurso, incluso aunque el certificado esté expedido por una empresa del grupo.

- El equipo de trabajo debe cumplir con la totalidad de requisitos sobre las Titulaciones, certificaciones y cursos de formación que se muestran en este apartado, presentando al menos 2 perfiles; uno de ellos de carácter tecnológico (Titulación Superior o Grado en Informática o Telecomunicaciones) y otro de ellos de carácter jurídico (Titulación Superior o Grado en Derecho).
- Habrá un responsable del servicio por parte del adjudicatario, que cumplirá con los requisitos expuestos en el punto inicial del presente apartado, en cuanto a titulación, certificaciones y formación, y que tendrá una disponibilidad vía telefónica, videoconferencia y correo electrónico de 8.00 a 18.00 de lunes a viernes.



- Al menos la persona del equipo de trabajo de perfil jurídico, acudirá al Hospital al menos 2 días a la semana en horario de 8.00 a 15.00 durante la duración del contrato, con el fin de recoger y resolver dudas sobre los entregables, sobre las solicitudes realizadas y aclarar posibles problemas in situ. Además, participará en las reuniones que el responsable designado por el HGUGM requiera. Este mínimo de 2 días serán los lunes y los jueves, no obstante, si el Hospital requiriera una semana cambiarlo de manera unilateral lo podrá hacer avisando 5 días laborables antes por escrito al responsable del servicio designado por el adjudicatario.
- El resto del servicio se prestará desde las dependencias del adjudicatario, facilitando al Hospital las vías de comunicación de al menos, un teléfono de contacto y correo electrónico adicionales a los del responsable de servicio, donde se harán llegar todas las peticiones e incidencias electrónicas. Adicionalmente, desde el Hospital, se dará acceso a las aplicaciones de gestión de incidencias con la finalidad de que estas sean resueltas desde las propias aplicaciones.
- No se permitirá el cambio del perfil que asista al Hospital, si no es por declaración jurada de la empresa, de que el profesional que presta el servicio cause baja de la misma. El Hospital, se reserva el derecho de solicitar el cambio de cualquiera de los recursos ante cualquier queja recibida por los usuarios incluyendo los del equipo de trabajo de la SSI, y el adjudicatario lo ejecutará como máximo en 10 días laborables tras la petición del Hospital, teniendo que sustituir dicho recurso sin que ello sea un problema para el cumplimiento de los acuerdos de nivel de servicio. El recurso que se incorpore, deberá cumplir con lo expuesto en los requerimientos del equipo de trabajo en cuanto a perfiles. Si durante la duración del expediente se requiriera el cambio de 2 perfiles de cualquier tipo, será motivo de rescisión de contrato.



## 5. COMITÉ DE SEGUIMIENTO

---

Los Comités de Seguimiento estarán formados por los responsables designados por el HGUGM y el responsable del Servicio de la empresa adjudicataria y su función principal será la de articularse como mecanismo para el seguimiento y control de las tareas de los servicios de peticiones e incidencias.

La periodicidad de las reuniones del Comité de Seguimiento será por defecto de una vez al mes, a petición del HGUGM. El responsable del HGUGM podrá modificar la periodicidad por defecto. Así mismo podrá convocarse de manera excepcional, a petición del responsable del HGUGM o el de la empresa adjudicataria.

Corresponderá al Comité de Seguimiento las siguientes funciones, sin perjuicio de otras que se les asigne durante la ejecución de la duración del expediente:

- Definición en detalle del alcance para los periodos contemplados, estableciendo los objetivos, cronograma de tareas y distribución de los recursos del servicio, orientados al cumplimiento de los entregables objeto del contrato.
- Seguimiento de la evolución del servicio y el grado de cumplimiento de los objetivos definidos para los diferentes periodos que se vayan estableciendo en comités anteriores.
- Aprobar cualquier documentación a presentar. En especial todas aquellas que describan de manera objetiva y formal la situación del servicio.
- Seguimiento del cumplimiento de los acuerdos de nivel de servicio (ANS)

De estas reuniones del Comité, el responsable de Servicio de la empresa adjudicataria levantará acta, que será revisada y aprobada por los miembros del Comité, para dar constancia de la evolución de los distintos servicios, de los posibles problemas detectados, de los requerimientos aprobados, de la desviación de objetivos, etc.



