

PLIEGO DE PRESCRIPCIONES TÉCNICAS

**MANTENIMIENTO Y SOPORTE DE LA PLATAFORMA DE FIRMA CENTRALIZADA,
AUTENTIFICACIÓN Y CUSTODIA DE DOCUMENTOS ELECTRONICOS Y DE
CERTIFICADOS DIGITALES DEL SERVICIO MADRILEÑO DE SALUD Y
SUMINISTRO DE LICENCIAS DE AMPLIACIÓN FUNCIONALIDAD PARA EL
SELLADO DE DOCUMENTOS**



La autenticidad de este documento se puede comprobar en www.madrid.org/csv
mediante el siguiente código seguro de verificación: **1221389787059159060006**

CONTENIDO

1. INTRODUCCIÓN	3
2. OBJETO DEL CONTRATO	4
3. ESPECIFICACIONES DE LOS PRODUCTOS INCLUIDOS EN LA RENOVACION DE MANTENIMIENTO Y SUMINISTRO DE NUEVAS LICENCIAS SELLADO ELECTRONICO.....	4
3.1 Descripción de los productos incluidos en la renovación de soporte y mantenimiento	4
3.2 Descripción del suministro: Licencias Siaval Crypto para nueva funcionalidad de sellado de tiempo 6	6
4. SERVICIOS DE SOPORTE, MANTENIMIENTO Y DE RESOLUCIÓN DE ANOMALÍAS DE FUNCIONAMIENTO.....	7
4.1 Condiciones de los servicios de mantenimiento, soporte y actualización	8
4.2 Acuerdo de nivel de servicio.....	10
4.3 Prestaciones Opcionales. Posible sustitución de elementos en fin de soporte o evolución en su forma de instalación o licenciamiento.	11
5. SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN.....	12
5.1. Normativa de seguridad y protección de datos	13
5.2. Encargado del Tratamiento	14
5.3. Limitación del acceso o tratamiento	14
5.4. Medidas de Seguridad.....	14
5.5. Destino de los datos al finalizar la prestación del servicio.....	18
5.6. Cesión o comunicación de datos a terceros.....	18
5.7. Responsabilidad en caso de incumplimiento	19
5.8. Cesión del contrato	20
6. CONTENIDO DEL PROGRAMA DE TRABAJO.....	21



1. INTRODUCCIÓN

De conformidad con lo que establece el artículo 28 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público y el artículo 73 del Reglamento General de la Ley de Contratos de las Administraciones Públicas, aprobado por Real Decreto 1098/2001, de 12 de octubre, se exponen a continuación los fines institucionales del organismo proponente cuyo cumplimiento requiere la realización de esta contratación. Igualmente, y a tal efecto, como parte de la documentación preparatoria, se determinan con precisión la naturaleza y extensión de las necesidades que pretenden cubrirse mediante el contrato proyectado, así como la idoneidad de su objeto y contenido para satisfacerlas.

Según se dispone en el Decreto 24/2008, de 3 de abril, del Consejo de Gobierno, por el que se establece el régimen jurídico y de funcionamiento del Servicio Madrileño de Salud, en el Decreto 73/2019, de 27 de agosto, del Consejo de Gobierno, por el que se modifica la estructura orgánica básica de las Consejerías de la Comunidad de Madrid (modificado por el Decreto 35/2020, de 13 de mayo, del Consejo de Gobierno) y en el Decreto 308/2019, de 26 de noviembre, del Consejo de Gobierno, por el que se establece la estructura directiva del Servicio Madrileño de Salud (SERMAS), corresponde a la Dirección General de Sistemas de Información y Equipamientos Sanitarios (DGSIES) “La planificación, diseño, implantación y mantenimiento de los sistemas y tecnologías de la información para la organización y funcionamiento del Servicio Madrileño de Salud, de acuerdo con las necesidades explicitadas por las unidades directivas”, y “La provisión y gestión de los servicios y equipamientos informáticos sanitarios del Servicio Madrileño de Salud”, todo ello sin perjuicio de las que correspondan a la Agencia para la Administración Digital de la Comunidad de Madrid, así como de las atribuidas a la Dirección General de Transparencia, Gobierno Abierto y Atención al Ciudadano.

