Servicio Madrileño de Salud
Dirección General de Sistemas
de Información Sanitaria

SaludMadrid

Comunidad de Madrid

Exp.: P.A. SER-5/2010-INF

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE REGIRÁN LA CONTRATACIÓN DE SERVICIOS DE DESPLIEGUE Y GESTIÓN DEL CENTRO DE SOPORTE ESPECIALIZADO Y RESPUESTA A INCIDENTES EN EL ÁREA DE SEGURIDAD DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN DEL SERVICIO MADRILEÑO DE SALUD (CESEAS-CERT)

Madrid, Mayo 2010

ÍNDICE

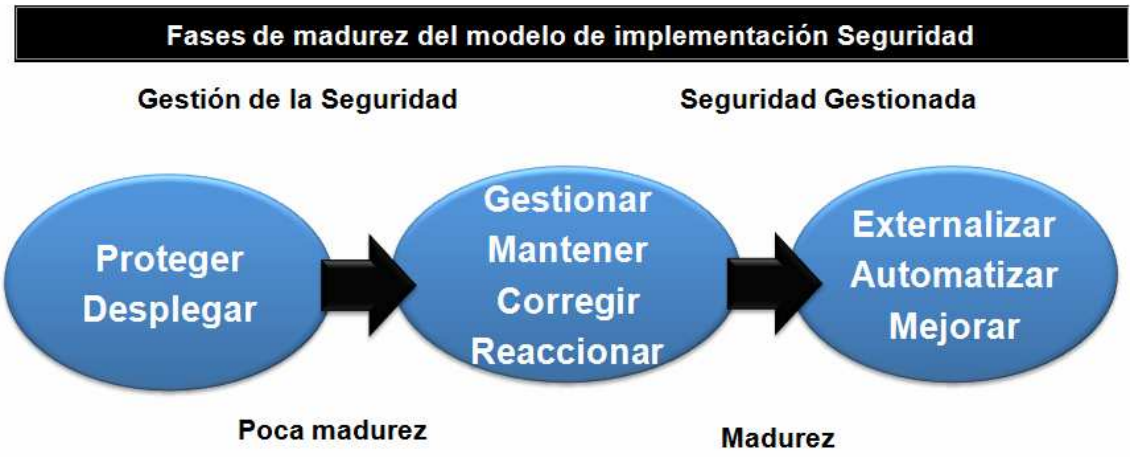
1. OBJETO DEL CONTRATO

El objeto del presente contrato es disponer de los Servicios de Despliegue y Gestión para la puesta en marcha y explotación del **Centro de Soporte especializado en el Área de Seguridad** de sistemas y tecnologías de la información del Servicio Madrileño de Salud (en adelante SERMAS), en la Consejería de Sanidad de la Comunidad de Madrid (CESEAS-CERT), gestionados desde la Dirección General de Sistemas de Información Sanitaria (en adelante DGSIS).

El CESEAS se constituirá como instrumento de prevención, detección, respuesta a amenazas e incidentes de seguridad, así como órgano responsable de la coordinación e implantación de políticas y medidas de seguridad de la organización, prestando a los diferentes centros dependientes de la Consejería de Sanidad, una serie de servicios tanto reactivos, como preventivos, con el objetivo de impulsar y dar soporte a la implantación de las medidas de seguridad por parte de dichos centros.

Se desea evolucionar el servicio de seguridad hacia un nuevo modelo, en el cual son fundamentales las siguientes premisas:

- **Orientación** hacia una seguridad gestionada
- **Integración** en el ciclo de vida de los proyectos de la DGSIS
- **Refuerzo** en el ámbito del cumplimiento normativo
- **Provisión** a los centros como un servicio, manteniendo siempre éstos un grado de autonomía suficiente para implantación de las medidas de seguridad
- **Gestión extremo a extremo** de elementos de seguridad en red
- **Alerta temprana** y prevención de incidentes y su respuesta protocolizada.



Para el desarrollo de este modelo de evolución desea contar con un servicio externalizado y especializado de asesoría técnica en materia de seguridad, de cuya contratación es objeto el presente pliego.

No está incluido ente los servicios de esta oficina la ejecución de proyectos de seguridad, ni las auditorías que prevé la actual legislación en materia de seguridad.

2. MARCO FUNCIONAL Y TECNOLÓGICO

2.1. Antecedentes

Tras los Decretos de 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 **(SERMAS)** y de 23/2008, de 3 de abril, del Consejo de Gobierno, por el que se establece la estructura orgánica del Servicio Madrileño de Salud, es la Dirección General de Sistemas de Información Sanitaria **(DGSIS)** la que, entre otras competencias, ostenta "El establecimiento de medidas de seguridad en el sistema sanitario público de la Comunidad de Madrid, de acuerdo con la normativa vigente de los ficheros automatizados que contengan datos de carácter personal, y la realización de auditorias en el ámbito de la protección de datos de carácter personal" y "La provisión y gestión de los bienes y servicios informáticos del Servicio Madrileño de Salud", todo ello sin perjuicio de las que correspondan a la Agencia de Informática y Comunicaciones de la Comunidad de Madrid en virtud de la Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas de la Comunidad de Madrid, y demás disposiciones aplicables. Sobre esta base se propone el expediente que se expone a continuación.

La amplia red asistencial del **SERMAS** conlleva la existencia de sistemas de información con una alta diversificación y heterogeneidad distribuidos en diferentes centros, por lo que se hace imprescindible disponer de los mecanismos adecuados para garantizar la seguridad en todos los ámbitos de actuación y con el máximo alcance.

La **DGSIS** dentro de su estructura organizativa cuenta con un Área específica cuyo cometido es la gestión de la seguridad de los sistemas de información en el ejercicio de sus competencias. En este marco de actuación y responsabilidad se plantea la contratación de los servicios de apoyo y soporte especializado en materia de seguridad y protección de datos que abarquen los Sistemas de Información que gestiona, a través del SERMAS-CERT. El contexto contractual incluirá también el soporte y apoyo en materia de seguridad en aquellos nuevos servicios que fruto de cualesquiera nuevas necesidades puedan surgir durante el periodo de ejecución contemplado en el presente pliego.

