

Este documento se ha obtenido directamente del original que contenía todas las firmas auténticas y se han ocultado los datos personales protegidos y los códigos que permitirían acceder al original.

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR LA CONTRATACIÓN DE “SERVICIOS PARA LA ACTUALIZACIÓN DEL PLAN DE SEGURIDAD DEL OPERADOR Y DE LOS PLANES DE PROTECCIÓN ESPECÍFICOS EXISTENTES Y DE ELABORACIÓN DE LOS PLANES DE PROTECCIÓN ESPECÍFICOS DE LAS NUEVAS INFRAESTRUCTURAS CRÍTICAS DESIGNADAS PARA EL OPERADOR SERVICIO MADRILEÑO DE SALUD”.

SEPTIEMBRE 2025

Índice

1. ANTECEDENTES Y OBJETO DEL CONTRATO	3
1.1. Antecedentes.....	3
1.2. Objeto del Contrato.....	4
2. DESCRIPCIÓN DE LOS SERVICIOS	5
3. EQUIPO DE PRESTACIÓN DEL SERVICIO	11
4. FASES Y PLAZOS DEL CONTRATO	13
5. DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS	14
5.1. Evaluación del servicio prestado.....	14
5.2. Dirección y seguimiento de los trabajos.....	14
5.3. Modificaciones en el equipo de prestación del servicio	15
5.4. Metodología a emplear.....	16
6. CONDICIONES GENERALES	17
6.1. Lugar de la prestación del servicio.....	17
6.2. Horario de la prestación del servicio.....	17
6.3. Medidas y recursos para la prestación del servicio	17
6.4. Propiedad de los trabajos.....	17
6.5. Calidad de los trabajos.....	18
6.6. Valoración y abono de los trabajos.....	18
7. SEGURIDAD DE LA INFORMACIÓN	19
7.1. Encargado del tratamiento	19
7.2. Limitación del acceso al tratamiento.....	19
7.3. Medidas de Seguridad	19
7.4. Destino de los datos al finalizar la prestación del servicio	22
7.5. Cesión o comunicación de datos a terceros	23
7.6. Responsabilidad en caso de incumplimiento.....	23
7.7. Cesión del contrato	24
8. DOCUMENTACIÓN TÉCNICA DE LA OFERTA	24

1. ANTECEDENTES Y OBJETO DEL CONTRATO

1.1. Antecedentes

A los efectos previstos en el artículo 116.4 de la Ley de Contratos del Sector Público, aprobada por la Ley 9/2017, de 8 de noviembre, se informa de lo siguiente:

Según se dispone en los Decretos 24/2008, de 3 de abril, del Consejo de Gobierno, por el que se establece el régimen jurídico y de funcionamiento del Servicio Madrileño de Salud, y 273/2023, de 27 de diciembre, del Consejo de Gobierno, por el que se modifica el 246/2023, de 4 de octubre, del Consejo de Gobierno, por el que se establece la estructura directiva del Servicio Madrileño de Salud, el Servicio Madrileño de Salud, a través de la Dirección General Asistencial, tiene entre sus competencia, la implantación, desarrollo y seguimiento de las políticas de seguridad en el ámbito sanitario público de la Comunidad de Madrid, de acuerdo con la normativa vigente en materia de seguridad e infraestructuras críticas.

Por otro lado, la Ley 8/2011, de 28 de abril, y el Real Decreto 704/2011, de 20 de mayo, y sus disposiciones adicionales, así como los requisitos del Reglamento de Protección de las Infraestructuras Críticas, se describen las medidas para la Protección de las Infraestructuras Críticas, es decir, aquellas que proporcionan servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Dentro de estos servicios, el ámbito de la salud es especialmente sensible, siendo considerado como uno de los sectores estratégicos para la protección de las infraestructuras críticas, debido a que una posible interrupción o destrucción de alguna de las infraestructuras propias imposibilitaría la continuidad de la prestación del servicio esencial sanitario en esa infraestructura en particular, pero, a mayores, incidiría en el exponencial incremento de la carga asistencial del resto de centros, afectando por tanto a la actividad asistencial que el Servicio Madrileño de Salud presta en su conjunto.

Los dos grandes objetivos de esta norma precitada son catalogar el conjunto de infraestructuras que prestan servicios esenciales a nuestra sociedad y diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas y ataques hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones.

Con fecha 30 de octubre de 2018, la Comisión Nacional para la Protección de las Infraestructuras Críticas aprobó, conforme a lo establecido en el artículo 11.2 de la Ley 8/2011, de 28 de abril, el Plan estratégico del Sector Salud, con objeto de identificar y

designar los operadores críticos que sustentan los servicios esenciales prestados por dicho sector.

