Comunidad de Madrid

DIRECCIÓN GENERAL DE SISTEMAS
DE INFORMACIÓN SANITARIA

CONSEJERÍA DE SANIDAD

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR LA CONTRATACIÓN DE UN SERVICIO DE AUDITORIA DE CUMPLIMIENTO DE LAS MEDIDAS DE SEGURIDAD EN 2016 EN EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL PARA LOS CENTROS DEL SERVICIO MADRILEÑO DE SALUD Y AUDITORIA DEL ESQUEMA NACIONAL DE SEGURIDAD

MAYO 2017

Índice

1. ANTECEDENTES Y OBJETO DEL CONTRATO

1.1. Antecedentes

El Servicio Madrileño de Salud (en adelante, SERMAS), perteneciente a la Consejería de Sanidad de la Comunidad de Madrid (en adelante, CSCM) engloba una de las mayores redes de centros y edificios de la Comunidad de Madrid, complicada al mismo tiempo por la elevada dispersión geográfica de estos centros en todas las zonas y territorios del entorno regional. Esta característica se aplica del mismo modo a los sistemas de información que soportan las actividades cotidianas de estos centros, los cuales se hayan repartidos por los centros usuarios de estos sistemas.

La actual legislación en materia de protección de datos y en especial el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, LOPD), aprobado mediante el Real Decreto 1720/2007, de 21 de diciembre, exigen la implantación y cumplimiento de una serie de medidas de seguridad, que dado el carácter y criticidad de los datos que albergan los sistemas de información de estos Centros, requieren de la adopción de medidas específicas, tales como la auditoría bienal de las medidas de seguridad.

Dichas auditorías se llevarán a cabo de acuerdo con lo establecido en el título VIII del Reglamento de desarrollo de la LOPD. Dicho Reglamento especifica:

> *1. A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.*
>
> *Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.*
>
> *2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.*
>
> *3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.*

El Real Decreto 3/2010 que regula el **Esquema Nacional de Seguridad** en el ámbito de la administración electrónica, en su artículo 34 y Anexo III, regula la auditoria de seguridad

> *Artículo 34. Auditoría de la seguridad.*

1. Los sistemas de información a los que se refiere el presente real decreto serán objeto de una auditoría regular ordinaria, al menos ***cada dos años****, que verifique el cumplimiento de los requerimientos del presente Esquema Nacional de Seguridad…….*

2. Esta auditoría se realizará en ***función de la categoría del sistema****, determinada según lo dispuesto en el anexo I y de acuerdo con lo previsto en el anexo III.*

1.2. Objetos del contrato

Un objeto del contrato es el servicio de apoyo a la realización de las auditorias de cumplimiento de las medidas de seguridad en 2016, en el **tratamiento de datos de carácter personal** para los ficheros de los Centros del Servicio Madrileño de Salud, tanto a los ficheros informatizados, como a los de carácter manual o mixto, a los que les corresponde realizarlas en el año 2017.

Otro objeto del contrato es la realización de una **auditoria regular ordinaria**, de las aplicaciones de la CSCM, con acceso electrónico de los ciudadanos a los servicios públicos, con los objetivos señalados en el Anexo III del RD 3/2010 que regula el Esquema Nacional de Seguridad

2. OBJETIVOS, ÁMBITO Y ALCANCE

2.1 Objetivos, actividades y alcance de la Auditoria Protección de Datos

Los objetivos principales que contempla, son la realización de las auditorías atendiendo a las siguientes tareas:

1. El contratista deberá, a la vista de los Centros y ficheros con los que tratará, organizar y dividir el trabajo de forma lógica, coordinando con los centros las agendas para las visitas de los auditores.
2. El contratista seguirá unas plantillas de informe de auditoría lo más específicas posible para el entorno sanitario. Asimismo, elaborará un formulario con un cuestionario inicial de cumplimiento de las medidas técnicas legales y organizativas de seguridad en el tratamiento de datos de carácter personal, (de conformidad con el título VIII del Reglamento de desarrollo de la LOPD), incluyendo una lista de puntos de comprobación. Lo remitirá a los Centros para realizar una recogida preliminar de información de forma previa a la visita de los auditores. Recabada esta información, el adjudicatario establecerá la planificación de las entrevistas entre él y el Responsable de Seguridad o Responsable de Ficheros del Centro. Considerando el elevado número de ficheros auditables en algunos Centros, se podrá exigir la realización de más de una entrevista en dichos Centros, con el fin de asegurar la calidad de la auditoría. Siempre se efectuarán las entrevistas en cada uno de los Centros.
3. El auditor deberá realizar la entrevista constatando el estado de cada uno de los epígrafes aplicables y exigibles por el contexto legal, y requiriendo y evaluando las evidencias necesarias para asegurar el cumplimiento. Se deben minimizar las necesidades de recopilación de información y el tiempo necesario por parte de los responsables de los ficheros o de Seguridad. El auditor deberá recoger evidencias de cada medida de seguridad auditada, las cuales deberán constar en el informe y ser adjuntadas en la documentación final.
4. Debe hacerse en el informe un seguimiento del historial del fichero, si ha habido cambios de estado: por alta nueva, modificación, supresión realizada y prevista próximamente, así como por subsumisión del fichero en otro existente.
5. Realizadas las entrevistas, el auditor de la empresa adjudicataria procederá a la elaboración de los informes borradores de auditoría. Estos serán remitidos a los Responsables de Seguridad de los Centros para la presentación de alegaciones si las hubiese y, una vez solventadas las discrepancias, se procederá a la entrega de los informes finales a cada uno de los Centros, donde se informará de las deficiencias y de las recomendaciones de mejora. Existirá un informe de auditoría por cada fichero auditado en el centro.
6. Asimismo, el auditor de la empresa adjudicataria elaborará un informe genérico por **centro**, de cumplimiento LOPD, donde se tengan en cuenta los artículos 5 al 34 (derechos ARCO, de información, consentimientos, comunicación, cláusulas, formularios, modelos, etc.)
7. Tras la entrega de los documentos a los Responsables de Seguridad de cada Centro, se evaluarán y aprobarán formalmente con cada Responsable de

Seguridad con el fin de asegurar y verificar el cumplimiento de cada apartado, e informar de las recomendaciones que apliquen para la mejora futura de la seguridad del Centro.

8. Debe tenerse en cuenta para el informe final de auditoría, y para el resto de entregables, los formatos que el SERMAS proporcione, o bien acordarse con éste formatos propios que el contratista pueda proporcionar. Dichos informes serán remitidos al SERMAS y a los Centros.
9. El contratista elaborará un informe ejecutivo y específico por Centro, así como un informe final con carácter general a partir de los informes detallados de todos los centros analizados conjuntamente, ambos en el formato y presentación que le sean indicados. El objetivo de estos informes es facilitar la tarea de comparar de forma transversal resultados y medidas correctoras; las especificaciones exactas de este informe se entregarán al contratista al inicio de los trabajos. Se incidirá en las medidas correctoras detectadas y en las líneas de mejoras o complementarias más generales, explicando alcances y plazos futuros. Para las mejoras propuestas, se deberá concretar y motivar el beneficio que se pretende alcanzar con cada mejora.
10. Será obligatorio que se aplique un tratamiento estadístico a los resultados, elaborando planes cuantificados de mejora, debiendo aportar los documentos con las fuentes a partir de las cuales se hayan obtenido los citados datos. También se entregarán los datos en un formato definido por la Dirección General de Sistemas de Información Sanitaria (en adelante, DGSIS) y del que entregará una plantilla al contratista, compatible con el Cuadro de Mando existente, y que incluirá, al menos los conceptos siguientes:
    a. fichero, centro, año y tipo de fichero
    b. artículo afectado y apartado
    c. grado de incumplimiento, grado de infracción, nota de evaluación
    d. evidencia, medida correctora, observaciones.

    Se deberá hacer mención en los datos entregados a las aplicaciones que se basan en cada uno de los ficheros y el grado de cumplimiento o nivel de seguridad que alcanzan.
11. Se efectuará una reunión final con representantes de la DGSIS, o de la Oficina de Seguridad de Sistemas de Información (en adelante, OSSI) y quien considere oportuno la CSCM, en la que se difundirán los resultados finales ya descritos.
12. Estos trabajos descritos, salvo casos excepcionales, serán realizados en las dependencias del Centro o del adjudicatario. Los trabajos serán supervisados a alto nivel por representantes de la DGSIS, que podrá intervenir en su desarrollo si lo considerase necesario. Toda la documentación utilizada o generada en los trabajos se devolverá al final de los mismos.

El contratista deberá concretar en su plan de trabajo el procedimiento que plantea seguir durante la ejecución de los trabajos con el fin de asegurar la calidad final del servicio ofertado, así como el alineamiento a los objetivos del proyecto y la estrategia marcada por la DGSIS.

