



DIRECCIÓN GENERAL DE SISTEMAS
DE INFORMACIÓN SANITARIA
CONSEJERÍA DE SANIDAD

PLIEGO DE PRESCRIPCIONES TÉCNICAS DE LOS SERVICIOS DE GESTIÓN INTEGRAL DE LOS CENTROS DE PROCESO DE DATOS DEL SERVICIO MADRILEÑO DE SALUD DE LA COMUNIDAD DE MADRID



La autenticidad de este documento se puede comprobar en www.madrid.org/csv
mediante el siguiente código seguro de verificación: **090873853554611528255**

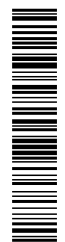


INDICE

1	INTRODUCCIÓN.....	6
2	OBJETO DEL CONTRATO.....	9
3	ASPECTOS GENERALES Y ÁMBITO DEL CONTRATO	10
3.1	ASPECTOS GENERALES DE LOS SERVICIOS OBJETO DEL CONTRATO	10
3.2	DESCRIPCIÓN DEL ÁMBITO DEL CONTRATO.....	11
4	DESCRIPCIÓN GLOBAL DE LOS SERVICIOS A CONTRATAR. LÍNEAS PRINCIPALES DE ACTIVIDAD.....	13
5	DESCRIPCIÓN DETALLADA DE LOS SERVICIOS SOLICITADOS	18
5.1	SERVICIOS DE ADMINISTRACION, OPERACIÓN Y GESTIÓN DE INFRAESTRUCTURAS DE CPD.....	18
5.1.1	Servicios de infraestructuras básicas comunes de los CPD	19
5.1.2	Servicios de infraestructuras TIC comunes de los CPD	20
5.1.3	Servicios de infraestructuras de sistemas de información	22
5.1.4	Servicios de administración de Data Lake (repositorio de almacenamiento de datos) sanitario 23	
5.1.5	Servicios comunes de gestión y gobierno.....	24
5.1.6	Servicios de diseño de arquitecturas y automatización de servicios TIC	26
5.1.7	Otros Servicios	27
5.2	SERVICIOS DE MANTENIMIENTO DE EQUIPAMIENTO HARDWARE Y SOFTWARE	27
5.2.1	Mantenimiento preventivo de los equipos	29
5.2.2	Asistencia software.....	29
5.3	SERVICIOS DE TRASLADO DE EQUIPAMIENTO TI Y ADECUACIÓN DE LAS CONFIGURACIONES A UN POSIBLE NUEVO CPD DEL SERMAS.....	30
5.4	SERVICIOS EN MATERIA DE SEGURIDAD DE LOS CENTROS DE PROCESO DE DATOS33	
5.5	PROGRAMA DE TRANSFORMACIÓN DEL MODELO DE SERVICIO	34
5.5.1	Automatización de tareas de operación basada en DevOps.....	38



5.5.2	Solución tecnológica de infraestructura Cloud privada en los CPD centrales del SERMAS	39
5.5.3	Dimensionamiento.....	45
5.5.4	Modelo de despliegue.....	47
5.6	PROGRAMA DE TRANSFORMACIÓN TECNOLÓGICA PARA CENTROS DE ATENCIÓN ESPECIALIZADA Y OTROS CENTROS DEL SERMAS	47
5.6.1	Transferencia de la gestión centralizada de la Historia Clínica Electrónica en Centros de Atención Especializada	47
5.6.2	Centralización de aplicaciones clínico/asistenciales y departamentales	49
6	FASES DEL SERVICIO.....	51
6.1	FASE DE PLANIFICACIÓN Y EJECUCIÓN DE LA TRANSFERENCIA DEL SERVICIO.....	52
6.1.1	Etapas de planificación de la transición	52
6.1.2	Fase de transferencia del servicio	53
6.2	FASE DE SERVICIO REGULAR	55
6.3	FASE DE DEVOLUCIÓN DEL SERVICIO	56
7	MODELO DE RELACIÓN Y GESTIÓN DEL SERVICIO.....	57
7.1	MODELO DE RELACIÓN	58
7.2	INTERLOCUTORES PARA GESTIONAR LA RELACIÓN.....	59
7.3	MODELO DE GESTIÓN DEL SERVICIO TI	59
8	ORGANIZACIÓN Y EQUIPO DE PRESTACIÓN DEL SERVICIO	60
8.1	CONFIGURACIÓN Y DIMENSIÓN	62
8.1.1	Descripción de los perfiles.....	62
8.1.2	Cualificación mínima exigida para los perfiles profesionales	68
8.2	HORARIOS DE PRESTACIÓN DEL SERVICIO	80
8.2.1	Horarios de operación y atención a incidencias tanto software como hardware.....	80
8.2.2	Horario de administración de sistemas, seguridad y redes. Guardias fuera de horario	80
8.2.3	Horario de consultoría y soporte nivel 3.....	81
8.2.4	Horario de intervenciones planificadas fuera del horario normal	81
8.3	NORMATIVAS Y PROCEDIMIENTOS	81



9	CALIDAD DEL SERVICIO	82
9.1	MODELO DE GESTIÓN DE LAS AUDITORÍAS	84
9.2	FORMACIÓN CONTINUADA. PLANES DE FORMACIÓN	86
9.3	EVOLUCIÓN Y MEJORES PRÁCTICAS	86
9.4	REQUISITOS DE LOS SISTEMAS DE ACCESO	87
9.5	HERRAMIENTAS	87
10	SEGUIMIENTO Y ACUERDOS DE NIVEL DE SERVICIO	87
11	INFRAESTRUCTURA DE TRABAJO Y SEGURIDAD	94
11.1	INFRAESTRUCTURA	94
11.2	SEGURIDAD DE LOS SISTEMAS	94
11.3	SEGURIDAD, CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS	95
11.3.1	Encargado de tratamiento	95
11.3.2	Limitación del acceso o tratamiento	96
11.3.3	Medidas de seguridad	96
11.3.4	Personal prestador del servicio	99
11.3.5	Cesión o comunicación de datos a terceros	99
11.3.6	Responsabilidad en caso de incumplimiento	100
11.4	Restricciones generales	100
12	PROPIEDAD DE LOS TRABAJOS Y PRODUCTOS	100
13	CONTENIDO DE LAS OFERTAS	101
14	RELACIÓN DE ANEXOS AL PLIEGO DE PRESCRIPCIONES TÉCNICAS	103



1 INTRODUCCIÓN

El Servicio Madrileño de Salud a través de la Dirección General de Sistemas de Información Sanitaria (DGSIS), tiene entre sus competencias “La planificación, diseño, implantación y mantenimiento de los sistemas y tecnologías de la información para la organización y funcionamiento del Sistema Sanitario Público de la Comunidad de Madrid”, así como “La provisión y gestión de los bienes y servicios informáticos del Servicio Madrileño de Salud”.

El funcionamiento de la Consejería de Sanidad de la Comunidad de Madrid (CSCM) y del Servicio Madrileño de Salud (SERMAS) se apoya en un conjunto de aplicaciones y sistemas de información que permiten su gestión. Especialmente se deben considerar los sistemas de información sanitarios asociados a Historia Clínica Electrónica tanto de Atención Primaria como de Atención especializada en funcionamiento en los hospitales digitales, ya que toda la gestión sanitaria soportada y las tareas administrativas de los mismos se encuentra alojada en aplicaciones y en infraestructuras tecnológicas que se deben administrar, operar, mantener y actualizar adecuadamente.

En ese marco competencial, actualmente, los sistemas de información sanitaria se alojan por un lado en los centros de proceso de datos (en adelante, CPD) corporativos, formados por un CPD extendido con dos sitios físicos diferenciados y un tercer CPD como centro de proceso de datos de contingencia. Y por otro lado, se encuentran los CPD locales. En línea con sus criterios estratégicos de evolución, el SERMAS lleva varios años consolidando servicios y sistemas que lleva aparejada la integración y centralización de procesos, minimizando y racionalizando los servicios distribuidos tanto desde el punto de vista funcional, como del tecnológico.

Así mismo, en el PLAN ESTRATEGICO DE INNOVACION Y MODERNIZACION DE LA GESTIÓN PUBLICA DE LA COMUNIDAD DE MADRID 2016-2019 PARA LA CONSEJERIA DE SANIDAD, se establecen entre los ejes de medidas de mejora y modernización de las políticas públicas esenciales, así como en el eje de estabilidad presupuestaria, las siguientes medidas:

- Centralización de los sistemas de gestión clínico-asistencial (historia clínica electrónica), en los Data Center corporativos de la DGSIS, con el consiguiente ahorro en licencias y mantenimiento de sistemas.
- Contribuir al ahorro energético de los hospitales.

Estas iniciativas de consolidación se han concretado en diversos planes de alta prioridad, entre los que cabe señalar los enmarcados en el Plan Director de Sistemas de Información de los hospitales desarrollado por la DGSIS (denominado plan ATHENE@), en donde se estableció una línea estratégica dirigida a continuar la modernización de los Sistemas de Información que dan soporte a la actividad realizada en los hospitales y que afectan de forma importante a la gestión y administración de los CPD, teniendo como premisas la centralización de sistemas de información de atención especializada, incluidos los sistemas de centralización de imagen médica, extendiendo el alcance hacia servicios de imagen no radiológica y



proporcionar el servicio hacia una solución corporativa y centralizada de imagen tanto radiológica y no radiológica. Dichos planes de actuación en el ámbito de los hospitales del SERMAS establecen el modelo futuro para los Sistemas Hospitalarios.

Con el objetivo de optimizar la utilización de los recursos y procurar el más alto nivel de servicio en los sistemas de información, los CPD responderán al criterio de mantener y evolucionar los servicios centralizados, continuar con las políticas de integrar, consolidar y centralizar los diferentes entornos funcionales, incluyéndolos en la misma instalación, aunque con las peculiaridades e independencia necesarias.

Por ello, desde hace varios años, los CPD Centrales del SERMAS, se han constituido en el Cloud Privado de la sanidad pública de la Comunidad de Madrid. Al profesional, tanto sanitario como administrativo, ya no le preocupan donde se encuentran alojados los sistemas de información que le permiten ejercer su actividad, actualmente lo que exigen y precisan es que los sistemas y aplicaciones estén disponibles las 24 horas del día, todos los días del año y que el rendimiento y la respuesta de dichos sistemas sea lo más ágil y rápida posible.

La DGSIS es responsable de los servicios de gestión y administración de los CPD, actividad que lleva a cabo actualmente mediante dos unidades funcionales denominadas CEDAS (acrónimo de Centro de Datos, Administración y Soporte) y CEDAS-HD (Centro de Datos, Administración y Soporte en Hospitales Digitales). Con este criterio, se proveen los servicios de consultoría, administración, operación, monitorización, resolución de incidencias de sistemas y suministro y mantenimiento del equipamiento necesario tanto para los sistemas de uso común, por ejemplo CIBELES-Tarjeta Sanitaria, como para otros de ámbito sectorial pero de arquitectura y datos centralizados, como AP-Madrid (sistema de información para Atención Primaria), Receta Electrónica, los sistemas de gestión de los hospitales con el Sistema de Información Clínico-Asistencial (SELENE y HCIS), instalados de forma centralizada, aplicaciones departamentales centralizadas asociadas (Farmacia, Dietética, Facturación,...), plataforma de integración, analítica avanzada y Big Data.

En la actualidad, en los CPD gestionados por CEDAS y CEDAS-HD residen los sistemas de información que proveen servicios centralizados a profesionales del SERMAS, a entidades sanitarias externas que se han de relacionar con el SERMAS y a los ciudadanos. En el anexo I, a solicitar por los licitadores, se puede encontrar el catálogo actual de los servicios ofrecidos cuyas infraestructuras tecnológicas se encuentran ubicadas en dos ámbitos:

- Los **Servicios Centralizados**, localizados en dos CPD situados en Madrid capital y en un tercero ubicado en Tres Cantos (Madrid). Actualmente, son gobernados de forma centralizada con el fin de cubrir necesidades de asistencia técnica y funcional en el ámbito de las tecnologías de la información y las comunicaciones (en adelante, TIC) de la red sanitaria y asistencial, Servicios Centrales y organismos dependientes de la CSCM.
- Los **Servicios Descentralizados**, asociados a la red hospitalaria del SERMAS.



En el modelo de gestión actual de los CPD del SERMAS se dispone de los mecanismos necesarios para permitir la coexistencia de diferentes proveedores en los diversos ámbitos de Aplicaciones y Sistemas de Información. Sin embargo, en este momento, se quieren aprovechar las sinergias de ambos grupos que gestionan los CPD en uno único. La evolución y mejora continua de este modelo actual posibilita que ambos grupos de trabajos converjan y se consoliden en un único grupo denominado CEDAS a partir de los 4 primeros meses del contrato. Esta unificación de ambos grupos debe hacerse en un periodo máximo de 1 mes.

Con este nuevo contrato se pretende obtener una mejor relación coste-eficiencia a través de una solución única para el conjunto de prestaciones, que permita un abordaje global de los servicios de gestión integral de los CPDs. Así, los dos ámbitos funcionales que actualmente y por razones históricas, gestionan los CPDs, pasarán a ser una única unidad funcional que aproveche las sinergias. La evolución y mejora continua que se ha realizado en los últimos años en los CPDs, junto con el nuevo modelo de organización que se pretende implantar, posibilita que ambos grupos de trabajo converjan y se consoliden en un único grupo denominado CEDAS.

Este pliego de prescripciones técnicas (en adelante, PPT) establecen las fases y los requisitos para proceder a la contratación de los citados servicios, con los siguientes objetivos:

- **Garantizar la calidad del servicio:** se precisa el más alto grado de calidad, especialmente en relación con la disponibilidad y la seguridad.
- **Asegurar la eficiencia en la prestación de los servicios:** asegurando una alta capacidad de prestación de los servicios requeridos, de manera proactiva, de modo que se garantice la estabilidad de los procesos, operaciones y sistemas de información del SERMAS.
- **Ofrecer un Catálogo de Servicios de administración de CPD homogéneo:** para lo cual debe establecerse un modelo único de gestión centralizada de las infraestructuras del SERMAS que proporcione un enfoque integrado de servicios, con especial foco en la satisfacción de los usuarios.
- **Establecer pautas comunes para la evolución a futuro de las arquitecturas tecnológicas y de las herramientas de gestión:** dichas arquitecturas tecnológicas, y las herramientas de gestión correspondientes, deben establecer los estándares a seguir desde el punto de vista de virtualización, consolidación, automatización, centralización y homogeneización del equipamiento, así como de su mantenimiento.
- **Reducir la complejidad al optimizar e integrar proveedores y servicios, facilitando el control y la adopción rápida de nuevas tecnologías por medio de herramientas técnicas específicas:** El SERMAS desea evolucionar sus plataformas en un proceso de transformación y consolidación definiendo un nuevo catálogo de servicios TI con el fin de disponer de la capacidad para operar, transformar e integrar sus plataformas tecnológicas tradicionales hacia entornos Cloud (nube), inicialmente de ámbito privado, que permita el auto aprovisionamiento de los servicios TIC.



- **Mantener un marco de seguridad técnico-legal conforme a la legislación vigente:** el marco de seguridad asociado a la información sanitaria requiere garantizar el cumplimiento de normativas vigentes en materia de seguridad y protección de datos, tanto desde el punto de vista legal como tecnológico, garantizado el cumplimiento de la legislación vigente aplicable.

En resumen, ese nuevo modelo de CEDAS deberá garantizar la prestación y calidad del servicio, con especial hincapié en:

- La implantación de una cultura común de servicio al cliente, entendiendo como tal a todos los usuarios de tecnologías y sistemas de información bajo su alcance.
- La incorporación de las mejores prácticas de gestión en el entorno TIC basadas en metodologías y normas, como, por ejemplo, ITIL v3 e ISO-20000, que permitan la prestación de un servicio de gestión y operación de CPD eficaz y eficiente, y conforme al estado del arte en la materia.
- El desarrollo de un modelo de procesos de gestión integral, mediante la evolución del modelo actual existente de los equipos de CEDAS y CEDAS HD, a un único Grupo de Gestión Integral denominado CEDAS, que facilite la estandarización y automatización de servicios TIC de soporte y agilice la gestión y seguimiento del Centro en lo que a servicios TIC se refiere.
- Anticipación en la detección de problemas, análisis de riesgos, así como en el diagnóstico y resolución de incidencias TIC y de incidentes de seguridad TIC.
- La disponibilidad de información fiable sobre la calidad de la prestación del servicio TIC y los servicios de apoyo correspondientes.
- La gestión de la capacidad, disponibilidad, evolución de los servicios, costes y contingencia sobre el entorno TIC.

Para asegurar la adecuada prestación de los servicios se debe contar con los medios materiales y humanos que sean precisos, con objeto de garantizar la cobertura suficiente en la gestión de las incidencias, peticiones y consultas, surgidas de la explotación de los servicios albergados en los CPD, así como para todas aquellas tareas necesarias para garantizar el Servicio de Gestión y Operación, según se determina en las cláusulas de este PPT y en el correspondiente pliego de cláusulas administrativas.

2 OBJETO DEL CONTRATO

El objeto del contrato lo constituye la prestación de los servicios de Administración, Gestión, Operación y mantenimiento de las infraestructuras básicas de los CPD, de las infraestructuras de redes, de los sistemas de almacenamiento y copias de seguridad (back-up), de los sistemas de seguridad y control de los accesos, en los Sistemas de Información actualmente centralizados y los que se incorporen en arquitectura centralizada a los CPD Corporativos de SERMAS durante la duración del contrato, así como en las



infraestructuras tecnológicas asociadas a los Sistemas de Información de los centros de Atención Especializada del SERMAS, conforme al Plan de Transformación de cada centro.

En el Plan de Transformación asociado a cada centro se establecerá la evolución prevista hacia el modelo de gestión centralizada de las infraestructuras correspondientes a los Sistemas de Información de dicho Centro, así como el grado de consolidación previsto para dicha infraestructura. Así mismo, con el objetivo de consolidación y centralización de servicios durante la duración del contrato, en los sistemas de información de los Centros de Atención Especializada, no sólo se prestarán servicios de gestión centralizada de infraestructuras sino también de transformación y adecuación a las arquitecturas tecnológicas del SERMAS. Es decir, si dichos sistemas, fruto de una homogenización de servicios son transformados hacia una arquitectura centralizada y multi-hospital que cumpla los estándares tecnológicos del SERMAS, se deberán prestar los servicios para la transformación y adecuación de las arquitecturas tecnológicas, de administración y de mantenimiento del hardware y software base, así como la puesta en práctica del nuevo modelo de prestación de éstos en las mismas condiciones que el resto de servicios ya centralizados.

Del mismo modo, se contemplará el cambio paulatino en el modelo de gestión del servicio de tal forma que se adapte a los planes de transformación que el SERMAS proponga, con especial atención a un modelo de servicio orientado a la nube privada (cloud), en el que se modelen y automaticen los procesos que en cada momento considere el SERMAS. Esta transformación podrá afectar a cualquier ámbito, no sólo a los sistemas en producción, preproducción y contingencia, sino que también podrán proponerse, por ejemplo, transformaciones relacionadas con las plataformas de desarrollo de aplicaciones con objeto de automatizar el ciclo de vida de las aplicaciones a lo largo de la duración del contrato, implantando modelos DevOps (desarrollo – desarrollo y operaciones – operaciones).

3 ASPECTOS GENERALES Y ÁMBITO DEL CONTRATO

3.1 ASPECTOS GENERALES DE LOS SERVICIOS OBJETO DEL CONTRATO

Estos servicios deben contemplar unos aspectos generales, de alto nivel, que se relacionan a continuación:

- Gestionar los sistemas de producción y de otros entornos de preproducción, contingencia y desarrollo en los CPD del SERMAS, asegurando la operación continua de los mismos durante 24 horas al día, 7 días a la semana, 365 días al año.
- Velar por la seguridad de los datos, aplicando las medidas técnicas y de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información.
- Realizar las labores previas necesarias para la correcta puesta en producción de los nuevos sistemas y aplicaciones que se adscriban a CEDAS.
- Realizar los proyectos de adecuación de entornos de producción, preproducción, contingencia y desarrollo entre cualquiera de los CPD del SERMAS, sin perjuicio de afectar a los servicios de



soporte CEDAS. A modo de ejemplo de este tipo de proyectos se contemplan proyectos de renovación tecnológica, de consolidación de servicios en nueva infraestructura, planes de transformación de los centros o de actualización de software base de los sistemas de información sanitarios.

- Diseñar el modelo de servicio, para adecuar los procedimientos de trabajo utilizados a las necesidades reales en cada momento, adaptándose a los cambios globales que la DGSIS impulse y que afecten a los distintos proveedores de servicios.
- Diseñar la transformación de las configuraciones de infraestructuras de los servicios centralizados y posibles nuevos servicios a centralizar de Centros de Atención Especializada, SUMMA 112 o en general cualquier centro dependiente del SERMAS, para adaptarlas a la nueva arquitectura de CPD y al modelo de gestión aplicable en cada caso.
- Mantener el hardware y software del equipamiento de TI que ya no disponga de garantía, contemplado en el Anexo III.
- Asesorar a la DGSIS sobre la evolución y adecuación de los sistemas para disponer de la configuración óptima en función de los planes y proyectos del SERMAS.
- Asesorar y ejecutar planes de transformación hacia una nueva arquitectura adaptativa en donde la automatización de tareas y de procesos de negocio así como el auto aprovisionamiento de servicios sean las premisas para mejorar y optimizar la prestación del servicio durante la vigencia del contrato.
- Análisis y evaluación de costes asociados en actividades del CEDAS así como de cualquier otra actividad global de la DGSIS en la que CEDAS tenga participación, de tal forma que se pueda hacer un análisis y evaluación de costes global junto con otras unidades de la DGSIS.
- Análisis de riesgos y propuestas de gestión de los mismos.
- Asesorar y evaluar medidas de seguridad específicas para el ámbito de los CPD y que se encuadren dentro de las directrices de seguridad globales adoptadas por el SERMAS.

3.2 DESCRIPCIÓN DEL ÁMBITO DEL CONTRATO

Desde los CPD que gestionan actualmente los grupos CEDAS y CEDAS HD se proporcionan servicio a un total de 279 aplicaciones centralizadas, además de 15 a 30 aplicaciones departamentales por cada hospital, que ya han empezado a centralizarse y que se espera terminar de centralizar gracias a este contrato.

A estas aplicaciones se accede desde:

- Servicios Centrales;
- Todos los hospitales (hasta 36, actualmente) y centros de especialidades (hasta 40, actualmente);



- Todos los centros de atención primaria (actualmente, hasta 261 centros de salud y 157 consultorios);
- Otros centros sanitarios;
- Los ciudadanos (desde Internet).

El número de profesionales con acceso a la Red Sanitaria a los que se presta servicio de Intranet, aplicaciones centralizadas, correo electrónico, y salida a Internet, ronda los 85.000. El número de ciudadanos con derecho a prestación sanitaria es de alrededor de 6.500.000.

En relación a los Centros de Proceso de Datos, CEDAS y CEDAS-HD actualmente gestionan los siguientes:

- Un CPD dependiente del SERMAS situado en el Centro de Actividades Ambulatorias del Hospital Universitario 12 de Octubre (CPD ATHENE@).
- Un CPD situado en locales de la Consejería en la calle Aduana (CPD ADUANA). Dadas las limitaciones de este CPD que impiden una evolución acorde con las necesidades del SERMAS, es posible que durante la duración del contrato se disponga de un nuevo CPD más adecuado. En caso de ser así, el CEDAS se encargará de la migración de los servicios y equipos TI, así como de la configuración y cambios asociados en los sistemas de información para su correcto funcionamiento en la posible nueva ubicación.
- Ambos CPD, aunque separados están conectados entre sí, y actúan como un CPD único extendido lo que permite que la configuración de los servicios en alta disponibilidad y la implantación de nuevos servicios en una configuración Activo/Activo tanto a nivel de servidor de aplicaciones como de servidores de Base de Datos.
- Un tercer CPD con equipamiento del SERMAS para tercera copia de datos y contingencia de los servicios críticos, en la actualidad la mayor parte, en modo “housing”, proporcionado por la Agencia para la Administración Digital de la Comunidad de Madrid, situado en Tres Cantos (CPD de Tres Cantos).
- Actualmente, en otros locales del SERMAS (CPD locales de centros de atención especializada hospitales y CPD del SUMMA 112) existe equipamiento informático homogéneo, que deberá también ser considerado como parte de la infraestructura gestionada por CEDAS. Durante la ejecución de este contrato, los CPD de los Centros de Atención Especializada podrán sufrir planes de transformación específicos que resultarán de la centralización total o parcial de los sistemas de información a los CPD de Servicios Centrales.

Está previsto que, durante la ejecución de este servicio, se continúe con la centralización de los Sistemas de Información albergados en los CPD de Centros de Atención Especializada, y deberán ser reubicados en los CPD de Servicios Centrales. El proveedor deberá realizar todos los servicios precisos para asegurar el



éxito de dicha centralización. También deberá asegurar la administración y la operación de esos sistemas, donde quiera que estén ubicados durante cualquier momento del proceso.

No son responsabilidad del adjudicatario de este contrato los servicios de infraestructura básica y de comunicaciones en CPD locales (aire acondicionado, electricidad, redes de usuario, redes WAN) de los hospitales contemplados dentro del alcance de este contrato. Aunque el adjudicatario de este contrato con periodicidad mensual deberá presentar un informe, proponiendo soluciones a las deficiencias detectadas que puedan poner en peligro el buen funcionamiento de los servicios distribuidos en los centros hospitalarios cuya administración y mantenimiento sí son responsabilidad del adjudicatario de este contrato.

4 DESCRIPCIÓN GLOBAL DE LOS SERVICIOS A CONTRATAR. LÍNEAS PRINCIPALES DE ACTIVIDAD

El SERMAS se encuentra en una fase de profunda y rápida modernización de sus sistemas de información, que tiene como objetivo la eficiencia en la prestación de los servicios sanitarios a los ciudadanos de la Comunidad de Madrid, por tanto, las tareas de implantación de nuevas aplicaciones permanecerán siendo críticas para la obtención de los objetivos estratégicos del SERMAS.

La DGSIS ha establecido una serie de directivas para sus sistemas de información (centralización, diseño de aplicaciones en tres capas, homogenización de plataformas tecnológicas, etc.) que permita una utilización más eficiente de sus recursos.

Así mismo el SERMAS desea adquirir mayor madurez en la forma de prestación de los servicios en un modelo que profundice en:

- Consolidar el modelo de virtualización, en este momento ya generalizado en las capas frontales.
- Normalizar el servicio TI, implantando las herramientas y transformando los procesos de operación y administración hacia un CPD definido por software, donde se ofrezcan paulatinamente los servicios en modo cloud privado, proporcionando a la Red Sanitaria Pública de la Comunidad de Madrid IaaS (infraestructura como servicio), PaaS (plataforma como servicio) y SaaS (software como servicio).
- Agilizar desde servicios de TI los Ciclos de Desarrollo y puesta en producción de nuevos servicios utilizando técnicas DevOps (procesos y métodos para tener una comunicación y colaboración entre el desarrollo, el control de calidad y las operaciones de TI).
- Seguir apostando por la eficiencia energética en los CPD del SERMAS (Green Data Center) y los sistemas abiertos.