Como consecuencia de ello, el SERVICIO MADRILEÑO DE SALUD de la COMUNIDAD DE MADRID, con número de identificación fiscal Q2801221I, fue designado por la Comisión Nacional para la Protección de Infraestructuras Críticas, como operador crítico a través de Resolución de la Secretaría de Estado de Seguridad, dependiente del Ministerio del Interior.

De dicho nombramiento y conforme a la normativa, se establecen una serie de responsabilidades como operador crítico entre las que se identifican:

- Elaborar el Plan de Seguridad del Operador (PSO) y proceder a su actualización periódicamente o cuando las circunstancias así lo exijan.
- Elaborar un Plan de Protección específico por cada una de las infraestructuras (PPE) identificadas como críticas en el Catálogo elaborado por el CNPIC (Centro Nacional de Protección de Infraestructuras Críticas).

La presente contratación tiene como único objetivo, la realización de todas las tareas necesarias para que el servicio madrileño de salud como operador crítico pueda cumplir con estas responsabilidades precisadas en tiempo y forma.

1.2. objeto del contrato.

El objeto del contrato es el servicio de apoyo para la revisión del Plan de Seguridad del Operador (PSO) y de los 3 Planes de Protección Específicos (PPE) ya establecidos y la realización de un Plan de Protección Específico por cada una de las 9 infraestructuras identificadas como críticas en el catálogo elaborado por el CNPIC.

2. DESCRIPCIÓN DE LOS SERVICIOS.

Se detallan a continuación las tareas a desarrollar por el adjudicatario, conducentes a la REVISIÓN de los planes PSO y PPE y elaboración de los PPEs, con los siguientes condicionantes:

Plan de Seguridad del operador (PSO)

Revisión del Plan PSO aprobado en el que quedó definida la política general del operador para garantizar la seguridad integral del conjunto de instalaciones o sistemas de su propiedad o gestión.

Tal y como quedó establecido el PSO, como instrumento de planificación del Sistema de Protección de Infraestructuras Críticas, CONTIENE:

- Política general de seguridad del operador y marco de gobierno.
 - Política.
 - Marco de Gobierno de seguridad integral.
 - Organización de seguridad.
 - Responsable de Seguridad y Enlace.
 - Delegados de Seguridad.
 - Formación y concienciación.
 - Modelo de gestión aplicado. El adjudicatario deberá desarrollar y documentar. un modelo específico para la gestión de la seguridad física.
 - Procedimientos para el desarrollo del marco de gobierno de seguridad. integral, a partir del modelo de gobierno existente en el SERMAS.
- Relación de servicios Esenciales prestados por el operador crítico.
 - Identificación de los servicios esenciales.
 - Mantenimiento del inventario de servicios esenciales.
 - Estudio y consecuencias de la interrupción del servicio esencial.
 - Interdependencias.
- Metodología de análisis de riesgo (amenazas físicas y lógicas).
 - Descripción de la metodología de análisis.
 - Tipologías de activos que soportan los servicios esenciales.
 - Identificación y evaluación de amenazas.
 - Valoración y Gestión de riesgos.
- Criterios de aplicación de Medidas de Seguridad Integral. Serán utilizados, los estándares internacionales de mejores prácticas de seguridad de la información ISO/IEC 270002, ISO 27001 sobre los requisitos para gestionar la seguridad de la información e ISO 22301 relativa a sistemas de gestión de la continuidad de negocio, aunque otros estándares o guías pueden ser empleados como complemento y mejora al estándar ISO.

Asimismo, el adjudicatario prestará asistencia y asesoramiento en el desarrollo de los programas o ejercicios que puedan derivarse del Plan Estratégico Sectorial, así como en su momento de los Planes de Apoyo Operativo.

Igualmente, el adjudicatario prestará apoyo en el diseño del Plan de Formación y eventual desarrollo del mismo, destinado al personal relacionado con la protección de las infraestructuras críticas. Tales como:

- Participación en ejercicios de simulación en incidentes de seguridad.
- Impartición de conocimientos, a nivel básico:
 - Sobre seguridad integral (seguridad física y ciberseguridad).
 - Sobre autoprotección.
 - Sobre seguridad del medio ambiente.
 - Sobre habilidades organizativas y de comunicación.
 - Sobre sus responsabilidades/actuaciones en caso de materializarse un incidente, o en el caso de que se active un nivel de amenaza 4 ó 5 del Plan de Prevención y Protección Antiterrorista y/o del Plan Nacional de Protección de las Infraestructuras Críticas.

Plan de Protección Específico (PPE)

Respecto a los 3 Planes de Protección Específicos ya aprobados existentes la revisión de los mismos contendrán las indicaciones a implementar, en caso de resultar pertinente las modificaciones de los mismos.

En lo relativo a los Planes de Protección Específico que deberán desarrollarse para cada una de las infraestructuras identificadas por el CNPIC, se prevé la elaboración de 9 PPEs con cargo al contrato.