En el caso de proponer mejoras a la metodología indicada, se deberá concretar y motivar el beneficio que se pretende alcanzar con cada mejora.

Alcance

El alcance del servicio ofertado en el presente pliego atiende a los siguientes ámbitos:

- El adjudicatario realizará auditorías a un mínimo de 45 centros u organismos que engloban un mínimo de 187 ficheros a auditar.
- La empresa adjudicataria aportará los perfiles diferentes para plantear la auditoría de los centros Hospitalarios, Centros de Atención Primaria, u órganos de gestión, de forma que se especialice el conocimiento en las particularidades de cada tipo de centro.
- Los centros poseen una elevada dispersión geográfica, por lo que la empresa adjudicataria deberá asumir cualquier tipo de gasto producido directa o indirectamente por dicha dispersión (siendo éstas: dietas, gasto de kilómetros, entre otros).
- El contratista deberá ser flexible en su horario y calendario con el fin de resolver y agilizar las visitas que se plantean con los Responsables de Seguridad de los Centros. La Comunidad de Madrid no asume ningún tipo de gasto o coste producido por la compensación horaria del personal del adjudicatario, ni de los gastos provocados por la revisión o modificación de las fechas de reunión o planteamiento de nuevos calendarios.

2.2 Objetivos, actividades y alcance de la Auditoria de Esquema Nacional de Seguridad

La realización de la una auditoria regular ordinaria, que verifique el cumplimiento de los requerimientos del Esquema Nacional de Seguridad (RD 3/2010)

Se realizara en función de la categoría del sistema, determinado según lo dispuesto en el Anexo I y de acuerdo con lo previsto en el Anexo III

En la realización de la auditoria se utilizaran los criterios, métodos de trabajo y de conducta generalmente reconocida, así como la normalización nacional e internacional aplicables a este tipo de auditorías:

-CCN-STIC 802 - Guía de Auditoría

-CCN-STIC 808 - Guía de Verificación del cumplimiento de las medidas en el Esquema Nacional de Seguridad

-UNE-ISO/IEC 27001:2007 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. (ISO/IEC 27001:2005)

-UNE-ISO/IEC 27002:2009 Tecnología de la Información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información

-UNE-ISO/IEC 20000 Tecnología de la información. Gestión del servicio

La auditoría se realizara en los siguientes términos (RD 3/2010 Anexo III):

- Que la política de seguridad define los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información.
- Que existen procedimientos para resolución de conflictos entre dichos responsables.
- Que se han designado personas para dichos roles a la luz del principio de "separación de funciones".
- Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
- Que se cumplen las recomendaciones de protección descritas en el anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
- Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección.

La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los puntos mencionados:

- Documentación de los procedimientos.
- Registro de incidentes.
- Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.
- Productos certificados. Se considerará evidencia suficiente el empleo de productos que satisfagan lo establecido en el artículo 18 «Adquisición de productos y contratación de servicios de seguridad».

El informe de la auditoria deberá dictaminar sobre:

-El grado de cumplimiento
- Identificar sus deficiencias
-Sugerir las posibles medidas correctoras o complementarias necesarias
-Las recomendaciones que se consideren oportunas.
-Los criterios metodológicos de auditoría utilizados,
- El alcance y el objetivo de la auditoría,
-Los datos, hechos y observaciones en que se basen las conclusiones formuladas.

Alcance

Serán objeto de auditoria de ENS, 35 aplicaciones pertenecientes a la CSCM, las cuales serán detalladas durante la primera fase de la auditoria

3. EQUIPO DE PRESTACIÓN DEL SERVICIO

El objetivo final del contrato es la realización de las auditorías de cumplimiento de las medidas de seguridad en el 2016, en el tratamiento de datos de carácter personal y la auditoria regular ordinaria de ENS. Para ello el contratista dedicará los recursos de personal que considere necesarios, por encima de los perfiles mínimos que se consideran imprescindibles, para obtener los resultados en el plazo establecido del contrato.
La DGSIS podrá requerir un reforzamiento del equipo de trabajo para alcanzar el cumplimiento de los plazos establecidos.

Por parte del contratista, se requieren los siguientes perfiles mínimos:

- **1 Responsable del proyecto**, que actuará como interlocutor único con el Director del proyecto designado por el SERMAS. El Responsable de proyecto deberá encontrarse al día del avance en la realización del proyecto, y continuamente en contacto disponible para el resto del equipo de trabajo con el objeto de poder informar del estado del proyecto o resolver los riesgos que pudieran producirse en el mismo.

