EXPEDIENTE 2023-0-41

PLIEGO DE CONDICIONES TÉCNICAS RELATIVO AL CONTRATO DE SERVICIO DE AUDITORÍA Y SOPORTE PARA EL ANÁLISIS DE SITUACIÓN Y LA ADECUACIÓN PARA EL CUMPLIMIENTO NORMATIVO EN MATERIA DE SEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES

[redacted]

Contenido

1 INTRODUCCIÓN

La entrada en vigor del Reglamento General de Protección de Datos (RGPD), que sustituyó a la normativa vigente en materia de Protección de Datos y que comenzó a aplicarse el 25 de mayo de 2018, supuso un importante cambio en la organización y los procedimientos de trabajo relativos a la seguridad y la protección de datos personales. El RGPD fue desarrollado en nuestro país a través de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que establece, entre otras medidas, la plena aplicación del nuevo Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS). Adicionalmente, en los últimos años han entrado en vigor otras normativas y guías, entre las que destacan el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, la Guía Nacional de Notificación y Gestión de Ciberincidentes y las Guías CCN-STIC del Centro Criptológico Nacional, que son normas, instrucciones, guías y recomendaciones con el fin de mejorar el grado de ciberseguridad de las organizaciones, estando especialmente dirigidas a las Administraciones Públicas.

Por otra parte, distintos organismos nacionales e internacionales vienen indicando un importante incremento en el número de incidentes de ciberseguridad en los últimos años, especialmente en el ámbito sanitario, tal y como indica el informe anual CCN-CERT IA-13/21 Ciberamenazas y Tendencias. La irrupción de la pandemia COVID19 en 2020 ha marcado un punto de inflexión, introduciendo nuevas capacidades y servicios en el ámbito sanitario (como la telemedicina y el teletrabajo), un incremento en el interés de los datos sanitarios y en su compartición con fines de investigación, y por consiguiente nuevos riesgos para la protección de los datos personales.

Por todo ello, el Hospital Universitario 12 de Octubre (en adelante H12O) plantea la contratación de un servicio de consultoría técnica especializada para la realización de todas las acciones necesarias para el cumplimiento normativo, documental y técnico, que el centro requiere en materia de Seguridad de la Información con el fin de garantizar el máximo nivel de protección posible a los datos personales y de la información que maneja en el ejercicio de sus funciones.

2 OBJETO

Constituye el objeto del contrato, la contratación del servicio para la ejecución correcta de tareas, según los estándares de calidad establecidos y las directrices de la Oficina de Seguridad de Sistemas de Información del Servicio Madrileño de Salud (OSSI), relativas a los siguientes objetivos:

- Documentación y acciones a realizar en cumplimiento de la legislación vigente, durante toda la vida del contrato, en materia de seguridad y protección de datos personales.
- Categorización y análisis de viabilidad de todas las aplicaciones instaladas en el H12O y realización de documentos para su posterior inclusión para los Registros de Actividades de Tratamiento.
- Análisis de riesgos e impacto de negocio (BIA) siguiendo la metodología MAGERIT y la herramienta PILAR, o aquellas que estime el H12O más convenientes.
- Tareas relativas a la constitución, modificación y mejoras de la Política de Seguridad, los Procedimientos e Instrucciones Técnicas y los requisitos mínimos objeto del ENS, además de todo aquello que se considere necesario de manera adicional por parte del H12O.
- Preparación técnica-documental y seguimiento del Comité de Seguridad de la Información del centro.

- Soporte al área de Asesoría Jurídica para la respuesta al ejercicio de los derechos de Supresión, Oposición, Portabilidad, Limitación, Acceso y Rectificación incluidas en el nuevo RGPD, incluyéndolas, tramitándolas y resolviéndolas, con las herramientas que determine en cada momento el H12O en tiempo y forma, y de manera correcta.
- Análisis, valoración técnica y funcional, así como elaboración de las respuestas a los incidentes de seguridad tanto propios como recibidos desde la Dirección General de Sistemas de Información y Salud Digital (DGSISD).
- Soporte a la relación institucional y técnica con la Oficina de Seguridad de la Información (OSSI) de la propia DGSISD, con el Comité Delegado de Protección de Datos del SERMAS (DPD), y con las áreas responsables en el ámbito de la ciberseguridad en la Comunidad de Madrid (Agencia para la Administración Digital de la Comunidad de Madrid – Madrid Digital), analizando y respondiendo a sus peticiones, necesidades y requerimientos de manera correcta y verificada por el centro.
- Realización de las Auditorías de Seguridad de la Información de obligado cumplimiento y las que pudieran considerarse necesarias por el H12O.
- Análisis de viabilidad de nuevos proyectos, incluyendo la preparación y revisión de la documentación necesaria para la contratación y la realización de convenios y acuerdos de colaboración con terceros y la elaboración de las evaluaciones de impacto (EIPD), en línea con las directrices de la OSSI en esta materia.