2.2. Objetivos

Los principales objetivos que se persiguen con la contratación de estos servicios pueden resumirse en los siguientes puntos:

- *Implantar un **modelo de servicio** de gestión de la seguridad alineado con las necesidades actuales de la Consejería de Sanidad.*
- *Prestar **apoyo experto** en materia de seguridad en los proyectos de desarrollo, mantenimiento y evolución de los sistemas de información que dan servicio a los entornos sanitarios de la Consejería de Sanidad de la Comunidad de Madrid.*
- *Mejorar las **medidas de seguridad** existentes y prestar **apoyo al desarrollo** de la función TIC.*
- ***Optimizar los costes** asociados a la gestión de la seguridad en el SERMAS.*
- *Disponer de **flexibilidad** ante necesidades no previstas.*
- *Disponer de una **visión global de la seguridad** del conjunto de la organización que permita trabajar de forma más eficiente, con mejor capacidad de respuesta y garantía de la continuidad del servicio.*

El adjudicatario, deberá tomar únicamente como referencia inicial las características y entornos del SERMAS, asumiendo que modificaciones en su estructura, organización o número de centros no supondrán una ampliación del servicio en caso de incremento de dichos parámetros.

Todas las actividades y servicios de seguridad comprendidos en el presente pliego técnico deberán estar orientados al cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica en su artículo 42.2, siendo el Adjudicatario el único responsable de garantizar dicho cumplimiento. El licitador podrá llevar a cabo auditorias escogidas de forma aleatoria para comprobar el cumplimiento de lo anteriormente escrito por parte del Adjudicatario.

2.3. Esquema Nacional de Seguridad

2.3.1. Introducción

Como parte de la Administración Pública, la Consejería de Sanidad de la Comunidad de Madrid (CSCM) está comprendida dentro del ámbito de aplicación que se establece en el Real Decreto 3/2010 que regula el Esquema Nacional de Seguridad para sus servicios de Administración Electrónica al que habrá que ajustarse.

2.3.2. Actuaciones

Por tanto, dentro de las actividades desempeñadas por el CESEAS-CERT, estará la la capacidad para llevar a cabo las siguientes actuaciones, enumeradas de modo no exhaustivo:

a) Determinar si el ámbito de acción de un proyecto se enmarca dentro del establecido para la aplicación del ENS, y que actuaciones proceden en este sentido.

b) Poder concretar el alcance que los requerimientos del ENS aplican a un determinado sistema de información.

c) Realizar una adecuada categorización de los sistemas existentes, de acuerdo a unos criterios de proporcionalidad razonables y mensurables, generados a partir de las directrices marcadas en el Anexo I del RD 3/2010.

d) Plasmar dicha categorización en la correspondiente declaración de aplicabilidad para el sistema o sistemas categorizados.

e) Efectuar los análisis de riesgos pertinentes, utilizando las metodologías y herramientas previamente acordadas con la DGSIS.

f) Proceder a realizar las evaluaciones y diagnósticos de la situación, siguiendo las directrices que fija el Anexo II del RD 3/2010, y apoyándose en estándares de seguridad y guías de buenas prácticas de reconocido prestigio a nivel mundial, tanto en el sector público como en el privado.

g) Identificar dentro del sistema la existencia de tratamientos de datos personales a los que haya de aplicar la legislación de Protección de Datos.

h) Establecer las recomendaciones que se consideren oportunas y convenientes, con el fin de cumplir los objetivos de adecuación al ENS, de cara a lograr un sistema de gestión de la seguridad de la información que se ajuste a las necesidades y exigencias requeridas.

i) Formalizar esas recomendaciones en el plan o los planes de acción necesarios.

j) Poder llevar a cabo tareas de gestión, o de apoyo y consultoría, durante la fase de implantación del plan o planes de acción.

k) Efectuar auditorias periódicas de aquellos sistemas que tengan ya implantado el ENS, elaborando los informes correspondientes, que serán elevados a la DGSIS.

3. ALCANCE Y PLAZO DE EJECUCIÓN

El adjudicatario del presente concurso deberá proporcionar el servicio de **Soporte especializado en el Área de Seguridad**, bajo la dirección de la DGSIS, realizando las actuaciones de prevención y resolución que se requieran como consecuencia de la implantación y evolución de las políticas e iniciativas de seguridad formuladas por el Servicio Madrileño de Salud de la Consejería de Sanidad.

Ello, sin perjuicio de eventuales modificaciones derivadas de cambios normativos, estructurales, o requerimientos del SERMAS, se consideran prioritarios los ámbitos de actuación que se citan, a título ilustrativo, en el siguiente capítulo.

El **plazo de ejecución** del contrato abarca desde la fecha de formalización hasta la finalización de las tareas objeto del mismo, tendentes a su puesta en producción y el servicio continuado durante un total de **24 meses** desde su firma.

Los servicios recogidos en el presente contrato serán prestados en **horario de 24 horas**, especialmente para las tareas de monitorización de servicios y equipamiento y tanto en las dependencias del adjudicatario como en las de cualquier centro dependiente de la Consejería de Sanidad, conforme mejor convenga a las necesidades de ésta.

Podrán usar herramientas tecnológicas, dispositivos de detección, licencias de software de monitorización o cualquier tipo de componente, plataforma o dispositivo necesario para la provisión de cualquier servicio solicitado por el SERMAS que correrán siempre por cuenta del adjudicatario.

Cualquier documento solicitado, alerta de vulnerabilidad o informe de cualquier tipo solicitado por el SERMAS, se deberá proporcionar en idioma castellano y en un formato de presentación conforme a las características de la identidad institucional (cabeceras, gráficos, logos) del SERMAS.

Cualquier elemento imprescindible software o hardware suministrado por el adjudicatario para la prestación del servicio, pasará a ser propiedad del SERMAS a la finalización del contrato, o se asegurará la continuidad del uso del mismo (para soluciones abiertas). El adjudicatario deberá presentar en cualquier momento que le sea solicitado:

- Información detallada de arquitectura desplegada.
- Configuraciones de servicios y dispositivos
- Recomendaciones para la continuidad del servicio
- Procesos y procedimientos operativos necesarios para poder continuar con los servicios desplegados
- Formación que le sea requerida para una adecuada transferencia de conocimiento
- Cualquier otra información que le sea solicitada

Las empresas licitadoras presentarán un compromiso de niveles de servicio y plazos de despliegue comprometidos, que serán evaluados conforme mejor se ajusten a los intereses del SERMAS.

4. SERVICIOS REQUERIDOS

4.1. Descripción general

La Consejería de Sanidad, considera que el modelo de evolución debe de estructurarse en base a cinco unidades de gestión de la seguridad, en torno a cuya actuación se desplegarán los servicios del CESEAS:

Unidad de Planificación y gestión de la seguridad:

Su objetivo es la gestión y seguimiento de la seguridad TIC en la Consejería de Sanidad. Será la responsable de la coordinación de la estrategia, así como del control de la calidad de los servicios prestados.