## 6. PENALIDADES

Las penalidades a aplicar sobre los acuerdos de nivel de servicio son los siguientes:

	DESCRIPCIÓN	CUMPLIMIENTO	PENALIDAD
1	Cada hora de incumplimiento de estancia in situ	Estancia in situ de 2 días a la semana según descripción de pliego de 8.00 a 15.00	0,05% cada hora de incumplimiento, sobre el importe total del contrato adjudicado
2	Cada día de incumplimiento de estancia in situ	Estancia in situ de 2 días a la semana según descripción de pliego de 8.00 a 15.00	0,5% cada día de incumplimiento, sobre el importe total del contrato adjudicado
3	Cada día de incumplimiento sobre la creación de cualquiera de documentos, políticas, protocolos, procesos y procedimientos para cumplimiento del RGPD	30 días naturales tras entrega de cada documento, política, protocolo, proceso o procedimiento	0,2% cada día de incumplimiento, sobre el importe total del contrato adjudicado
4	Incumplimiento en realización de Documentos de Registros de Actividades de Tratamiento de RGPD	30 días naturales tras la firma del contrato	0,2% cada día de incumplimiento, sobre el importe total del contrato adjudicado
5	Incumplimiento década día en el diseño y puesto en marcha de los procesos y procedimientos necesarios para mantener actualizados los Documentos de Registros de Actividades de Tratamiento de RGPD, basados en las particularidades e idiosincrasia del HGUGM	10 días naturales para diseñar y poner en marcha los procesos y procedimientos necesarios para mantener actualizados los documentos, basados en las particularidades e idiosincrasia del HGUGM	0,2% cada día de incumplimiento, sobre el importe total del contrato adjudicado
6	Incumplimiento en actualización de Documentos de Registros de Actividades de Tratamiento de RGPD	7 días naturales tras la notificación por parte del HGUGM	0,2% cada día de incumplimiento, sobre el importe total del contrato adjudicado
7	Incumplimiento en días como encargado de la realización de toda la documentación nueva de análisis de riesgos y evaluación de impacto relativa al HGUGM y la incluirá en las herramientas que decida en cada momento el HGUGM para cada nueva aplicación y/o Sistema de Información	30 días naturales desde el envío de la información que determine el HGUGM	0,2% cada día de incumplimiento, sobre el importe total del contrato adjudicado
8	Incumplimiento en días para la realización de las tareas relativas a la modificación y mejoras de la Normativa de Seguridad, Diagnóstico de Seguridad y Auditoría del CPD, los Procedimientos e Instrucciones Técnicas y todo aquello que se considere	90 días naturales desde el envío de la información que determine el HGUGM	0,5% cada día de incumplimiento, sobre el importe total del contrato adjudicado

La autenticidad de este documento se puede comprobar en [www.madrid.es/consumo](http://www.madrid.es/consumo) mediante el siguiente código seguro de verificación: 12953991340838368439

	necesario de manera adicional por parte del HGUGM.		
9	Incumplimiento en días para la realización de las tareas relativas a la constitución de nuevas necesidades que se consideren necesarias de manera adicional por parte del HGUGM.	14 días naturales desde el envío de la información que determine el HGUGM	0,2% cada día de incumplimiento, sobre el importe total del contrato adjudicado
10	Incumplimiento en horas para la realización de las tareas relativas al Comité de Seguridad	El plazo para la entrega de toda la documentación y entregables generados de necesidades para el Comité de Seguridad, será 96 horas antes de la fecha del siguiente Comité	0,1% cada hora de incumplimiento, sobre el importe total del contrato adjudicado
11	Incumplimiento en realización, tramitación y resolución de la respuesta al ejercicio de los derechos Supresión, Oposición, Portabilidad, Limitación, Acceso y Rectificación incluidas en el nuevo RGPD, en las herramientas que determine en cada momento el HGUGM	7 días naturales desde el envío de la información que determine el HGUGM	0,2% cada día de incumplimiento, sobre el importe total del contrato adjudicado
12	Incumplimiento en asesorar, gestionar y resolver todas las incidencias de seguridad en tiempo y forma, acorde con las necesidades del HGUGM	7 días naturales desde el envío de la información que determine el HGUGM	0,2% cada día de incumplimiento, sobre el importe total del contrato adjudicado
13	Incumplimiento en la realización de auditorías en base a la normativa y legislación vigente tanto del ENS y del RGPD	60 días naturales tras la petición del HGUGM	0,2% cada día de incumplimiento, sobre el importe total del contrato adjudicado
14	Incumplimiento sobre plazos de entrega de normativa vigente	El adjudicatario garantizará por encima de todo, que el HGUGM, pueda cumplir los plazos establecidos en la normativa vigente	5% sobre el importe total del contrato adjudicado
15	Incumplimiento de cada día en la subsanación de tarea o documento, política, proceso, protocolo o entregable no correcto a criterio del HGUGM	El adjudicatario tendrá 3 días naturales para subsanar	0,2% cada día de incumplimiento, sobre el importe total del contrato adjudicado
16	No uso de herramientas indicadas por el HGUGM	Uso de herramientas indicadas por HGUGM	2% sobre total del importe del contrato adjudicado
17	No gestión de herramientas indicadas por el HGUGM	Gestión de herramientas indicadas por HGUGM	2% sobre total del importe del contrato adjudicado