Dentro de las competencias asignadas también está “La implantación, de acuerdo con las necesidades detectadas por la Dirección General del Proceso Integrado de Salud, de nuevas Tecnologías de la información y la comunicación (TIC) y de tramitación electrónica en el Servicio Madrileño de Salud, que estén en relación con los ciudadanos, los profesionales y la atención sanitaria.”



De acuerdo con estas competencias, el SERMAS dispone de una plataforma implantada en sus centros de proceso de datos centrales principales del SERMAS, CPD Aduana y CPD ATHENE@ en Hospital Universitario 12 de octubre, que ofrece los servicios de firma centralizada, autenticación y custodia de documentos electrónicos y de certificados digitales para los profesionales del servicio madrileño de salud y los sistemas de información sanitaria.

Es necesario renovar los servicios de soporte y mantenimiento asociados a esta infraestructura e incluir nuevas funcionalidades para el sellado de documentos. Esta plataforma se basa en la familia de productos de firma centralizada SIAVAL, del fabricante SIA.

En base a la necesidad, se promueve el presente contrato.

2. OBJETO DEL CONTRATO

El objeto de esta contratación lo constituye la renovación del mantenimiento y soporte de los módulos de autenticación y firma electrónica en el uso de sistemas de información sanitaria y el de custodia de documentos electrónicos.

Se incluye además el suministro de licencias del módulo SIAVAL Crypto para incorporar los servicios de seguridad que permite implementar el Sello Electrónico en la Historia Clínica Electrónica o en cualquier aplicación que el SERMAS requiera, para ofrecer las mismas funcionalidades de firma electrónica y custodia segura de documentos.

3. ESPECIFICACIONES DE LOS PRODUCTOS INCLUIDOS EN LA RENOVACION DE MANTENIMIENTO Y SUMINISTRO DE NUEVAS LICENCIAS SELLADO ELECTRONICO

3.1 Descripción de los productos incluidos en la renovación de soporte y mantenimiento

En la actualidad el SERMAS dispone de los siguientes productos instalados de la familia SIAVAL SafeCert y de los servicios de confianza SIACERT Trusted Services.



- SIAVAL SafeCert es la plataforma de autenticación y firma centralizada, que permite la gestión del ciclo de vida completo de las claves y certificados, garantizando el control exclusivo por parte de los usuarios. La solución permite proteger las claves y certificados de los usuarios con mecanismos de seguridad robustos basados en la tecnología HSM.
- SIAVAL SafeCert Runtime y API SIAVAL Standalone: elementos de integración de SIAVAL Safecert que proporciona los servicios necesarios para hacer uso de la firma electrónica en los procesos de negocio.
- SIAVAL SafeCert Secure Appliance. Gestiona los servicios relacionados con la custodia y uso de los datos de creación de firmas, garantizando el almacenamiento seguro de las claves y que estas son usadas solamente por sus legítimos propietarios.
- SIAVAL.PDM.Custodia. Licencias de software del módulo de custodia de documentos firmados electrónicamente. Este sistema de Custodia de documentos tiene como funciones principales: permitir el movimiento, almacenado seguro y la conservación a lo largo del tiempo de documentos auditables, así como, establecer los procesos de firma y sellado según los estándares de archivado a largo plazo.
- SIACERT Trusted Services es la plataforma de Prestación de Servicios de Confianza, en conformidad a la actual Ley de Firma Electrónica como al nuevo Reglamento de Identificación y Confianza Europeo, que ofrece todas las garantías de seguridad no solo para la emisión de certificados cualificados sino para el resto de los servicios de confianza recogidos en el marco legal actual.
- SIACERT RA OnPremise. Proporciona los servicios de Autoridad de Registro para la gestión del ciclo de vida de los certificados, siendo posible el registro de los usuarios que tengan certificado reconocido emitido por la AC del Prestador de Servicios de Certificación del SERMAS.