Comprende actividades tales como:

- Coordinación de las diferentes Unidades
- Gestión y seguimiento del Plan Director de Seguridad Lógica
- Diseño nuevos servicios de seguridad
- Cuadro de Mando de Seguridad
- Seguimiento de Incidencias
- Modelo de Gestión de Activos
- Análisis de Riesgos
- Seguimiento de Tendencias
- Comité Estratégico de Seguridad
- Gobierno y monitorización del estado de la seguridad del SERMAS mediante consola única.

Unidad de cumplimiento normativo

Su objetivo es el desarrollo de actividades orientadas a la supervisión y apoyo al cumplimiento de la legislación vigente en materia de protección de datos, desarrollo de normativa interna, así como actividades de carácter general para comunicación y concienciación.

Comprende actividades tales como:

- Definición de políticas y procedimientos y desarrollo cuerpo Normativo
- Formación, concienciación y sensibilización en materia de Seguridad
- Plan de Comunicación en materia de seguridad
- Definición de estándares
- Certificación procedimientos
- Auditorías de cumplimiento Normativo
- Gestión derechos ARCO
- Comité de Cumplimiento Normativo

Unidad de implantación y continuidad de servicio

Su objetivo es la realización de actividades de apoyo a los centros y diferentes unidades organizativas de la Consejería para la implantación de medidas de seguridad

Comprende actividades tales como:

- Implantación y supervisión de medidas de seguridad
- Diseño Arquitectura Procesos de Seguridad
- Desarrollo de estándares
- Securización de entornos
- Auditorías técnicas
- Supervisión del sistema de seguridad
- Gestión de cortafuegos
- Gestión IDS/ISP
- Gestión seguridad en comunicaciones: RAS, VPN, Wifi
- Gestión PKI
- Gestión configuración seguridad SSOO
- Análisis de estrategias de recuperación y desarrollo de planes de continuidad del servicio continuidad del servicio (criterios, estrategias para puestos de trabajo, estrategias tecnológicas que afecten al almacenaje, comunicaciones, aplicaciones, servidores...).
- Comité de Continuidad del Servicio

Unidad de desarrollo y gestión de proyectos de seguridad

Su objetivo es la realización de actividades de asesoramiento y apoyo a los distintos proyectos e iniciativas de la Consejería de Sanidad, en coordinación con las distintas unidades organizativa (MEDAS, Oficinas Técnicas de Proyectos).

Comprende actividades tales como:

- Modelo de Seguridad en el Ciclo de Vida de Desarrollo
- Requerimientos de Autenticación y acceso a los sistemas
- Especificación de requerimientos de respaldo y recuperación para las aplicaciones
- Homologación de Tecnologías y Aplicaciones
- Análisis de Viabilidad Técnica
- Pruebas de seguridad y hacking ético (Coordinación)
- Comité Seguridad Lógica (pendiente de creación)
- Comité de Infraestructuras Corporativas pendiente de creación)

Unidad de Operaciones

Su objetivo es la realización de actividades de monitorización y respuesta a incidentes, así como provisión de servicios bajo demanda.

Comprende actividades tales como:

- Prevención y alerta temprana
- Gestión de incidentes de seguridad:
  - Respuesta a incidentes
  - Actuaciones de continuidad del servicio
  - Análisis Forense
- Monitorización del estado de la seguridad
  - Monitorización de dispositivos
  - Cumplimiento políticas
  - Análisis de vulnerabilidades
- Gestión de la configuración de dispositivos de seguridad
- Servicios adicionales que puedan prestarse de forma externalizada, tales como:
  - Revisión de código fuente
  - Gestión y correlación de logs de dispositivos
  - Aplicación de parches para corrección de vulnerabilidades
  - Soporte especializado in-situ bajo demanda

Para ello el proveedor ofertará una plataforma de monitorización que deberá incluir el suministro de equipos necesarios para su funcionamiento, licencias y servicios para la puesta en marcha, administración y mantenimiento. Deberá de proveerse de una consola única que permita definir políticas y métricas de riesgo, y disponer de un interfaz de alto nivel con posibilidad de obtener informes de seguridad y gestionar incidencias.

Esta plataforma incluirá módulos, incluyendo los elementos de hardware y software necesarios para su funcionamiento (correlación de logs, etc), con al menos las siguientes funcionalidades:

- IDS, o sistema de detección de intrusos
- Detección de anomalías
- HIDS – Host IDS
- Escáner de vulnerabilidades
- Monitor de uso de la red
- Monitor de disponibilidad de servicios
- Sistema de inventariado automático
- Detector de ataques de nivel 2
- Analizador forense

La plataforma deberá poder recibir eventos de dispositivos comerciales y de aplicativos desarrollados a medida, adaptándose a sus características y sin requerir su modificación. La solución propuesta deberá de disponer de una arquitectura, en alta disponibilidad y tolerante a fallos, que suministre al menos los siguientes elementos:

- Sensores recolectores
- Servidores de gestión

- Base de datos
- Consola web

Cualquier plataforma, dispositivo, necesario para la prestación del servicio podrá ser desplegado en las instalaciones del SERMAS o del adjudicatario, conforme mejor convenga a las necesidades del SERMAS.