  El responsable de proyecto ofertado debe cumplir los siguientes requisitos:

  - Formación mínima:
    - Titulación universitaria
  - Experiencia mínima:
    - 5 años como responsable de proyectos TIC.
    - En las siguientes tareas:
      - Auditoría, análisis o diseño de arquitecturas de comunicaciones.
      - Auditoría, análisis o diseño de soluciones de basadas en sistemas de seguridad.
      - Auditoría, análisis o diseño de soluciones TIC en el entorno sanitario (al menos 2 años).

- **3 Auditores**, especialistas en **protección de datos** que realizarán las tareas de auditoría y elaboración de los informes.

  Los auditores deben cumplir los siguientes requisitos:

  - Formación mínima:
    - Titulación universitaria ,FP Grado Superior (Informatica y Comunicaciones)
    - Formación en legislación relativa a la protección de datos de carácter personal, en particular, a la LOPD (al menos 40 horas).

- Experiencia mínima:
  - 3 años participando en proyectos o servicios de relación directa con usuarios.
  - En las siguientes tareas:
    - Auditoría, análisis o diseño de arquitecturas de comunicaciones.
    - Auditoría, análisis o diseño de soluciones basadas en sistemas de seguridad.
    - Auditoría, análisis o diseño de soluciones TIC en el entorno sanitario (al menos 1 año).

Los auditores deberán poseer un elevado conocimiento de las leyes y normativas relacionadas con la LOPD y asesorar en lo necesario a los Centros auditados acorde con las acciones a tomar en relación con estas leyes. La empresa licitadora podrá aportar otros perfiles, indicando el beneficio concreto obtenido para el proyecto en base a su participación.

- **2 Auditores**, especialistas en **auditoria de ENS** y elaboración de los informes.

  Los auditores deben cumplir los siguientes requisitos:

  - Formación mínima:
    - Titulación universitaria ,FP Grado Superior (Informática y Comunicaciones)
    - Formación en legislación relativa a la protección de datos de carácter personal, en particular, a la LOPD (al menos 40 horas).
  - Experiencia mínima:
    - 3 años participando en proyectos o servicios de relación directa con usuarios.
    - En las siguientes tareas:
      - Auditoría, análisis o diseño de arquitecturas de comunicaciones.
      - Auditoría, análisis o diseño de soluciones basadas en sistemas de seguridad.
      - Auditoría, análisis o diseño de soluciones TIC en el entorno sanitario (al menos 1 año).
      - Conocimiento de los requisitos del RD 3/2010

4. FASES Y PLAZOS DE CONTRATO

Auditoria de protección de datos

Fase I (SERMAS):

Una vez hayan sido determinados los centros cuyos ficheros vayan a ser objeto de auditoría, la OSSI llevará a cabo las siguientes tareas:

- Elaboración de plantillas para entregables.
- Contacto inicial con los Centros bajo las premisas concretas que decida la DGSIS.

Fase II

El contratista llevará a cabo las auditorías en función de la planificación e información recibidas. Podrá proponer sub-fases dentro de la planificación, dedicadas a los diferentes entornos de la CSCM:

- Atención Especializada
- Atención Primaria
- Servicios Centrales

Durante esta fase se tendrá en cuenta lo especificado en las cláusulas 2.1 Objetivos y actividades en la auditoría y 5.4 Metodología a emplear del presente pliego.

Auditoria ENS

El SERMAS identificara las aplicaciones que serán sometidas a la auditoria, con indicación del personal responsable de las mismas

El contratista definirá la aplicación de la metodología y los esquemas de trabajo propios del equipo de auditoria

5. DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS

5.1. Evaluación del servicio prestado

La DGSIS realizará de manera continuada la dirección, seguimiento y evaluación de los servicios contratados, sin perjuicio de las labores de coordinación, control, y aseguramiento que sobre el proceso global corresponden al contratista.

La DGSIS establecerá la metodología, formatos de entregables, alcance y contenido de los mismos, evaluando el cumplimiento y calidad de los trabajos realizados y marcarán las prioridades.

El contratista responderá de la correcta realización de los trabajos contratados y de los defectos que en ellos hubiere o que se pudieran derivar.

La DGSIS podrá rechazar en todo o en parte los trabajos realizados, en la medida que no respondan a los especificados en los objetivos de la planificación o no superasen los niveles de calidad acordados.