El detalle de los productos instalados en el SERMAS adquiridos en una compra inicial y en una ampliación posterior y sobre los que se requiere la contratación de los servicios de soporte y mantenimiento son los siguientes:

MANTENIMIENTO COMPRA INICIAL				
Entorno	Producto	P/N	Cantidad	Descripción
Producción	SIAVAL SafeCert Secure Appliance	SIA-SIAVAL-SFCRT-APP	2	Activo/Activo
	SIAVAL SafeCert Runtime	SIA-SIAVAL-RUNTIME	2	Activo/Activo
	API SIAVAL Standalone	SIA-SIAVAL-STNDLONE	2	Activo/Activo
	SIAVAL SafeCert End user Licence	SIA-SIAVAL-USR	18000	Usuarios
	SIACert RA OnPremise	SIA-SIAVAL-WF	2	Activo/Pasivo
Preproducción	SIAVAL SafeCert Secure Appliance	SIA-SIAVAL-SFCRT-APP	1	Activo
	SIAVAL SafeCert Runtime	SIA-SIAVAL-RUNTIME	1	Activo
	API SIAVAL Standalone	SIA-SIAVAL-STNDLONE	1	Activo
	SIACert RA OnPremise	SIA-SIAVAL-WF	1	Activo

MANTENIMIENTO AMPLIACIÓN				
Entorno	Producto	P/N	Cantidad	Descripción
Producción	SIAVAL SafeCert End user Licence	SIA-SIAVAL-USR	18000	Usuarios
	SIAVAL SafeCert End user Licence	SIA-SIAVAL-USR	4700	Usuarios
	SIAVAL Custodia	SIA-SIAVAL-PDM-CUSTODY	2	Activo/Pasivo
Preproducción	SIAVAL Custodia	SIA-SIAVAL-PDM-CUSTODY	1	Activo

3.2 Descripción del suministro: Licencias Siaval Crypto para nueva funcionalidad de sellado de tiempo

Se requiere el suministro de 2 licencias del módulo SIAVAL Crypto que permita implementar el Sello de Tiempo en los procesos que se requiera, entre otros destaca la Historia Clínica Electrónica.

Las funcionalidades que serán cubiertas con el suministro de nuevas licencias son las siguientes:



- Soporte para múltiples formatos de firma: XMLDSig, XAdES, PKCS#7, CAdES, S/MIME y PDF.
- Soporte para cifrado y descifrado de datos: XML Encryption y PKCS#7.
- Validación del estado de revocación de los certificados basado en CRL (vía LDAP, HTTP, file, etc) y en OCSP. Extracción de información y validación de certificados.
- Verificación de firmas en cualquiera de los formatos que genera el producto.
- Generación de sellados de tiempo internos (fechados) o utilizando servicios externos ofrecidos por TSA (TimeStamp Authority) a través de TSP (TimeStamp Protocol) para los estándares XAdES, CAdES, PKCS#7 y PDF.
- Soporte para múltiples autoridades de certificación. Diferentes niveles de validación en base a la política que se aplique a la hora de realizar la validación de un documento firmado. Los niveles posibles que se pueden establecer desde la administración son: o Solo integridad o Integridad y confianza o Integridad y caducidad
- Integridad y confianza o Integridad y caducidad o Integridad, caducidad y confianza o Validación completa
- Los servicios soportan, en base a la política de validación establecida en la administración, varios mecanismos de recuperación de la información de revocación de un certificado, de tal forma que pueden utilizar cualquiera de ellos (en un orden preestablecido) para recuperar los datos necesarios. Así, por ejemplo, si para un certificado están definidos la descarga de CRLs vía HTTP y vía LDAP y el primero de ellos no está disponible por cualquier causa, los servicios emplearán entonces el segundo para descargar toda la información.
- Soporte para múltiples algoritmos de firma y cifrado. o Capacidad de funcionamiento con caché de CRL y OCSP, diferenciada para certificados de usuario y de CAs, TSAs, etc para mejorar el rendimiento en la obtención de información de revocación de certificados. o Múltiples soportes para el almacenamiento de claves: HSM, PKCS#11 y PKCS#12.