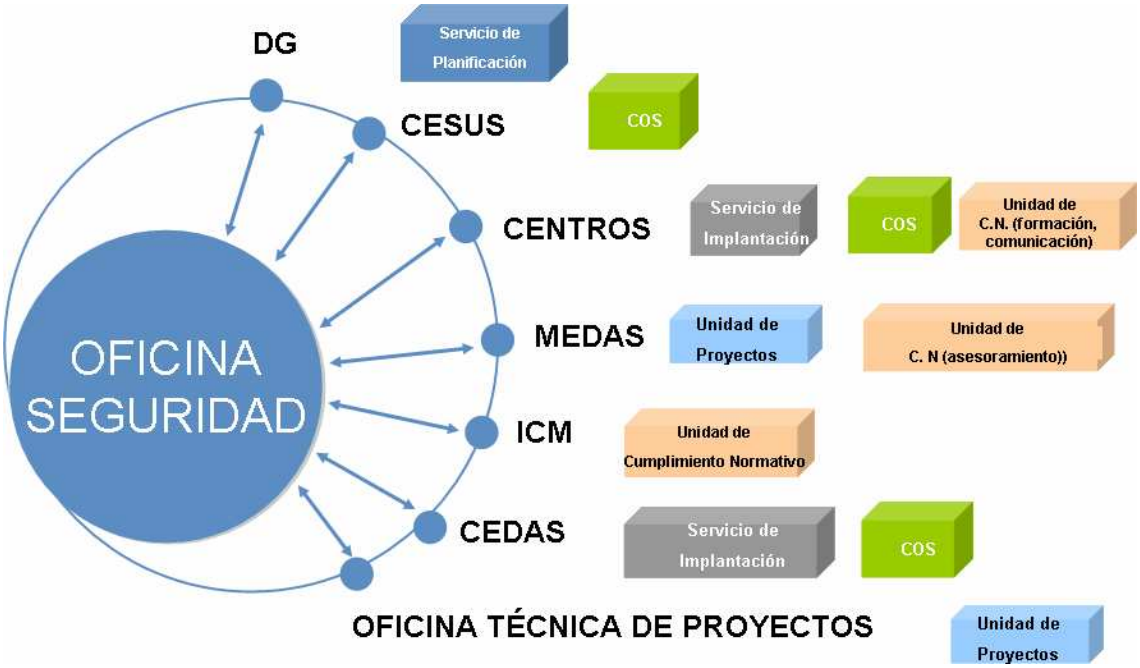
La plataforma desplegada para la recolección de eventos de seguridad, realizará la correlación con otras fuentes de información y generará alertas de seguridad en base a los requisitos establecidos por el SERMAS, que serán al menos los siguientes:

- Capacidad de monitorización de dispositivos de seguridad, elementos de electrónica de red y servidores del SERMAS, mostrando la información de manera integrada.
- Capacidad de generar alertas sobre comportamientos anómalos de cualquier dispositivo
- Permitir correlación de diferentes fuentes de información, como por ejemplo escaneo de vulnerabilidades, eventos de servidores de datos o dispositivos de seguridad e inventario de activos.
- Capacidad para implementar distintos enfoques de correlación.
- Facilidad de integración con distintas tecnologías fuente de eventos.
- Reglas de búsqueda de anomalías y de respuesta ante eventos, permitiendo respuestas automáticas ante determinados tipos de alarmas.
- Capacidad para ejecutar análisis de vulnerabilidades programados o bajo demanda, presentando informes sobre puntos débiles, recomendaciones, específicos para cada elemento analizado, y personalizados conforme a las especificaciones especificadas por el SERMAS.

<u>Otras unidades con inter-relación</u>

La implantación del nuevo modelo de seguridad en la Consejería, debe de contemplar la participación e integración de los distintos agentes:

- CESUS: Centro de atención a usuarios.
- CGR: Centro de Gestión de Red.
- CEDAS: Centro de proceso de datos y su Grupo de Gestión de Seguridad(CGS).
- Oficinas de proyectos en los distintos ámbitos (primaria, hospitales, otros).
- MEDAS: Centro de desarrollo de aplicaciones.
- Responsable de informática de los distintos centros
- ICM: Agencia de Informática y Comunicaciones de la Comunidad de Madrid



4.2. Recursos humanos y técnicos

El equipo de trabajo que la empresa adjudicataria dispondrá para la prestación del servicio, se compondrá de un núcleo estable que cada licitador deberá dimensionar de acuerdo a su mejor oferta y un conjunto de profesionales multidisciplinar (jurídico, técnico y de gestión de proyectos) en materia de seguridad para ofrecer los distintos servicios que se precisen bajo demanda.

La CSCM se reserva el derecho de efectuar todas las consultas que considere necesarias para comprobar y clarificar la veracidad de los historiales profesionales presentados en la oferta para la evaluación de la misma. La constatación fehaciente de datos que desvirtúen la realidad supondrá la exclusión de la oferta.

A estos efectos, se establecen los siguientes equipos:

Equipo estable de seguridad

Se considera un equipo mínimo de trabajo que durante el año 2010 se compondría de 5 personas, durante el año 2011 el equipo pasaría a ser de 9 personas y en el año 2012 de 11 personas, con una dedicación base de cada perfil de1760 horas anuales. Siendo a criterio de los licitadores ofrecer su propuesta argumentada de mejora.

Los perfiles se describen a continuación:

- **Perfil Jefe de equipo**:
  - Titulación mínima universitaria de grado superior.
  - Certificaciones mínimas reconocidas en el campo de la seguridad:
    - Titulación en sistemas de gestión en seguridad de la información de entidades reconocidas (AENOR, ISACA u otras)
  - Experiencia acreditada mínima:
    - 5 años con categoría de jefe de equipo

- 7 años acumulando las categorías de Consultor Estratégico y Consultor Senior.

Acreditará además al menos dos años de experiencia en el ámbito sanitario y al menos uno en materias de protección de datos.

- **Perfil Consultor Senior, especialista en protección de datos**:
  - Titulación mínima universitaria en derecho.
  - Experiencia acreditada mínima:
    - 6 años como especialista en el ámbito de asesoría legal en protección de datos
    - 2 años de experiencia en el ámbito sanitario

  Acreditará además al menos dos años de experiencia en cualquier ámbito que incluya datos del más alto nivel de protección.

- **Perfil de Consultor Senior, especialista en desarrollo de proyectos y sistemas de seguridad**:
  - Titulación mínima universitaria de grado superior en materias TIC (Informática o Telecomunicaciones).
  - Debe aportar certificaciones reconocidas en el campo de metodologías de desarrollo de sistemas de información y de sistemas de seguridad.
  - Experiencia acreditada mínima:
    - 3 años con categoría de Consultor Senior o 5 años acumulando las categorías de Consultor Senior y Consultor.

  Se trata de especialistas expertos tanto en la especificación, como en la implantación e instalaciones de sistemas de información, como en la definición de funcionalidades y requisitos de seguridad de dichos sistemas. Además se valorarán los conocimientos y formación en la especificación de requisitos e instalación y administración de servidores de Bases de datos corporativas, de aplicaciones (J2EE o .net), a sistemas web, tanto de forma exclusiva como en servidores virtualizados.

- **Perfil de Consultor Técnico Senior, especialista en centros de proceso de datos:**
  - Titulación mínima universitaria de grado superior en materias TIC (Informática o Telecomunicaciones).
  - Debe aportar certificaciones reconocidas en el campo de la administración de sistemas de información.
  - Experiencia acreditada mínima:
    - 3 años con categoría de Consultor Senior o 5 años acumulando las categorías de Consultor Senior y Consultor.