Con ello, el SERMAS desea adaptarse a los grandes retos futuros del mundo TI donde la velocidad del cambio y el rápido crecimiento de servicios digitalizados hacen que la automatización sea una premisa en la forma de prestación del servicio y además permita al SERMAS obtener los siguientes beneficios derivados:



- Rapidez en los Procesos (agilidad).
- Sostenibilidad y mantenimiento de los costes: Hacer mucho más, prácticamente con lo mismo.
- Escalabilidad y Flexibilidad (alineamiento con las necesidades de negocio y el volumen de demanda).
- Adaptabilidad: modificación simple de los procesos automatizados.
- Mejoras en los acuerdos de nivel de servicio TIC del SERMAS con sus centros sanitarios y SSCC, dado que los procesos automatizados, reducen errores y aumentan la eficiencia en la prestación del servicio.
- Incremento de la eficiencia y la productividad.

Tanto los sistemas actuales como los de futura implantación se caracterizan por su elevado nivel de criticidad y sensibilidad en la privacidad de los datos que manejan.

Estos condicionantes hacen que el nuevo servicio de CEDAS deba disponer de un equipo de trabajo formado por profesionales dedicados, con probada experiencia y cualificación en todas las áreas tecnológicas objeto de este contrato.

Los servicios solicitados para CEDAS se componen de las siguientes líneas principales de actividad:

1. Servicios de Administración, Operación y Gestión de infraestructuras de CPD. Estos servicios constituyen el núcleo del servicio de CEDAS y se descomponen en:

- 1.1. Servicios de infraestructuras básicas comunes de los CPD (CPD ADUANA y CPD ATHENEA). Se incluyen la monitorización, administración y gestión de:
- Sistemas de aire acondicionado.
 - Sistemas de alimentación ininterrumpida (UPS).
 - Generadores de alimentación de emergencia.
 - Conexiones disponibles en los cuadros de distribución eléctrica.
 - Sistemas de detección y extinción automática de incendios dentro del CPD.
 - Sistemas de cableado dentro del CPD, incluyendo paneles de parcheo y etiquetado de los mismos.
 - Instalaciones hardware de cualquier equipo, aunque sean ejecutadas por terceros, que deba albergarse en el CPD.
 - Espacios disponibles en las salas y los armarios de equipamiento (Racks.)
 - Sistemas de control de la seguridad física de los CPD, incluyendo control de los accesos de personal y cámaras de vigilancia.

En cualquier caso, los mantenimientos técnicos asociados a este equipamiento no forman parte del objeto de este contrato.

- 1.2. Servicios de infraestructuras TIC comunes de los CPD centrales (CPD Athene@, CPD de Aduana, CPD de Tres Cantos e infraestructura TI Athene@ Centralizada en los CPD



centrales o localizada en los CPD de los Centros de Atención Especializada y SUMMA 112) que incluyen:

- Redes de CPD.
 - Sistemas de control de acceso lógico y seguridad perimetral (cortafuegos, balanceadores, aceleradores criptográficos...).
 - Sistemas de correlación de eventos de seguridad.
 - Sistemas de monitorización de infraestructura y de servicios TI.
 - Redes de almacenamiento.
 - Sistemas de copia de seguridad (backup).
- 1.3. Servicios de infraestructuras de Sistemas de Información, contemplando entornos de producción, preproducción, formación, desarrollo y contingencia (incluidos en el listado de aplicaciones del Anexo II del pliego):
- Servidores y sistemas operativos.
 - Bases de datos.
 - Sistemas de integración.
 - Intranet.
 - Plataformas y servicios de explotaciones, analítica avanzada y de Big Data.
 - Servidores de aplicaciones.
 - Software de virtualización.
- 1.4. Servicios de administración de Data Lake (repositorio de almacenamiento de datos) sanitario, como apoyo para dar cumplimiento a la medida “Diseño de herramientas para la explotación de la información asistencial”, incluido dentro del Plan Estratégico de Innovación y Modernización de la Gestión Pública (PEIM). Dicha medida persigue agilizar la explotación de la información asistencial para maximizar el valor de dicha información, obteniendo una visión completa de la organización y permitiendo la detección temprana de desajustes y la toma de decisiones correctoras.
- 1.5. Servicios comunes de Gestión y Gobierno, asociados a la gestión de Niveles de Servicio, de Seguridad y de Contingencia.
- 1.6. Servicios de diseño de arquitecturas de automatización de servicios y auto aprovisionamiento: servicios asociados a una transformación paulatina de los sistemas de información centralizados para que puedan ser provisionados desde una arquitectura adaptativa y definida por software. Para ello se contemplan los servicios de consultoría, diseño, transformación de las tareas de operación y procesos de administración para que los procesos de negocio puedan ser consumidos desde una plataforma de auto aprovisionamiento en base a políticas de la organización de servicios IaaS, PaaS y SaaS.
- 1.7. Otros Servicios: Gestión de capacidad y de la disponibilidad en tiempo real, evaluación de costes y análisis de riesgos.



2. **Servicios de mantenimiento de equipamiento hardware y software base**, que garanticen los objetivos de calidad y disponibilidad de las infraestructuras tecnológicas del SERMAS, tanto de hardware como de software y/o firmware de base. Para ello, en esta línea de actividad se contemplan actividades tanto de carácter reactivo, orientadas a resolver todos los incidentes que lleguen a producirse, como de carácter preventivo, con objeto de evitar y reducir al mínimo la ocurrencia de incidentes operativos o de seguridad y su consiguiente impacto.
3. **Servicios de traslado de equipamiento TI y adecuación de las configuraciones a un posible nuevo CPD del SERMAS**, que sustituirá al de Aduana, con objeto de garantizar la continuidad de los servicios desplegados en los CPD. Actualmente el CPD de Aduana está al límite de su capacidad física, eléctrica y de refrigeración y no permite el crecimiento acorde a las necesidades del SERMAS. Durante la vigencia del contrato está previsto disponer de un nuevo CPD y será necesario trasladar, configurar y hacer la puesta en marcha de los equipos que están en un CPD y se tienen que llevar al nuevo.
4. **Servicios en materia de seguridad de los centros de proceso de datos**, que permitan implantar las medidas necesarias en el ámbito de los CPD, bajo la estrategia global de seguridad de la Oficina de Seguridad de Sistemas de Información (OSSI).
5. **Programa de transformación del modelo de servicio**, que incluirá actividades orientadas al diseño y puesta en marcha de los procesos y herramientas necesarios para el modelo único de gestión centralizada de infraestructuras hacia un nuevo modelo gestión para la prestación de servicio TI en modo Cloud privado, para lo cual el adjudicatario deberá ofrecer los recursos y servicios asociados de consultoría, diseño, transformación de las tareas de operación y procesos de administración para para que los procesos de negocio puedan ser provisionados desde una arquitectura de adaptativa y definida por software que permita una transformación paulatina de los sistemas de información centralizados para que puedan ser consumidos desde una plataforma de auto aprovisionamiento IaaS, PaaS, SaaS, en base a políticas del SERMAS.
6. **Programa de Transformación tecnológica para Centros de Atención Especializada**. Como ejes principales se deberán contemplar: La centralización de aplicaciones clínico/asistenciales y departamentales de los Centros de Atención Especializada y soporte a los sistemas que queden descentralizados.

En el Anexo III de este PPT se incluye el inventario de los principales elementos que son objeto de Administración, Gestión y Operación por parte de CEDAS.

De forma resumida, y referido a la situación actual, la siguiente es la relación de elementos a gestionar, independientemente de donde estén ubicados (siempre estarán en locales situados dentro de la Comunidad de Madrid):



- La infraestructura actualmente asociada a los Centros de Proceso de Datos de SERVICIOS CENTRALES o CPD_LOCALES Distribuidos del SERMAS pero con Gestión Centralizada
 - 268 servidores físicos y más de 1500 servidores virtualizados.
 - 279 aplicaciones centralizadas más de 15 a 30 departamentales centralizadas de varios hospitales.
 - 259 bases de datos Oracle y 36 bases de datos Microsoft SQL Server.
 - 2 Peta Bytes de almacenamiento en los CPD Centrales y Hospitales con infraestructura Athene@ en local (excluyendo imagen Médica).
 - 2 cabinas de almacenamiento DELL - EMC VMAX3.
 - 2 cabinas de almacenamiento AFA HPE 3PAR.
 - 4 cabinas de Almacenamiento DELL-EMC Data Domain de para backup a disco deduplicado y 13 en los hospitales.
 - 2 cabinas de almacenamiento DELL-EMC Unity y 2 DELL-EMC ISILON para los distintos niveles de imagen radiológica.
 - 3 cabinas de almacenamiento de objetos DELL-EMC ECS y 12 DELL-EMC ISILON para archivado e historificación.
 - 1 plataforma de Big Data basada en Cloudera Oracle DBA (Big Data Appliance).
 - 13 DELL-EMC VNX 5300 derivadas del proyecto Athene@ fase 1 (hospitales).
 - Distintos aceleradores, balanceadores y cortafuegos.
 - Sistemas de monitorización de aplicaciones (APM), correlación de eventos OSSIM y monitorización de infraestructura.
 - Equipamiento de Comunicaciones: LAN 10-40 Gigabit Ethernet, tanto de conexión de cobre como de conexión de fibra, SAN 16Gb.
- La infraestructura asociada del equipamiento Athene@ tanto en CPD locales de los Centros de Atención Especializada como en el Centro de Respaldo en CPD Centrales, como resultado del diseño y ejecución de cada Plan de Transformación de Gestión e Infraestructuras particular para cada Centro, está relacionada en el Anexo III.

El servicio CEDAS deberá dar soporte a aquellos elementos físicos y lógicos que puedan incorporarse a lo largo de la ejecución del contrato como consecuencia de la renovación tecnológica de los sistemas informáticos actualmente implantados, sin que ello dé lugar a la actualización del precio del contrato. Asimismo, los elementos que forman parte de la infraestructura podrán cambiar de ubicación, por esta razón habrá que prestar el servicio solicitado allí donde los equipos se encuentren en cada momento.



De igual manera, CEDAS deberá dar soporte con un incremento de hasta el 20% sobre el nivel de actividad inicial, sin coste adicional para el SERMAS, cuando se deba a la evolución natural de los sistemas instalados o nuevas aplicaciones de características similares no recogidos en los Anexos de este pliego. Dicho incremento se estimará, de común acuerdo, entre el contratista y el SERMAS, en base a parámetros de capacidad de proceso y número y complejidad de los nuevos entornos y aplicaciones. En caso de discrepancia, el SERMAS tendrá la facultad de la decisión final.

5 DESCRIPCIÓN DETALLADA DE LOS SERVICIOS SOLICITADOS

Cada uno de los servicios solicitados agrupará las actividades y tareas a realizar en una serie de elementos de una capa tecnológica. Los servicios que a continuación se mencionan deben ejecutarse de acuerdo al modelo de gestión aprobado por la DGSIS, garantizando la seguridad, la calidad y eficiencia que permitan el cumplimiento de los Acuerdos de Nivel de Servicio.

Un ejemplo sobre el nivel de detalle de procesos, actividades y tareas que deben considerarse como compromiso de cumplimiento, se encuentra explicitado en la matriz de responsabilidad, que se adjunta como anexo V. Es responsabilidad del contratista la actualización de esta matriz, si fuera necesario, en base los requisitos de los servicios solicitados en este contrato. En caso de interpretaciones dispares del contenido de la Matriz, la interpretación definitiva corresponde a la DGSIS.

5.1 SERVICIOS DE ADMINISTRACION, OPERACIÓN Y GESTIÓN DE INFRAESTRUCTURAS DE CPD

Los Servicios de Gestión de infraestructuras de CPD de SERMAS están asociados, en primera instancia, a las infraestructuras siguientes:

- Infraestructura residente en CPD Extendido (CPD ATHENE@, incluyendo la infraestructura central del plan Athene@ en cada una de sus Fases y CPD ADUANA).
- Infraestructura residente en el CPD TRES CANTOS administrada por CEDAS.
- Infraestructura del plan Athene@ residente en los CPD locales de los Centros de Atención Especializada.

Adicionalmente a las infraestructuras indicadas anteriormente, el contratista debe tener presente que, a medida que vayan progresando los proyectos de transformación tecnológica, las infraestructuras resultantes de los mismos deben ser administradas, operadas y gestionadas a través de este servicio.

A continuación, se describen en detalle los distintos servicios de administración, operación y gestión.

En todos los casos, los elementos sobre los que se prestará servicio son las infraestructuras de cada tipo que fueron enumeradas en el Cláusula 4 de este documento. El detalle de estos elementos se incluye en el anexo III.



5.1.1 Servicios de infraestructuras básicas comunes de los CPD

El alcance de estos servicios se centra en los dos CPD centrales que constituyen el CPD único (CPD Aduana y CPD Athene@). Los CPD locales de los Centros Atención Especializada no son objeto de estos servicios.

Se incluyen la monitorización, administración y gestión de:

- Sistemas de aire acondicionado.
- Sistemas de alimentación ininterrumpida (UPS).
- Generadores de alimentación de emergencia.
- Conexiones disponibles en los cuadros de distribución eléctrica.
- Sistemas de detección y extinción automática de incendios dentro del CPD
- Sistemas de cableado dentro del CPD, incluyendo paneles de parcheo y etiquetado de los mismos
- Instalaciones hardware de cualquier equipo, aunque sean ejecutadas por terceros, que deba albergarse en el CPD
- Espacios disponibles en las salas y los armarios de equipamiento (Racks).
- Sistemas de control de la seguridad física de los CPD, incluyendo control de los accesos de personal y cámaras de vigilancia.

Descripción general del servicio

- Detección y notificación de las incidencias que puedan ocurrir, a los responsables de su tratamiento, según los procedimientos establecidos. Seguimiento de las mismas hasta su completa resolución y cierre. Supervisión y gestión de los trabajos de terceros para la resolución de incidencias.
- Gestión de las instalaciones de ampliaciones o nuevo hardware, acometidas eléctricas y del cableado estructurado en CPD, asegurando que los instaladores disponen de la información necesaria para planificar sus acciones conforme a las normas de CEDAS para estas actividades.
- Ejecución de las labores de parcheo de los paneles de cableado estructurado, etiquetado de los cables y equipos, gestión de la documentación asociada y actualización de la base de datos de configuraciones (CMDB), en tiempo real, siguiendo los procedimientos establecidos.
- Gestión de la ocupación de espacios, horizontales y verticales, y la ocupación de los cuadros de alimentación en CPD y mangueras de distribución eléctrica en las salas, notificando las necesidades previstas cuando no puedan cubrirse con la capacidad disponible. Deberá mantenerse actualizada la documentación que refleja el estado de ocupación de estas infraestructuras.



- Control de accesos de personal a las salas de equipos, siguiendo los procedimientos establecidos. Control de los mecanismos de vigilancia física, incluyendo las cámaras de grabación de los locales principales.

5.1.2 Servicios de infraestructuras TIC comunes de los CPD

Estos servicios alcanzan a la infraestructura ubicada en los CPD Centrales, el CPD Tres Cantos y la infraestructura Athene@ que a inicio de este contrato está residente en los Centros de Atención Especializada. La relación de centros incluidos con equipamiento Athene@ fase I se incluye en el anexo III.

Los elementos sobre los que se prestarán este tipo de servicios son:

- Servidores blade y no blade.
- Redes de CPD, son aquellas redes internas dentro de los CPD que comunican los sistemas de información entre sí y con sus usuarios.
- Sistemas de control de accesos lógicos (Solo CPD centrales) incluyendo, al menos:
 - Cortafuegos.
 - Balanceadores de carga.
 - Aceleradores criptográficos.
- Sistemas de correlación de eventos de seguridad.
- Sistemas de monitorización de infraestructura, de redes o de aplicaciones.
- Sistemas de almacenamiento: son aquellos sistemas de almacenamiento SAN, NAS y de objetos que dan servicio de almacenamiento centralizado a todos los sistemas de información Operacionales, Informacionales y Móviles así como los servicios de réplica de datos entre CPD.
- Sistemas de copias de seguridad (backup) a disco deduplicado.

Descripción general del servicio

Administración, ajuste fino de la configuración, gestión de la capacidad y el rendimiento, supervisión, operación y despliegue de los elementos incluidos en el servicio, asegurando la prestación del servicio conforme a los acuerdos de nivel de servicio comprometidos. En particular:

- Operar, administrar, gestionar y dar asesoramiento técnico sobre los equipos incluidos en el servicio, garantizando la correcta resolución de las incidencias y asegurando la adecuada documentación y cierre de las incidencias o cumplimiento de las peticiones de servicio, de acuerdo con los procedimientos establecidos.
- Supervisar y monitorizar el correcto funcionamiento de las redes de CPD, los sistemas de control de acceso y las redes y sistemas de almacenamiento, mediante una correcta identificación e



implementación de eventos-alarmas que permitan alcanzar los requisitos de nivel de servicio establecidos, adoptando las medidas correctoras, tanto pro-activas, como reactivas, para minimizar impacto en los usuarios.

- Realizar las tareas de operación de aplicaciones, establecidas en los procedimientos, en horario de 7x24, de manera que no se comprometa la disponibilidad, ni el rendimiento adecuado de las mismas.
- Realizar la interlocución con terceros (fabricantes, desarrollo, etc.) para garantizarla resolución de incidencias en su ámbito de actividad, asegurando la coordinación orientada al cumplimiento de los niveles de servicio establecidos por la DGSIS.
- Realizar las actividades de gestión de la disponibilidad, capacidad y rendimiento, implementando una gestión pro-activa de las infraestructuras, identificando, registrando problemas y estableciendo planes de acción para erradicar sistemáticamente las incidencias o posibles incidencias en el servicio. Además, proporcionará planes de mejoras con el objetivo de reducir riesgos y el impacto en el servicio de posibles caídas o degradaciones de rendimiento en su ámbito de actividad, sin que necesariamente se hayan producido incidencias con anterioridad.
- Realizar una correcta Gestión de Cambios, incluyendo la documentación de los mismos y la actualización de la Base de Datos de Gestión de Configuración (CMDB), utilizando el producto disponible CA Service Desk.
- Llevar a cabo las labores de instalación y actualización de las tecnologías de su ámbito de responsabilidad, asegurando un correcto diseño y configuración del cambio, tanto en plazos como eficacia.
- Planificación, operación y administración de copias y restauraciones, incluyendo la gestión de incidencias y peticiones, ejecución de actividades planificadas y control de backups, y las solicitudes de información.
- Operación y administración de backup, incluyendo la configuración y administración de productos de backup, resolución de incidencias sobre los mismos, ejecución de las peticiones, y asesoramiento para la evolución de los sistemas. La restauración de los datos, almacenados en los medios de backup, se realizará siempre que sea necesario.
- Manejo de los medios de backup, según la política establecida, asegurando siempre la confidencialidad e integridad de los datos que contengan.
- Asesoramiento para el diseño de nuevos entornos tecnológicos, para dar solución a las nuevas necesidades que puedan surgir en el futuro, asumiendo las operativas que los nuevos sistemas requieran.



- Suministro, implantación y desarrollo de herramientas de Gestión de la Capacidad que permita al SERMAS en tiempo real, conocer el estado y el uso de las infraestructuras habilitadas para el funcionamiento de los distintos sistemas de información.
- Mantener actualizado el inventario y etiquetado de toda la planta instalada. Se valorará la dotación de una aplicación de gestión de inventario. Si el contratista dota de una aplicación de gestión de inventario para dar soporte a las actividades solicitadas en el pliego, deberá proveer, a la finalización del contrato, de la correspondiente descarga en formato normalizado, de todos los datos utilizados en el inventario. Así mismo, indicará en su oferta si las licencias de la aplicación de inventario se ceden para uso indefinido al SERMAS o únicamente para el período de contrato.

5.1.3 Servicios de infraestructuras de sistemas de información

Adicionalmente a lo ya indicado, las infraestructuras de Sistemas de Información se encuentran divididas en entornos de Producción, Preproducción, Formación, Desarrollo y Contingencia, como viene reflejado en el inventario incluido en el Anexo II. El detalle de las tecnologías de sistemas operativos, bases de datos, middleware, servidores de aplicaciones, motores de integración y software de virtualización a gestionar puede resumirse en:

- Software de virtualización: VMWare, Windows Hiper-V, Oracle VM.
- Servidores y Sistemas Operativos: sistemas Linux y Windows.
- Servidores de aplicaciones: OAS, Weblogic, Jboss, Tomcat, IIS (.Net).
- Bases de datos: Oracle, SQL, MySQL, Postgre SQL, Mongo DB, Informix.
- Servicios de Integración: Ensemble, Microsoft Biztalk y Openlink.
- Administración y soporte de las plataformas y servicios de sistemas de explotaciones y Analítica Avanzada y de Big Data: SAP Business Objects, Microsoft BI y Data Lake sanitario con Cloudera.
- Otros: Sharepoint Server.

Descripción general del servicio:

Administración, ajuste fino de la configuración gestión de la capacidad y el rendimiento, supervisión, operación y despliegue de los elementos incluidos en el servicio, asegurando la prestación del servicio conforme a los acuerdos de nivel de servicio comprometidos.

- Operación, administración, gestión y asesoramiento técnico sobre los equipos y productos incluidos en el servicio, garantizando la correcta resolución de las incidencias, asegurando la adecuada documentación y cierre de las incidencias o cumplimiento de las peticiones de servicio, siempre de acuerdo con los procedimientos establecidos.
- Supervisión y monitorización del correcto funcionamiento de los servidores y sistemas operativos, las bases de datos, las propias aplicaciones y los servidores de aplicación, mediante una correcta



identificación e implementación de eventos-alarmas que permitan alcanzar los requisitos de nivel de servicio establecidos, adoptando las medidas correctoras tanto proactivas como reactivas para minimizar impacto en los usuarios.

- Realizar las tareas de operación de aplicaciones, establecidas en los procedimientos, en horario de 7x24, de manera que no se comprometa la disponibilidad, ni el rendimiento adecuado de las mismas.
- Realizar la interlocución con terceros (fabricantes, desarrollo) para garantizar la resolución de incidencias en su ámbito de actividad, asegurando la coordinación orientada al cumplimiento de los niveles de servicio comprometidos, incluyendo la gestión de las garantías u otros contratos de mantenimiento y soporte.
- Soporte especializado de los fabricantes de los productos software más relevantes, instalados en la infraestructura de CEDAS. Con objeto de contar con este soporte especializado, se contará con hasta 1000 horas de este servicio, en todo el período de contrato, cuyo consumo se realizará a demanda de la DGSIS.
- Realizar las actividades de gestión de la disponibilidad, capacidad y rendimiento, implementando una gestión pro-activa de los servicios, identificando, registrando problemas y estableciendo planes de acción para erradicar sistemáticamente las incidencias o posibles incidencias en el servicio. Además proporcionará planes de mejoras derivados de un análisis de vulnerabilidad, con el objetivo de reducir riesgos y el impacto en el servicio ante posibles caídas de los sistemas, o degradaciones de rendimiento en su ámbito de actividad, sin que necesariamente se hayan producido incidencias con anterioridad (modelo preventivo).
- Realizar una correcta Gestión de Cambios, incluyendo la documentación de los mismos y la actualización automática de la Base de Datos de Gestión de Configuración (CMDB). Llevar a cabo las labores de instalación y actualización de las tecnologías de su ámbito de responsabilidad, asegurando un correcto diseño y configuración del lanzamiento/cambio tanto en plazos como en eficacia.
- Será responsabilidad del proveedor mantener actualizado el inventario tanto físico como lógico y el etiquetado de todo el equipamiento de la planta instalada en tiempo real.

5.1.4 Servicios de administración de Data Lake (repositorio de almacenamiento de datos) sanitario

Dentro del Plan Estratégico de Innovación y Modernización de la Gestión Pública (PEIM), enmarcado en el eje 2, MEJORA Y MODERNIZACIÓN DE LAS POLÍTICAS PÚBLICAS ESENCIALES, en el programa SANIDAD DE CALIDAD, dentro del proyecto MEJORA Y MODERNIZACIÓN DE LAS POLÍTICAS PÚBLICAS ESENCIALES se encuentra la medida “Diseño de herramientas para la explotación de la información asistencial”.



Dicha medida persigue el diseño de herramientas que permitan mayor agilidad para la explotación de la información asistencial ya existente (SIAE, CMBC, sistemas predictivos de salud pública), que permitan maximizar el valor de dicha información, obteniendo una visión completa de la organización y permitiendo la detección temprana de desajustes y la toma de decisiones correctoras.

Esto implica la definición, diseño y desarrollo de nuevos sistemas analíticos con modelos predictivos que permita extraer valor de los datos existentes en la organización, que permitan, entre otras cosas, optimizar la gestión global y local de la capacidad, alerta temprana de variabilidad en la práctica clínica, predicción, seguimiento y actuación en el ámbito de la cronicidad y aplicarlos a la toma de decisiones.

La aplicación de técnicas analíticas sobre estos datos pondrá al alcance de gestores y profesionales (tanto clínicos como administrativos) potentes herramientas de trabajo que contribuirán positivamente a mejorar la calidad de los servicios asistenciales prestados, así como la detección temprana de desajustes y alertas epidemiológicas.

En este sentido, se ha alcanzado un grado de madurez suficiente para dar un paso más y obtener de la ingente cantidad de datos disponible, el enorme valor latente que estos datos tienen.

Para ello el SERMAS ha invertido en una plataforma de Big Data basada en Cloudera Oracle DBA.

Dicha infraestructura así como posibles ampliaciones o de servicios asociados resultante de dichos proyectos se incorporarán al modelo de gestión centralizada y a los servicios de carácter continuado de CEDAS, tanto de administración, operación y gestión de infraestructuras de CPD, como de mantenimiento de equipamiento hardware y software base, sin costes adicionales para el SERMAS.

Este servicio de administración del repositorio de datos, Data Lake, estará alineado con el conjunto de servicios centralizados y de soporte y administración solicitados bajo la responsabilidad de este contrato.

5.1.5 Servicios comunes de gestión y gobierno

Adicionalmente a las actividades relacionadas con la prestación de los servicios de administración, operación y gestión descritos anteriormente, cada servicio debe contemplar una serie de actividades comunes a todos ellos. En este apartado se especifican dichas actividades comunes cuyo propósito principal es asegurar unos niveles adecuados de servicio, seguridad y contingencia en todos los servicios del SERMAS:

- **Actividades orientadas a controlar los niveles de Servicio:**
 - Medir los indicadores (KPI) y elaborar informes periódicos que sirvan para calcular los niveles de cumplimientos de los acuerdos de nivel de servicio (ANS) establecidos. La DGSIS verificará la exactitud de los indicadores medidos por el proveedor. Si se detectan desviaciones o mediciones erróneas, podrán aplicarse las penalizaciones establecidas, como si el indicador medido erróneamente estuviera por debajo de los niveles exigibles de cumplimiento de los ANS.



