ANEXO VI. Cláusulas TIC del Pliego de Prescripciones Técnicas

Se describen las cláusulas que en materia de Tecnología de la Información y Comunicaciones deben de seguirse. Estás clausulas son de aplicación, si así fuera el caso, a los componentes hardware y software que acompañan, complementen o mejoren el objeto principal de la licitación. En este caso, donde dice durante la "vigencia del contrato" ha de entenderse durante el periodo de garantía.

1.1 Instalación

El adjudicatario deberá incluir todas las tareas necesarias de instalación, configuración y parametrización para su puesta en funcionamiento incluyendo el coste de todos los servicios necesarios. Se incluirá también un plan de despliegue detallado en el que se describan las actuaciones a realizar y los hitos previstos, indicando una estimación orientativa de los tiempos de implantación, con el detalle de un cronograma, pero sin fechas explícitas dado que no son conocidas.

1.2 Licencias

La oferta deberá incluir todas las licencias de sistema operativo de servidores, gestor de bases de datos y cualquier otro software necesario para el funcionamiento del sistema, cuyo coste correrá por cuenta de la empresa adjudicataria. El proveedor ha de suministrar las licencias de fabricante de todos los productos a instalar, quedando estas a disposición del centro, para lo cual deberán registrarse a nombre del Equipo Provincial TIC de Córdoba en el sistema de registro del fabricante. Las licencias de uso de la aplicación (si fueran necesarias) durante el tiempo de vigencia del contrato serán las necesarias en número para todos los usuarios potenciales del sistema. Además, todas las licencias de aplicación, de sistema operativo, de gestor de bases de datos, de servidor web, etc. serán las correspondientes a la última versión del fabricante y no se admitirán versiones obsoletas o que se encuentren en fin de ciclo de vida (EOL) en ningún caso. Para ello, deberá detallarse en la oferta cada una de las versiones a instalar. Durante toda la vigencia del contrato, todas las versiones de cualquier software deberán ser actualizadas para que en todo momento estén dentro del soporte oficial del fabricante de las mismas.

1.3 Hardware

Todo el hardware necesario (PCs, servidores, cabinas de almacenamiento) para la efectiva implantación del sistema, así como su instalación, deberá ser provisto por el adjudicatario. En caso de que el hardware

adicional necesario no viniese integrado en el dispositivo, deberá ser enrackable en armarios racks de 19" y deberá disponer de elementos redundantes (fuentes de alimentación, tarjetas de red, sistema RAID, etc.). La instalación de este hardware se realizará en el CPD provincial del Hospital de Montilla y Hospital de Puente Genil con criterios de alta disponibilidad y tolerancia a fallos.

En todo caso esta solución deberá consensuarse con la Subdirección de Tecnologías de la Información y Comunicaciones de Córdoba (en adelante **STIC-COR**).

1.4 Puesto Cliente

En su caso, la aplicación proporcionada por el adjudicatario (cliente pesado, cliente web o cualquier otro) debe ser funcional desde de los puestos cliente disponibles en los centros del SAS. Si fuese un entorno web, el cliente debería funcionar siempre bajo protocolo seguro https. En la oferta se detallarán las versiones soportadas de Windows, siendo obligatoria su compatibilidad, al menos, con Windows 10 en la última versión disponible en la fecha de presentación de ofertas, así como los navegadores con los que es compatible, que deben ser siempre versiones soportadas por el fabricante de dichos navegadores durante la vigencia del contrato.