  Se trata de especialistas expertos las tecnologías relacionadas a centros de proceso de datos, tanto de aspectos de diseño óptimo de los servicios a alojar, como físicos de las instalaciones (arquitectura, situación, dotación, climatización, medidas contra el fuego, etc.), con especial énfasis a la seguridad y al ahorro de energía. Por último, se valorará casos de éxito de implantación de almacenamiento centralizado, conexiones de almacenamiento entre varias sedes, mecanismos de back-up y restauración centralizados y virtualizados, etc.

- **Perfil de Consultor Técnico Senior, especialista en comunicaciones:**
  - Titulación mínima universitaria de grado superior en materias TIC (Telecomunicaciones o Informática).

- Debe aportar certificaciones reconocidas en el campo de las comunicaciones y sistemas de seguridad asociados.
- Experiencia acreditada mínima:
  - 3 años con categoría de Consultor Senior o 5 años acumulando las categorías de Consultor Senior y Consultor.

Se trata de especialistas expertos en comunicaciones en redes Wan y LAN's, con experiencia en redes de alta capacidad con más de 50 nodos. Se valorará conocimiento de tecnologías base (protocolos), relacionados con TCP/IP, sobre su seguridad, así como de instalación de servicios base de red: DNS's, correo, LDAP's, DHCP, proxy's, http, web-services, etc. Se deberá igualmente acreditar conocimientos del mercado de equipamiento y soluciones de este tipo de tecnologías. De forma específica se considerarán los conocimientos o experiencias previas de instalación de sistemas de gestión de red: SNMP, RMON, etc, así como de herramientas de comunicaciones: sistemas de correo, de mensajería instantánea, presencia, de video-conferencia, video-colaboración, etc.

Equipo de apoyo para servicios específicos

El adjudicatario indicará de forma expresa dentro de su propuesta la cantidad de jornadas que ofrece para actuaciones no planificadas, mediante un equipo de apoyo de profesionales con perfil similar a los anteriores o adicionalmente con perfil y experiencia en al menos las materias demandadas, valorándose el estar en posesión de certificaciones reconocidas en cada campo.

El número de jornadas y perfiles será evaluado de forma conjunta dentro del criterio de adjudicación "Valoración del equipo de trabajo".

Si por las razones que fuera, tales como un incidente de seguridad, pudiera existir la necesidad de realizar trabajos fuera del horario habitual, en sábados o festivos, o en régimen de nocturnidad, el SERMAS no aceptará sobre-costes adicionales por estas circunstancias, que deberán ser absorbidos siempre por el contratista.

La ubicación de los integrantes del equipo de trabajo será tanto en las oficinas de la DGSIS u otros centros del SERMAS como en las del proveedor, conforme mejor responda a los intereses del SERMAS y con posibilidad de modificarse a lo largo de la prestación del servicio.

Además el adjudicatario deberá en todo momento poder garantizar los recursos humanos que satisfagan la demanda de requerimientos que se tenga durante la vigencia del contrato. En concreto, la ubicación del equipo estable será en las oficinas de la DGSIS-SERMAS, tanto en sus actuales ubicaciones como en otras posibles ubicaciones futuras, sin perjuicio de que tengan disponibilidad para desplazarse a los distintos centros dependientes del SERMAS.

Los medios de trabajo necesarios, tales como, ordenador personal, licencias software ofimático, etc. para el personal adscrito a la prestación del servicio correrán a cargo de la empresa adjudicataria.

Equipo de monitorización

Además de los equipos anteriores, el adjudicatario deberá asegurar la monitorización y el escalado de incidencias propias de nuestra red o debidas a agentes u ataques externos en horario de 24 horas, por un grupo específico y especializado.

4.3. Otras prestaciones a realizar

Además del detalle de los servicios y objetivos ya mencionados anteriormente, y sin perjuicio de ulteriores modificaciones derivadas de cambios normativos, estructurales, o requerimientos de la CSCM, se deben considerar prioritarios ciertos ámbitos de actuación, como los que se citan:

- Análisis de activos y de riesgos periódicos, que permitan identificar riesgos relevantes y medidas de seguridad implementadas para mitigarlos.
- Coordinación en la implementación de medidas para permitir la máxima homogeneidad posible en los centros dependientes de la CSCM.
- Control, alimentación y mejora constante del cuadro de mando integral de seguridad.
- Soporte a la gestión de identidades.
- Mantenimiento del Portal institucional de Seguridad.
- Soporte a la implantación de la Ley de Administración electrónica y mejora continua de los procesos contemplados en ella. Soporte a la implantación tecnológica del uso del DNIe y certificados digitales por los ciudadanos y profesionales.
- Adecuación progresiva de ficheros manuales.
- Soporte a los centros en la realización de las Auditorías legales.
- Validación de requisitos de seguridad en sistemas en producción y en sistemas de nueva creación, colaborando en su ciclo de vida completo.
- Soporte en el tratamiento y resolución de incidentes de seguridad, pruebas de intrusión, hacking ético, etc.
- Formación y concienciación constante a los profesionales, para incorporar buenas prácticas en seguridad.

En relación a las actuaciones derivadas de la aplicación del Esquema Nacional de Seguridad, el equipo de trabajo debe reunir conocimientos en las siguientes materias:

- Aplicación, en la práctica, de los fundamentos para la determinación de la categoría de un sistema, así como de la selección y aplicación de medidas de seguridad, de acuerdo a lo que establece el ENS.
- Metodologías para el análisis de riesgos en el ámbito de la Seguridad de la Información y de las TIC.
- Herramientas de apoyo al análisis de riesgos.
- Familia de normas ISO/IEC 27000, para la Gestión de la Seguridad de la Información y las buenas prácticas en la materia, así como los específicos para el ámbito de la Sanidad que puedan publicarse.
- Realización de auditorías técnicas, basadas en los estándares al respecto, como la ISO 17021 y la ISO 27015.
- Tecnologías y soluciones de firma electrónica.

- Conocimientos generales en materia de Derecho aplicado a las TIC, y específicos en los siguientes apartados:
    - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los datos de carácter personal.
    - Ley 59/2003, de 19 de diciembre, de firma electrónica.
    - Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
    - Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

- Real Decreto 1720/2007 de desarrollo de la LOPD
- Real Decreto 4/2010 Esquema Nacional de Interoperabilidad
- Ley 41/2002 Básica reguladora de la Autonomía del Paciente
- Así como de las resoluciones e instrucciones de la A.E.P.D. y de la A.P.D.C.M.

