Comunidad de Madrid
Dirección General de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN

MINISTERIO DE SANIDAD

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SERVICIOS DE RENOVACIÓN Y MANTENIMIENTO DE LA PLATAFORMA DE FIRMA CENTRALIZADA EN LA NUBE DEL SERVICIO MADRILEÑO DE SALUD

CONTENIDO

1. INTRODUCCIÓN 3

2. OBJETO DEL CONTRATO 4

3. DESCRIPCIÓN DETALLADA DE LOS SERVICIOS 4

3.1 Descripción de los productos incluidos en la renovación de soporte y mantenimiento 4
3.2 Licencias de uso Siaval Crypto para nueva funcionalidad de sellado de tiempo 5
3.3 Detalle del mantenimiento y renovación de HW 6
3.4 Detalle de otras especificaciones del Contrato 7

4. SERVICIOS DE SOPORTE, MANTENIMIENTO Y DE RESOLUCIÓN DE ANOMALÍAS DE FUNCIONAMIENTO 8

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 13
5.2 Normativa de protección de datos 13
5.3 Encargado del Tratamiento 14
5.4 Limitación del acceso o tratamiento 14
5.5 Instrucciones de Tratamiento. 14
5.6 Destino de los datos al finalizar la prestación del servicio 17
5.7 Cesión o comunicación de datos a terceros 18
5.8 Responsabilidad en caso de incumplimiento 18

6. CONTENIDO DE LA PROPUESTA TÉCNICA ..... ¡Error! Marcador no definido.

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 76/2023, de 5 de julio, del Consejo de Gobierno, por el que se establece la estructura orgánica básica de las Consejerías de la Comunidad de Madrid, y la Consejería de Digitalización en la que se crea la Dirección General de Salud Digital a la que le corresponde la asunción de competencias de la extinta Dirección General de Sistemas de Información y Salud Digital del Servicio Madrileño de Salud, creada según Decreto 66/2022, de 20 de julio. Por tanto la Dirección General de Salud Digital asume las funciones que corresponde: “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 Atención al Ciudadano y Transparencia y a la Dirección General de Estrategia Digital. Todo lo anterior según las disposiciones adicionales del Decreto 76/2023, de 5 de julio que contemplan que en todo aquello que suponga cambio de centro presupuestario y en lo relativo a la adaptación de los procesos de estructuras orgánicas, presupuestarias y contables deberá quedar adecuado, como máximo, el día 1 de enero de 2024.

De acuerdo con estas competencias, la Dirección General de Salud Digital (DGSD) dispone de una plataforma implantada en los Centros de Procesos de Datos (CPD) del Servicio Madrileño de Salud (SERMAS), CPDP-1 y CPDP-2, que ofrece los servicios de firma centralizada, autenticación y custodia de documentos electrónicos y de certificados digitales para los profesionales del SERMAS 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. Estos servicios son necesarios además para que los profesionales sanitarios puedan acceder a historia clínica del Sistema Nacional de Salud, iniciativa que promueve y patrocina el Ministerio de Sanidad y en la que colabora con la DGSD.

2. OBJETO DEL CONTRATO

El objeto de esta contratación es proceder a 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 y de certificados digitales del SERMAS, así como el mantenimiento y soporte del cuadro de mandos vinculado a dicha plataforma.

Además, se incluye la puesta a disposición de licencias de uso 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 la DGSD requiera, para ofrecer las mismas funcionalidades de firma electrónica y custodia segura de documentos y la renovación tecnológica de los componentes HW de los Appliances Safecert y Custodia.

3. DESCRIPCIÓN DETALLADA DE LOS SERVICIOS

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

En la actualidad la DGSD 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 Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, al REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, así como la normativa que la modifique y/o sustituya, o cualquier otra que resulte aplicable conforme a su ámbito de actuación.

- 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.

3.2 Licencias de uso Siaval Crypto para nueva funcionalidad de sellado de tiempo

Se requiere la puesta a disposición de dos licencias de uso 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 estas 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.