1.5 Compatibilidad Software Corporativo

El sistema deberá ser compatible a nivel de servidor y cliente con el software corporativo de protección frente a código dañino y con el resto de software definido como corporativo por la STIC-COR. Asimismo, los puestos cliente estarán incluidos en el Directorio Activo Corporativo DMSAS (Active Directory de Windows). Esto también será un requisito obligatorio para los servidores. Las excepciones de permisos de análisis de carpetas/directorios deberán indicarse en la oferta. La autenticación de usuarios se debe de realizar mediante Directorio Activo (LDAP) corporativo (DMSAS) bajo el marco de Gestión de Identidades establecido por el SSPA. Además, debe permitir la gestión de usuarios (altas, bajas y modificaciones de perfiles) bajo el marco de Gestión de Identidades establecido por el SSPA. El adjudicatario podrá solicitar a la STIC-COR durante el período de presentación de ofertas la realización de una prueba de concepto en los equipos del SAS.

1.6 Plan de Trabajo

En la oferta se deberá incluir todas las tareas necesarias de instalación, configuración y parametrización para su puesta en funcionamiento, describiendo tanto las actuaciones a realizar como los hitos previstos,

indicando una estimación orientativa de los tiempos de implantación, con el detalle de un cronograma, pero sin fechas explícitas dado que no son conocidas.

Se incluirán así mismo, el plan de trabajo necesario para la realización de las integraciones propuestas.

1.7 Bastionado de equipos

Los equipos de usuario final (estaciones de trabajo) incluidos en el alcance del servicio deben adecuar su configuración de seguridad a las indicadas en todo momento por el SAS y la Agencia Digital de Andalucía, conforme a la normativa de seguridad aplicable. En particular:

- Todo equipo de usuario final será entregado siempre con su sistema operativo actualizado y en su versión profesional para empresas. Las actualizaciones serán gestionadas por la plataforma de gestión de activos del SAS, Altiris. La instalación del agente Altiris se realizará en su caso por el equipo TIC. Si se justifican problemas con estas actualizaciones, la persona adjudicataria estará obligada a realizar dichas actualizaciones de forma manual en los mantenimientos periódicos del equipo (no superior a 3 meses).
- Debe tener instalado el software para gestión de inventario de activos de TI, OCS. La instalación del agente OCS se realizará en su caso por el equipo TIC.
- Debe tener instaladas las herramientas para protección frente a código dañino:
    - Como EPP (Endpoint Protection Platform) y EDR (Endpoint Detection and Response), CrowdStrike, para detectar, investigar y resolver actividades sospechosas en el puesto. La instalación del EDR se realizará por el equipo TIC.
    - Como protección frente a código dañino de tipo ransomware, microCLAUDIA. La instalación del MICROCLAUDIA se realizará por el equipo TIC.
- Los equipos con sistema operativo Windows deben estar incluidos en dominio para la aplicación de las políticas propias del SAS. Si el servicio no es compatible, deben acreditar medidas compensatorias para restringir el acceso a los recursos compartidos.

- Siguiendo las buenas prácticas de configuración segura, no estaría permitido:
    - Emplear cuentas privilegiadas (con permiso de administrador) en la operativa diaria de los equipos de usuario final.
    - Usar software no autorizado por el SAS y sin licencia. Está expresamente prohibido el uso de software de control remoto y los accesos externos solo se pueden realizar a través de la VPN corporativa que tiene establecida el Servicio Andaluz de Salud.

- Cambios de proveedores de navegación.

Durante el uso y mantenimiento de la solución se mantienen las siguientes medidas de seguridad:

1. La instalación de la solución debe ser on-premise, con acceso exclusivamente desde la red interna del hospital.
2. El personal de soporte del adjudicatario accederá exclusivamente mediante VPN, preferentemente configurada sede a sede.
   Bajo ningún concepto se realizarán extracciones o exportaciones de datos a entornos locales o de desarrollo fuera de la red del hospital.

Para su securización, y en caso de ser requerido, se añadirán medidas compensatorias con Hardware de tipo Firewall gestionado, que en todo caso correrá por cuenta del adjudicatario. La solución que se proponga deberá ser consensuada con la STIC-COR a fin de que sea integrable en la plataforma ya existente para tal fin.