- Elaborar informes describiendo y justificando las circunstancias que puedan afectar a las medidas de los KPI calculados.

Los informes deberán entregarse con periodicidad mensual, en un plazo máximo de 5 días naturales, a contar desde el fin del período de medición.

- **Actividades orientadas a mantener los niveles de seguridad de las capas tecnológicas:**

- Analizar, acometer acciones y asegurarse de la implementación de los estándares de seguridad de la tecnología, así como las arquitecturas y soluciones estándar de Sistemas de Información.
- Analizar e implementar las recomendaciones de seguridad para los servicios actuales y futuros y su adecuación para el cumplimiento de la Ley Orgánica de Protección de Datos (LOPD), Esquema Nacional de Seguridad (ENS), GDPR, así como con las leyes y normativa aplicables a los sistemas de información públicos sanitarios en este momento, incluyendo, informar a la DGSIS en tiempo real y llevar el registro de incidentes que hayan tenido consecuencias para sistemas o los datos.
- Detectar y notificar los incidentes, vulnerabilidades y mal uso que puedan ocasionar riesgos de seguridad siguiendo los procedimientos y estándares de la DGSIS. Asegurarse de la identificación y control de elementos de los equipos, y la existencia de autorización de los cambios a los mismos, así como investigar el uso que se da. Velar por el adecuado nivel de aplicación de parches de seguridad en los sistemas, así como establecer su Nivel de Criticidad de Implantación, conforme a la normativa interna e, igualmente, analizar el impacto de la implantación de los nuevos parches/versiones, Analizar y asegurarse del nivel de respaldo que tienen los equipos y sus elementos, la retención de las copias, los procedimientos de copia de seguridad y restauración (backup y restore), así como realizar pruebas de efectividad de dichos procedimientos de backup y restore de forma periódica. Analizar y promover la auditoría de los sistemas (log) y trazabilidad de las actividades, así como ayudar en la investigación y entendimiento de dichos logs

- **Actividades orientadas a mantener los Planes de Contingencia:**

Estas actividades se desarrollarán de forma acorde con la estrategia establecida desde el Plan de Continuidad de CEDAS y conforme al estándar ISO/IEC 24762:

- Revisar y mantener actualizado el Plan de Continuidad de CEDAS, teniendo en cuenta el escenario resultante de las siguientes actividades, actualmente próximas a su finalización:
 - Evolución y continuidad del CPD Extendido (CPD Aduana + CPD Athene@), e en su defecto cualquiera de las ubicaciones que formen el CPD Extendido del SERMAS.



- Evolución y continuidad del equipamiento en el CPD Tres Cantos.
- Implantar y mantener actualizada la organización y los recursos necesarios para garantizar la continuidad de los servicios mínimos en contingencia.
- Proponer, definir, implantar y mantener actualizados, con la aprobación de la DGSIS, procedimientos de recuperación, así mismo, proponer, definir e implantar procedimientos orientados a la definición de flujos u operativas de continuidad.
- Colaborar en el diseño y realización de las pruebas y/o simulacros de contingencia y proponer acciones correctivas de mejora, de acuerdo con el resultado de dichas pruebas.
- Validar que los procedimientos y políticas de respaldo y recuperación definidos soportan el nivel de servicio requerido por los sistemas y los usuarios. Validar que la actualización de la infraestructura (servidores, redes, almacenamiento, etc.) para soportar nuevos niveles de recuperación requeridos por la DGSIS se ajusta esos nuevos niveles.
- Elaborar informes puntuales y/o periódicos de incidentes críticos que puedan derivar o no en desastres.
- Participar en planes y acciones de mejora preventiva u otros mecanismos que se establezcan, orientados a garantizar la continuidad del negocio, y verificar los resultados de los mismos.

El detalle de las estrategias de continuidad de la DGSIS se dará a conocer exclusivamente al contratista, por razones de seguridad y confidencialidad.

Los simulacros y las pruebas serán realizados con periodicidad de 6 meses, siendo obligatoria una prueba completa a los 12 meses, por los mismos recursos que están prestando el servicio regularmente, y se realizarán en los horarios a convenir por la DGSIS.

La DGSIS podrá revisar el Modelo de Gestión, debido a necesidades de evolución del mismo, incluyendo los procesos, la definición de las actividades, responsabilidades, entradas y salidas del servicio que se consideren necesarios. En el caso de producirse dicha revisión, los cambios serán comunicados al proveedor con una antelación mínima de 30 días naturales, con respecto a su entrada en vigor, para que proceda a actualizar y corregir la documentación afectada.

5.1.6 Servicios de diseño de arquitecturas y automatización de servicios TIC

Estos servicios estarán orientados al diseño de arquitecturas y sistemas de automatización y auto aprovisionamiento de servicios, para la generación de eficiencias en la prestación de los servicios TIC y su evolución con una orientación de mejora continua, para adaptación plena a las necesidades del SERMAS.

Por tanto, incluirá actividades orientadas al diseño y puesta en marcha de los procesos y herramientas necesarios para la evolución del modelo único de gestión centralizada de infraestructuras hacia un modelo aún más evolucionado, para la prestación de los servicios TIC en modo cloud privado. Para ello, el



adjudicatario deberá ofrecer los recursos, herramientas software y servicios asociados de consultoría, diseño y transformación de las tareas de operación y procesos de administración para que los procesos de negocio puedan ser provisionados desde una arquitectura adaptativa y definida por software, que permita una transformación paulatina de los sistemas de información centralizados para que puedan ser consumidos desde una plataforma de auto aprovisionamiento IaaS, PaaS y SaaS, en base a políticas del SERMAS.

Estos servicios deben permitir la ejecución de las tareas y actividades definidas en base al programa de transformación del modelo de servicio solicitado en este PPT.

5.1.7 Otros Servicios

Se trata de servicios complementarios al resto de los contemplados en el contrato. Entre ellos:

- **Evaluación de costes:** se proporcionarán los informes de costes del servicio por el contratista, con el nivel detalle, alcance y periodicidad que determine la DGSIS, al menos, mensual.

Se dispondrá de un modelo de costes por servicio, diseñado y puesto en ejecución en el marco del contrato. Dicho modelo se desglosará según se estime por la DGSIS, como mínimo, por centro/sistema/tipo de usuario.

Se valorará la dotación de una aplicación de gestión de costes. Si el contratista dota de una aplicación de gestión de costes para dar soporte a las actividades solicitadas en el pliego, deberá proveer, a la finalización del contrato, de la correspondiente descarga, en formato normalizado, de todos los datos utilizados en esta evaluación de costes. Así mismo, indicará en su oferta si las licencias de la aplicación de costes se ceden para uso indefinido al SERMAS o únicamente para el período de contrato

- **Análisis de riesgos:** se llevará a cabo un análisis de los riesgos, en relación con las infraestructuras objeto del servicio, con la periodicidad determinada por la DGSIS, al menos, trimestral. Adicionalmente, la DGSIS podrá solicitar informes específicos de riesgos, sobre ámbitos concretos del servicio, que el contratista deberá proporcionar en el plazo que se acuerde. En los informes se incluirán propuestas de gestión de los riesgos detectados, en su caso.

5.2 SERVICIOS DE MANTENIMIENTO DE EQUIPAMIENTO HARDWARE Y SOFTWARE

Para asegurar los objetivos de calidad en la disponibilidad de los servicios TIC, se debe incluir en este contrato el mantenimiento del equipamiento informático, que asegure la intervención correctiva necesaria para resolver todos los incidentes, tanto de hardware como de software y/o firmware de base, que pudieran causar una interrupción del servicio. Todo ello asegurando unos tiempos de respuesta adecuados.

En concreto, se requiere el mantenimiento del equipamiento informático relacionado en el anexo III. En los citados anexos se incluye información relativa al equipamiento y al período de solicitud de mantenimiento para cada equipo.



Este servicio estará centralizado en un único punto donde se reciban y coordinen las peticiones de asistencia y se canalicen las consultas.

El acceso al servicio será a través de un número único de teléfono con llamada gratuita, donde se atiendan las peticiones, tanto de servicio, como de seguimiento de las incidencias e informes sobre las mismas.

El control del servicio estará organizado alrededor de una aplicación informática que gestione la asignación de incidencias al técnico que mejor las pueda atender, en razón a su proximidad geográfica y a su entrenamiento específico.

El contratista incluirá un conjunto de servicios y utilidades colaterales que garanticen el correcto funcionamiento del servicio de mantenimiento y proporcionen la información periódica necesaria sobre las incidencias ocurridas. Dicho conjunto se concretará en la fase del servicio Planificación de la Transición.

El contratista dispondrá de una aplicación de gestión de incidencias, en la que se registrarán todas las intervenciones llevadas a cabo, y a través de la cual proporcionará información detallada y de tipo estadístico de dichas intervenciones, con la periodicidad que se desee por parte del SERMAS. Como mínimo se dará esta información con carácter mensual siendo potestad de la DGSIS la solicitud de informes detallados en cualquier momento.

La prestación del servicio de mantenimiento será de 24 horas al día, todos los días del año para aquellos sistemas de misión crítica, que supongan una interrupción de los servicios (según Anexos III). En dichos anexos se indica otro equipamiento que contempla distintos tiempos de cobertura.

El contratista deberá proporcionar servicios de mantenimiento certificados por los fabricantes del equipamiento objeto de los mismos. Es necesario que el licitador propuesto como adjudicatario acredite, como requisito para la formalización del contrato, según se establece en el pliego de prescripciones administrativas, estar en disposición de prestar el servicio de mantenimiento certificado de los fabricantes del equipamiento objeto de dicho servicio, en concreto de los fabricantes siguientes: VMWARE, DELL-EMC, HPE, FUJITSU, FORTINET, F5, CHECKPOINT, INFOBLOX, RADWARE, CISCO, FLUKE, DYNATRACE, ENSEMBLE, MICROFOCUS DATA PROTECTOR, ALIEN VAULT, RED HAT, MICROSOFT.

El contratista debe disponer de personal técnico, dentro del área geográfica de la Comunidad de Madrid, convenientemente entrenado en todos los sistemas objeto de este contrato.

Este servicio de mantenimiento se estructura en 3 niveles de escalado de incidencias:

- **1º nivel:** correspondiente a la atención inicial de todas las llamadas por un técnico especialista del grupo técnico, que garantizará una atención especializada desde el mismo instante en que el usuario contacta con el proveedor de servicios, tanto para realizar consultas técnicas o plantear dudas acerca del uso y manejo de los sistemas, como para comunicar un problema.



- **2º nivel:** el contratista contará con un grupo de soporte técnico disponible las 24 horas del día, 7 días a la semana para resolver cualquier situación conflictiva que los técnicos locales no puedan manejar adecuadamente. Este grupo actuará igualmente como soporte de segundo nivel para los especialistas del grupo técnico que se encargan de clasificar las llamadas y diagnosticar los problemas comunicados por los usuarios.
- **3º nivel:** el contratista dispondrá de un tercer nivel de soporte técnico, que garantice la resolución de cualquier tipo de problema que pudiera surgir durante la vida útil de los equipos instalados.

En el caso de que el coste de mantenimiento de un equipamiento supere al coste de reposición o que, por obsolescencia de un equipamiento, se produzca, una discontinuidad en el soporte del fabricante que imposibilite dar el adecuado mantenimiento a ese producto, el contratista podrá proponer al SERMAS una sustitución de dicho equipamiento por uno nuevo, siempre que su calidad y potencia sea, al menos, la del equipamiento a sustituir. La sustitución se realizará sólo si el SERMAS la aprueba. En estos casos, igualmente, el SERMAS podrá proponer dicho cambio.

El SERMAS podrá interrumpir el contrato de mantenimiento de cualquiera de los elementos que considere oportuno, de manera unilateral y con preaviso de 60 días naturales. El importe correspondiente al servicio interrumpido se podrá destinar a incrementar el volumen de servicios de igual naturaleza que los contenidos en este pliego.

5.2.1 Mantenimiento preventivo de los equipos

Se realizará mantenimiento preventivo a los equipos contemplados en el contrato (anexos III), de acuerdo con las especificaciones de cada sistema, con el fin de evitar el deterioro de los mismos y reducir el riesgo de avería.

La prestación de este servicio se podrá hacer coincidir con el desplazamiento para la resolución de una avería. La frecuencia de las revisiones de mantenimiento preventivo será de, al menos, una cada 6 meses.

En el caso de que el mantenimiento preventivo de un determinado equipo requiera una parada planificada del mismo, se organizará con el responsable del Centro afectado el momento idóneo para realizar dicha parada.

5.2.2 Asistencia software

Consistirá en la prestación de los siguientes servicios asociados al software básico del equipamiento:

- **Servicio de asesoramiento telefónico.** Responderá a consultas relativas a procedimientos operacionales y sospecha de anomalías en el funcionamiento de los productos.
- **Servicio de información.** El contratista facilitará la información existente sobre la disponibilidad de nuevos niveles y versiones de los productos contratados.



- **Servicio de comunicación sobre el software.** El contratista facilitará modificaciones o soluciones alternativas a las anomalías de software que comunique el SERMAS, en un formato legible, junto con la documentación adecuada. El SERMAS facilitará, a su vez, los datos necesarios para reproducir el entorno en que se produjo la anomalía.
- **Servicio de instalación de actualizaciones.** El contratista facilitará al SERMAS asistencia técnica telefónica para la instalación de los nuevos niveles o versiones facilitados por el servicio de actualización, así como en relación a las soluciones proporcionadas por el servicio de comunicación sobre el software. Las adaptaciones del software a las necesidades del SERMAS y el establecimiento de parámetros específicos del mismo se harán por cuenta del contratista.
- **Servicio de documentación.** Previa petición del SERMAS, el contratista facilitará asistencia técnica para el diagnóstico e identificación de anomalías significativas en la versión vigente del software, así como para notificar y documentar adecuadamente tales anomalías.

5.3 SERVICIOS DE TRASLADO DE EQUIPAMIENTO TI Y ADECUACIÓN DE LAS CONFIGURACIONES A UN POSIBLE NUEVO CPD DEL SERMAS

El CPD de Aduana es uno de los CPD que forma parte del CPD extendido del SERMAS. Desde sus inicios este CPD se dimensionó acorde con las necesidades que en ese momento se tenían, contemplando un crecimiento acorde a los planes estratégicos del SERMAS. Actualmente el CPD ha llegado a su límite de crecimiento y son múltiples los problemas asociados a sus infraestructuras básicas: limitación de los equipos de aire acondicionado, limitación para ampliar la capacidad de las UPS y grupo electrógeno e imposibilidad de incorporar más equipamiento TI por limitación del espacio físico de la sala técnica entre otros problemas.

Debido a las limitaciones de este CPD, el SERMAS está analizando opciones para disponer de un nuevo CPD que sustituya al de Aduana. Durante la vigencia de este contrato se prevé que el SERMAS disponga de dicho CPD. En caso de ser así, el adjudicatario de este contrato tendrá que realizar la migración y puesta en marcha del equipamiento que preste servicio a los sistemas centralizados en el CPD Aduana a la nueva ubicación, configurando los servicios necesarios para que se preste el servicio con normalidad.

En dicho proceso, se requiere garantizar la máxima disponibilidad de servicio durante el traslado para los sistemas de información centralizados dentro del alcance de este contrato, teniendo en cuenta la protección de la información y la continuidad de los servicios ofrecidos desde el CPD extendido y en ningún caso las tareas asociadas implicarían una pérdida de servicio planificada por traslado superior a las cuatro horas.

Las migraciones se efectuarán en la fecha determinada por el SERMAS, siendo la previsión inicial de su ejecución durante fines de semana, en horarios nocturnos, fiestas, y, en general, aprovechando periodos de menor servicio para así minimizar el impacto.



El contratista una vez conocida la nueva ubicación y características del CPD sustituto de Aduana, deberá preparar un proyecto o plan de migración que garantice el menor impacto en el servicio. Para la ejecución de dicho plan, la DGSIS facilitará la relación con otros proveedores implicados en este proyecto.

Elementos mínimos a contemplar en un proyecto de traslado

El proyecto de migración debe contemplar como mínimo las siguientes actividades y tareas:

- **Actividad 1: Estudio y definición del plan de migración para todo el equipamiento de sistemas y de almacenamiento.**

Contempla las siguientes tareas:

- Actualización/realización del inventario de servidores, almacenamiento y elementos de conectividad asociados.
- Identificación de componentes adicionales de servicio en equipamiento de servidores, almacenamiento y conectividad requeridos para el proceso de la migración.
- Aprobación del diseño de la topología de la red de comunicaciones y SAN, para las nuevas ubicaciones y para el proceso de migración.
- Comprobación del modo de prestación correcta del servicio en funcionamiento en uno solo de los dos nodos activos del SERMAS, activación del respaldo y puesta en marcha en el destino.
- Estrategia y plan de migración teniendo en cuenta el entorno de aplicaciones actualmente operativo.

El entregable de esta actividad será el plan de migración, contemplando todas las tareas asociadas con sus hitos, así como el plan de pruebas y riesgos asociados.

- **Actividad 2: Desconexión y encendido del equipamiento.**

A continuación se detalla el contenido de esta actividad, incluyendo sus requisitos previos y entregables.

Se consideran requisitos para la ejecución de esta fase las siguientes:

- Haber validado el diseño y plan de migración.
- Disponer de la infraestructura necesaria de comunicaciones entre ubicaciones (sites).
- Disponer de las adecuadas condiciones de entorno de la salas del CPD destino en cuanto a fuentes de alimentación, refrigeración e infraestructura de suelo.
- Disponer de una copia de seguridad actualizada de toda la información.



- Una vez realizado el diseño de la solución y el plan y estrategia de traslado, el contratista asumirá las tareas de definir y ejecutar el plan de pruebas unitarias para cada uno de los equipamientos.

La Actividad 2 comprende las siguientes tareas:

- Adaptación y ejecución del plan de pruebas unitarias, incluyendo pruebas de conectividad, acceso, y funcionalidades software para los sistemas, coordinado con los servicios y aplicativos previamente definidos.
- Parada del equipamiento en CPD origen.
- Desinstalación del equipamiento.
- Fijación e instalación en la nueva sede.
- Instalación de elementos de conectividad adicional y configuración de los switches o directores.
- Conexión física de los servidores y de las cabinas de almacenamiento, elementos de conectividad y arranque en los CPD de destino.
- Puesta en marcha de las funcionalidades software disponibles en los servidores y almacenamientos, incluyendo las de copia local y remota.

Los entregables en la actividad 2 serán:

- Definición de plan de pruebas de conectividad y acceso de los sistemas:
 - Pruebas de acceso y visibilidad de servidores.
 - Pruebas de acceso y visibilidad en los almacenamientos.
- Plan de marcha atrás para cada uno de los sistemas y/o grupos de sistemas involucrados en la migración. Este plan permitirá, en caso de ser necesario, volver a la situación inicial.
- Infraestructura de gestión de almacenamiento instalada y en marcha.
- Actualización del plan de pruebas y resultado de las mismas.
- Documento de análisis de rendimiento y configuración.
- Presentación de los resultados.

Cualquier actividad o tarea adicional que el contratista considere necesario deberá ser incluido en el plan de migración. En todo momento y mientras dure la migración, el contratista garantizará con los mismos servicios para ambos CPD (Aduana y su sustituto).



5.4 SERVICIOS EN MATERIA DE SEGURIDAD DE LOS CENTROS DE PROCESO DE DATOS

Entre las diferentes unidades de la DGSIS está la Oficina de Seguridad (OSSI), encargada de establecer las directivas y planes globales en materia de seguridad de los sistemas de información. Adicionalmente, cada unidad es responsable de garantizar el cumplimiento de las directrices globales del SERMAS en materia de seguridad dentro de su ámbito competencial.

En lo que respecta a los CPD, CEDAS es responsable de garantizar la puesta en marcha de medidas técnicas y organizativas para asegurar el cumplimiento de los planes globales del SERMAS y específicamente, las directrices sobre este tema que se marquen desde la OSSI. Así mismo, las dependencias en las que se ubican los CPD disponen de una serie de medidas de seguridad que tienen que ser trasladadas a los CPD sin contravenir la legislación vigente o los planes globales del SERMAS en este aspecto.

En concreto, se considera especialmente relevante el cumplimiento de la normativa vigente en materia de seguridad y en particular con especial énfasis en las siguientes normas legales:

- Protección de infraestructuras críticas (PIC):
 - Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
 - Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Legislación de protección de datos de carácter personal:
 - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
 - Real Decreto 1720/2017 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 21 de diciembre, de protección de datos de carácter personal.
 - Reglamento General de Protección de Datos (RGPD). Norma europea que está en vigor desde el 25 de mayo de 2016, comenzará a aplicarse el 25 de mayo de 2018 y sustituirá a la actual normativa vigente.

Adicionalmente, es obligatorio el cumplimiento de normas directamente relacionadas con las instalaciones de un CPD (protección contra incendios, seguridad de accesos físicos y lógicos, actualizaciones de parches de seguridad y medidas similares).

Como aspecto estratégico dentro del SERMAS, la garantía de la seguridad es un aspecto crítico. En esta línea, el contratista de CEDAS tendrá que realizar las siguientes tareas:

- Colaborar con la OSSI y otras unidades de la DGSIS en la elaboración de planes y medidas de seguridad relacionadas con el alcance de este contrato y con objeto de asegurar el cumplimiento



de la normativa vigente de cualquier aspecto relacionado con la seguridad de los CPD y sistemas de información alojados en esos CPD.

- Adecuación y seguimiento de los procesos definidos por el Esquema Nacional de Seguridad (ENS).
- Instalación y gestión de las herramientas adecuadas para el control del cumplimiento del ENS, sugeridas por el CCN-CERT.
- Proponer medidas a adoptar para mitigar o corregir vulnerabilidades de seguridad en los CPD.
- Asesorar técnicamente a la DGSIS en las medidas a adoptar en materia de seguridad.
- Ejecutar aquellas medidas que se aprueben en la DGSIS y que estén relacionadas con el marco competencial de CEDAS.
- Realizar un seguimiento de la ejecución de los planes de seguridad en los distintos niveles (organizativo y/o técnico). Los desvíos o incumplimientos se analizarán proponiendo medidas que mitiguen esos retrasos.
- Emitir informes sobre normativa vigente, su modificación o derogación, que sea aplicable en materia de seguridad de los CPD y en general, en al ámbito competencial del CEDAS.
- Emitir cualquier informe a demanda de la DGSIS relacionado con cualquier aspecto de seguridad encuadrado en el ámbito de los CPD. Estos informes podrán ser solicitados por la DGSIS en cualquier momento durante la vigencia del contrato. Sin menoscabo de lo anteriormente indicado, al menos una vez al año se emitirá un informe sobre el estado global de la seguridad de los CPD.

La DGSIS potenciará y facilitará la comunicación con otras unidades para asegurar un marco común de seguridad global, en el que cada unidad de la DGSIS proponga y ejecute las medidas en materia de seguridad correspondientes a su ámbito de competencia.

Adicionalmente, la DGSIS podrá solicitar cualquiera de estas tareas u otras nuevas similares sobre otras normas técnico-legales vigente en cada momento y que sean de aplicación directa en los CPD.

5.5 PROGRAMA DE TRANSFORMACIÓN DEL MODELO DE SERVICIO

El SERMAS, mantiene los objetivos de continuar con las políticas de integrar, consolidar y centralizar los diferentes entornos funcionales, minimizando la prestación de servicios TI desde los CPD locales de hospitales y maximizando dicha prestación en los CPD centrales del SERMAS. El objetivo es proporcionar servicios TIC de la máxima calidad, alineados con los objetivos estratégicos de la organización, cada vez más eficientes, con unos costes sostenibles, mejorando el impacto medio ambiental y reduciendo la factura eléctrica.



El SERMAS persigue la transformación del modelo de servicio TI hacia un modelo de HYBRID IT donde las TI, en modo “tradicional”, sean transformadas y definidas en un catálogo de servicios en modo IaaS, PasS o SaaS, cuya base fundamental consista en la implantación de distintas herramientas Cloud Computing de ámbito, inicialmente, privado, en perfecta coordinación con las tareas de administración y operación regular, para evitar impacto de los cambios necesarios, en la prestación normal de los servicios y la producción de los sistemas de información.

El licitador debe presentar en su oferta un **“plan de transformación del servicio”** detallado, que describa los objetivos, fases, tareas/actividades y el horizonte temporal en que desarrollará la evolución y mejora continua del servicio hacia ese modelo.

Este plan de transformación tendrá como objetivo la gestión del cambio y la mejora del servicio en términos de incremento de la agilidad, funcionalidad, calidad, eficiencia y reducción de costes, debiendo estar alineado con las líneas estratégicas en materia de sistemas e infraestructuras de la organización.

Por tanto, las líneas estratégicas a las que debe ir enfocado el plan de transformación del servicio son las siguientes:

- Incremento de la eficiencia y productividad: permitiendo la operación y gestión de los CPD de manera automática y con la ayuda de un portal de autoservicio, haciendo uso de herramientas Cloud.
- Mejorar el alineamiento de TI con el negocio.
- Agilidad en la operación y administración: basado en concepto automatización que garantiza la inmediatez en la ejecución de procesos.
- Decremento de costes: potencial reducción de costes por la automatización de actividades repetitivas.
- Escalabilidad y flexibilidad: alineamiento con el volumen de demanda.
- Adaptabilidad: modificación rápida y simple de procesos automatizados.
- Mejora en los acuerdos de nivel de servicio (SLA): en base a que los procesos automatizados aúnen en la eficiencia y obtención de datos inmediata y veraz.
- Reducción de errores y mejora de la disponibilidad de los sistemas: la automatización y el autoservicio permite minimizar los procesos en los que la intervención humana pueda generar errores o retrasos.
- Satisfacción de los equipos de trabajo: mediante la eliminación de la ejecución de tareas repetitivas y no satisfactorias.
- Mejora en la seguridad global, permitiendo micro segmentación.

En consecuencia el nuevo modelo de prestación de servicios debe favorecer los mecanismos en la prestación de los servicios de información sanitarios para:

- Optimizar y hacer más eficiente el uso de los recursos disponibles.



- Homogeneizar y estandarizar los procesos y los servicios.
- Gobernar los servicios para que garanticen las necesidades del SERMAS y fomenten el trabajo colaborativo.
- Simplificar y aunar procesos.
- Facilitar la transferencia de conocimiento y la independencia tecnológica.
- Promover un mayor nivel de autonomía en la gestión.
- Facilitar un mejor control del rendimiento de los sistemas.

Estos requisitos derivan a que sea necesario la implementación de nuevas tecnologías que se adapten con rapidez y flexibilidad a la demanda, así mismo que faciliten la innovación y el despliegue de nuevos servicios.

Por tanto, el adjudicatario para la ejecución de plan de transformación pondrá a disposición del SERMAS las herramientas software y recursos humanos necesarios de consultoría, diseño, implantación y ejecución del programa de transformación del modelo de servicio durante la duración del contrato.