4. SERVICIOS DE SOPORTE, MANTENIMIENTO Y DE RESOLUCIÓN DE ANOMALÍAS DE FUNCIONAMIENTO

El adjudicatario realizará los servicios de soporte y mantenimiento para todos los activos objeto del presente procedimiento de contratación, hardware y software, por un periodo



unificado común y Cotérmino con fecha de finalización el 30/11/2023 en modalidad 24x7, incluyendo el soporte y mantenimiento de las nuevas licencias solicitadas. El soporte y mantenimiento debe incluir la intervención correctiva necesaria para resolver todos los incidentes, tanto de hardware como de software y/o firmware de base, que pudieran causar una interrupción del servicio. Todo ello asegurando unos tiempos de respuesta adecuados. Estos servicios incluyen la prestación del servicio de emisión y renovación de certificados cualificados de firma para los actuales 40.700 usuarios.

4.1 Condiciones de los servicios de mantenimiento, soporte y actualización

Estos servicios tienen las condiciones siguientes:

- La actuación para las incidencias de la infraestructura hardware se llevará a cabo in situ, es decir, en el lugar en el que esté instalado el elemento.
- El adjudicatario será responsable de los elementos objeto de la garantía in situ, y en caso de que se produzca cualquier incidencia en relación con los mismos deberá articular los mecanismos que sean necesarios para su resolución.
- Dependiendo de la complejidad, se evaluará la viabilidad de solventarlo con la sustitución del elemento averiado por otro de iguales o superiores características, original del fabricante y compatible con la infraestructura instalada, hasta que se haya producido la reparación del elemento averiado. En este caso, el adjudicatario deberá asegurar que se presta el servicio con total normalidad tras la sustitución.
- El adjudicatario dispondrá de un stock mínimo de materiales/piezas/equipos que le permita garantizar el cumplimiento de los tiempos máximos de resolución de incidencias.
- Para los dispositivos appliance se deberá garantizar que para cualquier fallo de alguno de sus componentes físicos (fuente de alimentación, memoria, disco, interfaz de red, etc.) deberá resolverse en un plazo máximo de 24 horas dentro una prestación del servicio de 24x7, incluyendo el desplazamiento a las instalaciones del SERMAS.
- En cuanto al software, y siempre que se refiera a recursos dentro del ámbito del proyecto, el adjudicatario deberá proporcionar el derecho de actualización a nuevas



versiones del producto y la disponibilidad de parches y revisiones menores, siempre y cuando sea necesario, en cualquiera de las plataformas para las que esté disponible el producto, durante todo el plazo de la garantía, sin sobrecoste adicional.

Se incluye:

- Acceso a los recursos de auto-servicio de las bases de datos de incidencias del fabricante en la modalidad establecida.
 - Acceso al portal web de soporte del fabricante
 - Acceso a las nuevas versiones de cualquier componente de la solución cuando estén disponibles. El adjudicatario deberá efectuar la entrega de las nuevas versiones por los medios electrónicos adecuados. Previamente, el adjudicatario entregará una lista de las nuevas funcionalidades de la versión, que incluirán mejoras generales, nuevas funcionalidades y/o correcciones a bugs de la solución.
 - Soporte para la puesta en producción de las nuevas versiones y parches del software de cualquier componente de la solución propuesta. Comprende todos los procesos de parametrización, pruebas y validación de las nuevas funcionalidades, en los diferentes entornos afectados. Este soporte deberá llevarse a cabo en todas las instalaciones donde se encuentre implantada la solución objeto de este pliego. Los procesos de puesta en producción se deberán ajustar al procedimiento establecido por el SERMAS vigente en cada momento.
 - Se incluirán informes de valoración de niveles de revisión de firmware y de software anuales, a realizar en las fechas elegidas por SERMAS
- El adjudicatario estará en disposición de recibir comunicaciones de avería o incidencias con una disponibilidad de 24x7. Este procedimiento contemplará, al menos, la apertura de incidencias por vía telefónica, mail, página web o SMS.
 - En el caso de que se produzca una incidencia, el adjudicatario asignará un técnico especializado en las soluciones que llevará el caso hasta la completa resolución de la incidencia.