5.2. Dirección y seguimiento de los trabajos

Corresponde a la DGSIS dirigir y supervisar los trabajos y velar por el cumplimiento de los niveles de servicio acordados. En este sentido, la DGSIS nombrará un Director de Proyecto cuyas funciones principales en relación con el objeto del presente pliego serán las siguientes:

- Velar por el cumplimiento y el nivel de calidad de los trabajos.
- Planificar y priorizar las actividades del equipo prestador del servicio.
- Supervisar y validar la ejecución de las actividades a realizar.
- Dar conformidad a los resultados finales del servicio.

Es potestad del Director del Proyecto exigir en cualquier momento la adopción de cuantas medidas concretas y eficaces sean necesarias en relación con la prestación del servicio, si a su juicio, la calidad o efectividad del mismo se pone en peligro ante cualquier circunstancia.

El contratista designará un Responsable de Proyecto ante la DGSIS, al margen del equipo de prestación del servicio, y perteneciente al equipo directivo de su organización. Este Responsable se encontrará en permanente contacto con el personal de la DGSIS designado por ésta y realizará, entre otras, las siguientes tareas:

- Coordinar el apoyo técnico y supervisar el servicio a prestar e informar al Director del Proyecto de la DGSIS de las posibles incidencias y seguimiento o desviaciones de plazos.

- Mensualmente remitir a la DGSIS un informe detallado que permita constatar el cumplimiento de la calidad del servicio prestado, sin menoscabo de que la misma pueda realizar aquellas actuaciones que considere oportuno para contrastar la veracidad de los datos aportados.
- Mensualmente, como mínimo, mantener con DGSIS una reunión de seguimiento del servicio prestado en el mes previo y validación de la propuesta para el mes siguiente a la misma.

5.3. Modificaciones en el equipo de prestación del servicio

Toda nueva incorporación al equipo prestador de los servicios deberá reunir los requisitos mínimos, en cuanto a titulación y conocimientos técnicos necesarios establecidos en el presente Pliego, según perfiles.

Excepcionalmente, la CSCM tendrá la potestad de exigir, cuando existan razones suficientemente motivadas que afecten al normal desarrollo de la prestación del servicio, el cambio de cualquiera de los componentes del equipo prestador de los servicios del contratista. Este cambio se solicitará por el Director de Proyecto que haya designado la CSCM, a través de las reuniones de Seguimiento, garantizando al contratista un preaviso de 15 días laborables, para que pueda proceder a la sustitución de dicho componente.

Si el contratista propusiera el cambio de cualquiera de los miembros del equipo prestador del servicio, se deberá comunicar por escrito a la CSCM con 15 días laborables de antelación, comunicando:

- Justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio.
- Presentación del candidato con perfil y cualificación técnica igual o superior al de la persona que se pretende sustituir.

En el supuesto de que se produzca modificaciones en los equipos, ya sean solicitadas por la DGSIS o por el contratista, se requerirá un solapamiento del personal durante un periodo mínimo de 10 días laborables.

Durante todo el plazo de ejecución, el contratista deberá mantener los niveles de calidad del servicio objeto del contrato, por lo que deberá instrumentar los servicios de suplencia que estime oportunos, que serán cubiertos, a ser posible, con el mismo personal suplente, a los efectos de ocasionar el mínimo impacto en la prestación del servicio.

El contratista deberá garantizar que dispone de los mecanismos adecuados para minimizar la rotación no planificada del personal, para evitar la pérdida no controlada de conocimiento, y el impacto en los niveles de servicio, imagen, dedicación adicional de la CSCM, etc., que esto suele llevar asociado.
Por rotación planificada se entiende aquella que se comunica a la CSCM como mínimo 15 días laborables antes de que se produzca, y se acompaña de un solapamiento del

recurso saliente con el entrante para la adecuada transferencia de conocimiento durante un periodo no inferior a 10 días laborables.