3 DESCRIPCIÓN TÉCNICA DEL SERVICIO

Como condición general para todos los puntos expuestos en este apartado, el visado de la correcta ejecución de las tareas y de la documentación elaborada, será realizado por el Responsable del Servicio nombrado por parte del H12O. Se determinará la realización de los trabajos mediante la solicitud escrita por parte del H12O, siendo el adjudicatario responsable de detallar las tareas técnicas requeridas para cubrir los objetivos planteados por el H12O.

La entrega del documento de especificación de requisitos para la elaboración de documentos, políticas, protocolos, procesos y procedimientos por parte del H12O al adjudicatario se realizará en formato electrónico o formato papel, recibiendo acuse de recibo en las siguientes 24 horas por parte del adjudicatario. En caso de no recibir dicho acuse de recibo y justificar el H12O su entrega mediante correos electrónicos, se considera entregado a efectos de contabilización de tiempos de realización de las tareas encomendadas. Toda la documentación generada por el adjudicatario será en formato electrónico bajo los parámetros y ajustes definidos por el H12O al inicio del contrato.

Todo el material, entregables, documentación generados durante la duración del contrato será propiedad del H12O, y no podrá ser utilizado por el adjudicatario para otros fines que no sean la prestación del servicio objeto de este contrato.

El adjudicatario utilizará el gestor documental y el resto de herramientas que en cada momento indique el H12O, siendo responsable el adjudicatario de la gestión de la parte correspondiente a seguridad. Si fuera necesario dar acceso a herramientas corporativas, el H12O será el encargado de facilitarlo al adjudicatario.

Independientemente de los plazos marcados en cada apartado del presente pliego, el adjudicatario garantizará por encima de todo que el H12O pueda cumplir los plazos establecidos en la normativa vigente en cada momento.

Si se determina por parte del H12O que una tarea o documento, política, proceso, protocolo o entregable no es correcto, el adjudicatario tendrá 3 días naturales para subsanar los mismos. En

caso de que, tras la nueva entrega por parte del adjudicatario, se determine por parte del H12O que sigue sin estar correcto, será motivo de aplicación de las penalidades correspondientes. Será motivo de rescisión de contrato la reiterada baja calidad de la documentación o tareas entregadas.

En caso del incumplimiento de las entregas por parte del adjudicatario, será motivo de la aplicación de las penalidades correspondientes.

3.1 Cumplimiento en materia de protección de datos

El adjudicatario realizará la revisión de todos los documentos, políticas, protocolos, procesos y procedimientos existentes en el H12O necesarios para el cumplimiento de la legislación vigente en materia de protección de datos y su creación en caso de que no se disponga de los mismos, de acuerdo a las pautas y directrices establecidas por la OSSI. Se tomará especial atención al Principio de Proactividad del RGPD, abordando las tareas que se deban realizar para cumplimiento normativo para todas las nuevas aplicaciones que vayan incluyéndose en el Hospital, y para las que, habiéndose instalado previamente, no dispongan de toda la documentación pertinente.

El plazo para la realización de los cometidos deberá ser cumplido en el plazo de 30 días naturales desde la entrega de cada especificación de requisitos definida por el H12O, salvo que se indique otra prioridad por parte del hospital y a excepción de los casos particulares de los Documentos de Registro de Actividad de Tratamiento y el Análisis de Riesgos y la evaluación del impacto que se ceñirán a los tiempos establecidos en sus apartados correspondientes.

Así mismo, el adjudicatario deberá prestar asesoramiento en materia de seguridad de la información y protección de datos para la revisión y desarrollo de contratos, pliegos consentimientos informados, etc.

3.1.1 Elaboración y actualización del Registro de Actividades de Tratamiento

Partiendo del inventario de Tratamientos del centro, se realizará un análisis exhaustivo de las aplicaciones instaladas en el H12O según los parámetros establecidos en el Registro de Actividades de Tratamiento, donde para cada aplicación se tendrá en cuenta su implicación en cada tratamiento/os, sus características técnicas y funcionales, su análisis de riesgos y sus procedimientos de gestión.

El plazo máximo para toda la generación de documentación y entregables de este análisis, es de 3 meses desde la firma del contrato. Además, el adjudicatario, diseñará y pondrá en marcha los procesos y procedimientos necesarios para mantener actualizados los documentos, basados en las particularidades e idiosincrasia del H12O.