Cada PPE tendrá los siguientes contenidos:

- Identificación y documentación de la organización de la seguridad en la infraestructura crítica (IC).
- Definición de los delegados de seguridad de las IICC.
- Mecanismos de coordinación.
- Mecanismos y responsables de aprobación.
- Identificación y documentación de los datos relativos a la instalación, denominación y tipo, propiedad y gestión, localización y estructura física, y descripción del servicio o servicios esenciales que proporciona junto con la relación con otras posibles infraestructuras necesarias para la prestación del servicio.

Será responsabilidad del proveedor la realización de las siguientes actividades en relación al PPE de cada infraestructura crítica seleccionada:

Arquitecturas

- Identificar y documentar las arquitecturas de los sistemas de información, tanto los tradicionales (ICT - Information and Communications Technology) como los de carácter industrial (ICS - Industrial Control System). El resultado será un documento que incluya inventario, arquitecturas, descripción, y diseño de arquitectura para los sistemas de información existentes.

Activos/elementos de la infraestructura crítica.

- Se incluirán en este apartado todos los activos que soportan la infraestructura crítica, diferenciando aquellos que son vitales de los que no lo son. En concreto se detallarán:

- Las instalaciones o componentes de la infraestructura crítica que son necesarios y por lo tanto vitales para la prestación del servicio esencial.
- Los sistemas informáticos (hardware y software) utilizados, con especificación de los fabricantes, modelos y versiones, etcétera.
- Las redes de comunicaciones que permiten intercambiar datos y que se utilicen para dicha infraestructura crítica.
- Arquitectura de red, rangos de IP públicas y dominios.
- Esquema(s) de red completo y detallado, de tipo gráfico y con descripción literaria, donde se recojan los flujos de intercambio de información que se realizan en las redes, así como sus perímetros electrónicos.
- Descripción de componentes de la red (servidores, terminales, hubs, switches, nodos, routers, firewalls,...) así como su ubicación física.

- Las personas o grupos de personas que explotan u operan todos los elementos anteriormente citados, indicando y detallando de forma particular si existe algún proceso externalizado a terceros. En este último caso, identificación de este personal.

- Los proveedores críticos que en general son necesarios para el funcionamiento de dicha infraestructura crítica y se interrelacionan con la misma, y específicamente:

- De suministro eléctrico.
- De comunicaciones (telefonía, internet, etc....).
- De tratamiento y almacenamiento de información (CPDs, etc.).
- De ciberseguridad (CERTs privados, SOC, etc.).

Sobre los proveedores nombrados por el operador, se especificarán los distintos Acuerdos de Nivel de Servicios que se tienen contratados y que son considerados esenciales.

Interdependencias.

Del mismo modo, se especificarán las interdependencias, bien con otras infraestructuras críticas del propio operador, o bien:

- Con otras infraestructuras estratégicas del propio operador que soportan el servicio esencial.
- Entre sus propias instalaciones o servicios.
- Con sus proveedores dentro de la cadena de suministro.
- Con los proveedores de servicios TIC contratados para esa infraestructura, tales como: proveedor(es) de telecomunicaciones, Centros de Proceso de Datos, servicios de seguridad (Centro de Operaciones de Seguridad, CERT privado, etcétera) y cualesquiera otros que se consideren.
- Con los proveedores de servicios de seguridad física, indicando los servicios prestados y el personal y medios empleados, CON IDENTIFICACIÓN DE LOS VS Y AUXILIARES.

Amenazas.

Identificar las amenazas a las que está expuesta la ICT e ICS. En alineación con la metodología de gestión de riesgos, basada en MAGERIT, y empleando la herramienta PILAR, el proveedor introducirá el inventario de activos e identificará las amenazas que potencialmente podrían afectar a dichos activos.

El resultado de esta actividad será un fichero de la herramienta PILAR (extensión .mgr) con la información indicada con anterioridad, y siguiendo el método que le será entregado con anterioridad a la ejecución de esta actividad.

Análisis de riesgos:

Se deberá incluir en el PPE los resultados del análisis de riesgos integral realizado sobre la infraestructura crítica. Dicho análisis de riesgos deberá seguir las pautas metodológicas recogidas en el PSO.

Se identificarán las amenazas asociadas a la infraestructura, tomando como referencia el árbol de amenazas proporcionado por el CNPIC/PILAR, considerando de forma especial aquellas amenazas de origen terrorista o intencionado, que han sido detectadas durante la realización del análisis de riesgos plasmando al menos:

- Las amenazas intencionadas, tanto de tipo físico como a la ciberseguridad, que afecten de forma específica a alguno de los activos que soportan la infraestructura crítica.
- Las amenazas que puedan afectar directamente a la infraestructura procedente de las interdependencias identificadas, sean éstas deliberadas o no.
- Las dirigidas al entorno cercano o elementos interdependientes tanto del anteperímetro físico como lógico que puedan afectar a la infraestructura.