5.4. Metodología a emplear

El adjudicatario trabajará con la metodología interna que estime oportuna pero siempre ajustándose a los elementos que le proporcionará la DGSIS, y siguiendo las etapas que dicha Dirección marque. En particular:

- La DGSIS establecerá el contacto inicial con los responsables de Seguridad de los Centros, obteniendo una primera toma de contacto y alertando de las actividades del plan de trabajo que se va a iniciar.
- La DGSIS, a partir de sus experiencias anteriores, proporcionará plantillas de informes de auditoría de forma orientativa y versiones de *checklist* o puntos de comprobación aproximados. El contratista trabajará con los documentos proporcionados por la DGSIS, actualizándolos, mejorándolos, y llegando a una versión de los mismos que considere adecuada y exhaustiva, elaborándolos de forma lo más específica posible para el entorno sanitario.
- La DGSIS entregará al contratista las plantillas necesarias para la realización de la auditoría. Toda la documentación utilizada o generada en los trabajos se devolverá al final de los mismos.
- El contratista remitirá a la DGSIS los informes de auditoría cumplimentados, para su supervisión. Una vez obtenida esta autorización, se remitirán a los Centros.
- Asimismo, el contratista remitirá a la DGSIS todos los informes detallados y ejecutivos, tanto específicos, como generales, que se detallan en las tareas del apartado de objetivos del presente pliego.
- La DGSIS participará en la reunión final en la que se difundirán los resultados finales ya descritos en el apartado citado. Los trabajos serán supervisados con periodicidad a alto nivel por la DGSIS, que podrá intervenir en su desarrollo si lo considerase necesario.

6. CONDICIONES GENERALES

6.1. Propiedad de los trabajos

Todos los documentos, productos y demás entregables resultantes de la ejecución del presente contrato serán propiedad del SERMAS, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos.

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

6.2. Calidad de los trabajos

Los estándares de calidad de servicio a prestar serán evaluados mensualmente. No obstante, durante el desarrollo de los trabajos, la DGSIS podrá establecer controles de calidad y acciones de aseguramiento de la calidad de la actividad desarrollada.

En cualquier caso, el contratista deberá proponer las mejoras de calidad que estime oportunas para optimizar la actividad desarrollada durante el tiempo de ejecución del presente contrato.

6.3. Normativa de seguridad y protección de datos

El contratista 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 la LOPD y normativa relacionada, serán por cuenta del contratista.

En el caso de que el contratista, en el ejercicio de la prestación del servicio, tuviera que manejar ficheros con datos de carácter personal en el marco del objeto del presente contrato, cumplirá con la legislación vigente en materia de protección de datos de carácter personal conforme a lo dispuesto en las leyes y decretos que resulten de aplicación, entre ellos los que se relacionan a continuación:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

- Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (RDLOPD), aprobado mediante el Real Decreto 1720/2007, de 21 de diciembre.
- Orden 1943/2005, del Consejero de Sanidad, por la que se aprueba el Código de Buenas Prácticas para usuarios de sistemas informáticos, así como otras normativas y estándares que en materia de seguridad sean adoptados por la Consejería.
- Y 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.

6.3.1. Encargado de tratamiento

El contratista, en la medida en que necesite acceder a datos de carácter personal bajo titularidad de la CSCM o de los órganos, entidades, gerencias, centros, direcciones, organismos o entes adscritos a la citada Consejería por razón de la prestación del servicio objeto del contrato, asumirá la figura de encargado de tratamiento prevista en la LOPD. Por lo tanto, el acceso y tratamiento de los citados datos de carácter personal por parte del contratista se entenderá siempre subsumido dentro de la categoría de acceso a datos por terceros del artículo 12 de la citada LOPD, y no como una cesión o comunicación de datos a terceros a los efectos previstos en la Ley Orgánica. Las obligaciones derivadas de ésta responsabilidad asumida por el contratista, serán recogidas en un documento específico que será firmado por el contratista de forma previa al inicio de los trabajos.

Por consiguiente las Direcciones, organismos, entidades o entes de derecho público de la CSCM ostentarán, en cualquier caso, y con respecto a los datos objeto de acceso o tratamiento, la condición de Responsable del Fichero o del tratamiento.

Al objeto de dar cumplimiento a lo previsto en el art. 12 de la LOPD, las cláusulas que se incluyen a continuación regularán el posible uso y tratamiento de datos de carácter personal por parte del encargado de tratamiento y por cuenta de la CSCM.

6.3.2. Limitación del acceso o tratamiento

El contratista 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.

6.3.3. Medidas de seguridad

No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por el Reglamento de desarrollo de la LOPD, respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

A los efectos de la prestación del servicio por parte del contratista, éste quedará obligado, con carácter general, por el deber de confidencialidad y seguridad de los datos de carácter personal. Y con carácter específico, en todas aquellas previsiones que estén contempladas en las actividades que formen parte del servicio adjudicado, se encontrará sujeto por las siguientes disposiciones, que concretan, de conformidad con el artículo 9 de la LOPD, los requisitos y condiciones que deberán reunir los ficheros y personas que participen en el tratamiento de los datos de carácter personal.