## 7. CERTIFICACIONES DE EMPRESA

### Certificaciones del adjudicatario

Las empresas licitadoras deberán estar en posesión y adjuntar las siguientes certificaciones o equivalentes vigentes:

- UNE EN ISO 9001:2015: Sistema de gestión de calidad
- UNE EN ISO 14001:2015: Sistemas de gestión medioambiental
- UNE EN ISO/IEC 27001:2013: Tecnología de la Información- Sistemas de gestión de la seguridad de la información.
- UNE EN ISO 20000:2011: Tecnología de la información- Gestión del servicio.
- ISO22301: Continuidad de negocio
- Acreditación de un centro de operaciones SOC 24x7
- Pertenencia a la organización FIRST (Forum of Incident Response and Security Teams)
- Estar acreditado o en trámite de acreditarse como Equipo de Respuesta ante Emergencias Informáticas (CERT, del inglés Computer Emergency Response Team) autorizado por la UCM – Universidad Carnegie Mellon
- Certificado ENS al menos nivel medio.

Toda esta documentación deberá incluirse con la documentación administrativa, la no inclusión podrá ser motivo de exclusión del procedimiento de licitación.





## 8. CONTENIDOS DE LAS PROPUESTAS TÉCNICAS

Las proposiciones deben responder al siguiente índice y contenido que se muestra a continuación en no más de 30 páginas con Fuente Arial y Tamaño de Fuente 12:

### 1. - Resumen ejecutivo

En la relación con los servicios ofertados para el cumplimiento del objeto del contrato, se definirán brevemente los objetivos y alcance, planteamiento general, organización y composición del equipo de trabajo, con horas estimadas por perfiles ofertados, compromisos asumidos, valores diferenciales y otros aspectos relevantes de la oferta.

### 2.- Acatamiento expreso

Acatamiento expreso a todas y cada una de las condiciones que se incluyan en los pliegos de prescripciones técnicas y de cláusulas administrativas.

### 3.- Descripción de la solución propuesta

Detalle exhaustivo de la propuesta de servicio. Se describirán el planteamiento para cada uno de los servicios contemplados en el contrato. Vías de comunicación, circuitos de trabajo para cada especificación técnica del servicio, metodología de trabajo aplicada al servicio.

### 4. Equipo de Trabajo

Descripción de la cualificación y experiencia del equipo de trabajo.

### 5. Otros Datos Técnicos

Cualquier otra información de interés para describir la solución y servicios ofertados.





## **9. SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN**

### **9.1 Normativa de seguridad y protección de datos**

En el caso de que el Adjudicatario, durante el ejercicio de la prestación del servicio, tuviera que tratar con datos de carácter personal del HGUGM por razón de la prestación del servicio, cumplirá con la legislación vigente en materia de protección de datos de carácter personal que resulte de aplicación, concreto 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); la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal; el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal; así como las disposiciones de desarrollo de las normas anteriores 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, el HGUGM 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 en el RGPD.

### **9.2 Encargado del Tratamiento.**

El Encargado del Tratamiento se compromete a cumplir las medidas y requisitos de seguridad exigidos por el HGUGM. El coste de las actuaciones de cualquier tipo, derivadas del cumplimiento de RGPD y normativa relacionada, serán por cuenta del Encargado del Tratamiento.

El tratamiento de datos de carácter personal por el Encargado del Tratamiento, se regirá por un contrato 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 ésta responsabilidad asumida por el Encargado del Tratamiento, serán recogidas en un documento específico que será firmado por el HGUGM y el Encargado del Tratamiento de forma previa al inicio de los trabajos.