El detalle de actividades y entregables que debe contener dicho plan dentro del ámbito del nuevo CEDAS es el siguiente:

- **ANÁLISIS DE LA SITUACIÓN ACTUAL**
Analizar la situación actual en cuanto a procesos y métodos de trabajo se refiere y proponer un nuevo modelo completo que permita adaptar la operativa cotidiana a los requisitos del SERMAS y al nuevo modelo de gestión de infraestructuras del SERMAS. El primer análisis y propuesta de modelo deberá entregarse por el contratista antes del comienzo de la Fase de Servicio Regular.
- **REVISIÓN Y ADAPTACIÓN DE LA ARQUITECTURA DE GESTIÓN ACTUAL.**
Liderar la generación de la evolución del actual marco centralizado de gestión de infraestructuras del SERMAS mediante la extensión del modelo de servicio vigente en la unidad funcional de CEDAS. Para ello, la arquitectura de gestión actual debe ser revisada y adaptada, de forma que contemple adecuadamente las peculiaridades de gestión de los centros de atención sanitaria del SERMAS.
- **ELABORACIÓN DE PROCEDIMIENTOS DE GESTIÓN CENTRALIZADA.**
Establecer un conjunto de métodos homogéneos de trabajo, procedimientos de actuación, arquitecturas tecnológicas y recursos humanos especializados, que sean de aplicación, con carácter común, a las actividades de gestión de todas las infraestructuras tecnológicas del SERMAS. En este sentido, es necesario que el contratista, por una parte, adapte los procedimientos existentes de CEDAS al nuevo ámbito y, por otra, elabore los nuevos procedimientos que, sin existir actualmente, sean requeridos como parte de la evolución del actual modelo de gestión centralizada.
- **HERRAMIENTA DE AUTOMATIZACIÓN DE PROCEDIMIENTOS.**
Implantar una herramienta o conjunto de herramientas que permita automatizar todos los procedimientos repetitivos que se ejecuten sobre los sistemas e infraestructuras, en especial los



relacionados con las subidas de versiones de aplicaciones y de sistemas de información en los entornos de producción y preproducción. Mediante la herramienta de automatización de procesos se agilizarán tareas tan importantes como los despliegues de versiones de aplicaciones y sistemas de información, tratamiento de ficheros de log, tratamiento de información histórica y cualquier actividad que contribuya a lograr los objetivos de rentabilidad y eficiencia en el ámbito de las actividades y tareas desarrolladas actualmente de manera manual en el ámbito de la ejecución de este contrato, incrementando a la vez la calidad y la seguridad en las operaciones.

El despliegue efectivo de estas herramientas, proporcionadas por el adjudicatario, deberá estar materializado dentro de los 12 primeros meses desde la entrada en vigor del contrato.

- **MODELO DE INTEGRACIÓN**

Definir los mecanismos que aseguren el funcionamiento coordinado de los ámbitos de servicio establecidos, que son los siguientes:

- Servicios de infraestructura TIC común.
- Servicios de infraestructura de sistemas de información.
- Servicios comunes de gestión y gobierno.

Definir un nuevo modelo de integración entre los actores de los servicios de infraestructura y los servicios de sistemas de información, con objeto de garantizar la adecuada coordinación entre los mecanismos de operación, soporte y gestión, tanto de las infraestructuras implicadas, como de las aplicaciones o sistemas de información involucrados. Dicho modelo de integración debe incluir, además de otros que puedan ser identificados posteriormente por el contratista o por la DGSIS, los procesos de:

- Puesta en producción.
- Solicitud de trabajos.
- Comunicación de incidencias.
- Reclamaciones, problemas y riesgos.
- Proceso de gestión de cambios y control de configuración.

- **PLAN DE CONTINUIDAD Y CONTINGENCIA**

Diseñar un nuevo plan de continuidad de los CPD del SERMAS, describiendo las actividades necesarias para asegurar la disponibilidad de los servicios en caso de contingencia y desarrollando y actualizando los planes de contingencia específicos para los Sistemas de Información citados en el Anexo VI.

- **CATALOGO DE SERVICIOS**

Elaborar un Catálogo de Servicios que puedan ser provisionados a través de un portal de auto servicios, en modelo Cloud, que incluya, además de los servicios relacionados con la gestión de infraestructuras de los servicios centrales y los servicios de gestión de infraestructuras orientados a cubrir las necesidades de los centros del SERMAS.



5.5.1 Automatización de tareas de operación basada en DevOps

Uno de los principales objetivos dentro del programa de transformación del modelo de servicio, a lo largo de la duración del contrato, es el de automatizar el ciclo de vida de las aplicaciones, implantando modelos DevOps (desarrollo y operaciones). Para ello, la DGSIS requiere del proveedor un plan específico al respecto con los objetivos de:

- Reducir el número de tareas manuales, que redundan en tener más tiempo para seguir con la automatización de otras tareas o poder acometer otras actividades de mayor valor.
- Crear un ambiente de codificación y modelamiento de las aplicaciones que facilita la cooperación entre los equipos de desarrollo y los equipos de operación.

Y debe estar apoyado sobre cuatro pilares fundamentales que cubren el Ciclo de Vida productivo:

- **Integración Continua**

La integración continua será la encargada de comprobar que cada actualización de código fuente no genere problemas en una aplicación que se está desarrollando. Permitirá a los equipos detectar problemas en una etapa temprana del ciclo. Dentro de la Integración Continua se realizarán las pruebas continuas que consistan en automatizar e integrar las pruebas individuales, funcionales y no funcionales en la cadena de entrega del software, y en ejecutar dichas pruebas automáticamente para cada compilación del código base. Jugará un papel muy importante los perfiles de integración para definir y garantizar el proceso.

- **Entrega e Implementación Continua**

La entrega continua se encargará, una vez alcanzado un grado de madurez adecuado en su fase de desarrollo, en controlar y realizar su lanzamiento a producción en cualquier momento, de modo que cualquier aplicativo o servicio esté listo siempre para la producción.

Las principales características son:

- El software se puede implementar en cualquier momento sin perjuicio para la producción y en cualquier fase del **Ciclo de Vida** del desarrollo.
- Facilita a los equipos de desarrollo priorizar la posibilidad de que se realice una instalación del software por encima de la incorporación de nuevas características de la misma.
- Facilita la construcción rápida de instalables de forma automática y con la disponibilidad de la puesta en producción de los sistemas en todo momento.
- Facilita la realización de instalaciones de cualquier versión en cualquier entorno y bajo demanda.

Para lograr el éxito de la entrega e implementación continua es necesaria una estrecha relación entre las áreas de Desarrollo, Integración y Operación



- **Operaciones Continuas.**

Sera la encargada de controlar y gestionar los cambios de software y hardware garantizando que no se producen interrupciones que puedan afectar a los usuarios finales. El proceso de aplicación de revisiones y el paso a la conformidad de las mismas estarán englobadas en esta función.

Mientras que el software y los servidores pueden desconectarse durante un mantenimiento planificado, las operaciones continuas se encargaran de que los clientes reciban servicio de una versión anterior de la aplicación hasta que la nueva se haya probado e implementado correctamente.

- **Evaluación y Mejora continua**

Será la encargada de evaluar los resultados y controlar las necesidades para la mejora de cada una de las etapas del proceso.

5.5.2 Solución tecnológica de infraestructura Cloud privada en los CPD centrales del SERMAS

En lo que concierne a la provisión e implantación de herramientas que permitan al SERMAS la transformación del modelo de gestión hacia un modelo de auto servicio en Cloud privado, proporcionando IaaS, PasS o SaaS, el adjudicatario pondrá a disposición del SERMAS una plataforma tecnológica en modo servicio y con mantenimiento, durante la duración de este contrato, para cubrir, al menos, las funcionalidades que se indican a continuación. Además, el adjudicatario deberá indicar el grado de cumplimiento en detalle de todos los requerimientos, así mismo el adjudicatario deberá indicar cuál sería su planteamiento en el caso de que no soporte alguna de las funcionalidades requeridas y detalladas a continuación:

- **A nivel general:**

- El adjudicatario deberá diseñar, instalar, implantar y mantener una solución Software y hardware de Cloud privada.
- La solución Software de Cloud privada deberá estar soportada por un fabricante. El adjudicatario deberá aportar certificación al respecto de dicho fabricante.
- La infraestructura debe proveer de una forma estándar e integral los siguientes servicios o disponer de las siguientes características:
 - Servicios Cloud IaaS
 - Servidores virtuales con distintos niveles de capacidad de proceso (Cloud IaaS)
 - Servidor físico dedicado
 - Servicios Cloud PaaS/SaaS



- Entorno de desarrollo ágil con la posibilidad de integración de Cloud Públicas que incorporen el mismo entorno de desarrollo, que ofrezca al menos las funcionalidades que aporta un entorno como “Cloud Foundry”
 - Características de hibridación
 - Hibridación con la infraestructura legacy actual de los CPD del SERMAS.
 - Hibridación con la actual Cloud Privada del SERMAS basada en tecnología VMware.
 - Hibridación con otras Cloud Públicas.
 - Portal de autoservicio.
 - La solución de Cloud Privada debe ser capaz de reutilizar las infraestructuras actuales del SERMAS (Cómputo, Almacenamiento e infraestructura de red).
 - El proveedor deberá disponer de capacidades de Cloud Pública en alta disponibilidad ubicada en Madrid compatible con la solución Cloud Privada propuesta, certificada en Esquema Nacional de Seguridad en su Nivel Alto.
 - El proveedor deberá ser capaz de proporcionar una solución de gestión de APIs, ubicada en Madrid, para la interconexión de otras entidades que puedan requerir integración con el servicio de Cloud Privada del SERMAS.
 - Cualquier optimización, script o mejora que el proveedor desarrolle sobre las herramientas suministradas para prestar el servicio de Cloud Privado debe ser comunicada a la DGSIS y pasará a ser propiedad de la DGSIS, sin que el proveedor pueda reclamar ningún tipo de compensación adicional.
- **Ámbito de uso**

Aunque no deben estar limitadas por diseño, las aplicaciones funcionales que la DGSIS solicita para esta Cloud Privada son las siguientes:

- Proyectos de implantación de una solución de auto provisión de **entornos de desarrollo** dentro del marco normativo de la DGSIS y siguiendo las directrices de trabajo marcadas por la misma en su relación con terceros:
 - Proporcionar entornos de trabajo de desarrollo para personal de la DGSIS.
 - Proporcionar entornos de trabajo de desarrollo para proveedores externos de la DGSIS.
 - Proporcionar a la DGSIS un entorno normalizado de compilación para desarrollos DGSIS.
- **Proyecto IaaS para albergar servicios de pruebas y POC para la DGSIS**
 - Proporcionar servicios IaaS que sean utilizados con métodos de auto provisión a los interesados bajo las normativas de la DGSIS tanto desde dentro de Macrolan como externamente desde Internet.
- **Proyecto de entorno de IaaS/PaaS/SaaS certificación/producción**



- Proporcionar entornos para aplicaciones departamentales de Hospitales que quieran ser centralizadas por parte de la DGSIS.
- Proporcionar entornos para aplicaciones centralizadas que establezca la DGSIS
- **Proyecto de Housing**
 - Proporcionar servicios IaaS / PaaS / SaaS para terceros dentro del ámbito de la DGSIS.
- **Requerimientos mínimos respecto a cómputo (servidores virtuales):**
 - Portal de auto aprovisionamiento.
 - Para los entornos de SSOO en IaaS deberá proveer plantillas de al menos los Sistemas Operativos (SSOO) Linux (Red Hat Enterprise, Suse, CentOS y Ubuntu) y Windows Server.
 - El entorno deberá proveer imágenes estandarizadas de SSOO, no obstante, el SERMAS podrá generar sus propias imágenes para su utilización directa desde la consola de generación de sistemas virtuales.
 - Sobre los servidores Cloud se deberán poder realizar al menos las siguientes operaciones:
 - Creación/borrado de un servidor.
 - Aprovisionamiento en base a funciones script.
 - Auto escalado (crecimiento y decrecimiento) del servidor virtual.
 - Arranque o parada del sistema.
 - Liberación o regeneración de un sistema.
 - Reinicio del sistema.
 - Creación de grupos de servidores.
 - Generación de sistemas que sean independientes físicamente.
 - En lo que se refiere a los sistemas (servidores) IaaS, sobre los que podrán realizarse por parte del SERMAS las operaciones indicadas anteriormente:
 - Servidores virtuales:
 - Deberán proveerse diferentes tipos de sistemas (en base a las vCPU y GB) asociados a cada entorno.
 - El ratio máximo de compartición de CPU para la virtualización será de 1 vCPU: 1 thread (con al menos 2.00 GHz).
 - Servidores dedicados:
 - Se deben poder asignar servidores Cloud en modo dedicado de hasta 40 vCPUs y 250 GB de memoria
 - El entorno PaaS deberá gestionar al menos las siguientes licencias: Licencias de SSOO (Linux RedHat y Windows Server) y licencias de BBDD Oracle (incluyendo Oracle RAC extendido) y Microsoft SQL en sus distintas versiones en base a las funcionalidades requeridas.



- Proveer mecanismos de:
 - Auto escalado de servidores en base a:
 - Especificaciones del balanceador de tráfico y el reparto de carga entre los servidores en base a políticas tanto de crecimiento como de decrecimiento.
 - Especificaciones en base a alta o baja utilización de la CPU.
 - Recuperación automática del servidor virtual ante problemas (por ejemplo detección de errores Health Check).
- Deberá proveer herramientas para la migración a Cloud de entornos de SSOO basados en Windows (Windows Server 2008 R2 SE & EE 64bit y Windows Server 2012 SE & R2 SE 64bit) y Linux (Red Hat en últimas versiones, CentOS 6.5 64bit, Ubuntu 14.04 LTS 64bit). De igual forma dispondrá de mecanismos automáticos para la exportación de máquinas virtuales de cara a la migración de los servidores a otras Cloud o infraestructura dedicada del SERMAS.
- En lo que se refiere al almacenamiento, cuando se asigne espacio a los servidores, éste podrá ser de tipo imagen, bloque o NAS y sobre el almacenamiento podrán realizarse copias instantáneas de los volúmenes (snapshots).
- **Requerimientos mínimos de elementos de red:**
 - Deberá aportar una solución definida por software de gestión de redes, integrable con la electrónica actual del SERMAS, que permita crear o eliminar redes de un proyecto, para así poder utilizar recursos como servidores virtuales. Permitirá crear/configurar/eliminar routers virtuales.
 - Las subredes deben poder incluir gestión de IPs privadas para recursos conectados en red así como ajuste automático de direcciones IPs con DHCP.
 - Aportar funciones de grupos de seguridad que permitan definir y configurar diferentes reglas para permitir o bloquear determinado tráfico a los servidores virtuales. Deben existir un grupo de reglas por defecto para todos los grupos de seguridad. Se debe poder configurar:
 - Tráfico entrante o saliente, especificando el origen o el destino.
 - Versión de IP.
 - Protocolo TCP, UDP, ICMP.
 - Número de puerto de inicio o fin.
 - Los routers virtuales deben poder conectar redes externas con redes internas, o varias redes internas, de la siguiente forma:
 - Creando un puerto en la subred para la que se desea añadir una conexión.
 - Añadiendo el puerto creado al router virtual como una interfaz.
 - Se deben utilizar las funciones SNAT y DNAT.



- Se deben poder conectar/desconectar redes entre diferentes proyectos dentro de la misma plataforma.
 - Crear y configurar puertos para conectar los recursos virtuales utilizados.
 - Utilizar y liberar direcciones IP Globales para poder acceder a los recursos virtuales vía Internet.
 - Utilizar un servicio DNS accesible desde un portal de servicio o vía API. El servicio DNS debe incluir las siguientes funciones de gestión de zonas en los dominios, gestión de registros DNS, conmutación ante errores, enrutamiento basado en latencia y función “Weighted Round Robin”
 - Crear/eliminar balanceadores de carga, para poder distribuir el tráfico a los servidores virtuales. Los balanceadores deben poder ser públicos (uso vía internet) e internos (uso vía red privada)
 - Los balanceadores virtuales deben poder realizar al menos, las siguientes operaciones:
 - Añadir/eliminar objetivos para la distribución de la carga.
 - Distribución en varias zonas de disponibilidad.
 - Supervisión de la anomalía en un objetivo de distribución de carga.
 - Conectar con otras redes independientes, a través de conectores de red, realizando las siguientes tareas:
 - Creación, modificación y eliminación del conector de red.
 - Creación, modificación y eliminación de endpoints conectores.
- **Requerimientos mínimos de BBDD relacionales en modo Cloud:**
 - Ofrecer bases de datos relacionales basadas en entornos cloud, en modo servicio.
 - El servicio de base de datos se encontrará alojado en entornos físicos separados, en modo activo-activo /standby (failover).
 - Posibilidad de proveer diferentes capacidades de disco (en base a GB/TB) para el servicio de base de datos, estos deberán ir desde 10 GB, hasta mínimo 10 TB de capacidad.
 - Posibilidad de proveer de forma automática por el cliente al menos dos métodos de alta disponibilidad para la BBDD, una basada en la alta disponibilidad de los CPD del SERMAS y una solución en otro CPD.
 - Deben existir al menos 2 métodos de recuperación de base de datos, especificando fecha y hora o a través de snapshot.
 - **Requerimientos mínimos de monitorización del Cloud:**
 - La infraestructura Cloud deberá disponer de un servicio de alertas por email (sin la implantación de ningún software adicional al IaaS) que posibilite al menos las siguientes tareas:
 - Funciones de autenticación.
 - Funciones de entrega:
 - SMTP.



- REST API.
 - Configuración de certificados:
 - Autenticación SPF.
 - Monitorización de estado de envíos.
 - Programación de emails.
 - Los datos recogidos por la monitorización deberán ser almacenados durante un periodo de al menos dos semanas.
- **Seguridad y acceso del entorno IaaS:**
 - Utilizar y configurar pasarelas VPN IPsec para conectar los routers virtuales con diferentes entornos.
 - Conectarse de forma segura a los entornos virtuales vía SSL-VPN, a través del router virtual:
 - Cada subred del entorno debe tener su propia función SSL-VPN.
 - Acceso a sistemas Linux mediante SSH y a Windows mediante RDP.
 - Crear/configurar/eliminar Firewalls, además de:
 - Crear reglas de firewall.
 - Registrar un conjunto de reglas para crear una directiva de firewall.
 - Especificar directivas para crear firewalls y asociarlos con routers virtuales.
 - La seguridad del entorno virtual debe ser proporcionada en modo servicio y debe cumplir al menos las siguientes funciones:
 - IDS/IPS – Proteger a los servidores de ataques que apunten a vulnerabilidades sobre SSOO o aplicaciones.
 - Firewall – Disminuir las posibilidades de ataques al bloquear comunicaciones no autorizadas en destino.
 - Antivirus - Escanear el sistema en busca de virus en tiempo real y proteger los servidores ante malware y otros ataques.
 - Reputación web – Proteger a las aplicaciones web de ataques de inyección de código SQL y otros ataques.
 - Monitorización de integridad - Asegurar la detección de la manipulación de archivos o registros.
 - Monitorización de logs - Asegurar la detección temprana de eventos de seguridad importantes para el SSOO o middleware.
 - Micro segmentación, Permitiendo el despliegue de cortafuegos granulares y la aplicación de políticas de seguridad en todas las cargas de trabajo en el centro de proceso de datos, independientemente de la topología y la complejidad de la red.



- Asignación dinámica de servicios avanzados y de seguridad a las cargas de trabajo, al margen de la red física subyacente. Mejorando el tiempo de respuesta, el enfoque global de seguridad y la integración de soluciones de terceros
- Funciones de gestión ya no solo a nivel global sino también a nivel de proyecto.
- Gestión basada en grupos (agrupación de usuarios con los mismos perfiles), usuarios (entidades únicas con accesos determinados) y roles. En lo que se refiere a los roles deberán existir al menos los siguientes:
 - Cliente: podrá gestionar/cancelar el contrato de servicio.
 - Administrador: podrá gestionar todos los proyectos del dominio.
 - Propietario de sistema: podrá añadir/eliminar recursos tales como servidores virtuales.
 - Operador: podrá realizar operaciones dentro de los proyectos en que esté incluido.
 - Observador: podrá monitorizar recursos dentro de los proyectos.
 - Miembro: podrá realizar ajustes de configuración, como cambio de contraseñas,...
- Función de gestión de claves, de esta forma se podrá centralizar la información requerida en comunicaciones SSL.
- **Otros requerimientos:**
 - Proveer una solución de orquestación vía portal de auto servicio o APIs que permita crear/configurar/eliminar entornos automáticamente, estos entornos podrán utilizar múltiples recursos virtuales.
 - Permitirá la conexión privada proporcionando funcionalidades y puertos necesarios entre la infraestructura IaaS y otros entornos. La conexión privada podrá realizarse mediante puertos físicos L3.

5.5.3 Dimensionamiento

La Cloud Privada deberá contar con 2 zonas de disponibilidad, una por CPD (CPD Athene@ y CPD de Aduana o su sustituto), con las siguientes características cada una:

- Nodos de gestión independientes a los nodos de cómputo.
- Conectividad de red a 10 GBE de interconexión y/o de 40 GBE para conectividad exterior que permita la interconexión de todos los elementos en configuración de alta disponibilidad y redundancia que garantice la gestión y el crecimiento futuro en base a la arquitectura propuesta por el proveedor para la Cloud Privada.
- Solución de Almacenamiento con una capacidad neta superior a 100 TIB ALL FLASH en configuración Activo/Activo, sin incluir mejoras derivadas por las funcionalidades de deduplicación y/o de comprensión para cada una de las zonas de disponibilidad. Este



dimensionamiento se corresponde con un tamaño medio de 200 Gigas por VM y su correspondiente replica. El diseño de la solución de Almacenamiento tanto en sus elementos físicos y Lógicos debe cumplir todos los requisitos de alta disponibilidad Local y Remota así como ofrecer todas las funcionalidades necesarias para la implementación en un entorno Critico Enterprise. Por tanto la disponibilidad de la solución debe ser de al menos 99.999 %.

Características técnicas mínimas de la solución de almacenamiento:

- Doble controladora
 - 256 GB por controladora
 - Al menos 16 canales FC a 16Gbps y 16 10 GBE
 - Tipos de RAID soportados: 0, 1, 1+0, 5, 5+0, 6
 - Discos de “2,5”.
 - Dimensionamiento base mínimo disponible, con 19 discos SSD entre 7 y 8 TB, configurados en dos grupos RAID-5 (8+1) y un disco de HS
 - Número mínimo de discos que ha de permitir instalar la cabina: 128
 - Latencia medias por debajo de 1msg
 - Rendimiento acceso secuencial bloque 32kb: Mayor o igual a 300.000 IOs
 - Rendimiento acceso aleatorio bloque 4kb: Mayor o igual a 500.000 IOs
 - Modos de replica: Asíncrona y Síncrona.
 - La solución debe permitir formar un clúster entre el almacenamiento de ambas zonas de disponibilidad de tal forma que se pueda configurar un failover automático que garantice cero tiempos de inactividad y cero pérdidas de datos. Esta funcionalidad debe permitirse sin la complejidad de soluciones tradicionales como dispositivos de virtualización de almacenamiento adicionales.
- 10 nodos de cómputo, cada uno con las siguientes características:
 - Dos procesadores de 16 Cores x86/64 bits, con tecnología integrada que favorezca la virtualización (facilite el cambio de contexto de máquinas virtuales y optimice procesos de I/O) y proporcione un sistema de ahorro de consumo de energía. La arquitectura de los procesadores debe permitir la conexión directa entre procesadores e integrar el controlador de memoria en el chip del procesador. Se deberá proveer siempre procesadores de la generación más nueva existente en el mercado en el momento de realizar el pedido del equipamiento. Cada uno de los procesadores ofertados debe tener al menos 2,60 GHz de frecuencia básica. El conjunto de procesadores debe tener una puntuación igual o superior a 1470 SPECint_rate2006, columna "Base", en el programa para el cálculo de rendimiento SPEC CPU2006.
 - 768GB de memoria (en módulos de memoria de la misma capacidad) – tecnología advanced ECC support o superior).
 - Tarjeta de Gestión y monitorización remota – General: Sistema/controladora de gestión remota del sistema integrada en el equipo con redirección gráfica. Se deberá incluir el



correspondiente software de consola. La tarjeta de gestión (y SW asociado) deberá venir activada y totalmente operativa.

- Tarjetas y puertos para Conectividad General 10 GBE y FC 16GB que permita la conexión en alta disponibilidad de red y separación de física y lógica de al menos la red de Servicio, almacenamiento y backup.
- El adjudicatario tendrá que suministrar todos los elementos necesarios para la instalación de dicha infraestructura en los CPD del SERMAS, por ejemplo, armarios de CPD, PDUs, cableado, SFPs.
- La solución deberá ser escalable en términos de red, cómputo y almacenamiento.

5.5.4 Modelo de despliegue

El licitador debe contemplar como mínimo la siguiente capacidad y modelo de despliegue, teniendo en cuenta que las actuaciones se iniciarán coincidiendo con el inicio de la etapa de prestación regular del servicio:

- Durante los seis primeros meses se realiza el análisis y diseño detallada de la solución, definiendo los modelos de integración necesarios. El adjudicatario deberá presentar un documento que detalle todo el HW y SW a suministrar como servicio. Ese documento tendrá que detallar cada uno de los servicios Cloud IaaS, PaaS y SaaS que proporcionará dicha infraestructura. El documento deberá ser aprobado por la DGSIS, antes de empezar a ser implementado.
- Durante los siguientes seis meses se entregará la infraestructura y se instalarán todos los componentes HW y SW, integrándola en cada uno de los dos CPD.
- Durante el segundo año de servicio el adjudicatario proporcionará una potencia equivalente a 1.800 vCPUs, si bien se espera que su uso no supere el 25%. Estas 1.800 vCPUs se entregan con un número de sistemas no inferior a 10 servidores por zona. 20 servidores x 2 sockets x 16 cores x Contención 3:1=1.920 vCPUs.
- Durante el tercer año de servicio se espera incrementar el uso de la plataforma hasta el 50% de la capacidad.
- En el cuarto año de servicio la plataforma se encontrará disponible al 100% para su uso.

Todas las actividades de diseño e implantación del nuevo modelo, así como todos los procedimientos operativos incluidos en él, han de cumplir con las normativas vigentes de cumplimiento en materia de estándares de arquitectura y seguridad de la información del SERMAS.

5.6 PROGRAMA DE TRANSFORMACIÓN TECNOLÓGICA PARA CENTROS DE ATENCIÓN ESPECIALIZADA Y OTROS CENTROS DEL SERMAS

5.6.1 Transferencia de la gestión centralizada de la Historia Clínica Electrónica en Centros de Atención Especializada

En los últimos años el SERMAS ha incorporado la historia clínica electrónica en diferentes hospitales. En concreto, los últimos 6 hospitales que se incorporaron a la red sanitaria, nacieron con historia clínica



electrónica incorporada desde sus inicios. Sin embargo, en otros hospitales, ha sido necesario implantar paulatinamente la historia clínica electrónica.