- El adjudicatario deberá proveer el servicio de garantía en castellano.
- El adjudicatario realizará informes preventivos sobre el estado de la configuración y los enviará periódicamente. Así mismo, tendrá disponible asesoramiento técnico especializado para revisar las conclusiones de cada informe preventivo y aportar directrices sobre cómo llevarlos a cabo.
- Para los productos software y hardware, el SERMAS podrá realizar un número ilimitado de accesos al servicio de apertura de incidencias

4.2 Acuerdo de nivel de servicio

Además de las condiciones indicadas previamente para el soporte del software, el adjudicatario deberá cumplir con el Acuerdo de Nivel de Servicio establecido en este apartado. Como tiempo máximo de resolución (T. máx.) se considera el periodo máximo que transcurre desde la comunicación de la incidencia hasta la resolución de la misma.

A efectos de los tiempos de respuesta a los incidentes, se tendrán en cuenta la siguiente clasificación por prioridades:

Nivel de gravedad	DESCRIPCIÓN DE LA SEVERIDAD DEL INCIDENTE	Respuesta inicial de Soporte 24x7
Nivel 1	Todas las funciones o una proporción sustancial de las funciones del software no están disponibles y no hay una solución provisional posible, o el sistema va tan lento que los tiempos de respuesta lo hacen inutilizable, y/ o hay un problema que ha causado o tiene el potencial de provocar un impacto crítico en el funcionamiento en los servicios de los sistemas de Información.	Dentro de 1 Hora
Nivel 2	Las funciones o una proporción sustancial de las funciones del software no están disponibles y hay una solución provisional posible, o el software ha disminuido su rendimiento de tal forma que los tiempos de respuesta hacen muy difícil su uso y/o hay un problema que causa o tiene potencial de provocar un impacto significativo en los servicios de los sistemas de Información	Dentro de 2 Horas



Nivel 3	Cualquier función del software que no está disponible o el software ha disminuido su rendimiento, o no funciona de la forma documentada, de tal forma que impacta en una reducción de eficiencia que tiene un impacto medio o bajo en los servicios de los sistemas de Información. Una solución provisional puede ser aceptable y se propone e implementa por la empresa adjudicataria.	Dentro de 4 Horas
Nivel 4	Cualquier petición de incremento de funcionalidades que tenga mínimo o ningún impacto en los servicios de los sistemas de Información y para las que no se requiere una solución inmediata. Solicitudes de información o consultas	Dentro de 1 Día Hábil

4.3 Prestaciones Opcionales. Posible sustitución de elementos en fin de soporte o evolución en su forma de instalación o licenciamiento.

Debido a la actualización tecnológica y mantenimiento realizados, así como al propio ciclo de vida de los productos, los elementos objeto de mantenimiento pueden ser susceptibles de sustitución o migración de los mismos, a nuevas versiones o productos actualizados que mejoren y/o amplíen las funcionalidades de la infraestructura y plataformas relacionadas.

El licitador podrá ofertar opcionalmente estas prestaciones, especificando expresamente en su propuesta los elementos afectados, la sustitución de elementos incluidos en mantenimiento por elementos actualizados incluyendo modelos de evolución de los productos en mantenimiento a productos con las mismas o superiores funcionalidades, siempre que dichos productos correspondan a las líneas y fabricantes indicados en el detalle técnico, incluyendo incluso los que requieran appliances para su instalación y funcionamiento.

En este caso de ser ofertado por el licitador, el hardware adicional se entregará sin coste adicional para cualquiera de los dos centros de proceso de datos donde se sustituya, cumpliendo los protocolos habituales para su etiquetado e inventariado.