- Las amenazas que afecten a los sistemas de información que den soporte a la operación de la infraestructura crítica y todos los que estén conectados a dichos sistemas sin contar con las adecuadas medidas de segmentación.
- Las amenazas que afecten a los sistemas y servicios que soportan la seguridad integral.

Asimismo, se identificarán las medidas de seguridad existentes, tanto permanentes como temporales y graduales:

- Organizativas y de gestión.
- Operacionales o procedimentales.
- De protección o técnicas.

Los resultados obtenidos en los análisis de riesgos serán introducidos por el adjudicatario en la herramienta PILAR, para la obtención de las corrientes valoraciones y su impacto según los riesgos identificados.

Plan de Tratamiento de Riesgos (para cada activo IDENTIFICADO).

El proveedor deberá de elaborar un Plan de Tratamiento de los Riesgos que permita llevar el riesgo a niveles aceptables, implantando para ello controles de índole técnico, documental y organizativo.

Para todas las medidas identificadas (existentes o complementarias a desarrollar), se deberá describir, como parte integrante del PPE:

- Listado de las medidas a disponer (físicas o de ciberseguridad).
- Una explicación de la operativa resultante para cada tipo de protección (físico y lógico).

El operador deberá especificar el conjunto detallado de medidas a aplicar para proteger el activo como consecuencia de los resultados obtenidos en el análisis de riesgos.

En concreto, por cada activo identificado, deberá incluir la siguiente información:

- Acción propuesta, con detalle de su ámbito (alcance) de aplicación.
- Responsables de su implantación, plazos, mecanismos de coordinación y seguimiento, etc.
- Carácter de la medida, permanente, temporal o gradual.
- Recursos estimados (personales y materiales)
- Duración estimada
- Prioridad



El proveedor será también responsable de trasladar dicho Plan de Tratamiento de Riesgos al fichero PILAR, indicando en él cómo evoluciona el cumplimiento de los controles/salvaguardas en función de las acciones propuestas.

Adicionalmente al uso de la herramienta PILAR, el contenido de los planes objeto del presente pliego, así como toda la documentación asociada, deberá ser editable en formato MS-Word, y asimismo conforme con las guías de contenidos mínimos y las guías de buenas prácticas (y sus actualizaciones correspondientes) publicadas por el CNPIC, así como con cualquier otra guía o documentación de referencia que durante la duración del presente contrato sea publicada por dicha entidad.

Para el perfeccionamiento del contrato se precisará:

- La aprobación por parte del CNPIC de los planes PSO y PPE de cada una de las infraestructuras.
- La certificación de la totalidad de las tareas recogidas en el presente pliego de condiciones técnicas, junto con las que fueran ofrecidas como mejora por el adjudicatario.

3. EQUIPO DE PRESTACIÓN DEL SERVICIO

El objetivo final del contrato es la revisión del PSO y de los PPEs existentes y de la elaboración de los nuevos Planes PPE. Para ello el contratista dedicará los recursos de personal que considere necesarios, por encima de los perfiles mínimos que se consideran imprescindibles, para obtener los resultados en el plazo establecido del contrato. El CENTRO DIRECTIVO podrá requerir un reforzamiento del equipo de trabajo para alcanzar el cumplimiento DENTRO de los plazos establecidos.

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

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

El responsable de proyecto ofertado debe cumplir los siguientes requisitos:

- Formación mínima:
 - Titulación universitaria.
 - Titulación como Director de Seguridad
- Experiencia mínima:
 - 5 años como responsable de proyectos PIC.
 - Experiencia demostrable en la elaboración de planes PSO y PPEs.
 - Auditoría, análisis o diseño de arquitecturas de comunicaciones.
 - Auditoría, análisis o diseño de soluciones basadas en sistemas de seguridad.
 - Auditoría, análisis o diseño de soluciones TIC.

- Consultores (3), especialistas en análisis de riesgos y cumplimiento normativo que realizarán las tareas de elaboración de la documentación necesaria para el desarrollo de los Planes PSO y PPEs.

Los consultores deben cumplir los siguientes requisitos:

- Formación mínima:
 - Titulación universitaria superior.
- Formación acreditada:
 - Gestión de la seguridad (CISM, CISA).
 - Metodologías de análisis y gestión de riesgos tales como Magerit, Mosler.
 - Esquema Nacional de Seguridad

- Protección de infraestructuras críticas

- Experiencia demostrable mínima en las siguientes tareas:

- 5 años participando en proyectos o servicios de seguridad TIC y/o seguridad física en las siguientes tareas:
 - Desarrollo de planes PSO y PPE
 - Adecuación al ENS.
 - Análisis de Riesgos conjuntos de Seguridad Física y Ciberseguridad.
 - Diseño e implantación de controles de Ciberseguridad
 - Participación en proyectos de sistemas de seguridad física.
 - Experiencia en el uso de la herramienta del CCN, PILAR.
 - Auditoría, análisis o diseño de soluciones basadas en sistemas de seguridad.