Actualmente la DGSIS proporciona la infraestructura y servicios de administración, gestión y operación de los sistemas de información de historia clínica electrónica en el CPD extendido, con copia en el tercer CPD para garantizar la contingencia. En concreto los hospitales con historia clínica electrónica basada en SELENE, tienen su infraestructura física y lógica en el CPD extendido. El contratista de CEDAS tendrá que seguir prestando estos servicios desde el primer mes del contrato.

Adicionalmente, el SERMAS inició en 2014 un proyecto de implantación de historia clínica electrónica basada en HCIS para 10 hospitales del SERMAS. El proveedor adjudicatario de ese proyecto actualmente presta los servicios de administración, gestión, monitorización y operación de la plataforma lógica. Sin embargo, la infraestructura física es administrada, gestionada, monitorizada y operada por CEDAS.

Tras la finalización del proyecto de implantación de la historia clínica electrónica basada en HCIS para 10 hospitales, CEDAS asumirá la administración, operación, monitorización y gestión de toda la plataforma física y lógica en la que se despliega HCIS. Se asumirán todos los entornos (certificación, formación, producción y cualquier entorno que se haya creado durante la implantación del proyecto). Para ello el contratista tendrá que realizar los siguientes trabajos:

- En el segundo mes del contrato, CEDAS junto con el proveedor que implanta HCIS realizará un plan de traspaso de infraestructura y servicios básicos (administración, gestión y operación). La DGSIS coordinará la comunicación entre CEDAS y el implantador del proyecto HCIS así como cualquier otro que esté implicado y cuya participación sea necesaria para hacer viable el traspaso de competencias (CESUS, MEDAS y Oficina de Seguridad entre otros).

La elaboración y aprobación de este plan no podrá ser superior a 2 meses.

El contratista de CEDAS, previa aprobación de la DGSIS, podrá solicitar que se incluya información adicional del proveedor implantador de HCIS, necesaria para hacer el traspaso en las condiciones más óptimas y siempre causando el menor perjuicio a los hospitales del SERMAS.

- Una vez que el plan de traspaso sea aprobado por la DGSIS, se procederá a comenzar los trabajos de traspaso. Inicialmente se empezará por aquellos hospitales cuyo HCIS está implantado por completo, continuando por los implantados en 2017 y 2018. En todo caso, corresponderá a la DGSIS aceptar la propuesta del orden de traspaso de los hospitales pudiendo fijar criterios diferentes a los propuestos en base a las necesidades del SERMAS.

El traspaso de los hospitales con HCIS implantado se hará en 3 meses tras la aprobación del plan de traspaso por la DGSIS. Se considerará traspasado un hospital cuando se hayan cumplido todas las tareas contempladas en el plan, incluyendo la documentación del proyecto. Corresponde a la DGSIS la formalización y aceptación del traspaso del servicio a CEDAS.



Aquellos hospitales que estén en fase de implantación de la historia clínica electrónica con HCIS al inicio de la elaboración del plan de traspaso, se pasarán a CEDAS una vez que HCIS esté implantado en su totalidad en el hospital y prestando servicio sin incidencias debidas a la implantación. Corresponde a la DGSIS y al hospital la aprobación de la finalización de la implantación, momento en el que se incorporará al plan de traspaso global del proyecto. En estos casos, se dispondrá de 2 meses para elaborar y aprobar el plan y 3 meses para hacer efectivo el traspaso.

Además de lo contemplado anteriormente, el SERMAS tiene previsto seguir implantando la historia clínica electrónica en los centros de atención especializada. Todo proyecto que el SERMAS inicie en esta línea, será implantado en infraestructura del CPD extendido y CEDAS será responsable de administrar, gestionar y operar su infraestructura física y lógica como con cualquier hospital SELENE o HCIS.

5.6.2 Centralización de aplicaciones clínico/asistenciales y departamentales

La ejecución de la fase III del Proyecto Athene@ (Centralización de los sistemas de Información Departamentales) para los primeros 8 hospitales ha supuesto una iniciativa de cambio en la prestación de los servicios donde se ha ejecutado con éxito la implantación de herramientas de Software Defined Network y de auto aprovisionamiento de servicios de infraestructuras. Ya se están prestando los primeros servicios de IaaS y PasS desde un portal de servicios Cloud privado, en este caso con herramientas de VMware.

Así mismo, dentro de la duración de este contrato se continuarán con los objetivos de cada fase, ampliando el alcance de Athene@ fase III para el resto de hospitales, o finalizando los proyectos de Athene@ fase II, implantación de Historia Clínica Electrónica en los hospitales tradicionales de la Comunidad de Madrid.

El adjudicatario, bajo las directrices del SERMAS, realizará las actividades de diseño de los proyectos tipo de transformación relacionados con dichos proyectos, estableciendo los requisitos clave para su implantación y asumirá las labores de administración de los nuevos servicios de infraestructuras de Sistemas de Información de Historia Clínica Electrónica Centralizados, en las condiciones definidas en el presente documento, sin ningún coste adicional.

Del mismo modo el contratista participará, prestando el soporte especializado que se requiera, en la ejecución del resto de los proyectos de transformación.

Es importante destacar que la infraestructura resultante de dichos proyectos se incorporará al modelo de gestión centralizada y a los servicios de carácter continuado de CEDAS, tanto de administración, operación y gestión de infraestructuras de CPD, como de mantenimiento de equipamiento hardware y software base.

El diseño del Plan de Transformación Tecnológica de los Sistemas de Información de los Centros de Atención Especializada persigue objetivos específicos de transformación de las configuraciones de los equipos y la infraestructura, en conjunto con la aplicación del Plan de Transformación del Modelo de Gestión anteriormente descrito.

Para ello, el contratista llevará a cabo, bajo las directrices del SERMAS, las actividades de diseño de los proyectos tipo de transformación, estableciendo los requisitos clave para su implantación. Así mismo, el



contratista participará, prestando el soporte especializado que se requiera, en la ejecución del resto de los proyectos de transformación.

Los proyectos de transformación específicos para cada Centro de Atención Especializada y otros centros del SERMAS pueden ser ejecutados por diferentes actores a través de iniciativas no contempladas en este contrato. Sin embargo, es importante destacar que la infraestructura resultante de dichos proyectos se incorporará al modelo de gestión centralizada y a los servicios de carácter continuado de CEDAS, tanto de administración, operación y gestión de infraestructuras de CPD, como de mantenimiento de equipamiento hardware y software base.

Todo proyecto incluido en este plan contempla lo siguiente:

- Las aplicaciones podrán ser trasladadas tanto física como lógicamente a una nueva arquitectura.
- Integración en la infraestructura del nuevo equipamiento que se pudiera incorporar a la misma, con criterios comunes y coherentes con la nueva arquitectura.
- Diseño e implantación de configuraciones que permitan reducir el tiempo de recuperación de los servicios basados en los tipos de configuraciones ya experimentados con éxito en los CPD de Servicios Centrales.
- Diseño e implantación de configuraciones de los sistemas de almacenamiento y de salvaguarda de la información, que permitan establecer un tiempo de recuperación de datos (RPO) igual a cero.
- Aumento de la disponibilidad de las configuraciones de los equipos que soporten los servicios críticos, para asegurar que estará por encima de 99,95%. Esto incluye el diseño de la parametrización adecuada de los equipos y el diseño de las estrategias de servicio que lo posibiliten.
- Mejora de la escalabilidad de las infraestructuras, con la posibilidad de extender la plataforma a medida que se incorporan nuevos servicios, reduciendo el tiempo de provisión de equipamiento que soporte los nuevos servicios.
- Reducción de la necesidad de intervenciones manuales para la ejecución de los Planes de Contingencia ante fallos de la infraestructura.
- Incremento del aprovechamiento de la capacidad de la infraestructura, reduciendo la infrautilización de la capacidad de proceso mediante la virtualización.
- Mejora de la capacidad de recuperación rápida ante desastres, mediante la prestación de servicio desde CPD geográficamente dispersos.
- Reducción de la complejidad de las infraestructuras mediante la consolidación de servicios en plataforma actualizada, que proporcionará mayor rendimiento y disponibilidad, así como estandarización de las infraestructuras actuales.
- Reducción del número de sistemas físicos necesarios y reducción del consumo de energía típico, gracias a la virtualización de infraestructuras hardware.



- El Proyecto de Transformación deberá diseñarse de manera que permita la continuidad de los servicios, con las mínimas interrupciones debidas a los trabajos de reconfiguración para adaptarlos al nuevo modelo.

En relación con los proyectos, será responsabilidad del contratista la elaboración del diseño de alto nivel y de las guías de ejecución de los diferentes proyectos, garantizando la coherencia con las infraestructuras y modelo de gestión ya implantados. Sin embargo, la ejecución de los proyectos de transformación para cada uno de los Centros no forma parte del objeto del presente contrato.

Es necesario diseñar el Plan de manera que las actividades se lleven a cabo en perfecta coordinación con las tareas de administración y operación regular, para evitar el impacto de los necesarios cambios en el servicio normal de los sistemas de información de los Centros de Atención Especializada

La infraestructura de Servicios Centrales y de CPD locales resultantes de la ejecución de los proyectos incluidos en este Programa de Transformación se incorporará al alcance de los servicios de este contrato relativos a la operación y administración de infraestructuras de CPD.

El contratista deberá proporcionar su planteamiento base para la realización del diseño de los Planes de Transformación, antes del comienzo de la Fase de Servicio Regular. Ese planteamiento base será completado y detallado por el contratista durante los seis primeros meses del servicio.

Este modelo tendrá como marco la arquitectura de referencia de Servicios Centrales y su modelo de gestión centralizada de infraestructuras (consultar Anexo IV). Permitirá evolucionar y modernizar las plataformas, los servicios y los modelos de gestión, para adaptarlos a la arquitectura de CPD extendido, total o parcialmente según el escenario en el que se ubique cada Centro, de manera que se puedan obtener los beneficios esperables de rentabilidad y eficiencia, a través de la centralización, consolidación, virtualización y homogeneización de los Sistemas de Información de los Centros de Atención Especializada.

6 FASES DEL SERVICIO

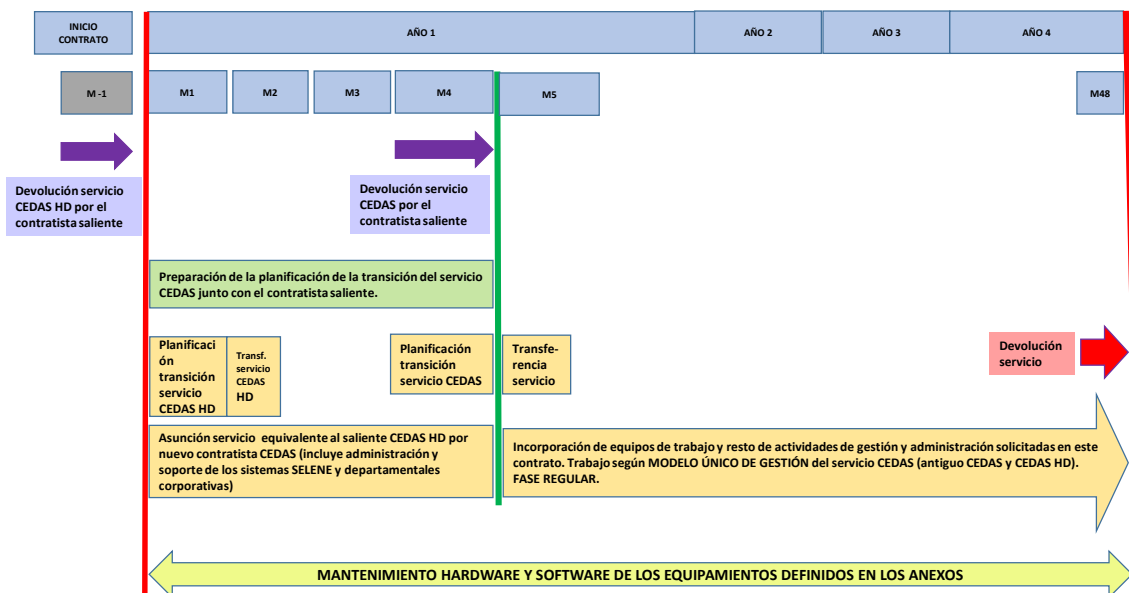
Se establecen las siguientes fases del servicio objeto de este contrato:

- FASE 1: Planificación y ejecución de la transferencia del servicio.
- FASE 2: Servicio regular.
- FASE 3: Devolución del servicio.

La fase 1 se repetirá para la incorporación de cada uno de los dos grandes ámbitos funcionales CEDAS-HD y CEDAS, que asumirá el contratista y para los que en la etapa de prestación regular del servicio proporcionará una solución global. Es decir, en el arranque del contrato comenzará la fase 1 para los servicios de CEDAS HD. Esta fase se volverá a repetir para incorporar los servicios de CEDAS a los 3 meses del inicio de contrato, coincidiendo con la devolución del servicio del CEDAS actual. En último término, tras llegar al modelo único de gestión, las fases 2 y 3 serán comunes.



La secuenciación y plazos para cada fase es la siguiente:



6.1 FASE DE PLANIFICACIÓN Y EJECUCIÓN DE LA TRANSFERENCIA DEL SERVICIO

6.1.1 Etapa de planificación de la transición

La fase de planificación de la transición se hará para asumir el servicio CEDAS HD saliente y posteriormente se repetirá una planificación de la transición para el servicio CEDAS saliente. En ambos casos, es una fase previa al inicio de la fase de transferencia del servicio. **Tendrá una duración máxima de 4 semanas.**

Los objetivos asociados a esta fase son los siguientes:

- Definición del calendario detallado para la transferencia del servicio. La DGSIS tendrá la capacidad de aprobar o modificar la fecha de inicio, duración y contenido de cada una de las fases, para garantizar la consecución de la transferencia completa en los plazos y condiciones deseadas.
- Definición y entrega del modelo de funcionamiento del servicio en todas sus fases (transferencia del servicio, servicio regular y devolución), del planteamiento base del plan de transformación y del modelo general para la incorporación de nuevos proyectos de sistemas de información (incluyendo, al menos, descripción de la estructura de proyecto a utilizar, los requisitos que



deben cumplir los agentes involucrados en el nuevo proyecto y el método de valoración de las tareas de planificación y ejecución del proyecto) . Así mismo, el contratista deberá proponer la metodología de planes de contingencia.

- Identificación y análisis, por parte del contratista, de todos los elementos logísticos y/o actividades funcionales asociados a la prestación de los servicios.
- Planificación de las actividades de transferencia del conocimiento del anterior proveedor y de la documentación del servicio.

El contratista entregará en su oferta las líneas base del plan de transición, contemplando la asunción de ambas partes del servicio (lo equivalente al CEDAS y CEDAS HD que se unificarán en este contrato).

Al inicio del contrato desarrollará en detalle los siguientes documentos:

- **Plan definitivo de transición del servicio.** El contratista preparará un plan detallado de actividades con cronograma, del proceso para la transferencia de la responsabilidad, incluyendo, al menos:
 - Formación específica y formal para la asunción del servicio.
 - Documentación necesaria para la asunción del servicio, sobre la base de la procedente del proveedor saliente. Es responsabilidad del contratista identificar y recopilar toda la información necesaria para la correcta prestación del servicio (documentación de los sistemas y aplicaciones, documentación técnica, procedimientos de actuación, etc.). En aquellos casos en los que no exista documentación previa necesaria para prestar el servicio, el contratista deberá planificar, de acuerdo con la DGSIS, y ejecutar su elaboración, sin coste adicional. Se presentará a la DGSIS, para su aprobación, la documentación concreta a crear y gestionar para la correcta prestación del servicio. Sin perjuicio de posteriores ajustes, por necesidades del servicio.
- **Plan de hitos principales de la transición incluyendo fechas y requisitos para que se produzcan.**
- **Plan de riesgos de la transición,** incluyendo la identificación de riesgos principales y las acciones asociadas para su control, con especial foco en la garantía de la continuidad en la resolución de incidencias y peticiones y la realización de los trabajos inacabados o “en vuelo”, entendidos como aquellas actividades o tareas que están iniciadas o previstas en el momento en el que entra en vigor el contrato.

En estos documentos se deberán identificar todas las actividades a llevar a cabo, las fechas de inicio y fin de cada una de ellas, la distribución de responsabilidades entre las partes, los criterios aplicables de aceptabilidad y cualquier otro detalle adicional que se estime pertinente. Adicionalmente, los documentos tendrán que ser aprobados por la DGSIS.

6.1.2 Fase de transferencia del servicio

Una vez aprobados los planes de la fase de planificación de la transición por la DGSIS, se iniciará la fase



de transferencia del servicio. **Esta etapa tendrá una duración máxima de 2 semanas.**

El objetivo de esta fase es el traspaso de los elementos básicos e imprescindibles para la prestación del servicio al contratista, en función de los planes establecidos en la etapa de planificación de la transición. Durante la misma, el contratista ejecuta el plan definitivo de transición con todas las actividades que le permitan prepararse para asumir la fase de servicio regular.

Todo el personal que participe en esta fase deberá firmar el preceptivo acuerdo de confidencialidad sobre la información que se reciba.

El contratista tiene obligación de documentar todas las actividades realizadas durante la etapa de ejecución de la transferencia del servicio y entregar esa documentación a la DGSIS cuando termine el proceso de transición.

Durante la etapa de ejecución de la transferencia del servicio, el contratista deberá, como mínimo, haber realizado las siguientes tareas:

- Ejecución de todas las actividades planificadas en relación a este hito en el plan definitivo de transición.
- Registro documental de todas las entregas de documentación habidas.
- Registro documental de todas las incidencias y hechos significativos de la ejecución de la transferencia del servicio.
- Presentación de la base de datos de conocimientos del equipo de trabajo.

La etapa de transferencia del servicio finaliza con el **hito de fin de la transferencia del servicio**, cuya fecha estará definida en el plan definitivo de transición aprobado por la DGSIS. Este hito marcará el inicio de la fase del servicio regular. Antes de dar por cumplido este hito, la DGSIS realizará una comprobación de verificación de la correcta realización de las actividades planificadas en el plan definitivo de transición y la revisión de la documentación generada en la transferencia del servicio, que incluirá una base de datos de los conocimientos del equipo de trabajo. El cumplimiento del hito se producirá cuando la DGSIS lo apruebe, en función del resultado de la comprobación de la correcta realización de las tareas y requisitos previos por parte del contratista. Si la DGSIS aprueba los trabajos realizados, el contratista iniciará la fase del servicio regular.

El cumplimiento del hito de transferencia de responsabilidad, deberá quedar formalmente documentado mediante actas de aceptación de la responsabilidad firmadas por el contratista y por la DGSIS.

En caso de que, el contratista no pueda asumir la fase del servicio regular, y no se apruebe por la DGSIS el cumplimiento del hito de fin de la transferencia del servicio, se aplicarán las penalizaciones previstas en el pliego de cláusulas administrativas.

En cualquier caso, desde el inicio del contrato, el contratista recibirá, todas las peticiones de servicio y trabajos inacabados. El contratista entrante es responsable de atender la lista de tareas y trabajos que estén iniciados o pendientes de inicio. Esto incluye, de manera expresa, la resolución de



incidencias que no hayan podido ser resueltas por el proveedor saliente. Así mismo, el contratista será responsable, desde el inicio del contrato, de los servicios objeto de presente contrato.

6.2 FASE DE SERVICIO REGULAR

La fase de prestación del servicio regular comenzará tras la aprobación formal del cumplimiento del hito de transferencia de la responsabilidad, según se establece en la fase de planificación y ejecución de la transferencia del servicio, y marcará el comienzo del período en el que serán exigibles las condiciones generales definidas en el presente pliego, así como el cumplimiento de los Acuerdos de Nivel de Servicio que se hayan establecido en el contrato, a los efectos de devengar penalizaciones, en su caso.

La fase de servicio regular finaliza formalmente con la fase de devolución del servicio. El servicio deberá seguir prestándose, pero adicionalmente habrá que realizar las actividades propias de la devolución del servicio. Durante el solape de ambas fases, la DGSIS reducirá el número de cambios y nuevos proyectos al mínimo posible, para reducir la complejidad de la gestión del servicio y facilitar la fase de devolución del servicio.

Durante la fase de servicio regular se podrán incorporar a los CPD del SERMAS nuevos proyectos de sistemas de información. Esto puede materializarse en nuevas dotaciones de hardware, tanto en los CPD centrales, como en los CPD locales. Toda esta infraestructura e incremento de servicios tendrá que ser incorporada en las mismas condiciones de prestación del servicio contemplado en el contrato. La DGSIS comunicará estas incorporaciones con una antelación mínima de 1 mes.

Con anterioridad a que se produzca una de estas incorporaciones, el contratista del servicio deberá planificar y preparar las actuaciones necesarias para facilitar la puesta en producción de los mismos.

La siguiente matriz describe los roles que cada grupo involucrado deberá realizar de cara a la integración de los nuevos sistemas de información. A continuación se describe el significado de los valores posibles:

- A: autoriza.
- I: es informado.
- R: es responsable de la tarea.
- S: da soporte o asesoramiento al responsable de la tarea.

ACTIVIDAD	DGSIS	GESTOR DEL SERVICIO DE GESTIÓN DE LAS ARQUITECTURAS	GESTOR DEL NUEVO SISTEMA DE INFORMACIÓN
Documento de requisitos arquitecturales y funcionales del nuevo proyecto de SI	R	I	I



ACTIVIDAD	DGSIS	GESTOR DEL SERVICIO DE GESTIÓN DE LAS ARQUITECTURAS	GESTOR DEL NUEVO SISTEMA DE INFORMACIÓN
Documento de requisitos infraestructurales del nuevo SI	A	I	R
Diseño de configuración que satisface requisitos	A	R	I
Diseño del plan de aprovisionamiento y despliegue de la infraestructuras	A	R	I
Ejecución del plan de aprovisionamiento	R	S	I
Ejecución del plan de despliegue de la infraestructura	I	R	S
Diseño del plan de despliegue de los SI	A	S	R
Ejecución del plan de despliegue de los SI	I	S	R

En todo caso, esta matriz de responsabilidades podrá ser modificada por la DGSIS, comunicando al contratista cualquier cambio con al menos 1 mes de antelación.

6.3 FASE DE DEVOLUCIÓN DEL SERVICIO

La devolución del servicio tendrá lugar por cualquiera de las siguientes causas:

- Termina del contrato por conclusión de duración y de las posibles prórrogas.
- Resolución del contrato de forma anticipada por cualquiera de las razones previstas en el contrato.

En todos los casos el objetivo de la fase de devolución del servicio será garantizar la transferencia del conocimiento adquirido o generado durante la prestación del servicio, por parte del contratista, hacia la DGSIS, o hacia el proveedor que establezca el SERMAS, sin que ello repercuta en una pérdida del control del nivel de calidad del servicio.

Durante la fase de devolución del servicio, el contratista estará obligado a devolver el control de los servicios objeto del contrato, simultaneándose los trabajos de devolución con los de prestación del servicio regular, sin coste adicional.



Al inicio de la fase de devolución del servicio, se hará una evaluación y planificación de todas las actividades necesarias. Dicho traspaso se realizará en el plazo que la DGSIS considere conveniente con una **duración máxima de 4 semanas** desde la notificación del inicio de esta fase por parte de la DGSIS. La notificación de inicio se entenderá realizada de oficio 4 semanas antes de la conclusión de la duración del contrato y sus posibles prórrogas. Esta duración podrá ser modificada por la DGSIS previa notificación al contratista con al menos 3 meses de antelación.

El contratista deberá realizar la devolución del servicio, asegurando que se mantienen correctamente, durante el traspaso, el control de servicios y deberá colaborar activamente con la DGSIS y, en su caso, con el futuro proveedor durante este proceso, para facilitar la transferencia del conocimiento y la responsabilidad sobre los servicios.

El compromiso de devolución del servicio del contratista a la DGSIS incluye la entrega a la DGSIS de una versión actualizada de toda la documentación e información manejada para la prestación del servicio antes de la finalización del contrato.

Durante la fase de devolución del servicio, el personal del contratista colaborará con el personal propio o designado por la DGSIS para facilitar, al máximo, la transferencia de la responsabilidad al futuro proveedor entrante.

7 MODELO DE RELACIÓN Y GESTIÓN DEL SERVICIO

Dentro del ámbito del servicio objeto del contrato, la DGSIS ha definido unos objetivos para el control del cumplimiento del contrato y del servicio proporcionado por el contratista. Estos objetivos de control deben garantizar que tanto la prestación del servicio del día a día, como en su evolución se ajustan a los objetivos del contrato.

Los principales objetivos de control son:

- Diseño e implantación del modelo común de gestión.
- Ejecución del programa de transformación del modelo de servicio.
- Diseño de los proyectos tipo del programa de transformación tecnológica en centros de atención especializada u otros centros del SERMAS que pudieran incorporarse.
- Seguimiento y/o asistencia técnica de la ejecución de proyectos de transformación.
- Integración, dentro del modelo de servicio y gobierno de los distintos centros de atención especializada transformados.
- Cumplimiento de los objetivos del contrato.
- Control de la gestión del servicio prestado.
- Control y ejecución de los proyectos de evolución de la plataforma.
- Control y estrategia de la evolución tecnológica.



7.1 MODELO DE RELACIÓN

El modelo de relación tiene como objetivo asegurar la coordinación e integración eficiente del contratista del contrato con los agentes relevantes para la prestación del servicio.

Los más importantes son:

- **Dirección General de Sistemas de Información Sanitaria.** Incluye a sus principales unidades Operativas (CENTRO DE SOPORTE A USUARIOS DE LAS APLICACIONES Y SISTEMAS DE INFORMACIÓN (CESUS), MANTENIMIENTO, EVOLUCIÓN Y DESARROLLO DE APLICACIONES ANALISIS DE DATOS SANITARIOS (MEDAS)), Oficina de Proyectos y Oficinas técnicas, así como cualquier proveedor de servicio que tenga contratado para la prestación de servicios.
- **Agencia para la Administración Digital de la Comunidad de Madrid.** Para la coordinación de las actividades en el centro de contingencia, en el CPD TRES CANTOS, para la conexión con redes WAN y de usuario, así como para la coordinación con el resto de sistemas de información corporativos, no sanitarios, de la Comunidad de Madrid.
- **Departamentos de TI de los centros de atención especializada, SUMMA 112 y otros centros del SERMAS.** Estos departamentos en función de su tamaño y complejidad, disponen de servicios propios de gestión TI, que dan soporte a las necesidades funcionales de los distintos centros. Siguiendo las directrices generales marcadas en este capítulo y una vez iniciado el contrato, la DGSIS y el contratista desarrollarán todos los detalles del modelo de relación para permitir una gestión eficiente de la relación, gobierno y gestión del servicio.

El modelo de relación debe cubrir todos los niveles de información y decisión, desde el nivel operativo hasta el estratégico, facilitando la toma de decisiones, el seguimiento de los objetivos globales y la resolución de potenciales conflictos.

Por otra parte, el modelo de relación deberá garantizar la flexibilidad y la adaptación del servicio a la evolución del negocio, pudiendo cambiar durante la vigencia del contrato, en particular ante eventuales reorganizaciones.