### **9.3 Limitación del acceso o tratamiento.**

El Encargado del Tratamiento limitará el acceso o tratamiento de datos de carácter personal pertenecientes a los ficheros bajo titularidad del HGUGM, 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.



## 9.4 Medidas de Seguridad.

A los efectos de la prestación del servicio por parte del Encargado del Tratamiento, quedará obligado, con carácter general, por el deber de confidencialidad y seguridad de los datos de carácter personal (y de otros datos de carácter confidencial del HGUGM que puedan tratarse). Y con carácter específico, en todas aquellas previsiones que estén contempladas en las actividades que formen parte del servicio adjudicado, en especial:

- El Encargado del Tratamiento 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 prestación del servicio sanitario, sin límite temporal alguno.
- El Encargado del Tratamiento, 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.
- El Encargado del Tratamiento utilizará los datos de carácter personal única y exclusivamente, en el marco y para las finalidades determinadas en el objeto del servicio adjudicado y del presente documento, y bajo las instrucciones del Responsable del Tratamiento, para aquellos aspectos relacionados con sus competencias.
- Accederá a los datos de carácter personal responsabilidad del Responsable del Tratamiento únicamente cuando sea imprescindible para el buen desarrollo de los servicios para los que ha sido contratado.
- En caso de que el tratamiento incluya la recogida de datos personales en nombre y por cuenta del Responsable del Tratamiento, el Encargado del Tratamiento 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 Encargado del Tratamiento considera que alguna de las instrucciones del Responsable del Tratamiento infringe el RGPD 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, el Encargado del Tratamiento 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.
- Garantizará la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- 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, 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.
- En caso de que el Encargado del Tratamiento 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 de carácter personal 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.
- El Encargado del Tratamiento comunicará y hará cumplir a sus empleados, y a cualquier persona con acceso a los datos de carácter personal, las obligaciones establecidas en los apartados anteriores, especialmente las relativas al deber de secreto y medidas de seguridad.
- El Encargado del Tratamiento 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 de carácter personal a los que pueda tener acceso en su condición de Encargado del Tratamiento, salvo autorización expresa 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, que garanticen la seguridad de los datos de carácter personal 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 Encargado del Tratamiento 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. Así mismo, el del Encargado del Tratamiento tendrá acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- El Encargado del Tratamiento 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 de carácter personal, o la puesta en conocimiento por parte de terceros no autorizados de información confidencial obtenida durante la prestación del servicio.
- El Encargado del Tratamiento 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 a la HGUGM a los que pueda tener acceso en el transcurso de la prestación del servicio.



- Los diseños y desarrollos de software deberán, observar con carácter general, la normativa de seguridad de la información y de protección de datos de la Comunidad de Madrid y:
- En todo caso observarán los requerimientos relativos a la identificación y autenticación de usuarios, estableciendo un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado, limitando la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.
- En ningún caso el equipo prestador del servicio objeto del contrato tendrá acceso ni realizará tratamiento de datos de carácter personal contenidos o soportados en los equipos o recursos mantenidos.

### **9.5 Destino de los datos al finalizar la prestación del servicio.**

Una vez cumplida o resuelta la relación contractual acordada entre el Responsable del Tratamiento y el Encargado del Tratamiento, el Encargado del Tratamiento deberá solicitar al Responsable del Tratamiento instrucciones precisas sobre el destino de los datos de carácter personal de su responsabilidad, pudiendo elegir éste último entre su devolución, remisión a otro prestador de servicios 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.

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

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

En caso de que el Encargado del Tratamiento necesitara subcontratar todo o parte de los servicios 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 Encargado del Tratamiento y las instrucciones que dicte el Responsable del Tratamiento.

Corresponde al Encargado del Tratamiento exigir por contrato al subencargado el cumplimiento de las mismas obligaciones asumidas por él a través del presente documento.

El Encargado del Tratamiento seguirá siendo plenamente responsable ante el Responsable del Tratamiento en lo referente al cumplimiento de las obligaciones.



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

El Encargado del Tratamiento será considerado responsable del tratamiento en el caso de que destine los datos a otras finalidades, los comunique o los utilice incumpliendo las estipulaciones del encargo, respondiendo de las infracciones en que hubiera incurrido personalmente.