Toda acción o necesidad de documentación, de tramitación, de entrega, actualización relativa a los Registros de Actividades de Tratamientos, incluyendo la inclusión de nuevas aplicaciones durante la duración del contrato, quedará cubierta por el adjudicatario mediante el presente pliego, contando con 7 días laborables para la entrega tras su notificación por parte del H12O.

3.1.2 Evaluaciones de Impacto en la Protección de Datos (EIPD)

El adjudicatario prestará soporte en el análisis de necesidad de realización de una EIPD, así como en su posterior desarrollo, teniendo en cuenta que la EIPD será obligatoria en algunos tratamientos nuevos que se vayan a incorporar, o en otros que ya se estén llevando a cabo. Para ello, se tomará como base la metodología y las herramientas establecidas por la OSSI y la AEPD.

3.1.3 Respuesta al ejercicio de derechos de Protección de Datos

El adjudicatario dará una respuesta eficiente y eficaz a las reclamaciones que los ciudadanos y/o sociedades pudieran cursar en el ejercicio de sus derechos de Protección de Datos (Supresión, Oposición, Portabilidad, Limitación, Acceso y Rectificación), así como aquellas que provengan de la Agencia Española de Protección de Datos, cuando así sea requerido por el H12O. Esta respuesta se ajustará estrictamente a los plazos de ejecución establecidos por la normativa.

3.2 Cumplimiento del Esquema Nacional de Seguridad

3.2.1 Desarrollo de la Política de Seguridad

El adjudicatario desarrollará, junto al interlocutor y los referentes propios del H12O, la Política de Seguridad del centro alineada con la Política de Seguridad del SERMAS. Se establece un plazo de 3 meses para su consecución desde la adjudicación del contrato.

De igual forma, el adjudicatario dará cumplimiento a los requisitos mínimos y los principios básicos en los que se sustenta el ENS y apoyará, llegado el momento la acreditación del centro en el ENS, al menos en su nivel MEDIO.

3.2.2 Desarrollo de normativa de seguridad, procedimientos e instrucciones técnicas

El adjudicatario colaborará y prestará su apoyo en la actualización y desarrollo de la documentación relativa para cumplir con el ENS, por ejemplo, procedimiento de calificación de información, procedimiento de borrado de metadatos, normativa de uso de dispositivos portátiles, etc.).

3.2.3 Análisis de riesgos

De la misma manera, el adjudicatario realizará un análisis de riesgos e impacto de negocio (BIA) siguiendo la metodología MAGERIT y la herramienta PILAR, o las metodologías y herramientas definidas desde el H12O de acuerdo a las directrices de la OSSI, durante los primeros 3 meses desde la firma del contrato. De esta manera se revisarán los activos, las dependencias y el tratamiento de los riesgos y se obtendrá un informe final del análisis de riesgos con la herramienta PILAR en el plazo máximo indicado.

3.3 Cumplimiento de otras normativas sectoriales

En la realización de sus actividades, el adjudicatario deberá tener en cuenta también, no solo lo indicado en el RGPD y en el ENS, sino aquella otra normativa sectorial que resulte de aplicación atendiendo al tipo de actividad realizada por el Hospital.

3.4 Soporte técnico-documental del Comité de Seguridad de la Información

El adjudicatario dará soporte técnico-documental y de seguimiento del Comité de Seguridad de la Información del centro, desplegando un referente en las reuniones, gestionando las reuniones y sus actas y ejecutando y dando seguimiento a las acciones correspondientes.

3.5 Análisis, resolución y respuesta a incidentes de Seguridad de la Información

El adjudicatario hará frente a la notificación y resolución de incidentes de seguridad o brechas de seguridad, dependiendo si el incidente afecta a información, a datos personales o a ambos; en coordinación con los organismos competentes, ya sean incidentes reportados por el propio centro o por entidades externas (DGSISD, OSSI, Madrid Digital, AEPD, CCN, etc.).
Los tiempos de respuesta en este caso, vendrán establecidos por la gravedad del propio incidente de acuerdo a la Guía Nacional de Gestión de Incidentes de Ciberseguridad y a las directrices corporativas.

3.6 Soporte en la relación con la DGSISD, la OSSI y MD

Tanto la DGSISD como su Oficina de Seguridad (OSSI), y el área de Ciberseguridad de Madrid Digital (MD), son entidades dependientes de la administración de la Comunidad de Madrid, siendo de vital importancia una relación constante con éstas en materia de Seguridad de la Información y protección de datos. Será función del adjudicatario el dar soporte a esta relación y favorecer una respuesta efectiva a las peticiones o reclamaciones expuestas por dichas entidades.