El licitador deberá indicar en la propuesta de sustitución los motivos que justifican la sustitución siendo obligatorio en su caso indicar:

- Sustitución de elementos por obsolescencia o evolución de los productos adquiridos hacia modelos de instalación diferentes a los actualmente instalados, especialmente en los casos en los cuales los productos existentes puedan



evolucionar a modelos de funcionamiento que requieran o incluyan la instalación en elementos hardware o appliances los cuales serán incluidos en la sustitución.

- Cambios en los modos de licenciamiento, siempre que el nuevo modelo propuesto mantenga, amplíe y no limite las capacidades existentes en la actualidad. En los supuestos en los que se oferte la sustitución de cualquier modo de licenciamiento actual por un modelo de licenciamiento por CPU, se entenderá que no existe limitación en cuanto a la configuración, arquitectura o capacidad de CPU.
- Fin de soporte por el fabricante de alguno de los elementos en mantenimiento.

Dicha sustitución y el plan presentado para su ejecución requerirá la aprobación de cada uno de los organismos afectados, e incluirá todas las actividades de migración necesarias para llevarla a cabo.

Los nuevos elementos sustituidos se considerarán incluidos en mantenimiento hasta la finalización del contrato.

Los equipos sustituidos, en el supuesto que incluyan hardware como soporte para su funcionamiento, deberán ser debidamente etiquetados cumpliendo con las normas de control y etiquetado de equipos establecidas en cada uno de los centros afectados, y a su vez, la firma adjudicataria deberá informar, en el caso de afectar al SERMAS, de los códigos de los equipos sustituidos y sustitutos. Las configuraciones de los equipos nuevos sustitutos serán en todo caso idénticas o superiores, y nunca inferiores a las del propio equipo sustituido.

5. SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

El contratista debe ser consciente de la importancia de la seguridad de la información en el ciclo de vida de cada uno de los sistemas de información de la CSCM en los que intervenga para este caso la plataforma de firma centralizada, autenticación y custodia de documentos electrónicos y de certificados digitales para los profesionales del servicio madrileño de salud y los sistemas de información sanitaria, tanto a nivel lógico como físico, ya sea en su mantenimiento, mejoras, desarrollos o evolutivos. Como contratista



debe garantizar la disponibilidad del servicio que presta y la de los sistemas de información, así como las demás dimensiones de seguridad: autenticidad e integridad de los datos. Se debe tener en consideración que afecta no sólo a los sistemas de información y sus datos en entornos de producción, sino también a los demás entornos existentes.

El contratista debe, igualmente, seguir y ejecutar las directrices, normas, procedimientos y/o estándares de seguridad, que le sean indicados. También se debe comunicar cualquier incidencia que el contratista detecte, por los medios que se establezcan en la DGSIES, con el fin de controlar los riesgos que puedan surgir de estas incidencias. Además, el contratista deberá indagar, por sí mismo, sobre las medidas de seguridad que le afecten a su servicio o procesos de la organización, relacionados con los sistemas de información de la CSCM.

Igualmente, el contratista deberá atender a los requerimientos del área encargada de la seguridad de la información dentro de la DGSIES, así como colaborar con ésta en todo lo necesario para el oportuno cumplimiento de los requisitos legales y normativos en esta materia.

5.1. Normativa de seguridad y protección de datos

En el caso de que el Adjudicatario, en el ejercicio de la prestación del servicio, tuviera que tratar con datos de carácter personal de la CSCM por razón de la prestación del servicio cuya finalidad es la de mantenimiento y soporte de los módulos de autenticación, firma electrónica y el de custodia de documentos electrónicos, cumplirá con la legislación vigente en materia de protección de datos de carácter personal que resulte de aplicación, en 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); Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD); 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, y a los efectos de este contrato, las Direcciones, organismos, entidades o entes de derecho público de la CSCM tendrán 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.

5.2. Encargado del Tratamiento

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

5.3. Limitación del acceso o tratamiento

El Adjudicatario limitará el acceso o tratamiento de datos de carácter personal pertenecientes a los ficheros bajo titularidad de cualquiera de las Direcciones, organismos, entidades o entes de derecho público de la CSCM, 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.