El modelo de relación constará principalmente de:

- Una estructura de comités que sirva como principal elemento de decisión y seguimiento del contrato y de los servicios prestados por el contratista.
- La definición de unos interlocutores de ámbito de actividad que actuarán de interlocutores en la relación por ambas partes, tanto a nivel de comité, como en el día a día.
- Un modelo de trabajo general (modelo de gestión CPD de CEDAS), con las fronteras e interacciones claramente delimitadas a nivel actividad y esquematizada en una matriz de responsabilidades, cuyo modelo, a modo de ejemplo, se incluye en el Anexo V.



Será de especial relevancia el modelo que el contratista proponga para la correcta integración dentro del modelo marco de CEDAS de aquellos servicios que se presten a los centros de atención especializada. Este modelo deberá cubrir entre otras:

- Modelo de gestión: Incidencias, Problemas, Cambios, Riesgos.
- Gestión de la demanda.
- Necesidades específicas de informes y seguimiento.
- Procedimientos de contacto y escalado.

La primera versión del modelo de relación deberá entregarse por el contratista antes del comienzo de la primera Fase de Transferencia del Servicio. Corresponderá a la DGSIS la aprobación de ese modelo así como la solicitud de cambios posteriores sobre él, previo aviso al contratista.

7.2 INTERLOCUTORES PARA GESTIONAR LA RELACIÓN

Se establecerá, previamente al inicio de la fase de transferencia del servicio, una estructura de interlocutores que se responsabilizarán de las actividades de relación del servicio. El contratista deberá definir y asignar estos interlocutores e informar a la DGSIS de ello y cualquier cambio de los mismos con suficiente antelación (al menos, con 15 días naturales). Estos cambios sólo podrá realizarse si la DGSIS los aprueba.

El contratista, en su diseño de modelo de relación, deberá definir las funciones asignadas a los que desempeñen los roles identificados. Entre los roles que desempeñen estas tareas de relación estarán al menos:

- Responsable del contrato.
- Director del proyecto.
- Coordinador servicios CEDAS a hospitales con historia clínica electrónica centralizada.
- Responsable de la explotación.
- Responsable de los niveles de servicio prestados por el contratista.
- Coordinador de la oficina de gestión.
- Consultores tecnológicos del servicio o específicos de los planes de transformación.

7.3 MODELO DE GESTIÓN DEL SERVICIO TI

El contratista deberá definir, antes del inicio de la fase de servicio regular, un modelo de gestión del servicio, basado en las mejores prácticas y normas existentes en el mercado (ISO 20000, ISO 27001, ITIL v3 o COBIT 4.1) y futuras evoluciones de los estándares del mismo, compatible con la matriz de responsabilidades y adaptado al modelo de gestión de CPD de CEDAS.

Los procesos operativos que implican comunicación entre los proveedores del servicio de explotación y el resto de las funciones de TI de CEDAS tendrán que ser normalizados de acuerdo con los modelos y patrones que establezca la DGSIS y cumpliendo los requisitos que ésta determine. Incluyendo, aunque no



limitándose, a los procesos de puesta en producción, solicitud de trabajos, comunicación de incidencias, reclamaciones y problemas y solicitudes al proceso de gestión de cambios y gestión de configuración.

8 ORGANIZACIÓN Y EQUIPO DE PRESTACIÓN DEL SERVICIO

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.

En cualquier caso, la organización de los recursos técnicos corresponderá a la empresa contratista que asume la obligación de ejercer de modo real, efectivo y continuo, sobre el personal integrante del equipo de trabajo encargado de la ejecución del contrato, el poder de dirección inherente a todo empresario. En particular asumirá la negociación y pago de los salarios, la fijación de su jornada de trabajo, la concesión de permisos, licencias y vacaciones, las sustituciones de trabajadores en casos de baja o ausencia, las obligaciones legales en materia de Seguridad Social, incluido el abono de cotizaciones y el pago de prestaciones, cuando proceda, las obligaciones legales en materia de prevención de riesgos laborales, el ejercicio de la potestad disciplinaria, así como cuantos derechos y obligaciones se deriven de la relación contractual entre empleado y empleador, y ello sin perjuicio de la verificación por la Dirección del Proyecto por parte de la CSCM, enfocando los recursos en función de las necesidades de los distintos proyectos y en los diferentes ámbitos y/o soluciones descritos, de forma que se proporcione cobertura completa a todo el alcance del pliego en cada momento.

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.

El SERMAS nombrará un Director del servicio de gestión integral de los centros de proceso de datos (Director CEDAS) que será el encargado del seguimiento de la ejecución del contrato. Este Director velará por el cumplimiento del contrato y se encargará de las relaciones con el contratista para todo lo referente a este contrato. Supervisará y evaluará el desempeño de servicio.

El Director CEDAS podrá delegar sus funciones en una persona de su equipo. Así mismo, podrá incorporar al proyecto durante su realización, las personas que estime necesarias para verificar y evaluar todas las actuaciones a su cargo.

El contratista garantizará la continuidad del servicio en cualquier circunstancia y en cualquier época del año.

Los recursos humanos que el contratista asigne a la prestación de los servicios objeto de este contrato, en ningún caso podrán alegar derecho alguno en relación con la Administración contratante, ni exigirse a ésta responsabilidades de cualquier clase, como consecuencia de las obligaciones existentes entre el prestador



de los servicios y sus empleados, aún en el supuesto de que los despidos o medidas que pudiera adoptar el contratista, se basen en el incumplimiento, interpretación o resolución del contrato.

El personal adscrito al servicio no recibirá ninguna instrucción directa del personal de la CSCM, salvo a través del responsable del servicio y de la propia organización en niveles que el contratista proponga.

La DGSIS solicitará al responsable del servicio del contratista, en el caso del incumplimiento de los acuerdos de nivel de servicio, que realice los cambios adecuados para la correcta prestación del servicio. El contratista dispondrá de un plazo de quince días para subsanar las deficiencias. En el caso de que se produzca el cambio de recursos, estos deberán ser de igual categoría y cumplir con los requisitos establecidos para el perfil.

Si bien la DGSIS entiende que la gestión de los recursos técnicos del contratista no forma parte de su responsabilidad, sí que lo es obtener una rentabilidad de la inversión. Por ello, el adjudicatario deberá garantizar que dispone de los mecanismos adecuados para minimizar la rotación no planificada del personal que compone el equipo prestador del servicio, para evitar la pérdida de capacidad de gestión del servicio y la pérdida no controlada de conocimiento.

Por rotación planificada de un recurso técnico asignado se entienden los cambios promovidos por el contratista, por causas ajenas a la DGSIS, que cumplen los siguientes requisitos:

- Deberá solicitarlo con al menos 20 días de antelación, con justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio.
- Presentación de posibles candidatos para un perfil cuya cualificación sea igual o superior al de la persona que se pretende sustituir.
- Verificación por la DGSIS del cumplimiento de los requisitos por los candidatos propuestos.
- En caso de llevarse a cabo la sustitución a solicitud del contratista, y de cara a subsanar los posibles inconvenientes de adaptación al entorno de trabajo y al proyecto, se establecerán períodos de solapamiento sin coste adicional. Dicho plazo de solapamiento mínimo entre el perfil entrante y el saliente será de 2 semanas.

En todo caso, la incorporación o sustitución de recursos técnicos deberá mantener los requisitos establecidos como mínimos para cada perfil.

El incumplimiento de las condiciones anteriores, implicará la consideración de una rotación no planificada que dará lugar a la penalidad prevista al efecto en la cláusula 1.18 del PCAP.

El contratista asumirá la provisión y mantenimiento de equipamiento de hardware y software necesario para el desempeño de las tareas encomendadas al equipo de trabajo. Así mismo, proveerán a los miembros de cada uno de los equipos del material de oficina y fungibles correspondientes.

Dada la amplitud de los sistemas a gestionar, que incluye una gran variedad de sistemas operativos, bases de datos y aplicaciones, resulta imprescindible distribuir la administración de los mismos en perfiles



técnicos especializados que dispongan de la formación y experiencia adecuada para gestionar un entorno de misión crítica sanitario y de gestión de grandes volúmenes de información.

En consecuencia de todo lo expuesto, antes del comienzo de la fase de transferencia del servicio, el contratista deberá presentar un modelo organizativo, que cubra la totalidad de las áreas de conocimiento de los entornos tecnológicos contemplados en el contrato.

El servicio prestado por el contratista deberá poseer la flexibilidad necesaria para adaptarse a la evolución funcional y tecnológica, siendo responsabilidad del contratista la formación del equipo para capacitarlo en las tecnologías que el SERMAS adopte en sus CPD.

Si como consecuencia de algún proyecto asociado al programa de transformación del modelo de servicio el contratista tiene que incorporar perfiles nuevos, el contratista tendrá que incorporarlos o sustituir aquellos que dejan de tener un perfil acorde con la prestación del servicio. En estos casos, el contratista presentará un plan de sustitución de recursos con el cambio de los perfiles con al menos 30 días de antelación. La DGSIS será quien en último término acepte o rechace la propuesta. En todo caso, el cambio de unos perfiles por otros tendrá que hacerse conservando el número de recursos así como el nivel de titulación y años de experiencia, no pudiendo ser intercambiado un perfil por otro de menor titulación y experiencia.

El contratista dimensionará de la manera adecuada el servicio, de manera que se cumplan los Acuerdos de Nivel de Servicio y los requisitos de trabajo presencial y en disponibilidad o guardia, que se explican en este pliego.

8.1 CONFIGURACIÓN Y DIMENSIÓN

En su oferta el contratista entregará, una propuesta de plan de trabajo para llevar a cabo el servicio, detallando las actividades, cronograma, equipo de prestación del servicio y cuanta información considere oportuna.

El equipo de prestación del servicio tendrá una dimensión y configuración adecuada a las tareas de la prestación normal del servicio, atendiendo a las distintas fases del servicio.

8.1.1 Descripción de los perfiles

Atendiendo a las necesidades planteadas en el pliego, se distinguen 3 bloques:

- Oficina de gestión del servicio.
- Operación y explotación del CPD.
- Oficina de proyectos para el plan de transformación.

En todo caso, existirá un Director de Proyecto que coordinará los trabajos de los distintos bloques y será el interlocutor principal del Director designado por el SERMAS.

A continuación se detalla los distintos perfiles:



- **Director de Proyecto:** 1 persona de lunes a viernes no festivos, en horario de 9h a 18h. Disponible desde el inicio del contrato.

Será responsable del gobierno de la operación y de los servicios requeridos en este contrato. Con capacidad decisoria y ejecutiva suficiente dentro de su organización, ya que centralizará sus relaciones con el Director de CEDAS de la Consejería de Sanidad. Las funciones del Director de Proyecto serán las siguientes:

- Organizar la ejecución de los trabajos y poner en práctica la metodología, planificación y órdenes de trabajo adoptados y aprobados.
- Ostentar la representación del equipo técnico afecto a la ejecución del contrato en sus relaciones con la DGSIS y, en concreto, con el Director de CEDAS, en lo referente a la ejecución de los trabajos.
- Observar y hacer observar las normas y procedimiento.
- Asegurar la calidad de los trabajos y los entregables del proyecto.
- Comunicar al Director de CEDAS los informes evolución del servicio y proponerle las modificaciones que estime necesarias para el mejor desarrollo de los servicios requeridos en este contrato.
- Presentar al Director de CEDAS para su conformidad y aceptación los estudios, informes y documentación definitivos.
- Suministrar al Director de CEDAS la información estadística y de detalle que permita el seguimiento de la prestación de servicios, al menos conforme a lo establecido en los correspondientes pliegos de prescripciones técnicas.
- Levantar acta de los acuerdos e instrucciones recibidas en las reuniones con el director del proyecto, a quien se le deberá presentar para su conformidad en un plazo no superior a 48 horas.

- **Coordinador de la Oficina de Gestión del Servicio:** 1 persona de lunes a viernes no festivos, en horario de 9h a 18h. Disponible desde el inicio del contrato.

Se encargará de coordinar los proyectos y tareas relacionadas con la gestión del servicio. Será responsable del seguimiento de la planificación, gestión y seguimiento de los proyectos en los que tenga que intervenir CEDAS, tanto internos como globales de la DGSIS. Junto con la Dirección del Proyecto y dependiendo directamente de dicha Dirección, se encargará de la coordinación conjunta del resto de grupos de CEDAS dando un único punto de vista común de la actividad conjunta del servicio.

- **Coordinador Proyectos Hospitalares:** 1 persona de lunes a viernes no festivos, en horario de 9h a 18h. Disponible desde el inicio del contrato.

Se encargará de coordinar las actividades y proyectos en el ámbito de los centros de atención especializada, en especial de aquellos proyectos relacionados con el programa de transformación tecnológica para dichos centros.



- **Técnicos de la Oficina de Gestión del Servicio:** número de técnicos que el licitador considere adecuado para cubrir las actividades requeridas en el pliego, siendo como mínimo 2 personas de lunes a viernes no festivos, en horario de 9h a 18h. 1 disponible desde el inicio del contrato y 1 disponible una vez que haya finalizado el contrato CEDAS, coincidiendo el inicio de la fase de transferencia del servicio CEDAS.

Se encargará de dar soporte y gestionar los distintos proyectos y actividades que se lleven a cabo en la Oficina de Gestión del Servicio.

- **Técnicos de apoyo para la Oficina de Gestión del Servicio:** 2 personas de lunes a viernes no festivos, en horario de 9h a 18h.

Uno disponible desde el inicio del contrato, se encargará de las tareas de gestión de la documentación, revisando y manteniendo actualizados los repositorios con documentación de los proyectos o guías relacionadas con las tareas operativas y de explotación. Será responsable del control de calidad documental.

El segundo recurso se encargará de las tareas de apoyo administrativo del servicio CEDAS. Se incorporará una vez que haya finalizado el contrato CEDAS, coincidiendo con el inicio de la fase de transferencia del servicio CEDAS.

- **Arquitecto de Seguridad:** 1 persona de lunes a viernes no festivos, en horario de 9h a 18h. Disponible desde el inicio del contrato.

Dentro de la política global de seguridad definida por la Oficina de Seguridad (OSSI), el arquitecto de seguridad de CEDAS se encargará de establecer los planes específicos de seguridad en el ámbito de los CPD con especial foco a las normas legales de obligado cumplimiento. En concreto, hará foco en el Esquema Nacional de Seguridad, legislación de protección de datos de carácter personal así como la relacionada con la Protección de Infraestructuras Críticas.

- **Coordinador de Explotación:** 1 persona de lunes a viernes no festivos, en horario de 9h a 18h. Disponible desde el inicio del contrato.

Será responsable del grupo de operaciones y explotación de los CPD centrales del SERMAS. Coordinará las tareas necesarias para desplegar servicios nuevos o modificados, así como velar por la disponibilidad del personal necesario en cada tarea de la explotación.

- **Consultores Tecnológicos:** en el número que el licitador estime adecuado para cubrir todas las áreas funcionales requeridas en este pliego, como mínimo 7 personas de lunes a viernes no festivos, en horario de 9h a 18h. Disponibles desde el inicio del contrato con dedicación al 50% y con dedicación al 100% en el horario indicado, una vez que haya finalizado el contrato CEDAS, coincidiendo con el inicio de la fase de transferencia del servicio CEDAS.

Realizarán tareas de consultoría en los distintos ámbitos tecnológicos necesarios para cubrir todas las áreas funcionales y actividades requeridas en el pliego. En concreto:

- Integraciones.
- Aplicaciones y Middleware.
- Bases de datos.



- Comunicaciones y seguridad.
- Tecnologías Microsoft.
- Sistemas operativos y almacenamiento.
- Backup.
- **Técnicos Especialistas Senior:** en el número que el licitador estime adecuado para cubrir todas las áreas funcionales requeridas en este pliego, como mínimo 13 personas. Disponibles desde el inicio del contrato con dedicación al 50% y con dedicación al 100%, una vez que haya finalizado el contrato CEDAS, coincidiendo con el inicio de la fase de transferencia del servicio CEDAS. Realizarán tareas y actividades requeridas en este pliego para las actividades de transición, administración, gestión y operación de infraestructuras y sistemas.
- **Técnicos Especialistas Junior:** en el número que el licitador estime adecuado para cubrir todas las áreas funcionales requeridas en este pliego, como mínimo 14 personas. Disponibles desde el inicio del contrato con dedicación al 50% y con dedicación al 100%, una vez que haya finalizado el contrato CEDAS, coincidiendo con el inicio de la fase de transferencia del servicio CEDAS. Realizarán tareas y actividades requeridas en este pliego para las actividades de transición, administración, gestión y operación de infraestructuras y sistemas.
- **Coordinador de Operaciones:** 1 persona de lunes a viernes no festivos, en horario de 9h a 18h. Disponible desde el inicio del contrato.
- **Operadores:** en el número que el licitador estime adecuado para cubrir todas las áreas funcionales requeridas en este pliego, como mínimo 15 personas. Disponibles desde el inicio del contrato aquellos que el licitador considere necesarios siendo como mínimo 3 para realizar las tareas de operaciones en el ámbito de responsabilidad que tenga que asumir según las fases del servicio, trabajando junto con los operadores del CEDAS saliente. En todo caso, todos ellos deben estar disponibles al 100% una vez que haya finalizado el contrato CEDAS, coincidiendo con el inicio de la fase de transferencia del servicio CEDAS. La franja horaria de prestación de este servicio será de 24 horas al día, los 7 días de la semana. El contratista deberá llevar a cabo la planificación de turnos oportuna para asegurar la calidad del servicio exigida en el presente pliego.
- **Coordinador de Infraestructuras:** 1 persona de lunes a viernes no festivos, en horario de 9h a 18h. Disponible desde el inicio del contrato.
- **Jefes de Sala:** en el número que el licitador estime adecuado para cubrir las necesidades del pliego en cuanto a trabajos relacionados con las infraestructuras, siendo como mínimo 1 persona. Disponible(s) una vez que haya finalizado el contrato CEDAS, coincidiendo con el inicio de la fase de transferencia del servicio CEDAS.
- **Coordinador de la Oficina de Proyectos para el Plan de Transformación:** 1 persona de lunes a viernes no festivos, en horario de 9h a 18h. Disponible una vez que haya finalizado el contrato CEDAS, coincidiendo con el inicio de la fase de transferencia del servicio CEDAS.
Se encargará de coordinar los proyectos relacionados con el Plan de Transformación del Modelo de Servicio. Será responsable del seguimiento de la planificación, gestión y seguimiento de los



proyectos derivados del Plan, coordinándose en las tareas comunes con la Oficina de Gestión del Servicio y el Coordinador de Explotación, todos ellos bajo la Dirección del Proyecto.

- **Arquitectos Tecnológicos de la Oficina de Proyectos para el Plan de Transformación:** en el número que el licitador estime adecuado para cubrir las necesidades del pliego en cuanto a los proyectos derivados del Plan de Transformación del Modelo de Servicio. Como mínimo serán 3 arquitectos para cada una de las siguientes tecnologías:
 - Arquitecto en Big Data. Asesorará a la DGSIS en la definición y mantenimiento de una arquitectura de Big Data Analytics y Data Lake sanitario que responda a las necesidades del SERMAS, colaborando con otras unidades de la DGSIS. Disponible desde el inicio del contrato con dedicación al 100%.
 - Arquitecto para Automatización y Orquestación. Establecerá un programa de automatización de infraestructuras y servicios con objeto de mejorar los tiempos de respuesta y reducir los costes. Recomendará herramientas de automatización y orquestación para la puesta en marcha de los planes aprobados por el SERMAS. Disponible con dedicación 50%, una vez que haya finalizado el contrato CEDAS, coincidiendo con el inicio de la fase de transferencia del servicio CEDAS.
 - Arquitecto para DevOps. Asesorará a la DGSIS en la evolución y puesta en marcha de una arquitectura DevOps junto con otras unidades de la DGSIS. En concreto, colaborará estrechamente con MEDAS en la planificación y diseño de soluciones en este ámbito, alineándose en todo momento con los objetivos globales del SERMAS. Disponible con dedicación 50%, una vez que haya finalizado el contrato CEDAS, coincidiendo con el inicio de la fase de transferencia del servicio CEDAS.
- **Técnicos de la Oficina de Proyectos para el Plan de Transformación:** en el número que el licitador estime adecuado para cubrir las necesidades del pliego en cuanto a proyectos y trabajos relacionados con el Plan de Transformación del Modelo de Servicio, siendo como mínimo 1 persona. Disponibles desde el inicio del mes 5 del contrato, coincidiendo con el inicio de la fase de transferencia del servicio del CEDAS saliente.

En la tabla siguiente se muestra un resumen de los perfiles y número mínimo de recursos solicitados:

PERFIL	Número mínimo de recursos solicitados	Dedicación
Director de Proyecto	1	100%
Coordinador de la Oficina de Gestión del Servicio	1	100%
Coordinador Proyectos Hospitales	1	100%



Técnicos de la Oficina de Gestión del Servicio	2	1 al 100% desde el inicio y todos al 100% cuando finalice el servicio CEDAS
Técnicos de apoyo para la Oficina de Gestión del Servicio	2	1 al 100% desde el inicio (documentalista) y los 2 al 100% cuando finalice el servicio CEDAS
Arquitecto de Seguridad	1	100 %
Coordinador de Explotación	1	100 %
Consultores Tecnológicos (Integraciones, Aplicaciones/Middleware, Bases de Datos, Comunicaciones/Seguridad, Tecnologías Microsoft, Sistemas Operativos/Almacenamiento, Backup)	7	50% desde el inicio y 100% cuando finalice el servicio CEDAS
Técnicos Especialistas Senior	13	50% desde el inicio y 100% cuando finalice el servicio CEDAS
Técnicos Especialistas Junior	14	50% desde el inicio y 100% cuando finalice el servicio CEDAS
Coordinador de Operaciones	1	100%
Operadores	15	Los que sean necesarios (mínimo 3) para garantizar el servicio desde el inicio y todos al 100% cuando finalice el servicio CEDAS
Coordinador de Infraestructuras	1	100%
Jefes de Sala	1	100% cuando finalice el servicio CEDAS
Coordinador de la Oficina de Proyectos para el Plan de Transformación	1	100% cuando finalice el servicio CEDAS
Arquitectos Tecnológicos de la Oficina de Proyectos para el Plan de Transformación (mínimo para Big Data, Automatización/Orquestación, DevOps)	3	100% desde del inicio del contrato para el Arquitecto en Big Data y



		50% cuando finalice el servicio CEDAS para el resto de Arquitectos
Técnicos de la Oficina de Proyectos para el Plan de Transformación	1	100% cuando finalice el servicio CEDAS

8.1.2 Cualificación mínima exigida para los perfiles profesionales

A continuación se detallan los requisitos de cada perfil detallando su cualificación mínima exigida, experiencia y conocimientos específicos.

El Real Decreto 1027/2011, de 15 de julio, por el que se establece el Marco Español de Cualificaciones para la Educación Superior (MECES), establece cuatro niveles de cualificación en función de los resultados de aprendizaje que proporcionan los estudios oficiales: el nivel de Técnico Superior (FP) se incluye en el Nivel 1, el de Grado universitario en el Nivel 2, el de Máster universitario en el Nivel 3, y el de Doctor en el Nivel 4

En todos los casos cuando se mencione titulación universitaria de nivel 3 se entenderá referida a la posesión de estudios de máster universitario o su equivalencia según MECES. De manera análoga para la titulación universitaria de nivel 2 referida a la posesión de grado universitario o su equivalencia según MECES.

A efectos de valoración la presentación de candidatos doctorados universitarios, se considerará equivalente a la titulación universitaria de nivel 3.

Los conocimientos específicos relacionados deberán ser cubiertos por el grupo de personas de un determinado perfil, en su conjunto, y será obligatorio que el grupo cuente con al menos, una de cada una de las certificaciones requeridas, sin que se precise que todos los miembros del grupo cumplan todos los conocimientos específicos. En cambio, los requisitos del perfil sí deberán cumplirse por cada una de las personas adscrita a cada perfil profesional. En el planteamiento de cobertura horaria habrá que tener en cuenta la distribución de los conocimientos en las personas, para asegurar la disponibilidad de los conocimientos necesarios durante el horario de servicio.

En concreto, para el grupo de perfiles **técnicos especialistas senior y junior**, las certificaciones deberán ser cubiertas por el grupo de personas, en su conjunto, y será obligatorio que el grupo cuente con al menos, una de cada una de las 14 certificaciones. Será valorable en los criterios de valoración, si el grupo de técnicos especialistas senior y junior cuenta con más de una certificación por cada una de las 14 requeridas, así como que estén distribuidas entre el mayor nº de técnicos. Tanto el número de certificados como el ratio de su distribución entre los recursos ofertados se deben mantener a lo largo de la vigencia del contrato, independientemente de la rotación o sustitución de recursos que se haga.



PERFIL: DIRECTOR DE PROYECTO

REQUISITOS PERFIL

- Titulación universitaria de nivel 3 con 5 años de experiencia en un puesto similar o titulación universitaria de nivel 2 con 7 años de experiencia en un puesto similar.
- Dotes de organización.
- Capacidad de gestión y liderazgo a la vez que capacidad para trabajar en equipo.

CONOCIMIENTOS ESPECÍFICOS

- Dirección de equipos humanos.
- Gestión de calidad.
- Gestión de proyectos orientados al cumplimiento de objetivos.
- Certificación ITIL Expert.
- Certificaciones en gestión de proyectos: Prince2, PMP o similares.

PERFIL: COORDINADOR DE LA OFICINA DE GESTIÓN DEL SERVICIO

REQUISITOS PERFIL

- Titulación universitaria de nivel 3 con 4 años de experiencia en un puesto similar o titulación universitaria de nivel 2 con 5 años de experiencia en un puesto similar.
- Dotes de organización.
- Capacidad de gestión y liderazgo a la vez que capacidad para trabajar en equipo.

CONOCIMIENTOS ESPECÍFICOS

- Dirección de equipos humanos.
- Gestión de calidad.
- Definición y seguimiento de métricas.
- Certificación ITIL Expert.
- Certificaciones en gestión de proyectos: Prince2, PMP o similares.



PERFIL: COORDINADOR DE PROYECTOS HOSPITALES

REQUISITOS PERFIL

- Titulación universitaria de nivel 2 con 5 años de experiencia gestionando proyectos en el ámbito sanitario.
- Dotes de organización.
- Capacidad de gestión y liderazgo a la vez que capacidad para trabajar en equipo.

CONOCIMIENTOS ESPECÍFICOS

- Dirección de equipos humanos.
- Certificación ITIL Foundation.
- Certificaciones en gestión de proyectos: Prince2, PMP o similares.
- Experiencia gestionando proyectos con los principales sistemas de Historia Clínica Electrónica sanitarios existentes en el SERMAS (HCIS y SELENE).

PERFIL: TÉCNICO DE LA OFICINA DE GESTIÓN DEL SERVICIO

REQUISITOS PERFIL

- Titulación universitaria de nivel 2 con 4 años de experiencia gestionando proyectos en servicios similares
- Dotes de organización.
- Capacidad de gestión y liderazgo a la vez que capacidad para trabajar en equipo.