- Los licitador/es aportarán una memoria descriptiva de las medidas que adoptarán para asegurar la confidencialidad, disponibilidad e integridad de los datos manejados y de la documentación facilitada.
- La empresa adjudicataria y el personal encargado de la realización de las tareas guardará secreto profesional sobre todas las informaciones, documentos y asuntos a los que tenga acceso o conocimiento durante la vigencia del contrato, estando obligado a no hacer públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo contractual.
- El contratista, mediante la suscripción del contrato de adjudicación, asumirá el cumplimiento de lo previsto en las presentes cláusulas, que de conformidad con el artículo 12 de la LOPD regulan su acceso como encargado del tratamiento de los ficheros de datos de carácter personal.
- El contratista realizará un estudio previo de los datos de carácter personal a tratar, identificando su naturaleza y las medidas de seguridad que requieran de conformidad con lo establecido en el Reglamento de desarrollo de la LOPD.
- El diseño y desarrollo de los sistemas de información que traten datos de carácter personal facilitará operativamente, que estos sean cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. Igualmente, estos tratamientos almacenarán los datos de carácter personal de forma que permitan el ejercicio del derecho de acceso, rectificación, cancelación u oposición, siendo responsabilidad del contratista habilitar mecanismos y procedimientos que faciliten el ejercicio de estos derechos.
- La documentación se entregará al contratista para el exclusivo fin de la realización de las tareas objeto de este contrato, quedando prohibido para el contratista y para el personal encargado de su realización, su reproducción por cualquier medio y la cesión total o parcial a cualquier persona física o jurídica. Lo anterior se extiende asimismo al producto de dichas tareas.
- Igualmente, estos diseños o 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.
- Para los ficheros de protección de nivel alto el contratista creará los correspondientes registros de accesos a los sistemas de información (trazabilidad) que traten datos de carácter personal y el cifrado de las comunicaciones, así como los mecanismos técnicos que permitan obtener fácilmente información de auditoría a partir de dichos registros.
- 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.
- El contratista, a la finalización del contrato, emitirá un informe en el que indicará el tipo de datos de carácter personal tratados, el nivel protección exigible a los ficheros creados y las medidas de seguridad implementadas en cada caso.

- El contratista 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 fichero, y de la DGSIS, para aquellos aspectos relacionados con sus competencias.
- El contratista adoptará, en todas aquellas previsiones que estén contempladas en las actividades que formen parte del servicio adjudicado, las medidas de índole técnica y organizativa establecidas en el artículo 9 de la LOPD, que garanticen la seguridad de los datos de carácter personal, y que eviten su alteración, pérdida o tratamiento no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- El contratista adoptará, en todo caso, cuando se traten datos especialmente protegidos, de las medidas de seguridad correspondientes al nivel de seguridad alto del Título VIII de medidas de seguridad del Reglamento de desarrollo de la LOPD, de conformidad con el artículo 81 de dicho Reglamento, y en particular de las detalladas en los artículos 103 (registro de accesos) y 104 (telecomunicaciones).
- El contratista no comunicará los datos accedidos o tratados a terceros, ni siquiera para su conservación. No obstante, de conformidad la normativa vigente, se autoriza al encargado de tratamiento para proceder a la subcontratación de terceras entidades, bajo las siguientes condiciones:
  - Se podrán subcontratar las tareas y actividades contempladas en el alcance del servicio adjudicado de conformidad con lo previsto en el correspondiente pliego de prescripciones;
  - Se deberán comunicar a la CSCM los nombres de las entidades subcontratadas, así como las actividades y finalidades contempladas en el ámbito de cada subcontratación;

- Los tratamientos de datos personales llevados a cabo por las entidades subcontratadas se realizarán con estricta sujeción a las instrucciones previstas en el pliego. El contratista deberá formalizar con cada entidad subcontratada las correspondientes cláusulas de conformidad con el artículo 12 de la LOPD, que deberán indicar expresamente que las entidades subcontratadas asumirán, a su vez, la figura de encargados de tratamiento, y que, en el caso de que destinen los datos a otra finalidad, los comuniquen o los utilicen incumpliendo las instrucciones descritas en el punto anterior, o cualquier otro requisito exigible, serán considerados, también, responsables del tratamiento, respondiendo de las infracciones en que hubieran incurrido personalmente.

- Sin perjuicio de lo anterior, 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 33 y 34 de la LOPD.