## **9.8 Cesión del contrato.**

El Encargado del Tratamiento no podrá ceder total o parcialmente, los derechos y obligaciones que se deriven del contrato sin autorización expresa escrita del Responsable del Tratamiento, que fijará las condiciones de la misma, no autorizándose la cesión de los contratos a favor de empresas incursas en causa de inhabilitación para contratar.



## 10. COMPROMISO MEDIOAMBIENTAL

El contratista adoptará las medidas oportunas para el cumplimiento de la legislación ambiental en vigor en relación al trabajo realizado. Además, se asegurará que su personal está debidamente formado y es competente en materia de buenas prácticas ambientales. El HGUGM se reserva el derecho a solicitar al contratista evidencia sobre el cumplimiento de los requisitos legales ambientales que sean de aplicación o de la adecuada formación del personal.

El contratista deberá adoptar las medidas preventivas que estén a su alcance con el fin de evitar cualquier incidente que pueda derivar en una contaminación del medio ambiente, como puedan ser los vertidos líquidos indeseados, abandono de residuos o su incorrecta gestión, en especial, de aquellos considerados como peligrosos. El Hospital se reserva el derecho de repercutir al contratista el coste de reparación del daño ambiental derivado de un incidente ambiental causado por ellos”.

Compromisos ambientales:

- Desarrollar su actividad con una actitud responsable frente al Medio Ambiente.
- Cumplir con la normativa ambiental en vigor y con los requisitos legales aplicables a su actividad.
- Informar de todos los incidentes con repercusión ambiental que tengan lugar en el desarrollo de su actividad en las instalaciones del HGUGM.
- Segregar los residuos en origen y gestionarlos conforme a la normativa en vigor priorizando el reciclado frente a la eliminación.
- Retirar los residuos generados y en caso de depositarlos en los contenedores del Hospital, se realizará bajo el consentimiento del personal del Hospital responsable de la contratación.
- Emplear equipos con marcado CE y realizarles un mantenimiento preventivo con el fin de que las emisiones y ruidos se mantengan dentro de los límites especificados en las características técnicas.
- Establecer todas las medidas al alcance para evitar vertidos y derrames.
- No verter productos químicos a la red de saneamiento y a cumplir en todo caso las especificaciones del fabricante en relación a la dosificación y empleo de los productos.
- Consumir agua, energía y demás recursos que necesite para el desarrollo de los trabajos de una forma responsable.
- Reutilizar todos los materiales que sea posible.
- Apagar los equipos siempre que su funcionamiento no sea necesario.
- Colaborar con el personal del Hospital.
- Etiquetar correctamente todos los productos químicos que maneje. Realizar todos los trasvases en lugares protegidos y en caso de derrame, recogerlo con absorbentes y depositarlos en el contenedor correspondiente.





## 11. CONSIDERACIONES SOCIALES

La empresa adjudicataria no debe practicar o apoyar la discriminación en la contratación, remuneración, acceso a la capacitación, promoción, despido o jubilación basada en la raza, origen social o nacional, casta, nacimiento, religión, discapacidad, género, orientación sexual, responsabilidad familiar, estado civil, afiliación a sindicatos, opiniones políticas, edad o cualquier otra condición que pueda dar origen a la discriminación.

La empresa adjudicataria no debe interferir en el ejercicio de los derechos de su personal para observar sus creencias o prácticas o para satisfacer sus necesidades relacionadas con la raza, origen social o nacional, religión, discapacidad, género, orientación sexual, responsabilidad familiar, afiliación a sindicatos, opiniones políticas, o cualquier otra condición que pueda dar origen a la discriminación.

La empresa adjudicataria no debe permitir ningún comportamiento que sea amenazador, abusivo, explotador o sexualmente coercitivo, incluyendo gestos, lenguaje, y contacto físico en el lugar de trabajo.



## 12. CLÁUSULAS ADICIONALES

---

El presente pliego junto, junto al de Cláusulas Administrativas Particulares, será incorporado como parte del contrato que se suscriba con el adjudicatario.

**Madrid, 22 de agosto de 2023.**

**El Subdirector de Sistemas de Información**

**Manuel Pérez Vallina**



La autenticidad de este documento se puede comprobar en [www.madrid.org/csv](http://www.madrid.org/csv)  
mediante el siguiente código seguro de verificación: **129539913408368439**