CONOCIMIENTOS ESPECÍFICOS

- Dirección de equipos humanos.
- Certificación ITIL Foundation.
- Certificaciones en gestión de proyectos: Prince2, PMP o similares.



**PERFIL: TÉCNICO DE APOYO PARA LA OFICINA DE GESTIÓN DEL SERVICIO
(GESTIÓN DOCUMENTAL Y CALIDAD)**

REQUISITOS PERFIL

- Titulación universitaria de nivel 2 con 4 años de experiencia en un puesto similar.

CONOCIMIENTOS ESPECÍFICOS

- Certificación ITIL Foundation.
- Gestión de documentación y calidad.
- Experiencia con gestión documental y calidad en entornos de TI.

**PERFIL: TÉCNICO DE APOYO PARA LA OFICINA DE GESTIÓN DEL SERVICIO
(ADMINISTRATIVO)**

REQUISITOS PERFIL

- Titulación de Técnico Superior (FP) nivel 1 con 4 años de experiencia en un puesto similar.
- Persona habituada a tratar en entornos TI.

CONOCIMIENTOS ESPECÍFICOS

- Gestión de agendas, elaboración de gráficos e informes, gestión de material administrativo, salas de reuniones y hojas de inventario.
- Conocimientos avanzados del paquete MS Office en versiones actualizadas.
- Conocimiento y manejo del lenguaje informático de componentes hardware (potencia CPUs, memoria, periféricos) y software.



PERFIL: ARQUITECTO DE SEGURIDAD

REQUISITOS PERFIL

- Titulación universitaria de nivel 2 con 5 años de experiencia gestionando proyectos de seguridad en proyectos similares.
- Dotes de organización.
- Capacidad de gestión y liderazgo a la vez que capacidad para trabajar en equipo.

CONOCIMIENTOS ESPECÍFICOS

- Conocimiento de la legislación vigente en materia de seguridad de entornos TIC.
- Experiencia con los principales marcos legales y buenas prácticas como ISO 27001, PCI-DSS, Esquema Nacional de Seguridad, GDPR, LOPD y reglamentos relacionados.
- Certificaciones CISSP, CISM/CISA.

PERFIL: COORDINADOR DE EXPLOTACIÓN

REQUISITOS PERFIL

- Titulación universitaria de nivel 2 con 5 años de experiencia en un puesto similar.
- Dotes de organización.
- Capacidad de gestión y liderazgo a la vez que capacidad para trabajar en equipo.

CONOCIMIENTOS ESPECÍFICOS

- Dirección de equipos humanos.
- Gestión de calidad.
- Gestión de modelos de servicio para explotación de CPD.
- Certificación ITIL Foundation.
- Experiencia trabajando con entornos tecnológicos similares a los del SERMAS.



PERFIL: CONSULTORES TECNOLÓGICOS

REQUISITOS PERFIL

- Titulación universitaria de nivel 2 con 5 años de experiencia en un puesto similar o titulación de Técnico Superior nivel 1 con 8 años de experiencia en un puesto similar.

CONOCIMIENTOS ESPECÍFICOS

- Integraciones: Ensemble, Biztalk 2016 y Openlink.
- Formación en administración de Ensemble.
- Servidor de aplicaciones: Oracle OAS 10.1.3, Weblogic 10, JBOSS.
- Bases de datos: Oracle 11g y 12c, SQL Server 2005 y superiores, Mongo DB.
- Oracle RAC, Oracle Dataguard.
- IIS, Apache, .Net, WSUS, Panda.
- Sharepoint Server 2007 y superiores.
- Sistemas operativos: Linux Red Hat Enterprise y Windows en últimas versiones (al menos las 3 últimas).
- Virtualización con VMWare, Hyper-V.
- Sistemas de almacenamiento en red (SAN y NAS), réplica de cabinas, switches de fibra (DELL EMC: VMAX, VNX, Unity, ECS, ISILON, CENTERA, BROCADE; HPE: 3PAR)
- Diseño de arquitecturas de comunicaciones, redes y seguridad.
- Formación y experiencia CheckPoint, Fortinet, F5, Radware Alteon, ISS, AlienVault.
- Gestión y monitorización de sistemas y redes con Nagios, Fluke y Dynatrace DCRUM.
- Experiencia en sistemas de alta disponibilidad y en disaster recovery.
- Servicios de cluster: LVM, multipath, Red Hat cluster suite, Microsoft.
- Arquitectura J2EE.
- Scripting: VBS, Python, PHP, Bash.
- Satellite Server.
- Aplicaciones de backup: Data Protector y NetBackup. Oracle RMAN.
- Sólidos conocimientos sobre LOPD e ISO 27000. Adecuación de sistemas y bases de datos a los requerimientos legales, LOPD, LSSI, ENS, GDPR.
- Experiencia con Hadoop, Cloudera, MongoDB, Openstack COA o equivalentes.
- Formación en Cloudera.



PERFIL: CONSULTORES TECNOLÓGICOS

- Certificaciones: ITIL Foundation, MCSA, Oracle OCP, Weblogic OCA, Red Hat RHCJA, Red Hat RHCSA, Checkpoint, Fortinet NSE, F5 CA, Alteon RCAS-AL, CISCO CCNP, VCP6-DCV, VCP6-CMA, VCA6-NV.
- Experiencia con plataformas VNA.
- Experiencia con plataformas Cloudera, experiencia con plataformas de historia clínica electrónica CERNER SELENE y DXC HCIS o equivalentes.

PERFIL: TÉCNICOS ESPECIALISTAS SENIOR Y JUNIOR

REQUISITOS PERFIL

- Técnicos especialistas senior: titulación universitaria de nivel 2 con 3 años de experiencia como técnico senior o 5 acumulados como técnico senior y técnico junior; o bien, titulación de técnico superior nivel 1 con 5 años de experiencia como técnico senior o 7 años de experiencia como técnico senior y técnico junior.
- Técnicos especialistas junior: titulación universitaria de nivel 2 con 3 años de experiencia o titulación de técnico superior nivel 1 con 5 años de experiencia.
- En ambos casos, la experiencia será en entornos de alta disponibilidad y criticidad similar al servicio CEDAS.

CONOCIMIENTOS ESPECÍFICOS

- Sistemas operativos: Linux Red Hat Enterprise y Windows en sus últimas versiones (al menos las 3 últimas). Experiencia en el ajuste de configuraciones de los sistemas.
- Bases de datos: Oracle 11g y 12c, SQL Server 2005 y superiores, Mongo DB. Experiencia en la optimización de sentencias SQL y ajustes de bases de datos en las tecnologías indicadas.
- Oracle RAC, Oracle Dataguard. Alta disponibilidad y clusterización de sistemas en aplicativos en tres capas (presentación, lógica de negocio y backend) para las versiones Oracle 11g y 12c.
- Servidor de aplicaciones: Oracle OAS 10.1.3, Weblogic 10, JBOSS.
- Arquitectura J2EE. Experiencia en análisis de comportamiento de aplicativos J2EE. Sólidos conocimientos de pruebas de carga sobre sistemas y aplicaciones.
- Experiencia demostrable en administración y soporte de aplicaciones Java de misión crítica sobre Oracle en entornos con miles de usuarios.



PERFIL: TÉCNICOS ESPECIALISTAS SENIOR Y JUNIOR

- IIS, Apache, .Net, WSUS, Panda.
- Sharepoint Server 2007 y superiores.
- Integraciones: Ensemble, Biztalk 2016 y Openlink.
- Formación en administración de Ensemble.
- Sistemas de almacenamiento en red (SAN y NAS), réplica de cabinas, switches de fibra (DELL EMC: VMAX, VNX, Unity, ECS, ISILON, CENTERA, BROCADE; HPE: 3PAR)
- Comunicaciones y redes TCP/IP. Administración y gestión de redes LAN. Herramientas de gestión de red.
- Seguridad: Administración de firewall, balanceadores de carga, aceleradores criptográficos, auditorías de seguridad de sistemas, tecnologías de cifrado y autenticación.
- Experiencia en configuración y administración de soluciones de comunicaciones y seguridad.
- Experiencia con Hadoop, Cloudera, MongoDB, Openstack COA o equivalentes.
- Formación en Cloudera.
- Gestión y monitorización de sistemas y redes con Nagios, Fluke y Dynatrace DCRUM.
- Experiencia en sistemas de alta disponibilidad y en disaster recovery.
- Servicios de cluster: LVM, multipath, Red Hat cluster suite, Microsoft.
- Scripting: VBS, Python, PHP, Bash.
- Satellite Server.
- Aplicaciones de backup: Data Protector y NetBackup. Oracle RMAN. Experiencia con backup a disco (EMC Data Domain).
- Confección de procedimientos y guías de operación.
- Formación y experiencia CheckPoint, Fortinet, F5, Radware Alteon, ISS, AlienVault, CISCO Nexus, Crossbeam.
- Virtualización con VMWare, Hyper-V, KVM.
- Servicios DNS, Directorio activo, DFS.
- Certificaciones: ITIL Foundation, MCSA, Oracle OCA, Weblogic OCA, Red Hat RHCJA, Red Hat RHCSA, Checkpoint, Fortinet NSE, F5 CA, Alteon RCAS-AL, CISCO CCNA, VCA6-DCV, VCA6-CMA, VCA6-NV.
- Experiencia con plataformas VNA.
- Experiencia con plataformas Cloudera, experiencia con plataformas de historia clínica electrónica CERNER SELENE, DXC HCIS y APMADRID o equivalentes.



PERFIL: COORDINADOR DE OPERACIONES

REQUISITOS PERFIL

- Titulación universitaria de nivel 2 con 3 años de experiencia en un puesto similar o titulación de Técnico superior nivel 1 con 5 años de experiencia en un puesto similar.
- Dotes de organización.
- Experiencia demostrable con la operación de entornos críticos.

CONOCIMIENTOS ESPECÍFICOS

- Operación y monitorización de sistemas de información y servidores.
- Operación y monitorización de infraestructuras de CPD.
- Gestión de incidencias y ejecución de tareas siguiendo guías y procedimientos.
- Creación y formalización de guías y procedimientos operativos.
- Conocimientos básicos de sistemas operativos Windows y Linux.
- Conocimientos básicos de aplicaciones de backup (HP Data Protector).
- Experiencia demostrable trabajando con herramienta CA Service Desk.

PERFIL: OPERADOR

REQUISITOS PERFIL

- Titulación de Técnico superior nivel 1 con al menos 1 año de experiencia en operación de entornos críticos.

CONOCIMIENTOS ESPECÍFICOS

- Operación y monitorización de sistemas de información y servidores.
- Operación y monitorización de infraestructuras de CPD.
- Gestión de incidencias y ejecución de tareas siguiendo guías y procedimientos.
- Conocimientos básicos de sistemas operativos Windows y Linux.
- Conocimientos básicos de aplicaciones de backup (HP Data Protector).



PERFIL: COORDINADOR DE INFRAESTRUCTURAS

REQUISITOS PERFIL

- Titulación universitaria de nivel 2 con 3 años de experiencia en un puesto similar o titulación de Técnico superior nivel 1 con 5 años de experiencia en un puesto similar.
- Dotes de organización.

CONOCIMIENTOS ESPECÍFICOS

- Creación y formalización de guías y procedimientos operativos para el mantenimiento y gestión de infraestructuras de CPD.
- Gestión de incidencias y ejecución de tareas en entornos en infraestructuras críticas de CPD. Operación y monitorización de infraestructuras de CPD.
- Gestión y mantenimiento de los activos e inventario de CPD.
- Experiencia demostrable trabajando con CA Service Desk y SCADA Honeywell.
- Experiencia demostrable gestionando, instalando y manteniendo infraestructuras y equipos de CPDs en entornos críticos.

PERFIL: JEFE DE SALA

REQUISITOS PERFIL

- Titulación de Técnico superior nivel 1 con 3 años de experiencia en un puesto similar.

CONOCIMIENTOS ESPECÍFICOS

- Operación y monitorización de infraestructuras de CPD.
- Gestión de incidencias y ejecución de tareas siguiendo guías y procedimientos.
- Gestión de incidencias y ejecución de tareas en entornos en infraestructuras críticas de CPD. Operación y monitorización de infraestructuras de CPD
- Creación y formalización de guías y procedimientos operativos para el mantenimiento y gestión de infraestructuras de CPD.
- Gestión y mantenimiento de los activos e inventario de CPD.
- Experiencia demostrable trabajando con CA Service Desk y SCADA Honeywell.
- Experiencia demostrable gestionando, instalando y manteniendo infraestructuras y equipos de CPDs en entornos críticos.



PERFIL: COORDINADOR DE LA OFICINA DE PROYECTOS PARA EL PLAN DE TRANSFORMACIÓN

REQUISITOS PERFIL

- Titulación universitaria de nivel 3 con 5 años de experiencia en un puesto similar o titulación universitaria de nivel 2 con 7 años de experiencia en un puesto similar.
- Dotes de organización.
- Capacidad de gestión y liderazgo a la vez que capacidad para trabajar en equipo.

CONOCIMIENTOS ESPECÍFICOS

- Dirección de equipos humanos.
- Gestión de calidad.
- Definición y seguimiento de métricas.
- Desarrollo y gestión de documentación.
- Experiencia demostrable con proyectos de transformación de modelos de servicio en entornos de criticidad y volumen similares.
- Certificación ITIL Foundation.
- Certificaciones en gestión de proyectos: Prince2, PMP o similares. Experiencia global similar a la del conjunto de conocimientos específicos del grupo de consultores tecnológicos.

PERFIL: ARQUITECTOS TECNOLÓGICOS DE LA OFICINA DE PROYECTOS PARA EL PLAN DE TRANSFORMACIÓN

REQUISITOS PERFIL

- Titulación universitaria de nivel 2 con 4 años de experiencia en un puesto similar.
- Capacidad para trabajar en equipos mixtos funcionales y técnicos.
- Habilidades de comunicación.

CONOCIMIENTOS ESPECÍFICOS

- Arquitecto en Big Data:
 - Experiencia en proyectos de Enterprise Data y Analytics y Data Lakes.



PERFIL: ARQUITECTOS TECNOLÓGICOS DE LA OFICINA DE PROYECTOS PARA EL PLAN DE TRANSFORMACIÓN

- Definición y mantenimiento de arquitecturas de Big Data.
- Planificación de diseños y soluciones para apoyar a los equipos de desarrollo.
- Experiencia con entornos y servicios cloud, procesos, procedimientos y estándares de tecnologías analíticas.
- Conocimiento de herramientas, lenguajes, procesos y procedimientos.
- Certificaciones: Hadoop, Cloudera.
- Arquitecto para Automatización/Orquestación:
 - Experiencia en proyectos de automatización y orquestación de infraestructuras y servicios en entornos con media/gran escala de disponibilidad y virtualización.
 - Definición de programas de automatización y orquestación.
 - Experiencia realizando estudios de beneficios y retornos de inversión en proyectos de automatización y orquestación.
 - Conocimiento de herramientas de automatización, integración y orquestación (vRealize, NSX, Openstack).
 - Certificaciones: VMWARE (VCA-DCV, VCA-NV, VCP-CMA), Openstack COA.
- Arquitecto para DevOps:
 - Experiencia en entornos de construcción, implementación, paso a producción y operación de productos software.
 - Experiencia trabajando con software en modelo SaaS.
 - Conocimiento y experiencia en entornos GIT, CI/CD. Experiencia con herramientas DevOps tipo Ansible, Puppet, Chef o Saltstack.
 - Experiencia en la definición, diseño, evolución y mantenimiento de arquitecturas DevOps.
 - Conocimiento avanzado de arquitecturas, herramientas, lenguajes de programación, procesos y procedimientos.
 - Certificaciones: Red Hat Certificate of Expertise in Ansible Automation, DevOps Foundation Certified, Dynatrace Associate, SCRUM.



PERFIL: TÉCNICO DE LA OFICINA DE PROYECTOS PARA EL PLAN DE TRANSFORMACIÓN

REQUISITOS PERFIL

- Titulación universitaria de nivel 2 con 4 años de experiencia gestionando proyectos en servicios similares
- Dotes de organización.
- Capacidad de gestión y liderazgo a la vez que capacidad para trabajar en equipo.

CONOCIMIENTOS ESPECÍFICOS

- Dirección de equipos humanos.
- Experiencia con proyectos de transformación de modelo de servicio.
- Certificación ITIL Foundation.
- Certificaciones en gestión de proyectos: Prince2, PMP o similares.

8.2 HORARIOS DE PRESTACIÓN DEL SERVICIO

8.2.1 Horarios de operación y atención a incidencias tanto software como hardware

Los operadores cubrirán a través de un sistema de turnos, un servicio 24x7, 365 días al año, en dos centros distintos, de manera presencial.

El contratista, en su oferta, deberá especificar el equipo de prestación del servicio que asignará de manera presencial a esta actividad.

8.2.2 Horario de administración de sistemas, seguridad y redes. Guardias fuera de horario

Debe garantizarse la cobertura, de lunes a viernes, no festivos, de presencia de técnicos especialistas suficientes, en horario de 7 a.m. a 7 p.m. Al menos el 60% del equipo estará presencialmente en las instalaciones del SERMAS pudiendo reclamar en cualquier momento la presencia de cualquier miembro del equipo de trabajo para cualquier actividad o trabajo relacionado con las tareas propias del servicio descrito en este pliego.



El contratista, en su oferta, deberá especificar el equipo de trabajo que asignará de manera presencial a esta actividad.

Guardias fuera de horario. El contratista asegurará un mínimo de 7 recursos de perfil equivalente a técnicos especialistas para guardias no presenciales fuera de horario. Este personal deberá poder realizar actuaciones presenciales en caso de ser necesario. Los costes de desplazamiento serán responsabilidad del contratista y no supondrán costes adicionales al SERMAS. Estos recursos deberán cubrir entre todos ellos las siguientes áreas de conocimiento:

- Integraciones.
- Servidores de aplicaciones y middleware.
- Bases de datos.
- Comunicaciones y seguridad.
- Tecnologías Microsoft.
- Sistemas operativos y almacenamiento.
- Backup.
- Infraestructura de los CPD.
- Gestión de Operaciones 24x7 y Monitorización.

Así mismo, en su oferta, el contratista deberá especificar el modo de actuación que seguirá el personal de guardia para asegurar la debida atención a las incidencias u otras emergencias que puedan surgir.

8.2.3 Horario de consultoría y soporte nivel 3

Debe garantizarse la cobertura, de lunes a viernes, no festivos, de presencia de especialistas suficientes, en horario de 9 a.m. a 6 p.m.

El contratista, en su oferta, deberá especificar el equipo de trabajo que asignará de manera presencial a esta actividad.

8.2.4 Horario de intervenciones planificadas fuera del horario normal

Para garantizar la disponibilidad de especialistas, listos para intervenir en la realización de actividades planificadas sobre los sistemas, en los horarios adecuados para minimizar el impacto en los usuarios, el contratista tendrá que garantizar la dotación suficiente de personas para la realización de dichas actividades, a llevar a cabo fuera de los horarios establecidos anteriormente. El contratista asumirá la realización de estas intervenciones sin coste adicional.

8.3 NORMATIVAS Y PROCEDIMIENTOS

El proveedor está obligado a cumplir las normas, estándares y procedimientos de la DGSIS.

Estas normativas y procedimientos podrán ser evolucionados o actualizados por la DGSIS, estando el proveedor en la obligación de adoptarlas. En estos casos la DGSIS informará al proveedor de los cambios



que procedan con 30 días de antelación a su entrada en vigor, periodo durante el cual el proveedor está obligado a formar a su personal afectado.

9 CALIDAD DEL SERVICIO

El contratista deberá describir en su oferta su propuesta de modelo de Aseguramiento de la Calidad y la forma en que lo aplicará al servicio. El contratista deberá entregar la primera versión detallada de dicho modelo antes del comienzo de la Fase de Servicio Regular.

Los objetivos del aseguramiento de la calidad del servicio son:

- Identificar, supervisar y controlar todas aquellas actividades, tanto técnicas como de gestión, que son necesarias para garantizar que los servicios alcanzan la calidad requerida.
- Proporcionar evidencias de que las actividades de supervisión y control se han llevado a cabo.

El proceso de aseguramiento de la calidad utilizará como entrada todos los documentos disponibles para cada actividad de servicio, la información de la solicitud de servicio y resto de información disponible en cada momento. Deberá generar, al menos, las siguientes salidas:

DOCUMENTO	RESPONSABLE
Plan de calidad del servicio	Contratista
Registro de verificaciones realizadas	Contratista
Registro de desviaciones detectadas	Contratista
Registro de acciones correctivas	Contratista
Registro de problemas	Contratista
Informes de auditoría del servicio	DGSIS
Plan de acción consecuencia de las auditorías	Contratista

Antes del inicio de la fase de Servicio Regular, el contratista deberá preparar y documentar, un plan de calidad para cada Servicio. El contratista deberá considerar el aseguramiento de la calidad como un proceso horizontal e independiente, pero alineado con el proceso de prestación del servicio. El aseguramiento de la calidad se extenderá a lo largo de todo el contrato y se irá adaptando según las necesidades que demande la DGSIS.

Dichos planes de calidad tendrán como objetivo la identificación de mecanismos, recursos y actividades a través de los cuales se identificarán, supervisarán y controlarán todas aquellas actividades técnicas y de gestión que son necesarias para asegurar que tanto el servicio como sus resultados alcanzan la calidad requerida.

El plan de calidad deberá incluir los siguientes apartados (según aplique en cada caso):



- **Gestión de una petición:** en este punto se deberá definir y documentar en el plan, los roles, fases, actividades, tareas, controles y herramientas, que posteriormente implantará y por las que pasará cada petición desde que es recibida por el contratista hasta que se realiza la entrega a la DGSIS. El fin último de la implantación de esta metodología de gestión de peticiones es asegurar que la inclusión de nuevas funcionalidades o correcciones de defectos en el software no tienen impacto negativo en el rendimiento y funcionamiento de las aplicaciones y se realiza de manera coordinada en todos los centros incluidos.
- **Gestión de la documentación:** dado que el contratista deberá mantener actualizada la documentación de todas las aplicaciones bajo su responsabilidad siguiendo los procedimientos y normativas de la DGSIS, deberá identificar para la documentación existente o que generará durante la prestación del servicio, qué roles la elaborarán, qué roles la revisarán, qué roles la aprobarán y qué mecanismos asegurarán la adecuada trazabilidad a lo largo del proceso de desarrollo de software apoyándose en la metodología de gestión de configuración implantada.
- **Definición de las métricas e indicadores:** se deberán indicar los mecanismos que se van a implantar para poder hacer seguimiento de los indicadores de nivel de servicio y establecer las actividades de análisis y seguimiento de estos.

Para el establecimiento de los criterios de medida, se utilizan las siguientes definiciones:

- **Tiempo de respuesta:** tiempo que transcurre desde que se graba la solicitud hasta el momento en que se comienza por parte del contratista la ejecución de las acciones necesarias para la realización del servicio solicitado. Varía en función de la urgencia transmitida.
- **Tiempo de resolución:** tiempo que transcurre desde que se produce la comunicación por parte del usuario hasta el momento en que se han finalizado los pasos necesarios para su resolución (a la espera de su validación final por el usuario). Varía en función de la urgencia transmitida.
- **Tiempo de gestión:** tiempo dedicado por el grupo a la gestión de cada incidencia, sin ser responsabilidad suya la grabación, respuesta o resolución de la misma. Varía en función de la urgencia transmitida.
- **Urgencia:** refleja la premura con que es necesario resolver una solicitud. Para las tareas de mantenimiento se definen tres niveles de urgencia:
 - Urgencia 1 (Máxima): cuando es necesaria la resolución inmediata al estar ocasionando interrupción del trabajo del usuario.
 - Urgencia 2 (Media): si existe una alternativa momentánea para que el usuario pueda continuar con su trabajo.
 - Urgencia 3 (Baja): el resto de incidencias o averías.



- En caso de no indicarse urgencia (valor 0), se asumen las condiciones de urgencia 3.

Adicionalmente, los servicios se medirán en base a un esquema de acuerdos de nivel de servicio, cuyos umbrales mínimos serán los indicados en este pliego de prescripciones técnicas.

9.1 MODELO DE GESTIÓN DE LAS AUDITORÍAS

Al menos una vez al año, la DGSIS realizará auditorias de calidad planificadas o independientes de cualquier comunicación al proveedor, para verificar el cumplimiento de los requisitos de calidad establecidos en el presente contrato, del plan de calidad de servicio y del modelo operativo. Estas auditorías alimentarán el indicador correspondiente, del modelo de supervisión de los niveles de servicio descrito en el Modelo de Relación.

En todos aquellos casos en que la DGSIS decida la realización de una auditoria al contratista, éste deberá garantizar el acceso total, incondicional e irrevocable a los documentos que estén relacionados a prestaciones de servicios objeto de este contrato.

Las correspondientes auditorias se llevarán a cabo cada vez que lo requiera la DGSIS, debiendo ser comunicadas al proveedor con, al menos, 5 días de anticipación a la fecha de su inicio.

El contratista proporcionará la asistencia y la información que requieran las auditorias, sin cargo adicional.

El proceso de auditoría se regirá por las siguientes normas generales:

- Las auditorías podrán ser solicitadas y ejecutadas en cualquier momento.
- El contratista cooperará en la auditoría, respondiendo de inmediato a las informaciones solicitadas para la ejecución de misma, y auxiliando a los auditores conforme sea necesario.
- Toda información adicional o cambios de conducción de un proceso o como resultado de auditoría, será considerada información confidencial, según los términos y condiciones del contrato.
- La realización de la auditoria en ningún momento eximirá al proveedor del cumplimiento de los compromisos derivados de la prestación los servicios de acuerdo a los términos incluidos en este contrato.

A la finalización de la auditoria las partes revisarán los reparos (no conformidades y/o faltas) detectados.

El proveedor deberá establecer un plan de acción con:

- Acciones concretas para asegurar que las no conformidades y faltas detectadas no vuelvan a aparecer en la próxima auditoría.
- Identificación de responsables y fechas límite para la ejecución de las acciones.

El contratista deberá presentar a la DGSIS el plan de acción en el plazo de 15 días desde la comunicación de los resultados finales de la auditoría. Será responsabilidad del contratista el cumplimiento de las acciones y plazos establecidas en el plan de acción. En sucesivas auditorias, la DGSIS verificará la subsanación de los reparos pudiendo generar nuevas no conformidades en caso de no haberse subsanado.

No presentar en los plazos indicados un Plan de Acción para los reparos, incumplir dicho Plan de Acción,



no subsanar las no conformidades o la reiteración de no conformidades en más de 2 auditorías permitirá a la DGSIS aplicar las penalizaciones equivalentes al no cumplimiento completo de los Acuerdos de Nivel de Servicio relacionados con las auditorías.