3.7 Realización de Auditorías de Seguridad

Será función del adjudicatario la realización de auditorías anuales que darán soporte a la Política de Seguridad del centro y a la legislación vigente (RGPD y ENS), estableciendo las no conformidades, oportunidades de mejoras encontradas, y dando seguimiento a las mismas.

El plazo para la realización de estas auditorías será de 60 días naturales desde su petición por el H12O.

3.8 Análisis de viabilidad de nuevos proyectos

A petición del interlocutor del centro, el adjudicatario realizará un análisis de viabilidad técnico y jurídico, desde el prisma de Seguridad de la Información y de la protección de datos, de los nuevos proyectos de sistemas de información que correspondan, estableciendo los posibles riesgos en la ejecución de los mismos y aportando posibles mejoras. El adjudicatario será el encargado de gestionar la documentación del análisis de riesgos y evaluación de impacto (EIPD) relativa al proyecto y la incluirá en las herramientas que decida en cada momento el H12O. Tanto los análisis de viabilidad como las EIPD se harán de acuerdo a las directrices de la OSSI y tendrán que ser validados por ésta para considerarse adecuadamente realizados.

Se establecerá un plazo de 7 días naturales de respuesta a cada solicitud cursada, siempre que no concurran más de dos solicitudes.

4 EQUIPO DE TRABAJO Y HORARIO DEL SERVICIO

El presente pliego se expone como un servicio, que se prestará en horario de 8:00 a 15:00 y, para ello, **el adjudicatario presentará el equipo de trabajo que considere más adecuado para cumplir con el alcance de los trabajos especificado**. En todo caso, **el adjudicatario deberá destinar un mínimo de 3 personas en el horario establecido** que cumplan al menos con los siguientes requisitos.

Cada una de las personas que trabajen prestando el servicio deberán disponer de la titulación indicada y cumplirán al menos con 2 Certificaciones, 2 cursos de formación y toda la experiencia mínima exigida de lo que se expone a continuación:

1. Un gerente de proyecto (dedicación parcial, al menos del 20%).

   - Titulaciones:
     - Titulado Superior o Grado en Informática o Telecomunicaciones o Titulado Superior o Grado en Derecho.

   - Certificaciones:
     - Auditor ISO 27001.
     - CISA (Certified Information Systems Auditor).
     - CISSP (Certified Security Systems Security Professional).
     - Delegado de Protección de Datos según RGPD.

   - Formación:
     - Curso de formación de al menos 100 horas en Delegado de Protección de Datos.
     - Curso de formación de al menos 40 horas en ENS.
     - Curso de Formación de al menos 40 horas en RGPD.

   - Experiencia mínima exigida:
     - Sector sanitario público (mínimo de 4 años).
     - Conocimiento de las herramientas utilizadas en la Administración Pública Sanitaria para la resolución y gestión de consultas o análisis de riesgos, así como la relativa

al seguimiento y consecución de los hitos establecidos anualmente en el Contrato Programa.
- En la resolución y asesoramiento de contratos, consentimientos informados, protocolos relativos a ensayos clínicos, etc., en lo referente a cumplimiento normativo de protección de datos y medidas de seguridad aplicables (mínimo de 4 años).

2. Dos consultores técnico-jurídicos (a tiempo completo):

- Titulaciones:
  - 1 Titulado Superior o Grado en Informática o Telecomunicaciones.
  - 1 Titulado Superior o Grado en Derecho.

- Certificaciones:
  - Auditor ISO 27001.
  - CISA (Certified Information Systems Auditor).
  - CISM (Certified Information Security Management).
  - CISSP (Certified Security Systems Security Professional).
  - Delegado de Protección de Datos según RGPD.

- Formación:
  - Curso de formación de al menos 100 horas en Delegado de Protección de Datos.
  - Curso de formación de al menos 40 horas en ENS.
  - Curso de Formación de al menos 40 horas en RGPD.

- Experiencia mínima exigida:
  - Sector sanitario público (mínimo de 2 años).
  - Conocimiento de las herramientas utilizadas en la Administración Pública Sanitaria para la resolución y gestión de consultas o análisis de riesgos.
  - En la resolución y asesoramiento de contratos, consentimientos informados, protocolos relativos a ensayos clínicos, etc., en lo referente a cumplimiento normativo de protección de datos y medidas de seguridad aplicables (mínimo de 2 años).

No serán valorados los cursos de formación expedidos por el licitador sobre los empleados que presenta al concurso, incluso aunque el certificado esté expedido por una empresa del grupo.