1.8 Integraciones

Las integraciones necesarias deberán ser pactadas entre el adjudicatario, el responsable del contrato y la STIC-COR, que como mínimo serán con el **directorio activo corporativo (DMSAS) y a previo requerimiento del responsable del contrato, RIS, HIS, PACS, y/o VNA.**

Si en algún momento el SAS, a través de su Oficina Técnica de Interoperabilidad, requiriera la modificación de algunas de las integraciones existentes, será obligación del adjudicatario, sin coste adicional, la realización de dichas modificaciones para que todo quede perfectamente integrado de nuevo. Dichas modificaciones siempre serán coordinadas por la STIC-COR.

Cualquier integración con otros sistemas de información corporativos del SAS que sea necesaria se realizará atendiendo a las directrices establecidas por la Oficina Técnica de Interoperabilidad de la Subdirección de Tecnologías de la Información y comunicaciones del Servicio Andaluz de Salud.

1.9 Esquema detallado de la instalación

Se incluirá un esquema detallado de la arquitectura hardware/software de los componentes que conforman la solución. En éste se añadirán como mínimo:

Servidores implantados (tipo y número), esquema funcional que detalle el funcionamiento de la aplicación en relación con la arquitectura hardware / software montada, licenciamiento solicitado para cada uno de ellos, conectividad de estos, uso y servicio de la infraestructura hardware, esquema lógico y físico detallado de toda la instalación, conectividad con el resto de aplicativos, resumen detallado de los procedimientos que ejecuta cada servidor y el motivo de su ejecución, etc.
Se proporcionará toda la documentación técnica necesaria del producto, así como los manuales de uso, con al menos 1 ejemplar escrito en español.

1.10 Mantenimiento

En el pliego de Prescripciones Técnicas se describe cómo ha de ser el mantenimiento correctivo, las incidencias, etc., en lo que respecta a las incidencias en general, estén o no relacionadas con el área TIC. Con respecto al software/hardware TIC, ha de atenderse, además, a lo indicado en este anexo.

Se detallará el enfoque y planteamiento global del servicio de mantenimiento y soporte del sistema de información en cuanto al alcance, a la organización del mismo, la metodología y herramientas de seguimiento. Se describirán tanto aspectos funcionales (capacidades del producto, apartados, módulos, estructura y arquitectura tecnológica, etc.) como organizativos del proceso de actualización (dependencias, funciones y perfiles), metodológicos (cronograma de incidencias y de evolución del producto, procedimientos, tareas, flujos, etc.); tanto operativos, como de gestión y de planificación de los servicios. Serán expresados con el máximo nivel de detalle y especificidad.

Las posibles nuevas versiones o revisiones del sistema de información que complemente (en su caso) al objeto de este contrato estarán a disposición del hospital en el plazo máximo de 6 meses desde su liberación.

Las actualizaciones deben garantizar la compatibilidad con versiones anteriores, y deberá respetarse cualquier personalización o parametrización a nivel de centro.

Cuando se produzca una modificación de versión, reléase, etc. que requiera la migración de los datos existentes en el sistema de información, todo el coste asociado será asumido por adjudicatario.

El adjudicatario, junto con el hospital, definirá un plan de contingencias para que, si algunas de las acciones a seguir provocaran un corte de servicio del sistema, se pueda dar continuidad y permitir la prestación de servicio.

1.10.1 Mantenimiento Preventivo

Se incluirá un plan detallado de mantenimientos preventivos de toda la configuración tanto del software de base como del software del sistema de información, en el que se detalle qué actuaciones se realizarán y con qué periodicidad.