Tanto la formación acreditada como la experiencia demostrable deberán ser cubiertas por el grupo de consultores en su conjunto.

Formación acreditada: será obligatorio que el grupo cuente con al menos, una de cada una de las certificaciones requeridas.

Experiencia: No se precisa que todos los miembros del grupo consultor tengan experiencia en todas las tareas solicitadas, pero si el grupo de consultores en su conjunto.

4. FASES Y PLAZOS DE CONTRATO

Fase I

Comenzará inmediatamente tras la firma del contrato, consistiendo en la revisión del Plan de Seguridad del Operador (PSO) y de los 3 Planes de Protección Específicos ya aprobados.

Fase II

Consistirá en la elaboración de los Planes de Protección Específicos. Esta fase comenzará tras la superación de la Fase I, si bien el adjudicatario y la DGA podrán acordar la realización de tareas previas de documentación en cualquier momento tras la firma del contrato.

Plazo de ejecución

El plazo máximo de ejecución de los trabajos objeto del presente pliego de prescripciones técnicas será de 15 meses desde la firma del contrato.

5. DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS

5.1. Evaluación del servicio prestado

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

La Gerencia de Seguridad Corporativa del SERMAS establecerá los formatos de entregables y supervisará el alcance y contenido de los mismos, evaluando el cumplimiento y calidad de los trabajos realizados y marcando las prioridades.

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

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

5.2. Dirección y seguimiento de los trabajos

Corresponde a la Gerencia de Seguridad Corporativa del SERMAS dirigir y supervisar los trabajos y velar por el cumplimiento de los niveles de servicio acordados.

En este sentido, la Gerencia de Seguridad Corporativa del SERMAS nombrará un director de Proyecto cuyas funciones principales en relación con el objeto del presente pliego serán las siguientes:

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

Es potestad del director del Proyecto exigir en cualquier momento la adopción de cuantas medidas concretas y eficaces sean necesarias en relación con la prestación del servicio, si

a su juicio, la calidad o efectividad del mismo se pone en peligro ante cualquier circunstancia.

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 Gerencia de Seguridad Corporativa del SERMAS, enfocando los recursos en función de las necesidades, de forma que se proporcione cobertura completa a todo el alcance del pliego en cada momento.

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

- Coordinar el apoyo técnico y supervisar el servicio a prestar e informar al director del Proyecto de las posibles incidencias y seguimiento o desviaciones de plazos.
- Mensualmente remitir a la Gerencia de Seguridad Corporativa del SERMAS un informe detallado que permita constatar el cumplimiento de la calidad del servicio prestado, sin menoscabo de que la misma pueda realizar aquellas actuaciones que considere oportuno para contrastar la veracidad de los datos aportados.
- Mensualmente, como mínimo, mantener con la Dirección del Proyecto una reunión de seguimiento del servicio prestado en el mes previo y validación de la propuesta para el mes siguiente a la misma.

5.3. Modificaciones en el equipo de prestación del servicio

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

Excepcionalmente, la Dirección del Proyecto tendrá la potestad de exigir, cuando existan razones suficientemente motivadas que afecten al normal desarrollo de la prestación del servicio, el cambio de cualquiera de los componentes del equipo prestador de los servicios del contratista. Este cambio se solicitará por el Director de Proyecto, a través de las

reuniones de Seguimiento, garantizando al contratista un preaviso de 15 días laborables, para que pueda proceder a la sustitución de dicho componente.

Si el contratista propusiera el cambio de cualquiera de los miembros del equipo prestador

del servicio, se deberá comunicar por escrito a la Gerencia de Seguridad Corporativa del SERMAS con 15 días laborables de antelación, comunicando:

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

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

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

El contratista deberá garantizar que dispone de los mecanismos adecuados para minimizar la rotación no planificada del personal, para evitar la pérdida no controlada de conocimiento, y el impacto en los niveles de servicio, imagen, dedicación adicional, etc., que esto suele llevar asociado.

Por rotación planificada se entiende aquella que se comunica a la Dirección del Proyecto como mínimo 15 días laborables antes de que se produzca, y se acompaña de un solapamiento del recurso saliente con el entrante para la adecuada transferencia de conocimiento durante un periodo no inferior a 10 días laborables.

5.4. Metodología a emplear

El adjudicatario trabajará con carácter global con la metodología interna que estime oportuna pero siempre ajustándose a los elementos que le proporcionará la Gerencia de Seguridad Corporativa del SERMAS, y en concreto en relación a la seguridad física deberá seguir la metodología Mosler aplicada a las necesidades de SERMAS, y en cuanto a la seguridad lógica, Magerit.