Las personas del equipo acudirán presencialmente al H12O al menos 2 días a la semana. Los días serán establecidos por el H12O, siendo el horario de 8:00 a 15:00 durante la duración del contrato, con el fin de recoger y resolver dudas sobre los entregables, sobre las solicitudes realizadas y aclarar posibles problemas in situ. Además, participarán en todas las reuniones que el responsable designado por el H12O requiera.

El resto del servicio se prestará desde las dependencias del adjudicatario, facilitando al Hospital las vías de comunicación de al menos, un teléfono de contacto y correo electrónico adicionales a los del responsable de servicio, donde se harán llegar todas las peticiones e incidencias electrónicas. Adicionalmente, desde el Hospital, se dará acceso a las aplicaciones de gestión de incidencias, con

la finalidad de que estas sean resueltas desde las propias aplicaciones, así como a las aplicaciones de colaboración corporativas.

El adjudicatario deberá estar disponible en horario de 15:00 a 19:00 para la atención al H12O ante incidentes o necesidades urgentes que no puedan esperar a la jornada laboral ordinaria.

No se permitirá el cambio del perfil que asista al Hospital, si no es por declaración jurada de la empresa, de que el profesional que presta el servicio cause baja de la misma o concurra otro motivo debidamente justificado. El Hospital se reserva el derecho de solicitar el cambio de cualquiera de los recursos ante cualquier queja recibida por los usuarios incluyendo los del equipo de trabajo de Servicio de Sistemas de Información, y el adjudicatario lo ejecutará como máximo en 10 días laborables tras la petición del Hospital, teniendo que sustituir dicho recurso sin que ello sea un problema para el cumplimiento de los acuerdos de nivel de servicio. El recurso que se incorpore, deberá cumplir con lo expuesto en los requerimientos del equipo de trabajo en cuanto a perfiles. Si durante la duración del expediente se requiriera el cambio de 2 perfiles de cualquier tipo, será motivo de rescisión de contrato.

5 COMITÉ DE SEGUIMIENTO

El Comité de Seguimiento estará formado por los responsables designados por el H12O y el responsable del Servicio de la empresa adjudicataria y su función principal será la de articularse como mecanismo para el seguimiento y control de las tareas de los servicios de peticiones e incidencias.

La periodicidad de las reuniones del Comité de Seguimiento será por defecto de una vez al mes, a petición del H12O. El Responsable del Servicio del H12O podrá modificar la periodicidad por defecto. Así mismo podrá convocarse de manera excepcional, a petición del responsable del H12O o el de la empresa adjudicataria.

Corresponderá al Comité de Seguimiento las siguientes funciones, sin perjuicio de otras que se les asigne durante la ejecución de la duración del expediente:

- ✓ Definición en detalle del alcance para los periodos contemplados, estableciendo los objetivos, cronograma de tareas y distribución de los recursos del servicio, orientados al cumplimiento de los entregables, objeto del contrato.

- ✓ Seguimiento de la evolución del servicio y el grado de cumplimiento de los objetivos definidos para los diferentes periodos que se vayan estableciendo en comités anteriores.

- ✓ Aprobar cualquier documentación a presentar. En especial todas aquellas que describan de manera objetiva y formal la situación del servicio.

- ✓ Seguimiento del cumplimiento de los acuerdos de nivel de servicio (ANS).

De estas reuniones del Comité, el responsable de Servicio de la empresa adjudicataria levantará acta, que será revisada y aprobada por los miembros del Comité, para dar constancia de la evolución de los distintos servicios, de los posibles problemas detectados, de los requerimientos aprobados, de la desviación de objetivos, etc.

6 ACREDITACIONES DE LA EMPRESA LICITANTE

Las empresas licitadoras deberán estar en posesión y adjuntar las siguientes certificaciones o equivalentes vigentes:

- UNE EN ISO 9001:2015: Sistema de gestión de calidad.
- UNE EN ISO 14001:2015: Sistemas de gestión medioambiental.
- UNE EN ISO/IEC 27001:2013: Tecnología de la Información- Sistemas de gestión de la seguridad de la información.
- UNE EN ISO 20000:2011: Tecnología de la información- Gestión del servicio.
- ISO22301: Continuidad de negocio.
- Pertenencia a la Red Nacional de SOC (RNS).
- Acreditación de un centro de operaciones SOC 24x7 con certificación del ENS en categoría media.
- Pertenencia a la organización FIRST (Forum of Incident Response and Security Teams).

Madrid, a fecha de firma

EL JEFE DE SERVICIO DE INFORMATICA

Firmado digitalmente por: CRUZ BERMUDEZ JUAN LUIS
Fecha: 2023.06.01 09:19

Fdo: Juan Luis Cruz Bermúdez