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 adjudicatario. La empresa adjudicataria 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.

Independientemente de las actas de reuniones o informes de seguimiento que se soliciten por la DGSIS en cualquier momento, el seguimiento del servicio se realizará mediante un conjunto de indicadores estructurados en un cuadro de mando que será provisionado por el adjudicatario (a menos que la DGSIS indique lo contrario), consolidando la información de seguridad proporcionada desde los distintos proyectos y ámbitos de actuación.

Como resultado de la realización de estas actividades, los sistemas de información de la DGSIS deberán mantener el nivel de seguridad acorde a los requisitos establecidos en el marco jurídico y en la normativa que le aplica.

Los estándares de calidad de servicio a prestar serán evaluados mensualmente, al menos a través de los siguientes indicadores, pudiendo ser ampliados durante la prestación de los trabajos:

DESCRIPCIÓN	VALOR MENSUAL
Número de actuaciones sobre modificaciones de ficheros hechas por el equipo prestador del servicio (*)	10
Número de sistemas revisados dentro de la actividad de medidas de seguridad (y por tanto, que disponen de una definición o mejora de requisitos de seguridad) por el equipo de trabajo (*)	3
Número de recomendaciones de seguridad bimestrales emitidas por el equipo de trabajo (*)	10
Periodo de actualización del Portal Institucional de Seguridad y Protección de Datos	Semanal (mensual junio-julio-agosto)
Tiempo de respuesta del equipo de trabajo o apoyo ante peticiones	Máx. 12h (L-V de 9 a 18h; Resto 60h)
Número de actuaciones que incumplen los acuerdos de nivel de servicio aceptados	0
Porcentaje o número de revisiones de las políticas de seguridad, sobre las que se ha hecho seguimiento, se ha revisado su cumplimiento, o han sido aprobadas o modificadas	10
Número de cursos impartidos o de empleados formados en seguridad de la Información.	1/20

Número de comunicaciones del equipo de trabajo relativas a iniciativas de concienciación de la Seguridad.	3
Porcentaje de incidentes de seguridad que han tenido una actuación por parte del equipo de trabajo.	95%
Número de no conformidades en los informes de auditoría legales.	< 5
Número de no conformidades en los informes de auditoría de calidad sobre el servicio prestado.	< 2
Retraso en la entrega de los informes, trabajos o actividades requeridas.	< 2 días

(*) El nivel mensual de cumplimiento establecido es el que permite alcanzar el objetivo global para todo el período de contrato. La DGSIS podrá autorizar una planificación de los trabajos en periodos diferentes al mensual, lo que podrá afectar al cumplimiento mensual del servicio, pero siempre manteniendo el cumplimiento global.

6. CALENDARIO DE EJECUCIÓN REQUERIDO

6.1. Plazo de ejecución y horario del servicio

La prestación de los servicios se realizará durante un periodo de **2 años**, asegurando los mismos durante 24 horas al día, 7 días a la semana y 365 días al año.

La composición básica del equipo debe tener flexibilidad, de forma que ante determinadas circunstancias, la DGSIS pueda modificar el programa de trabajo y requerir un mayor número de personas asignadas al proyecto.

6.2. Planificación

Los trabajos se desarrollarán en las fases siguientes:

- **FASE I, periodo de transición:** A su vez se deben tener en cuenta dos etapas: **Los primeros 30 días desde el inicio de los trabajos**. Constitución del equipo de trabajo, identificación de las tareas inmediatas a realizar y suministro por parte del Director de Proyecto de la DGSIS de toda la información relativa para establecer el marco de trabajo. En este periodo en adjudicatario deberá tomar el total control del servicio, en las facetas de asesoría y coordinación de proyectos. Después se contará con un mes y medio adicional para la preparación y despliegue de todos los elementos de monitorización que se requieran. Esta fase se ejecutará durante el ejercicio 2010 y requerirá la presencia de un jefe de proyecto y de 5 consultores dedicados.
- **FASE II**, **periodo de ejecución estable**: Desde el final de la Fase 1, anterior, y hasta un mes y medio antes de la finalización del contrato. Además esta fase incluye dos periodos diferenciados en el número de recursos asignados: Durante el ejercicio 2011: funcionamiento a pleno rendimiento del equipo de trabajo completamente integrado con la estructura organizativa del SERMAS y disposición de un grupo añadido de otros cuatro consultores para labores de monitorización y despliegue de proyectos. Y durante los 8 primeros meses de 2012, cuando se considera imprescindible contar con dos consultores más dedicados a labores de mejora continua que eviten los incidentes detectados en fases anteriores.
- **FASE III**: durante el último mes y medio del ejercicio 2012, para la preparación de la **transferencia de conocimiento** y actividades para la renovación de los servicios: relación de actividades cerradas y en curso. Para este periodo se deberá contar con la continuidad de los 11 consultores previos, junto con el responsable de la oficina, aunque con dedicaciones específicas que faciliten dicha transferencia.

En cuanto a anualidades, la disposición del mínimo de técnicos por perfil será:

Unidad /Actividades	Recursos → Dedicación		
	2010	2011	2012
Planificación ▪ Coordinación unidades ▪ Cuadro de Mando ▪ Gestión PDS ▪ Dirección Proyectos Troncales ▪ Coordinación Comités	1 → 100%	1 → 100%	1 → 100%
Cumplimiento ▪ Gestión auditorias ▪ Soporte especializado ▪ Desarrollo Cuerpo Normativo	2 →100% 1 →50%	2 →100%	2 →100%
Unidad de implantación y continuidad ▪ Soporte al PDS en los centros ▪ AARR ▪ Desarrollo Planes de contingencia ▪ Gestión proyectos de implantación de medidas de contingencia y/o continuidad	1→100% 1→50%	4 →100%	4 →100%
Unidad de proyectos ▪ Revisión de aspectos de seguridad en sistemas/proyectos críticos ▪ Revisión de seguridad en sistemas/ proyectos existentes ▪ Gestión SCV nuevos sistemas/proyectos	1 →100%	2 →100% 1 →50%	3→100%
Unidad de operaciones ▪ Despliegue del catálogo de servicios ▪ Operación de servicios ▪ Seguimiento ANS y supervisión	0	1 →50%	2 →100%
Total	**6**	**10**	**12**

Las especialidades de los consultores se podrán modificar a lo largo del contrato, con avisos previos de un mínimo de 15 días.