1.10.1.1 Copias de Seguridad

Será responsabilidad del adjudicatario la definición, configuración, verificación periódica y validación de la correcta realización de las copias de seguridad del sistema de información objeto de este contrato, con todos sus módulos, así como la información clínica almacenada. Para ello, el hospital dispone de una infraestructura de back-up provincial que será en la que deba basarse el adjudicatario para las especificaciones mencionadas (definición, configuración, verificación y validación). El software corporativo utilizado para la realización de las copias de seguridad es veritas Netbackup. Así mismo, el adjudicatario deberá realizar la definición, configuración, verificación periódica y validación de las restauraciones periódicas para garantizar que las copias están disponibles por si fuera necesario restaurarlas en un futuro. Como mínimo se realizará una restauración cada seis meses. Será el hospital quien realice las copias diariamente (basándose en la definición hecha por el adjudicatario) y su traslado a ubicaciones remotas.

1.10.1.2 Rendimiento

La empresa adjudicataria atenderá a los requerimientos que los técnicos de la STIC-COR soliciten, para el mejor funcionamiento del SGBD, tales como distribución de almacenamientos, normas de indización, optimización de consultas, integraciones, etc.

En caso de detectarse un consumo excesivo de recursos hardware se procederá a su evaluación por el adjudicatario y en caso necesario se requerirá la evaluación y auditoría por expertos en el SGBD, la cual correrá por cuenta del adjudicatario.

1.10.2 Mantenimiento Evolutivo

Se detallará todas aquellas acciones encaminadas a la mejora y optimización del sistema, orientado a la de rendimiento y mejora técnica del producto. Se indicará la cadencia de implantación de nuevas versiones del producto, comunicando previamente al STIC-COR el alcance, viabilidad y requerimientos de la misma, indicando al tiempo, las mejoras que se incorporan.

Todo el sistema debe admitir, sin excepción alguna, las actualizaciones o parches críticos y de seguridad recomendados por el fabricante del sistema operativo, del gestor de bases de datos o del servidor web (en su caso). Dichas actualizaciones se ejecutarán a criterio de la STIC-COR en el horario más oportuno. Las actuaciones en este sentido serán coordinadas por la STIC-COR y se requerirá la posterior revisión del sistema por parte del adjudicatario que garantizará la compatibilidad con versiones anteriores. Esto aplica al sistema operativo de la parte servidora, al sistema de gestión de bases de datos, al servidor web o a cualquier otro elemento necesario para el funcionamiento del sistema. En todo caso, el adjudicatario deberá realizar, como mínimo, dos actualizaciones al año (parches, subidas de versión, etc.) de cualquier componente de la infraestructura. Para ello, se deberá suministrar a la STIC-COR un plan detallado de la actualización a realizar con la antelación suficiente (al menos con 15 días de antelación) en actualizaciones que se puedan prever, o con la máxima anticipación posible en caso de actualizaciones de urgencia.

Serán a cargo del adjudicatario las pruebas y posibles adaptaciones del software a cambios en versiones de puesto cliente promovidas por la Subdirección de Tecnologías de la Información y Comunicación del SAS (en adelante **STIC**).

1.10.3 Mantenimiento Correctivo. Definición del servicio de soporte

Se incluirán aquellos aspectos del proceso de comunicación de incidencias, de puesta en marcha de los grupos encargados de su tramitación, de su efectiva resolución, los mecanismos de envío y de instalación propuestos.

1.10.3.1 Soporte de primer nivel

El soporte de la aplicación, en primer nivel, será prestado por el adjudicatario y por los técnicos de la STIC-COR. Las competencias de los técnicos de la STIC-COR contemplan la primera atención al sistema, comprobando conectividad al mismo y al resto de las electrónicas y servicios del hospital, siendo el resto de las actividades competencia del adjudicatario.

1.10.3.2 Soporte de segundo nivel

Por parte del adjudicatario se prestará, en un segundo nivel de soporte, apoyo al primer nivel de soporte. Este segundo nivel se concretará fundamentalmente en los aspectos que a continuación se reseñan, pero que también contempla otras necesidades que durante la vigencia del contrato puedan surgir:

- Asistencia en el uso y operación diaria de la aplicación.
- Resolución de incidencias.

- Apoyo técnico en las tareas relacionadas con la instalación y la parametrización de la aplicación, tanto en servidor como en clientes.