El objetivo de las Auditorías de Calidad de los Servicios Contratados es proporcionar visibilidad y control a la DGSIS, sobre el grado de cumplimiento del proveedor con los aspectos formales del servicio. En particular, se llevará a cabo una comprobación objetiva de los siguientes aspectos:

- Verificación del cumplimiento del Plan de Calidad de Servicio, de las condiciones contractuales y de los procedimientos de trabajo establecidos, haciendo especial hincapié en los mecanismos de aseguramiento de la calidad propuestos por el proveedor para sus propias actividades (controles, revisiones, pruebas, auditorías internas del proveedor, etc.).
- Condiciones contractuales: verificando, entre otros aspectos, el cumplimiento de los requisitos de administración y gestión (entornos, herramientas, comunicaciones, etc.), requisitos de recursos y requisitos de seguridad incluidos en el contrato.
- Procedimientos de trabajo: verificando el cumplimiento del modelo de gestión de servicio y los procedimientos y prácticas operativas definidas para la prestación del servicio (actividades, y entregables).
- Revisión de la subsanación de las no conformidades y faltas de auditorías anteriores y de la ejecución del Plan de Acción propuesto para su subsanación.

La auditoría se desarrollará siguiendo las siguientes actividades:

- Comunicación del plan de auditoría.
 - Fechas previstas.
 - Procesos a revisar.
 - Documentación a entregar.
- Ejecución de las tareas de auditoría.
 - Entrevistas personales.
 - Revisión de documentación incluyendo registros y evidencias.
- Elaboración de plan de acción con acciones correctoras.
 - Planes con acciones, fechas comprometidas y personas responsables.
- Seguimiento de las acciones.
 - Registro y evidencia de las acciones desarrolladas y del cumplimiento de los objetivos establecidos.
- Cierre de auditoría.
 - Medida del indicador de ANS obtenida como consecuencia de proceso de auditoría.
 - Informe final.

Para cada auditoría se generará un plan de auditoría y un informe de auditoría. Durante la auditoría se revisará la actividad de todos los tipos de servicio contratados.



Las actividades “Elaboración del plan de acción” y “Seguimiento de acciones” se realizarán únicamente si la auditoría identifica No Conformidades o Faltas.

Los resultados de la auditoría servirán para calcular el ANS asociado con la misma.

La auditoría se realizará mediante revisiones de los distintos aspectos que se contemplen en el contrato, en los Planes de Calidad de los servicios, en los procedimientos operativos, en el plan detallado de infraestructuras, y en el plan detallado de actividades de transferencia del conocimiento. El equipo auditor buscará la conformidad con los aspectos establecidos en estos documentos. Para cada aspecto revisado existirán tres posibles valoraciones:

- **Conforme:** si se cumple completamente con lo indicado en estos documentos.
- **No Conforme:** si hay evidencias de incumplimiento.
- **Falta:** adicionalmente, se incluirán como “falta” aquellos hechos identificados que afecten o puedan afectar, a juicio del equipo auditor, a la calidad del servicio, pero que no supongan un incumplimiento formal de los compromisos establecidos. Las faltas identificadas en un Informe auditoria podrían derivar en No Conformidades en futuras auditorias si no se subsanan.

Adicionalmente a las valoraciones, se podrán hacer observaciones o comentarios del auditor con recomendaciones de mejora o señalando aspectos que deban ser tenidos en consideración para la mejora del servicio.

Todas las no conformidades, faltas y observaciones serán incluidas en el informe de auditoría, de cara a ser tenidos en cuenta en los acuerdos de nivel de servicio.

9.2 FORMACIÓN CONTINUADA. PLANES DE FORMACIÓN.

La reducción del tiempo medio de resolución de incidencias depende del conocimiento de la instalación, de la formación, del compromiso y del alineamiento del equipo del proveedor con dicho objetivo; por tanto, el proveedor, al aceptar la oferta se compromete a formar adecuadamente al personal que preste el servicio. Así mismo, deberá garantizar que el personal que presta el servicio está formado en los procedimientos y prácticas operacionales para garantizar la explotación del servicio. Para ello, se considera necesaria la implementación de una base de conocimiento accesible y auditable por la DGSIS. Esta base de conocimiento deberá tener una primera versión implementada antes del inicio de la prestación del servicio, durante la fase de Transición.

El contratista entregará, antes del comienzo de la primera Fase de Transferencia del Servicio, el Plan de Formación que tiene previsto para el personal que preste servicio.

9.3 EVOLUCIÓN Y MEJORES PRÁCTICAS

El contratista, como parte de sus servicios, deberá proporcionar el soporte y asesoramiento requerido para la definición de las políticas y mejores prácticas que aseguren las necesidades futuras de la DGSIS, tanto, en los aspectos de tecnología, aplicaciones, procedimientos y metodología.



9.4 REQUISITOS DE LOS SISTEMAS DE ACCESO

Si el contratista propone que alguna parte del servicio se preste desde sus propias dependencias, incluirá una descripción suficientemente detallada de los requisitos técnicos y funcionales que, en ningún caso, supondrán costes adicionales al SERMAS. Tales requisitos deben asegurar la operatividad y la seguridad de los sistemas y la información, con el mismo nivel que se exige dentro de las instalaciones de la DGSIS.

En todo caso, la propuesta del contratista tendrá que ser aprobada por la DGSIS, pudiendo denegar la propuesta o solicitar cambios para su aprobación posterior. En ningún caso podrá contravenir lo contemplado en el apartado de Recursos Humanos ni otros apartados de este pliego de prescripciones técnicas.

9.5 HERRAMIENTAS

El contratista está obligado a la utilización de las herramientas de administración, supervisión, monitorización, gestión y control que la DGSIS identifique necesarias. El contratista asume también la utilización de las herramientas disponibles en la actualidad. Cualquier otra herramienta que específicamente necesite el contratista para la adecuada provisión de sus servicios, deberá contar con la aprobación de la DGSIS.

La DGSIS se reserva el derecho de modificar las herramientas de administración, supervisión, monitorización, gestión y control utilizadas en el servicio, a lo largo del contrato. El contratista acatará dicho cambio y utilizará las herramientas que la DGSIS adopte para estas tareas.

Cualquier optimización, script o mejora que el contratista desarrolle sobre las herramientas disponibles para prestar el servicio debe ser comunicada a la DGSIS y pasará a ser propiedad de la DGSIS, sin que el contratista pueda reclamar ningún tipo de compensación adicional.

10 SEGUIMIENTO Y ACUERDOS DE NIVEL DE SERVICIO

Inicialmente se establecerán unos indicadores estimados con el objetivo de proporcionar información fiable de la calidad y agilidad de prestación del servicio desde el primer momento.

Periódicamente, se evaluará de acuerdo a lo incluido en el informe de revisión del servicio, la ejecución de la prestación, revisando el cumplimiento de los niveles de servicio acordados y establecidos. Esta periodicidad dependerá del indicador a valorar.

La no consecución de los Acuerdos de Nivel de Servicio pactados determinará un decremento en el importe de facturación en los términos establecidos en el pliego de cláusulas administrativas.

INDICADORES DE DISPONIBILIDAD DE SISTEMAS DE INFORMACIÓN



INDICADOR	DESCRIPCIÓN INDICADOR	NIVEL PERMITIDO	PERIODICIDAD
Aplicación en horario crítico o aplicación crítica (*)	Disponibilidad	$\geq 99,5\%$	Mensual
	Máximo número de paradas	2	Anual
	Máximo tiempo por parada	30 minutos	Anual
Aplicación en horario no crítico o aplicación no crítica (*)	Disponibilidad	$\geq 99,3\%$	Mensual
	Máximo número de paradas	4	Anual
	Máximo tiempo por parada	1 hora	Anual

(*) Tomando el inventario de aplicaciones y equipamientos objeto del contrato, se establecerá por la DGSIS al inicio del contrato la clasificación de aplicación crítica o no crítica, para cada uno de los ítems del mencionado inventario. Así mismo, se establecerá el horario de criticidad para cada uno de dichos ítems. Esa clasificación y horarios podrá ser objeto de revisión durante la ejecución del contrato, por causas de servicio, debidamente justificadas.

(**) El criterio para calcular el nivel permitido será el resultado de dividir el número de minutos que los servicios han estado disponibles entre el número total de minutos de ese mes.

INDICADORES DE BACKUP Y RECOVERY

INDICADOR	DESCRIPCIÓN INDICADOR	NIVEL PERMITIDO	PERIODICIDAD
Auditoría de backup	Backups fallidos incluyendo los relanzamientos / total de backup	0	Mensual
	% simulaciones de restore realizadas con éxito	$\geq 99,5\%$	Semestral

INDICADORES DEL CUMPLIMIENTO DE PLAZOS EN TAREAS PLANIFICADAS Y PROYECTOS

INDICADOR	DESCRIPCIÓN INDICADOR	NIVEL PERMITIDO	PERIODICIDAD
Ejecución de tareas operativas planificadas	Relación entre el tiempo de retraso en la finalización y la duración total contemplada en el plan, expresada en %	$\leq 15\%$	Mensual
Estado de la ejecución de proyectos	Desvío respecto al último plan acordado	$< 20\%$	Trimestral

INDICADORES DE GESTIÓN DE INCIDENCIAS Y PETICIONES

INDICADOR	DESCRIPCIÓN INDICADOR	TIEMPO DE RESOLUCIÓN	NIVEL PERMITIDO	PERIODICIDAD
Resolución de incidencias de prioridad A	% de incidencias resueltas en plazo $<$ tiempo de resolución, desde la notificación por la unidad de soporte a usuarios o detectadas proactivamente	3 horas	100%	Mensual
Resolución de incidencias de prioridad B	% de incidencias resueltas en plazo $<$ tiempo de resolución, desde la notificación por la unidad de soporte a usuarios o detectadas proactivamente	5 horas	$\geq 90\%$	Mensual
		8 horas	100%	Mensual
Resolución de incidencias de prioridad C	% de incidencias resueltas en plazo $<$ tiempo de resolución, desde la notificación por la unidad de soporte a usuarios o detectadas proactivamente	24 horas	$\geq 85\%$	Mensual
		6 días	100%	Mensual



INDICADOR	DESCRIPCIÓN INDICADOR	TIEMPO DE RESOLUCIÓN	NIVEL PERMITIDO	PERIODICIDAD
Reaperturas de incidencias de prioridad A	% de incidencias resueltas que vuelven a provocar una nueva incidencia	N/A	≤ 2	Mensual
Reaperturas de incidencias de prioridad B, C	% de incidencias resueltas que vuelven a provocar una nueva incidencia	N/A	≤ 3	Mensual
Peticiones (REQ)	% peticiones ejecutadas, desde que son aprobadas por el responsable	4 días	$\geq 85\%$	Mensual
		7 días	100%	Mensual

Prioridad A: Interrupción de un servicio sin alternativa de funcionamiento.

Prioridad B: Degradación o interrupción de un servicio que tiene alternativa de funcionamiento.

Prioridad C: Degradación del servicio pero no impide el trabajo de los usuarios.

Peticiones (REQ): Solicitudes que no son incidencias.

INDICADORES DE GESTIÓN Y CONTROL DEL SERVICIO

INDICADOR	DESCRIPCIÓN INDICADOR	NIVEL PERMITIDO	PERIODICIDAD
Informes de seguimiento definidos	% de informes entregados en los plazos planificados	100%	Mensual
Informes de capacidad y estado de las infraestructuras	% de informes entregados en los plazos planificados	100%	Trimestral
Informes ad hoc solicitados	% de informes entregados en los plazos planificados	100%	Mensual

INDICADORES EN AUDITORÍAS



INDICADOR	DESCRIPCIÓN INDICADOR	NIVEL PERMITIDO	PERIODICIDAD
Número de reparos graves	Número de “no conformidades”, incumplimientos graves o generalizados de procedimientos importantes, recogidos en los planes de calidad o auditorías solicitadas sobre el servicio	≤ 2	Con cada auditoría
Número de reparos leves	Número de incumplimientos leves, no generalizados de procedimientos importantes o de cualquier otro tipo de normas de funcionamiento recogidos en los planes de calidad.	≤ 10	Con cada auditoría

INDICADORES DE GESTIÓN DEL CONOCIMIENTO

INDICADOR	DESCRIPCIÓN INDICADOR	NIVEL PERMITIDO	PERIODICIDAD
Organización del equipo de trabajo	% de integrantes del equipo conformado por profesionales con el perfil de acuerdo al solicitado.	100%	Mensual
	Número de recursos aportados / número mínimo de recursos solicitados	≥ 1	Mensual
Formación recibida	% capacitación del equipo de trabajo ante el uso de herramientas tecnológicas, de infraestructuras...	100%	Trimestral



INDICADORES DE GESTIÓN Y CONTROL DEL PROGRAMA DE TRANSFORMACIÓN DEL MODELO DE SERVICIO

INDICADOR	DESCRIPCIÓN INDICADOR	NIVEL PERMITIDO	PERIODICIDAD
Informes de seguimiento definidos en el programa de transformación	% de informes entregados en los plazos planificados	100%	Trimestral
Informes de capacidad y estado de las infraestructuras: - Análisis de la situación - Revisión y adaptación de la arquitectura de gestión actual	% de informes entregados en los plazos planificados	100%	Análisis de la situación: Una única vez antes del comienzo de la fase de servicio regular. Resto mensual
Informes ad hoc solicitados (Elaboración de procedimientos de gestión centralizada (1), modelo de integración (2), Plan de continuidad y contingencia (3))	% de informes entregados en los plazos planificados	100%	Mensual para 1 Única entrega para 2 y 3



INDICADORES DE CUMPLIMIENTO DEL PROGRAMA DE TRANSFORMACIÓN DEL MODELO DE SERVICIO

INDICADOR	DESCRIPCIÓN INDICADOR	NIVEL PERMITIDO	PERIODICIDAD
Disponibilidad de un portal de autoservicio	Inclusión de procedimientos y procesos automatizados según modelo de transformación.	100%	Trimestral
	Elaboración y actualización de un catálogo de servicios que puedan ser provisionados a través del portal	100%	Trimestral
Herramienta/s automatización procedimientos	Implantación herramienta/s de automatización de procedimientos repetitivos	100%	Una única vez. A los 12 meses de la entrada en vigor del contrato.
Modelo de transformación	% cumplimiento hitos del modelo entregado	100%	Trimestral
Solución tecnológica de infraestructura cloud privada	% requisitos hardware de la plataforma cumplidos	100%	Una única vez. A los 6 meses de la entrada en vigor de la etapa de prestación regular del servicio.
Prestación del servicio de solución tecnológica de infraestructura cloud privada	% requisitos software de la plataforma cumplidos	100%	Trimestral
	% funcionalidades de la plataforma cumplidos	100%	Trimestral
	% ámbitos de uso implantados en la infraestructura cloud privada	100%	Trimestral



11 INFRAESTRUCTURA DE TRABAJO Y SEGURIDAD

11.1 INFRAESTRUCTURA

La DGSIS proveerá los entornos (hardware y software) necesarios para facilitar la prestación del servicio, incluyendo desarrollo, certificación/preproducción, producción y contingencia. Del alcance anterior se excluye el equipamiento personal (PCs y teléfonos móviles, principalmente), que deberá aportar el contratista, sin coste adicional para el SERMAS.

Corresponderán al contratista los gastos de comunicaciones de voz y datos para soportar conexiones a instalaciones del SERMAS, desde instalaciones externas al SERMAS, en caso de ser necesarias. En relación a los teléfonos móviles, será obligatorio que al menos el director de proyecto, coordinador de explotación y consultores dispongan de teléfono móvil y que esté operativo para el trabajo diario en el horario establecido.

También corresponde al contratista la contratación de una línea dedicada punto a punto desde las instalaciones del CPD extendido hasta la sede del contratista desde la que el personal no in-situ preste el servicio. Los gastos de esta línea serán a cargo del contratista que dispondrá de 1 mes desde la fecha de firma del contrato para la puesta en marcha de esta línea.

El SERMAS proporcionará en sus instalaciones servicios básicos de red y conectividad a Internet a los miembros de los equipos que así lo requieran.

11.2 SEGURIDAD DE LOS SISTEMAS

El contratista, en el ejercicio de la prestación del servicio, deberá tener en cuenta los siguientes aspectos de seguridad en los sistemas a su cargo:

- **Seguridad de aplicaciones:** los sistemas, aplicaciones o herramientas a los que la DGSIS facilite el acceso al contratista para ejecutar sus trabajos, deberán ser utilizadas únicamente con este fin.
- **Seguridad de la información:** la información y datos que el contratista deba utilizar para la realización de sus trabajos, o sea producida como consecuencia de los mismos, es propiedad de la DGSIS, y no podrá ser utilizada para otros fines que no sean la prestación del servicio, quedando prohibida su copia en cualquier soporte, sin previa autorización. En caso de autorización para el uso o copia de cualquier información, el contratista deberá destruirla físicamente, cualquiera que sea su formato, una vez finalizados los trabajos para los que fueron creados.
- **Seguridad de comunicaciones:** al margen de los requisitos señalados a este respecto, el contratista deberá implementar mecanismos de control de acceso que garanticen la seguridad, integridad y confidencialidad de los datos que se encuentren en los equipos dedicados al servicio y ubicados en sus instalaciones.



- **Seguridad física:** las instalaciones del contratista deberán contar con acceso restringido y controlado, en el que deberán estar ubicados todos los equipos desde los que sea posible acceder a los Sistemas de Información de DGSIS. Además, deberán establecerse políticas de seguridad para el acceso al puesto de trabajo de cada una de las personas que trabajan en el servicio.
- **Seguridad, confidencialidad de la información:** el contratista debe mantener ficheros de auditora con información detallada (usuario, puesto, fecha y hora, recursos accedidos, etc.) que aseguren la puesta en marcha y el cumplimiento de todas estas medidas de seguridad.

11.3 SEGURIDAD, CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

El adjudicatario se compromete a cumplir las medidas y requisitos de seguridad exigidos por la CSCM. 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.
- 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 491/2013, de 25 junio, por la que se aprueba la política de seguridad de la información en el Ámbito de la administración Electrónica y de los sistemas de información de la Consejería de Sanidad de la Comunidad de Madrid.
- 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.

11.3.1 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 (Contrato de Encargado de Tratamiento), que



será firmado por el adjudicatario de forma previa al inicio de los trabajos, y que figura como Anexo al Pliego de Cláusulas Administrativas Particulares.

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.

11.3.2 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.

11.3.3 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 de otros datos de carácter confidencial de la CSCM que puedan manejarse). 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 en su oferta 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, dado el carácter confidencial de los mismos, de manera indefinida
- 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.
- 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.
- 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, a elección del responsable del fichero, 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 los datos dejen de ser pertinentes para la finalidad o tratamiento. En caso de destrucción, se proporcionará por el contratista un certificado fehaciente de la misma.
 - 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.

11.3.4 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. También estarán obligados al deber de secreto respecto a datos confidenciales de la CSCM de carácter no personal.

El contratista se compromete a formar e informar a su personal en las obligaciones que de tales normas dimanen, para lo cual programará las acciones formativas necesarias.

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.

11.3.5 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 CSCM, 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 elección del responsable del fichero, a la CSCM, al igual que cualquier soporte o documentos utilizados. En caso de destrucción, se proporcionará por el contratista un certificado fehaciente de la misma.



11.3.6 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.

11.4 Restricciones generales

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

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

12 PROPIEDAD DE LOS TRABAJOS Y PRODUCTOS

Todos los estudios y documentos, así como los productos y subproductos elaborados por el contratista como consecuencia 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 contratista 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, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa del SERMAS.

13 CONTENIDO DE LAS OFERTAS

Los licitadores deberán aceptar explícitamente en su propuesta, la totalidad de las cláusulas recogidas en los pliegos. Además deberán describir las peculiaridades de cada propuesta para que pueda ser valorada.

Las ofertas serán presentadas tanto en formato tradicional en papel, como en formato electrónico. La oferta técnica deberá recoger en su globalidad, los apartados del siguiente modelo propuesto, con independencia de que el licitador pueda hacer llegar adicionalmente cuanta información complementaria considere de interés. En base al contenido requerido, no se estima necesaria una extensión superior a 80 páginas. **Las mejoras para la valoración de los criterios de valoración, deberán incluirse en el sobre que se especifica para cada una más adelante**, el resto de la documentación de la oferta se incluirá en el sobre 2-A.

0. ÍNDICE

1. RESUMEN EJECUTIVO

Resumen del contenido de la propuesta, resaltando lo que el licitador considere más importante.

2. MODELO DE SERVICIO

Incluyendo dos apartados:

2.1 Modelo global

Descripción de la organización del equipo de prestación del servicio, distribución de responsabilidades y tareas, coordinación, dedicación al proyecto, flujos de comunicación, mecanismos de control, lugar de prestación del servicio para los perfiles de operador y técnicos especialistas, previsiones para guardias fuera del horario normal de prestación del servicio y servicios de consultoría y soporte nivel 3, etc, en relación con su adecuación a las necesidades y objetivos del proyecto. En su caso, propuestas que especifiquen mecanismos que permitan absorber nuevos requisitos, ampliaciones y propuestas de incorporación de recursos en cada actividad, así como los criterios objetivos que lo determinen.

2.2 Planteamiento específico por fases

Planteamiento para cada una de las fases de los servicios a prestar: descripción funcional, operativa y de relación, de acuerdo con los requisitos de la cláusula 6 Fases del Servicio, del presente pliego. Se podrán incluir propuestas concretas de mejoras en las fases de



planificación y transferencia inicial, para una mejor consecución de los objetivos del servicio.

2.3 Plan de transformación del servicio

El licitador debe presentar en su oferta un “plan de transformación del servicio” detallado, que describa los objetivos, fases, tareas/actividades y el horizonte temporal en que desarrollará la evolución y mejora continua del servicio hacia ese modelo.

3. ASEGURAMIENTO DE LA CALIDAD

El licitador deberá describir en su oferta su propuesta de modelo de Aseguramiento de la Calidad y la forma en que lo aplicará al servicio

5. ASPECTOS RELATIVOS A ACTUALIZACIONES DE LA INFRAESTRUCTURA Y DEL SOPORTE A USUARIOS

Se incluirán las propuestas relativas a las actualizaciones de la infraestructura y del soporte a usuarios. En particular, lo relativo a propuestas que detallen la integración y coordinación funcional y técnica con las unidades del SERMAS afectadas por el servicio, en especial con el servicio de gestión y administración de Centros de Proceso de Datos, así como a la rápida disponibilidad de las actualizaciones de la plataforma, de los parches que corrijan errores detectados y del soporte de usuarios. También se podrá incluir un plan detallado y cuantificado de actualización de versiones de los productos y software involucrado y un plan de documentación ajustado a las necesidades concretas.

6. PROPUESTA METODOLÓGICA Y DE CONTINUIDAD DEL SERVICIO

Descripción de la metodología global, las diferentes fases y para cada una de las líneas de trabajo y servicios, así como el plan general de aseguramiento de la calidad y de continuidad del servicio.

Así mismo se valorará la propuesta de una metodología de migración a entornos cloud privados y públicos. Para su valoración el licitador incluirá la documentación detallada de dicha metodología y el enfoque y adaptación de dicha metodología a las particularidades del SERMAS. Se valorará la metodología global, las diferentes fases y para cada una de las líneas de trabajo y servicios, así como el plan general de aseguramiento de la calidad y de continuidad del servicio. **La propuesta de una metodología de migración a entornos cloud privados y públicos se incluirá en el sobre 2-A de la documentación**

7. SEGURIDAD DE LA INFORMACIÓN. MEDIDAS DE PROTECCIÓN DE DATOS PERSONALES Y DOCUMENTACIÓN

Los licitador/es aportarán en su oferta una memoria descriptiva de las medidas que adoptarán para asegurar la confidencialidad, disponibilidad e integridad de los datos manejados y de la documentación facilitada. Como se requiere el acceso a datos clínicos, se puntualizarán todas aquellas medidas, tanto técnicas como organizativas que aseguren la confidencialidad y las de registro que permita un completo seguimiento de la integridad de la información. Se podrá incluir



un Plan de Seguridad general aplicable al servicio, herramientas informáticas para controlar la posibilidad de acceso a la información por parte de los técnicos de la empresa, herramientas que faciliten la obtención de información relativa a los accesos y actuaciones realizadas sobre los datos, así como medidas técnicas para preservar la seguridad de la información en actuaciones y accesos remotos.

8. MEJORAS

Los licitadores podrá aportar una serie de mejoras que se valoran en los criterios de valoración del Pliego de Cláusulas Administrativas:

- Mejora en la calidad del equipo humano asignado al proyecto (**se incluirá en el sobre 2-A de la documentación**): Mayor número de certificaciones profesionales y valoración de su distribución para el conjunto del equipo humano propuesto para el bloque de Técnicos Especialistas Senior y Junior.
 - Número total de certificaciones acreditadas documentalmente por encima de las 14 mínimas exigidas.
 - Número total de personas poseedoras de certificaciones.
- Oferta de jornadas de consultores especialistas en materia de CPD, efectuadas por personal distinto al incluido en la oferta, para toda la duración del contrato (**se incluirá en el sobre 2-B de la documentación**).
- Oferta de servicios de retirada y destrucción de material hardware obsoleto conforme a normativa legal medioambiental vigente (**se incluirá en el sobre 2-B de la documentación**).
- Dotación de aplicaciones de gestión de costes y gestión de inventario para dar soporte a las actividades solicitadas en el pliego (**se incluirá en el sobre 2-B de la documentación**).
- Mejora en la dotación de infraestructura de cloud privada para los CPD centrales del SERMAS (**se incluirá en el sobre 2-A de la documentación**)

14 RELACIÓN DE ANEXOS AL PLIEGO DE PRESCRIPCIONES TECNICAS

A continuación se enumeran los ANEXOS Técnicos del PPT. Por motivos de confidencialidad, estos anexos se pondrán a disposición de los licitadores exclusivamente en la forma establecida en el Pliego de Cláusulas Administrativas y previa firma de acuerdo de confidencialidad.



ANEXO	DENOMINACIÓN
ANEXO I	CATÁLOGO ACTUAL DE SERVICIOS DE ATENCIÓN Y SOPORTE TIC
ANEXO II	LISTADO DE APLICACIONES, CRITICIDAD Y HORARIO DE SERVICIO
ANEXO III	RELACIÓN DE EQUIPOS QUE PRECISAN LA CONTRATACIÓN DE SERVICIOS DE MANTENIMIENTO DE INFRAESTRUCTURAS HARDWARE Y SOFTWARE INSTALADOS EN LOS CPDS DEL SERMAS
ANEXO IV	GUÍA DE ESTÁNDARES PARA DESARROLLO DE APLICACIONES EN LA CSCM
ANEXO V	MATRIZ DE RESPONSABILIDADES DE PROCESOS Y ACTIVIDADES DE SERVICIO
ANEXO VI	INVENTARIO DE SISTEMAS QUE PRECISAN DE PLANES DE CONTINGENCIA EN EL TERCER CPD

Madrid,
EL DIRECTOR GENERAL DE SISTEMAS
DE INFORMACIÓN SANITARIA

Fdo: José Antonio Alonso Arranz



La autenticidad de este documento se puede comprobar en www.madrid.org/csv
mediante el siguiente código seguro de verificación: **090873853554611528255**