- El contratista 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 contratista 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 de tratamiento, salvo autorización expresa del Responsable del Fichero o de la Dirección General de Sistemas de Información Sanitaria del Servicio Madrileño de Salud. En este supuesto, deberá destruir o devolver los datos accedidos, al igual que cualquier resultado del tratamiento realizado, y cualquier soporte o documento en el que se hallen, por los medios que se determinen, según cualesquiera instrucción del responsable del Fichero a la finalización de la prestación del servicio o cuando las datos dejen de ser pertinentes para la finalidad o tratamiento.

Los sistemas de información del contratista deberán proporcionar mecanismos que permitan la extracción de datos de forma disociada, conforme a lo contemplado en esta materia en el Reglamento de desarrollo de la LOPD, cuando sea requerido.

De conformidad con la normativa en materia de protección de datos de carácter personal, no procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando la CSCM dicha conservación. El contratista conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con la CSCM.

- El contratista comunicará al Responsable del fichero y a la DGSIS, 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 contratista 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 Consejería de Sanidad a los que pueda tener acceso en el transcurso de la prestación del servicio.

6.3.4. Medidas de seguridad del personal prestador del servicio

Quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal quedarán obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar la relación contractual, así como a la renuncia expresa de los derechos de propiedad intelectual que les pudiera corresponder y compromiso del cumplimiento de las obligaciones de protección de datos de carácter personal.

El contratista 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.

El personal prestador del servicio objeto del contrato tendrá acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

6.3.5. Cesión o comunicación de datos a terceros.

Los datos de carácter personal o documentos objeto del tratamiento no podrán ser comunicados a un tercero bajo ningún concepto, sin el consentimiento previo del titular del dato y el conocimiento de la Comunidad de Madrid, aunque sea para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, sin perjuicio de las excepciones previstas en la LOPD y en su Reglamento de desarrollo.

El contratista tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con un fin distinto al que figure en el objeto del contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

Una vez cumplida la prestación contractual, los datos de carácter personal utilizados deberán ser destruidos o devueltos a la Comunidad de Madrid, al igual que cualquier soporte o documentos utilizados.

6.3.6. Responsabilidad en caso de Incumplimiento

En el caso de que el contratista destine los datos a otra finalidad, los comunique o los utilice incumpliendo las obligaciones especificadas, o cualesquiera otra exigible por la normativa, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente, de conformidad con el artículo 12.4 de la LOPD, estando sujeto, en su caso, al régimen sancionador establecido de conformidad con lo dispuesto en los artículos del 43 al 49 de la LOPD.

6.4. 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 DGSIS, 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.

7. DOCUMENTACIÓN TÉCNICA DEL PROGRAMA DE TRABAJO

En el programa de trabajo se describirán las tareas a desarrollar, en términos ajustados al presente pliego, recursos materiales disponibles para la ejecución del contrato, prestaciones superiores a las solicitadas y cualquier otra circunstancia que incida en la ejecución de los trabajos.

El programa de trabajo deberá presentarse en un plazo de 30 días desde la firma del contrato, y contendrá una planificación temporal pormenorizada de todas las tareas y deberá estructurarse de acuerdo con el siguiente índice, si bien los licitadores podrán incluir la información adicional que consideren pertinente

Descripción general del servicio

i. Planteamiento para la ejecución del proyecto. En relación con el desarrollo de las actividades de verificación de la adecuación de las medidas y controles, según lo establecido en la LOPD y su desarrollo reglamentario, en cuanto a la organización del mismo, la metodología, el grupo propuesto y su estructura.

   Planteamiento, alcance y objetivo de la auditoria de las aplicaciones al ENS

ii. Plan de trabajo para el desarrollo del servicio

iii. Mecanismos para el control del proyecto. Actividades relacionadas con el control del proyecto, dado el elevado volumen de ficheros y la dispersión geográfica de los centros.

iv. Recursos técnicos. Detalle de la puesta a disposición de herramientas tecnológicas, en la medida en que contribuya eficazmente a la consecución de los objetivos del servicio objeto del contrato.

Madrid,

EL DIRECTOR GENERAL DE
SISTEMAS DE INFORMACIÓN SANITARIA

Firmado digitalmente por JOSE ANTONIO ALONSO ARRANZ
Organización: COMUNIDAD DE MADRID
Fecha: 2017.05.11 10:09:46 CEST
Huella dig.: 7031864e638ba0641a631fb6b5e6bb330a751c59

Fdo.: José Antonio Alonso Arranz