5.4. Medidas de Seguridad

A los efectos de la prestación del servicio por parte del Adjudicatario, en su calidad de 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 de la CSCM 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 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 prestación del servicio sanitario, 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.
- El Adjudicatario 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, y de la Dirección General de Sistemas de Información y Equipamientos Sanitarios del Servicio Madrileño de Salud, perteneciente al SERMAS, 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, 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 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 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 todo caso, y previo a la formalización del contrato de prestación de servicios, el Encargado del Tratamiento informará, mediante una declaración, al Responsable del Tratamiento de la ubicación de sus servidores, así como desde dónde se van a prestar los servicios asociados a los mismos, y cualquier cambio que se produzca a lo largo de la vida del contrato en relación a la ubicación de los servidores, conforme al artículo 122.2 de la Ley 9/2017, de 8 de noviembre, de Contratos del sector público.
- 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 Adjudicatario 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 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 de carácter personal a los que pueda tener acceso en su condición de Encargado del Tratamiento, salvo autorización expresa del Responsable del Tratamiento o de la Dirección General de Sistemas de Información y Equipamientos Sanitarios del SERMAS.
- 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 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. Así mismo, el del Adjudicatario tendrá acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- El Adjudicatario comunicará al Responsable del Tratamiento y a la Dirección General de Sistemas de Información y Equipamientos Sanitarios del SERMAS, 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 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 a la CSCM 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.

5.5. 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.

5.6. Cesión o comunicación de datos a terceros

El contratista 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 sub-encargada, 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 sub-encargado, 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.

5.7. 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.

Restricciones generales

En el marco de la ejecución del contrato, y respecto a los sistemas de información que le dan soporte, las siguientes actividades están específicamente prohibidas:



- La utilización de los sistemas de información para la realización de actividades ilícitas o no autorizadas, como la comunicación, distribución o cesión de datos, medios u otros contenidos a los que se tenga acceso en virtud de la ejecución de los trabajos y, especialmente, los que estén protegidos por disposiciones de carácter legislativo o normativo.
- La instalación no autorizada de software, modificación de la configuración o conexión a redes.
- La modificación no autorizada del sistema de información o del software instalado, el uso del sistema distinto al de su propósito.
- La sobrecarga, prueba, o desactivación de los mecanismos de seguridad y las redes, así como la monitorización no autorizada de redes o teclados.
- La reubicación física y los cambios de configuración de los sistemas de información o de sus redes de comunicación.
- La instalación de dispositivos o sistemas ajenos al desarrollo del contrato sin autorización previa, tales como dispositivos USB, soportes externos, ordenadores portátiles, puntos de acceso inalámbricos o PDA's.
- La posesión, distribución, cesión, revelación o alteración de cualquier información sin el consentimiento expreso del propietario de la misma.
- Compartir cuentas e identificadores personales (incluyendo contraseñas y PINs) o permitir el uso de mecanismos de acceso, sean locales o remoto a usuarios no autorizados.
- Inutilizar o suprimir de forma no autorizada cualquier elemento de seguridad o protección o la información que generen.

5.8. Cesión del contrato

El contratista no podrá ceder total o parcialmente los derechos y obligaciones que se deriven del contrato sin autorización expresa escrita de la DGSIES, 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.



6. CONTENIDO DEL PROGRAMA DE TRABAJO

El contratista elaborará un programa de trabajo que contenga una propuesta técnica que dé una respuesta clara, concisa, completa y detallada de los servicios de mantenimiento y soporte, así como, del suministro propuesto, teniendo en cuenta los requerimientos recogidos en el presente pliego.

El programa de trabajo deberá ajustarse a las necesidades expresadas y no incluir información genérica que no se relacione directamente con los objetivos aquí descritos.

La documentación del programa de trabajo se presentará en castellano y en soporte electrónico.

Madrid,
LA DIRECTORA GENERAL DE SISTEMAS DE INFORMACIÓN
Y EQUIPAMIENTOS SANITARIOS