3.3 Detalle del mantenimiento y renovación de HW

El detalle de los productos instalados en la actualidad en la DGSD y sobre los que se requiere la contratación de los servicios de soporte y mantenimiento son los siguientes:

MANTENIMIENTO				
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	65.700	Usuarios
	SIAVAL SafeCert MS CAPI Connector CALs	SIA-SIAVAL-CAPI	10.000	Usuarios
	SIACert RA OnPremise	SIA-SIAVAL-WF	2	Activo/Pasivo
	SIAVAL Custodia	SIA-SIAVAL-PDM-CUSTODY	2	Activo/Pasivo
	SIAVAL Safecert Crypto Licence	SIA-SIAVAL-Crypto	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
	SIAVAL Custodia	SIA-SIAVAL-PDM-CUSTODY	1	Activo
	SIAVAL Safecert Crypto Licence	SIA-SIAVAL-Crypto	1	Activo

RENOVACIÓN TECNOLÓGICA Safecert			
Entorno	**Producto**	**P/N**	**Cantidad**
Producción	HW - SIAVAL SafeCert Secure Appliance	SIA-HW-SIAVAL-SFCRT-APP	2
Preproducción	HW - SIAVAL SafeCert Secure Appliance	SIA-HW-SIAVAL-SFCRT-APP	1

RENOVACIÓN TECNOLÓGICA Custodia			
Entorno	**Producto**	**P/N**	**Cantidad**
Producción	HW - SIAVAL Custodia	SIA-HW-SIAVAL-PDM-CUSTODY	2
Preproducción	HW - SIAVAL Custodia	SIA-HW-SIAVAL- PDM-CUSTODY	1

3.4 Detalle de otras especificaciones del Contrato

3.4.1 Certificados SSL

CERTIFICADOS SSL	
Descripción	**Cantidad**
Standard OV SSL	48
Multi-Domain OV SSL	3
Wilcard OV SSL	4
Extra Domains for OV Certificates	8

3.4.2 Certificados sello, componente y firma de código

CERTIFICADOS SELLO COMPONENTE Y FIRMA DE CÓDIGO	
Descripción	**Cantidad**
Certificado de sello electrónico cualificado para AAPP nivel medio.	16
Certificado de componente cliente para autenticación de las aplicaciones de negocio corporativas a los servicios de pasarela.	20
Certificado de firma de código.	2

3.4.3 Automatización de bajas en la plataforma de gestión de la autoridad de registro

Generación de un proceso de bajas automáticas en la plataforma de gestión de la autoridad de registro (RA), en base a un fichero con el listado de bajas generado previamente por SERMAS y la DGSD.

3.4.4 Disponibilidad HSMs

HSMss	
Cantidad	**Descripción**
3	LUNA NETWORK HSM S750 (FM READY,SW7.2.0,FW7.0.3/7.2.0)
1	LUNA PED HSM S750
1	LUNA BACKUP HSM
20	Client Licenses, Luna Network HSM 7

3.4.5 Mantenimiento y Adaptación del Cuadro de Mandos

El Cuadro de mandos para la explotación de los datos de la RA, ha sido recientemente actualizado pero dado que se van a incorporar nuevos elementos a la plataforma es posible que además de su mantenimiento durante el periodo de contratación se requieran algunas adaptaciones en el mismo, una vez estos elementos estén implantados en la RA.

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 de 36 meses de duración, en modalidad 24x7.

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 65.700 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 DGSD y al menos con periodicidad trimestral.
- 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 trimestralmente. 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, la DGSD y los usuarios del SERMAS podrán 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:

Código indicador	Nivel de gravedad	DESCRIPCIÓN DE LA SEVERIDAD DEL INCIDENTE	Respuesta inicial de Soporte 24x7
S01	Nivel 1	Indisponibilidad de todas las funciones o cualquiera de los elementos de la plataforma de firma 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 la plataforma o en otras aplicaciones.	Dentro de 1 Hora
S02	Nivel 2	Las funciones o cualquiera de los elementos de la plataforma de firma 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 la plataforma o en otras aplicaciones.	Dentro de 2 Horas
S03	Nivel 3	Cualquier función del software que no está disponible o cualquier elemento de la plataforma de firma 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 la plataforma o en otra aplicación. Una solución provisional puede ser aceptable y se propone e implementa por la empresa adjudicataria.	Dentro de 4 Horas
S04	Nivel 4	Cualquier petición de incremento de funcionalidades que tenga mínimo o ningún impacto en los servicios de la plataforma o en otras aplicaciones y para las que no se	Dentro de 1 Día Hábil