En concreto, para el desarrollo de los Planes de Protección Específicos, la Gerencia de Seguridad Corporativa del SERMAS establecerá el contacto inicial con los responsables de Seguridad de los Centros responsables de las Infraestructuras, obteniendo una primera toma de contacto y alertando de las actividades del plan de trabajo que se va a iniciar.

6. CONDICIONES GENERALES

6.1. Lugar de prestación del servicio

El lugar de realización de los trabajos estará ubicado en las dependencias que habilite al respecto el SERMAS, sin perjuicio de que exista la necesidad de desplazamiento a cualquiera de los centros sanitarios para dar cumplimiento a cualquiera de los cometidos.

Asimismo, se contempla la posibilidad de que el SERMAS decida la prestación de servicios, de todo o parte del equipo, con lugar de trabajo establecido en las dependencias del contratista, si así lo considera oportuno.

6.2. Horario de prestación del servicio

El horario de servicio se acordará por parte de la Gerencia de Seguridad Corporativa con el contratista. La dedicación de los recursos ofertados será de jornada completa, en horario de mañana y tarde comprendido entre las 8 y las 19:00, de lunes a viernes.

6.3. Medios y recursos para la ejecución del servicio

El contratista asumirá la provisión y mantenimiento de equipamiento de hardware y software necesario para el desempeño de las tareas encomendadas. Asimismo, proveerá del material de oficina y fungibles correspondientes.

6.4. Propiedad de los trabajos

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

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

6.5. Calidad de los trabajos

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



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

6.6. Valoración y abono de los trabajos.

VALORACIÓN Y ABONO DE LOS TRABAJOS

Los trabajos no se considerarán terminados hasta que el PSO y los PPE sean, a propuesta del CNPIC, aprobados por la Secretaría de Estado de Seguridad. La fecha límite de entrega de los trabajos será el 31 de diciembre de 2026.

Tras la entrega de la actualización del Plan de Seguridad del Operador (PSO), de los 3 Planes de Protección Específicos a actualizar y de los 9 Planes de Protección Específicos a realizar, y previa certificación de conformidad de la realización del servicio, se abonará un único pago, correspondiente al 100% del importe total.

Los pagos se realizarán mediante transferencia bancaria, previa presentación de la factura.

7. SEGURIDAD DE LA INFORMACIÓN

En el caso de que el adjudicatario, en el ejercicio de la prestación del servicio, tuviera que tratar con datos de carácter personal de la Gerencia de Seguridad Corporativa, cumplirá con la legislación vigente en materia de protección de datos de carácter personal que resulte de aplicación, en concreto el Reglamento (UE) 2016/679, del Parlamento Europeo Y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos RGPD); Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD); así como las disposiciones de desarrollo de las normas anteriores o cualesquiera otras aplicables en materia de Protección de Datos que se encuentren en vigor a la adjudicación de este contrato o que puedan estarlo durante su vigencia.

Así, y a los efectos de este contrato, las Direcciones, organismos, entidades o entes de derecho público de la CSCM tendrán la consideración de responsable del tratamiento y el adjudicatario tendrá la consideración de Encargado del Tratamiento conforme a lo establecido en los artículos 28 y 29 en el RGPD.

7.1. Encargado del tratamiento

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

7.2. Limitación del acceso al tratamiento

El adjudicatario limitará el acceso o tratamiento de datos de carácter personal pertenecientes a los ficheros bajo titularidad de cualquiera de las Direcciones, organismos, entidades o entes de derecho público de la CSCM, limitándose a realizar el citado acceso o tratamiento cuando se requiera imprescindiblemente para la prestación del servicio y/o de las obligaciones contraídas, y en todo caso limitándose a los datos que resulten estrictamente necesarios.

7.3. Medidas de Seguridad

A los efectos de la prestación del servicio por parte del adjudicatario, en su calidad de encargado del tratamiento quedará obligado, con carácter general, por el deber de confidencialidad y seguridad de los datos de carácter personal (y de otros datos de carácter confidencial de la CSCM que puedan tratarse). Y con carácter específico, en todas aquellas previsiones que estén contempladas en las actividades que formen parte del servicio adjudicado, en especial:

- El Adjudicatario y el personal encargado de la realización de las tareas guardarán y asegurarán la confidencialidad, disponibilidad e integridad sobre todas las informaciones, documentos y asuntos a los que tengan acceso o conocimiento durante la vigencia del contrato, no revelando, transfiriendo o cediendo, ya sea verbalmente o por escrito, a cuantos datos conozcan como consecuencia de la prestación del servicio sanitario, sin límite temporal alguno.
- El adjudicatario, mediante la suscripción del contrato de adjudicación, asumirá el cumplimiento de lo previsto en las presentes cláusulas, atendiendo en especial, a los artículos 28, 29, 30 y 32 del RGPD.
- El adjudicatario utilizará los datos de carácter personal única y exclusivamente, en el marco y para las finalidades determinadas en el objeto del servicio adjudicado y del presente documento, y bajo las instrucciones del responsable del tratamiento, y de la Gerencia de Seguridad Corporativa del Servicio Madrileño de Salud, perteneciente al SERMAS, para aquellos aspectos relacionados con sus competencias.
- Accederá a los datos de carácter personal responsabilidad del responsable del tratamiento únicamente cuando sea imprescindible para el buen desarrollo de los servicios para los que ha sido contratado.
- En caso de que el tratamiento incluya la recogida de datos personales en nombre y por cuenta del responsable del tratamiento, el encargado del tratamiento deberá seguir los procedimientos e instrucciones que reciba del responsable del tratamiento, especialmente en lo relativo al deber de información y, en su caso, la obtención del consentimiento de los afectados.
- Si el encargado del tratamiento considera que alguna de las instrucciones del responsable del tratamiento infringe el RGPD, la LOPDGDD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, informará inmediatamente al responsable del tratamiento.
- En caso de estar obligado a ello por el artículo 30 del RGPD y 31 de la LOPDGDD, el encargado del tratamiento mantendrá un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable del tratamiento, que contenga la información exigida por el artículo 30.2 del RGPD.
- Garantizará la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- Dará apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.
- Dará apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

- Pondrá a disposición del responsable del tratamiento toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen al responsable del tratamiento u otro auditor autorizado por este.
- En caso de estar obligado a ello por el artículo 37.1 del RGPD y por el artículo 34 de la LOPDGDD, designará un delegado de protección de datos y comunicará su identidad y datos de contacto al responsable del tratamiento, cumpliendo con todo lo dispuesto en los artículos 37, 38 y 39 del RGPD y 35 a 37 de la LOPDGDD.
- En caso de que el Encargado del Tratamiento deba transferir o permitir acceso a datos personales responsabilidad del responsable del tratamiento a un tercero en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable del tratamiento de esa exigencia legal de manera previa, salvo que estuviese prohibido por razones de interés público.
- Se prohíbe el tratamiento de datos por terceras entidades que se encuentren en terceros países sin un nivel de protección equiparable al otorgado por la normativa de protección de datos de carácter personal vigente en España, salvo que se obtenga la preceptiva autorización de la Agencia Española de Protección de Datos para transferencias internacionales de datos, de conformidad con los artículos 44, 45, 46, 47, 48, y 49 del RGPD.
- El adjudicatario comunicará y hará cumplir a sus empleados, y a cualquier persona con acceso a los datos de carácter personal, las obligaciones establecidas en los apartados anteriores, especialmente las relativas al deber de secreto y medidas de seguridad.
- El Adjudicatario no podrá realizar copias, volcados o cualesquiera otras operaciones de conservación de datos, con finalidades distintas de las establecidas en el servicio adjudicado, sobre los datos de carácter personal a los que pueda tener acceso en su condición de encargado del tratamiento, salvo autorización expresa del responsable del tratamiento o de la Gerencia de Seguridad Corporativa del SERMAS.
- Adoptar y aplicar las medidas de seguridad estipuladas en el presente contrato, conforme lo previsto en el artículo 32 del RGPD, que garanticen la seguridad de los datos de carácter personal responsabilidad del responsable del tratamiento y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.
- El adjudicatario se compromete a formar e informar a su personal en las obligaciones que de tales normas dimanen, para lo cual programará las acciones

formativas necesarias. Así mismo, el del Adjudicatario tendrá acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

- El adjudicatario comunicará al responsable del tratamiento y a la Gerencia de Seguridad Corporativa del SERMAS, para aquellos aspectos relacionados con sus competencias, de forma inmediata, cualquier incidencia en los sistemas de tratamiento y gestión de la información que haya tenido o pueda tener como consecuencia la alteración, la pérdida o el acceso a datos de carácter personal, o la puesta en conocimiento por parte de terceros no autorizados de información confidencial obtenida durante la prestación del servicio.
- El adjudicatario estará sujeto a las mismas condiciones y obligaciones descritas previamente en el presente documento, con respecto al acceso y tratamiento de cualesquiera documentos, datos, normas y procedimientos pertenecientes a la CSCM a los que pueda tener acceso en el transcurso de la prestación del servicio.
- Los diseños y desarrollos de software deberán, observar con carácter general, la normativa de seguridad de la información y de protección de datos de la Comunidad de Madrid y:
 - En todo caso observarán los requerimientos relativos a la identificación y autenticación de usuarios, estableciendo un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado, limitando la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.
 - En ningún caso el equipo prestador del servicio objeto del contrato tendrá acceso ni realizará tratamiento de datos de carácter personal contenidos o soportados en los equipos o recursos mantenidos.