En la primera quincena de cada mes se presentará a la DGSIS la consolidación de los indicadores correspondientes al mes previo y las recomendaciones para el siguiente período derivadas de los niveles alcanzados.

6.3. Dirección y seguimiento de los trabajos

Corresponde a la DGSIS-SERMAS dirigir y supervisar los trabajos y velar por el cumplimiento de los niveles de servicio acordados. En este sentido, la DGSIS-SERMAS 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 licitador designará un Responsable de Proyecto ante la DGSIS, al margen del equipo estable, y perteneciente al equipo directivo de su organización. Este Responsable se encontrará en permanente contacto con el personal de la DGSIS-SERMAS 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-SERMAS de las posibles incidencias y seguimiento o desviaciones de plazos.
- Mensualmente remitir a la DGSIS-SERMAS 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-SERMAS una reunión de seguimiento del servicio prestado en el mes previo y validación de la propuesta para el mes siguiente a la misma.

6.4. Modificaciones en el equipo de trabajo

El equipo humano del adjudicatario que se incorporará tras la formalización del contrato para la ejecución de los trabajos deberá estar formado por los mismos componentes relacionados en la oferta, incluso durante el periodo vacacional que se deberá cubrir de forma adecuada estableciendo los turnos necesarios entre las personas que conforman el equipo de trabajo.

Durante el periodo de vigencia del contrato de prestación, la empresa deberá garantizar la permanencia de los recursos que forman parte del núcleo del equipo de trabajo propuesto.

Cualquier modificación en los integrantes del equipo de trabajo aprobado requerirá la aprobación de DGSIS-CSCM quien se reserva el derecho de rechazar la incorporación al equipo de trabajo de aquellas personas que, a su juicio, no estén en posesión de las capacidades requeridas para la ejecución del contrato. 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.

La empresa deberá notificar esta circunstancia, al menos con 15 días de antelación a la partida del recurso. En este caso, la empresa deberá reponer el recurso, con perfil y nivel de conocimiento equivalente o superior al recurso saliente. Durante al menos 10 días laborables, la empresa deberá simultanear los dos recursos, saliente y entrante, a efectos de traspaso de conocimientos del proyecto en el que se encontraba ubicado el recurso saliente, sin coste adicional para la CSCM (facturando un solo recurso).

La DGSIS-CSCM se reserva el derecho de rechazar en cualquier momento, a las personas del equipo de trabajo que, a su juicio, no estén en posesión de las capacidades requeridas para la ejecución del contrato. Este cambio se solicitará por el Director de Proyecto que haya designado la CSCM, a través de las reuniones de Seguimiento, garantizando al adjudicatario 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 produzcan estas modificaciones en los equipos, se requerirá un solapamiento del personal durante un periodo mínimo de 10 días laborables.

Durante todo el plazo de ejecución, el adjudicatario 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 adjudicatario 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.

7. CONDICIONES GENERALES

7.1. Propiedad de los trabajos

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

El adjudicatario 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 de la DGSIS.

7.2. Certificaciones

Al objeto de justificar la conformidad del licitador con normas de garantía de calidad de que disponga, se aportarán los certificados de garantía de calidad basados en la serie de normas internacionales ISO 9000, europeas EN 29000 o españolas UNE 66900 y expedidos por organismos conformes con la serie de normas europeas EN 45000.

Igualmente, se tendrán en cuenta certificados de calidad equivalentes expedidos por otros organismos de normalización establecidos en cualquier Estado Miembro de la Unión Europea. En defecto de los certificados anteriores el licitador aportará pruebas de medida equivalentes de control de calidad.

Asimismo y dado el ámbito de seguridad de la información de los trabajos a realizar se aportará Certificación del Sistema de Gestión de la Seguridad de la Información de la empresa según ISO 27001, ISO 20000 de Gestión de Procesos y UNE-EN-ISO 14001:2004 de Gestión Medioambiental.

7.3. Calidad de los trabajos

Los estándares de calidad de servicio a prestar serán evaluados mensualmente, al menos a través de los indicadores reflejados en el apartado **5.1.** No obstante lo anterior, durante el desarrollo de los trabajos, la DGSIS-SERMAS podrá establecer controles de calidad y acciones de aseguramiento de la calidad de la actividad desarrollada.

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

7.4. Normativa de seguridad y protección de datos

El adjudicatario se compromete a cumplir las medidas y requisitos de seguridad exigidos por la CSCM. El coste de las actuaciones de cualquier tipo, incluidas las auditorías,

derivadas del cumplimiento de la LOPD y normativa relacionada, serán por cuenta del adjudicatario.

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 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid
- 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.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (RDLOPD).
- 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.

7.4.1. Encargado de tratamiento

El adjudicatario, 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 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. 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 Ley Orgánica 15/1999, 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 adjudicatario, serán recogidas en un documento específico que será firmado por el adjudicatario 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 citada Ley Orgánica 15/1999, 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.

7.4.2. 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.

7.4.3. Medidas de seguridad.

No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por el R.D. 1720/2007 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 adjudicatario, 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 adjudicatario, 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 Ley Orgánica 15/1999 regulan su acceso como encargado del tratamiento de los ficheros de datos de carácter personal.
- El adjudicatario 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 RD 1720/2007, de 11 de junio.
- 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 adjudicatario habilitar mecanismos y procedimientos que faciliten el ejercicio de estos derechos.
- La documentación se entregará al adjudicatario para el exclusivo fin de la realización de las tareas objeto de este contrato, quedando prohibido para el adjudicatario 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 adjudicatario 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 auditoria 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 adjudicatario, 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 Dirección General de Sistemas de Información Sanitaria del Servicio Madrileño de Salud, perteneciente a la CSCM, 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 RD 1720/2007, 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 con el artículo 21 del RDLOPD, 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 la estipulación cuarta de las presentes cláusulas;
- 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.

El Responsable de la contratación por parte del adjudicatario deberá comunicar a la Agencia de Protección de Datos de la Comunidad de Madrid cualquier contrato que celebre y que incluya el tratamiento de datos de carácter personal por parte de un tercero, con anterioridad a la firma del mismo

- 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 adjudicatario deberán proporcionar mecanismos que permitan la extracción de datos de forma disociada, conforme a lo contemplado en esta materia en el RD 1720/2007, sea requerido.

De conformidad con el art. 22 del RDLOPD, 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 Dirección General de Sistemas de Información Sanitaria del Servicio Madrileño de Salud, 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.