		requiere una solución inmediata. Solicitudes de información o consultas	

Estos ANS se revisarán mensualmente en el seno del comité operativo que se integra por un responsable del servicio por parte del adjudicatario y por el interlocutor designado por la DGSD como director del contrato. Este podrá autorizar el acompañamiento de los especialistas de la empresa o de la DGSD que puedan proporcionar mejor información. En caso de discrepancias, se revisarán por el comité de dirección, formado por el director del contrato, el responsable del servicio y un Subdirector General de la DGSD y un directivo de la empresa adjudicataria con responsabilidad en la materia del expediente, siendo la Administración quien decida finalmente sobre el adecuado cumplimiento de los ANS.

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, amplié y no límite 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 a la DGSD, 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 Comunidad de Madrid, en los que intervenga para este caso la plataforma de firma centralizada, autentificación 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

DGSD, 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 Comunidad de Madrid.

Igualmente, el contratista deberá atender a los requerimientos del área encargada de la seguridad de la información dentro de la DGSD, 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

Considerando lo dispuesto en el artículo 2 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), donde se describe la obligación de exigir a las entidades del sector privado que presten servicios o provean soluciones a las entidades públicas, la entidad contratante, considera necesario que la entidad licitadora, esté en condiciones de exhibir la correspondiente Declaración o Certificación de Conformidad con el Esquema Nacional de Seguridad, para la categoría de seguridad de que se trate, de los sistemas que intervengan en la prestación de los servicios indicados, así como mantener la conformidad vigente durante la vigencia del contrato.

En el supuesto de que el adjudicatario no pudiera mantener la conformidad con el ENS -por pérdida, retirada o suspensión de la Certificación de Conformidad o imposibilidad de mantener la Declaración de Conformidad-, deberá comunicar esta circunstancia, de forma inmediata y sin dilación indebida, a la entidad contratante, quien considerará el impacto en la prestación objeto del contrato de dicha circunstancia.

La entidad adjudicataria asume su obligación de cumplir plenamente con el Esquema Nacional de Seguridad.

Adicionalmente, la entidad adjudicataria 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.

5.2 Normativa de protección de datos

El adjudicatario en el ejercicio de la prestación del servicio tratará datos personales de la entidad contratante o la unidad que aquella designe conforme las competencias que ésta pudiera tener asignadas, por lo que deberá cumplir 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, la entidad contratante o la unidad que aquella designe conforme las competencias que ésta pudiera tener asignadas, 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.

5.3 Encargado del Tratamiento

El Adjudicatario, se compromete a cumplir las medidas y requisitos de seguridad exigidos por el Responsable de 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 ésta responsabilidad asumida por el Adjudicatario, serán recogidas en un documento específico que será firmado por el Responsable de tratamiento y el Adjudicatario de forma previa al inicio de los trabajos.

5.4 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.

5.5 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 prestación del servicio por parte del Adjudicatario, 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 de carácter personal o empresarial, 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 del deber de seguridad de los datos personales, 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, 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 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 personales 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 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 dimanan, para lo cual programará las acciones formativas necesarias, incluida la formación en protección de datos y seguridad. Así mismo, el del 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 prestación del servicio.

5.6 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 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 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. La devolución o destrucción de la información no eximirá al adjudicatario del cumplimiento de confidencialidad aquí reflejado.

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.

5.7 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 los servicios auxiliares necesarios para el normal funcionamiento de los servicios.

- En caso de que el Adjudicatario 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 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.

5.8 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 los mismos, 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.

Madrid,
LA DIRECTORA GENERAL DE SALUD DIGITAL

Firmado digitalmente por: RUIZ HOMBREBUENO NURIA
Fecha: 2023 12 15 17:02