7.4. Destino de los datos al finalizar la prestación del servicio

Una vez cumplida o resuelta la relación contractual acordada entre el responsable del tratamiento y el encargado del tratamiento, el encargado del tratamiento deberá solicitar al responsable del tratamiento instrucciones precisas sobre el destino de los datos de carácter personal de su responsabilidad, pudiendo elegir éste último entre su devolución, remisión a otro prestador de servicios o destrucción íntegra, siempre que no exista previsión legal que exija la conservación de los datos, en cuyo caso no podrá procederse a su destrucción.

7.5. Cesión o comunicación de datos a terceros

El adjudicatario no comunicará los datos accedidos o tratados a terceros, ni siquiera para su conservación. Así, el encargado del tratamiento no podrá subcontratar ninguna de las prestaciones que formen parte del objeto del pliego y que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios.

- En caso de que el encargado del tratamiento necesitara subcontratar todo o parte de los servicios contratados por el responsable del tratamiento en los que intervenga el tratamiento de datos personales, deberá comunicarlo previamente y por escrito al responsable del tratamiento, con una antelación de 1 mes, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa sub-encargada, así como sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable del tratamiento no manifiesta su oposición en el plazo establecido.
- El sub-encargado, también está obligado a cumplir las obligaciones establecidas en este documento para el Encargado del Tratamiento y las instrucciones que dicte el responsable del tratamiento.
- Corresponde al encargado del tratamiento exigir por contrato al subencargado el cumplimiento de las mismas obligaciones asumidas por él a través del presente documento.
- El encargado del tratamiento seguirá siendo plenamente responsable ante el responsable del tratamiento en lo referente al cumplimiento de las obligaciones.

7.6. Responsabilidad en caso de incumplimiento

El encargado del tratamiento será considerado responsable del tratamiento en el caso de que destine los datos a otras finalidades, los comunique o los utilice incumpliendo las estipulaciones del encargo, respondiendo de las infracciones en que hubiera incurrido personalmente.

Restricciones generales.

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

- La utilización de los sistemas de información para la realización de actividades ilícitas o no autorizadas, como la comunicación, distribución o cesión de datos, medios u otros contenidos a los que se tenga acceso en virtud de la ejecución de los trabajos y, especialmente, los que estén protegidos por disposiciones de carácter legislativo o normativo.

- La instalación no autorizada de software, modificación de la configuración o conexión a redes.
- La modificación no autorizada del sistema de información o del software instalado, el uso del sistema distinto al de su propósito.
- La sobrecarga, prueba, o desactivación de los mecanismos de seguridad y las redes, así como la monitorización no autorizada de redes o teclados.
- La reubicación física y los cambios de configuración de los sistemas de información o de sus redes de comunicación.
- La instalación de dispositivos o sistemas ajenos al desarrollo del contrato sin autorización previa, tales como dispositivos USB, soportes externos, ordenadores portátiles, puntos de acceso inalámbricos o cualquier otro dispositivo.
- 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.

7.7. Cesión del contrato

El contratista no podrá ceder total o parcialmente, los derechos y obligaciones que se deriven del contrato sin autorización expresa escrita de la Gerencia de Seguridad Corporativa del SERMAS, que fijará las condiciones de la misma, no autorizándose la cesión de los contratos a favor de empresas incursas en causa de inhabilitación para contratar.

8. DOCUMENTACIÓN TÉCNICA DE LA OFERTA

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

La oferta contendrá una planificación temporal pormenorizada de todas las tareas y deberá estructurarse de acuerdo con el siguiente índice, si bien los licitadores podrán incluir la información adicional que consideren pertinente:

- Descripción general del servicio
- Planteamiento para la ejecución del proyecto. En relación con el desarrollo de las actividades de verificación de la adecuación de las medidas y controles, según lo establecido en la normativa vigente y su desarrollo reglamentario, en cuanto a la organización del mismo, la metodología, el grupo propuesto y su estructura.
- Planificación del proyecto. Los licitadores indicarán y explicarán el enfoque a utilizar para el desarrollo del proyecto, incluyendo propuesta de planificación, cronograma, y metodología (aplicada a las necesidades de SERMAS) explicada lo más detalladamente posible, que en relación a la seguridad física será Mosler, y en seguridad lógica, Magerit en su última versión.
- Descripción pormenorizada del equipo de trabajo y su participación en proyectos similares.
- Mecanismos para el control del proyecto. Actividades relacionadas con el control del proyecto, dado el elevado volumen de ficheros y la dispersión geográfica de los centros.
- Recursos técnicos. Detalle de la puesta a disposición de herramientas tecnológicas, en la medida en que contribuya eficazmente a la consecución de los objetivos del servicio objeto del contrato.

Madrid, a fecha de firma.

Órgano proponente.

Firma y sello de la persona que suscribe: ALMUDENA QUINTANA MORGADO
Fecha: 2020.02.24 12:37

Almudena Quintana Morgado.