7.4.4. 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.

7.4.5. 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 Ley Orgánica 15/1999 y en el RD 1720/2007.

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.

7.4.6. 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.

7.5. Cesión del contrato

El Adjudicatario 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.

8. DOCUMENTACIÓN TÉCNICA DE LAS OFERTAS

Los licitadores deberán presentar y argumentar en sus ofertas el modelo de evolución que consideran más adecuado en función de nuestras características particulares. El modelo propuesto por el licitador, debe contemplar las interacciones entre las distintas unidades que se mencionan, siendo altamente valorable que no sean planteados modelos generalistas sin una adecuada particularización a las características del SERMAS.

Las empresas licitadoras deberán presentar con un adecuado nivel de detalle una Cartera de Servicios a prestar desde el SERMAS-CERT, junto con un plan para el despliegue de los servicios ofertados.

En la memoria técnica de la oferta 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.

La memoria contendrá una planificación temporal pormenorizada de todas las tareas, así como la composición de los equipos de trabajos que se oferten.

Con el fin de facilitar la valoración de las ofertas presentadas, estas deberán estructurarse **OBLIGATORIAMENTE** bajo riesgo de exclusión, de acuerdo al siguiente índice y contenido:

a. Índice.

b. Características generales.

i. Identificación de la oferta y persona de contacto
ii. Acatamiento con carácter general de las condiciones del pliego

c. Características del servicio.

i. Planteamiento general para la prestación del servicio solicitado, describiendo la visión del ofertante sobre el servicio a realizar en base a su conocimiento y/o experiencia en trabajos similares y el retorno y beneficios que recibirá la SERMAS.
ii. Organización del servicio, describiendo en detalle el modelo de trabajo propuesto y el grado de involucración / participación del personal de la SERMAS.
iii. Metodología para la prestación de los servicios
iv. Mecanismos para asegurar la calidad y seguridad en la prestación del servicios
v. Planificación detallada de los trabajos a realizar desglosando tareas e hitos a cumplir. La información aportada deberá incluir:
    - Procedimiento y metodología propuestos para el servicio de Gestión y Soporte Especializado en seguridad a proyectos tecnológicos de nueva creación y para sistemas en producción.
    - Propuesta de cuadro de mando para el seguimiento del servicio de Gestión y Soporte Especializado en Seguridad.
    - Plan de devolución del servicio a la finalización del contrato para garantizar la transferencia del servicio a un eventual nuevo proveedor, sin impactar en los niveles del servicio prestado.

d. Equipo técnico.

i. Dimensionamiento y perfiles del equipo de trabajo propuesto con la relación nominal de los componentes del equipo, incluyendo tanto el Director como los equipos estables y de apoyo continuado. Se deben adjuntar los Currículum Vitae de las personas que forman tanto el núcleo estable del servicio como del personal que participará en la prestación del mismo dando apoyo continuado, especificando unidad de ubicación del modelo y dedicación.

   En este apartado NO se incluirá ninguna información relativa a las mejoras en cuanto al mayor número de recursos humanos asignados al proyecto, que se detallarán en el apartado "Prestaciones superiores o complementarias a las exigidas".

ii. Cuestionarios individuales referidos en el apartado "Equipo de trabajo y dedicación", según modelo recogido al final del pliego. Conocimiento adquirido en la implantación de soluciones similares Específicamente en el ámbito de servicios de gestión de seguridad de la información en el entorno sanitario público.

e. Prestaciones superiores o complementarias a las exigidas.

i. Mejoras y/o servicios adicionales que proponga el licitador y que supongan un valor añadido a la prestación del servicio objeto del contrato y que sean aceptadas como tales por el Servicio Madrileño de Salud de la Consejería de Sanidad de la Comunidad de Madrid

f. Otros datos técnicos.

Las ofertas se centrarán en los **aspectos concretos de las necesidades aquí descrita**s, no resultando adecuado ni valorable la inclusión de otra información que no esté directamente relacionada funcional o tecnológicamente con este expediente, ni que por ser genérica, no se encuentre específicamente adaptada a él.

No se considera adecuada ninguna oferta con una extensión superior a las 60 páginas incluyendo todos los apartados del índice propuesto.

Deberán incluir toda la información escrita, más la que opcional y complementariamente deseen añadir, en un soporte electrónico (CD, DVD u otro soporte o mecanismo de acceso) con ficheros grabados en los formatos de ofimática habituales.

Para cualquier duda durante la redacción de las propuestas, en relación con el contenido de este Pliego Técnico pueden poderse en contacto con la Subdirección General de Planificación, Arquitectura e Innovación tecnológica. Todas las dudas, serán atendidas por escrito mediante el procedimiento que se considere oportuno.

Madrid a 12 de mayo de 2010

SUBDIRECTOR DE PLANIFICACIÓN,

ARQUITECTURA E INNOVACIÓN TECNOLÓGICA

Fdo.: Pedro Jesús Pastor Muñoz

9. ANEXO I – CUESTIONARIO DE PERSONAL

Datos comunes

Identificación oferta:	
Empresa licitante:	
Categoría ofertada:	
Apellidos y nombre:	
Empresa de pertenencia:	

Titulación académica

Título académico	Centro	Años	Fecha expedición	TIC

Años: Duración oficial

TIC: si/no según pertenezca o no a tecnologías de la información y las comunicaciones

Datos dependientes de los criterios de adjudicación

Antigüedad en empresa, antigüedad en categoría y experiencia TIC

Empresa	Categoría	F-alta	F-baja	Meses	Actividad Informática

Formación en tecnologías de la información

	Entorno del proyecto			Otros entornos		
Curso	Horas	Empresa	F-inicio	Horas	Empresa	F-inicio

Datos relativos a los proyectos (para experiencia en entornos tecnológico y funcional)

Nombre Proye	Fecha inicio	Fecha fin	Entidad usuaria	Funcionalidad

Funcionalidad: breve descripción de la/s funcionalidad/des del proyecto

Experiencia en el entorno tecnológico

Categoría	Meses	Base de Datos	Sistemas Operativos	Lenguajes Programación	Otros

Categoría: La ejercida en el proyecto

Indicar el entorno concreto de Base de Datos, S.O., Lenguaje de Programación, o cualquier otro entorno relevante en los que tenga experiencia.

Experiencia en el entorno funcional

Categoría	Meses	Descripción detallada de funcionalidad

Nota: Todas las fechas deberán consignarse en el formato dd/mm/aaaa