1.11 Seguridad

Las proposiciones deberán garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información que constituyen el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad.

En concreto, se deberá asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que son objeto de la presente contratación.

Para lograr esto, se aplicarán las medidas de seguridad indicadas en el anexo II del ENS, en función de los tipos de activos presentes y las dimensiones de información relevantes, considerando las categorías de seguridad en las que recaen los sistemas de información objeto de la contratación según los criterios establecidos en el anexo I del ENS, como mínimo, las medidas establecidas para sistemas de categoría básica.

Deberá también tenerse en cuenta lo dispuesto en el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (modificado por el Decreto 70/2017, de 6 de junio) y en su desarrollo a partir de la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y normativa asociada.

La empresa adjudicataria deberá tener en cuenta lo dispuesto en la Resolución de 8 de abril de 2021, de la Dirección Gerencia del Servicio Andaluz de Salud, por la que se aprueba la Política de Seguridad de las Tecnologías de la información y la comunicación (TIC) del Servicio Andaluz de Salud, así como las guías y procedimientos aplicables elaborados por la Unidad de Seguridad TIC Corporativa de la Junta de Andalucía y la Unidad de Seguridad TIC del Servicio Andaluz de Salud.

Además, deberá atender a las mejores prácticas sobre seguridad recogidas en las series de documentos CCN-STIC (Centro Criptológico Nacional - Seguridad de las Tecnologías de Información y Comunicaciones), disponibles en la web del CERT del Centro Criptológico Nacional (http://www.ccn-cert.cni.es/).

Para todas las tareas de montaje, instalación y puesta en marcha que estén relacionadas con la integración/interoperabilidad de sistemas de información, ciberseguridad, conectividad a la red telemática y/o cualquier otra actuación relacionada con las TIC, se deberán seguir las indicaciones del equipo TIC del centro, así como la unidad de Seguridad TIC.

La empresa adjudicataria deberá colaborar con el SAS en el cumplimiento de sus obligaciones en materia de (i) medidas de seguridad, (ii) comunicación y/o notificación de brechas (logradas e intentadas) de medidas de seguridad a las autoridades competentes o los interesados, y si corresponde, (iii) colaborar en la realización de evaluaciones de impacto relativas a la protección de datos personales y consultas previas al respecto a las autoridades competentes, teniendo en cuenta la naturaleza del tratamiento y la información de la que disponga. Para ello, comunicará previamente los datos de contacto en el ámbito TIC del responsable del sistema y el responsable de seguridad, y si procede, delegado de protección de datos.

Asimismo, pondrá a disposición del SAS, a requerimiento de éste, toda la información necesaria para demostrar el cumplimiento de las obligaciones previstas en el contrato y colaborará en la realización de auditorías e inspecciones llevadas a cabo, en su caso, por el SAS.

Respecto a la cadena de subcontrataciones con terceros, en su caso, la empresa adjudicataria principal lo pondrá en conocimiento previo del SAS para recabar su autorización y estarán sujetos a las mismas obligaciones impuestas para esta en materia de seguridad, confidencialidad y protección de datos.

En el contrato se debe establecer los procedimientos de coordinación en caso de incidentes de seguridad o de continuidad (desastres).

La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5 de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en el ENS.

1.12 Datos “in-situ”

En ningún caso se aceptará la existencia de datos de carácter personal en la nube, sin autorización expresa de la STIC-COR.

1.13 Metodología y Calidad

Existe un documento de Estándares y Normativa de Desarrollo, que el proveedor deberá conocer y aplicar en su medida. Se encuentran definidos en Confluence, en la siguiente dirección Web:

https://ws001.sspa.juntadeandalucia.es/confluence/display/NORMATIVATIC/Normativa+TIC

Además, serán a cargo del adjudicatario las pruebas y posibles adaptaciones del software a cambios en versiones de puesto cliente promovidas por la STIC.