ANEXO Cláusulas TIC del Pliego de Prescripciones Técnicas

Contenido

1 Objeto

Se describen las cláusulas que en materia de Tecnología de la Información y Comunicaciones deben de seguirse. Estás clausulas son de aplicación a los componentes hardware y/o software que acompañan, complementen o mejoren el objeto principal de la licitación.

1.1 Plan de Trabajo

En la oferta se deberán incluir todas las tareas necesarias de instalación, configuración, parametrización y despliegue para su puesta en funcionamiento, describiendo tanto las actuaciones a realizar como los hitos previstos, teniendo en cuenta que el coste de todos los servicios necesarios será por cuenta del adjudicatario. Se incluirá un cronograma que recoja una estimación orientativa de los tiempos de implantación de los hitos previstos.

Se incluirán así mismo, el plan de trabajo necesario para la realización de las integraciones propuestas (si fuera el caso).

1.2 Licencias

La oferta deberá incluir todas las licencias necesarias para el funcionamiento del sistema, incluyendo las de sistema operativo de servidores, gestor de bases de datos y cualquier otro software requerido, cuyo coste correrá por cuenta de la empresa adjudicataria.

El proveedor deberá suministrar licencias oficiales del fabricante para todos los productos a instalar, que quedarán a disposición del centro y registradas a nombre del Equipo Provincial TIC de Córdoba en el sistema de registro del fabricante correspondiente.

Las licencias de uso de las aplicaciones (si fueran necesarias) deberán contemplar un número suficiente para cubrir todos los usuarios potenciales del sistema durante la vigencia del contrato.

En ningún caso se admitirán sistemas operativos, gestores de bases de datos, servidores web o cualquier otro software que se encuentre en fin de ciclo de vida (EOL end of life), ya sea software de pago o freeware. Todas las licencias deberán corresponder a la última versión soportada por el fabricante, especificándose detalladamente en la oferta las versiones exactas de cada componente a instalar.

El adjudicatario se compromete a mantener todas las versiones del software (sistema operativo, sistema de gestión de base de datos, software propio, etc.) actualizadas y dentro del soporte oficial

del fabricante, durante toda la vigencia del contrato, garantizando en todo momento la ausencia de versiones obsoletas o en EOL.

1.3 Hardware

Todo el hardware necesario (PCs, servidores, cabinas de almacenamiento, etc.) 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 preferentemente en el CPD provincial del Hospital Universitario Reina Sofía 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**).

En la oferta se detallará todo el hardware necesario.

1.4 Puesto de usuario

En su caso, el aplicativo proporcionado 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 y utilizando certificados SSL proporcionados por el SAS o por una entidad certificadora de confianza. En la oferta se detallarán las versiones soportadas de Windows, siendo obligatoria su compatibilidad, al menos, con Windows 11 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.

Los documentos que se generen desde la aplicación, el software de gestión, el sistema de información, etc., deben poder abrirse con Libre Office, al ser esta la herramienta de ofimática definida por el Servicio Andaluz de Salud. En caso de que no sea posible, y solo funcionase con Microsoft Office, el coste de estas licencias correrá a cargo del adjudicatario.

1.5 Compatibilidad

El sistema deberá ser compatible a nivel de servidor y cliente con el software definido como corporativo por la STIC-COR. El adjudicatario podrá solicitar a la STIC-COR durante el período de presentación de ofertas cuál es el software definido como corporativo y/o la realización de una prueba de concepto en los equipos del SAS.

1.6 Bastionado de equipos

Los equipos incluidos en el alcance del servicio (servidores, PCs, equipamiento electromédico, equipamiento industrial, etc.) deben adecuar su configuración de seguridad a las indicadas en todo momento por la Unidad de Seguridad TIC del SAS (en adelante USTIC) y la Agencia Digital de Andalucía, conforme a la normativa de seguridad aplicable en cada momento. En particular:

- Todos los equipos serán entregados siempre con su sistema operativo actualizado y en su versión profesional para empresas. Las actualizaciones serán gestionadas por la plataforma de gestión de activos establecida por el SAS para cada tipo de equipamiento. Este aspecto deberá ser consensuado con la STIC-COR. 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).
- Todos los equipos suministrados deben tener instalado el software para gestión de inventario de activos TI establecido por STIC-COR. La instalación del agente necesario se realizará en su caso por el equipo STIC-COR.
- Todos los equipos deben tener instaladas las herramientas para protección frente a código dañino:
    - EDR (Endpoint Detection and Response) para detectar, investigar y resolver actividades sospechosas en el puesto. La instalación del EDR se realizará por STIC-COR. Las excepciones de permisos de análisis de carpetas/directorios deberán indicarse en la oferta.
    - Como protección frente a código dañino de tipo ransomware, la herramienta indicada en cada momento por CCN-CERT o CERT-Andalucía. La instalación del agente se realizará por STIC-COR.
- Los equipos con sistema operativo Windows deben estar incluidos en el Directorio Activo Corporativo DMSAS 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 sólo se pueden realizar a través de la VPN corporativa que tiene establecida la Junta de Andalucía.
    - Utilizar proveedores de acceso a internet distintos de la Red Corporativa de la Junta de Andalucía (en adelante RCJA).

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

1. La instalación de la solución debe ser preferentemente on-premise en un CPD ubicado dentro de la RCJA. En todo caso, se requiere autorización expresa de la USTIC previa realización de un Análisis de Riesgos y de una Evaluación de Impacto en la seguridad de la información.
2. El personal de soporte del adjudicatario accederá exclusivamente mediante VPN, preferentemente configurada sede a sede. Después de cada conexión que realice, deberá emitir un informe y dirigirlo a la STIC-COR indicando el momento de la conexión, el motivo y las acciones realizadas. Bajo ningún concepto se realizarán extracciones o exportaciones de datos a entornos locales o de desarrollo fuera de RCJA.

1.7 Integraciones

Las integraciones necesarias, tanto para el funcionamiento del sistema como las expresamente exigidas por STIC-COR, estarán incluidas dentro del proyecto y todo el coste asociado (desarrollos, plataformas de integración, etc.) será asumido por el adjudicatario.

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

Cualquier integración 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 o por la STIC-COR.

1.8 Esquema detallado de la instalación

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

- Equipos necesarios para dar servicio (tipo y número).
- Esquema lógico que detalle el funcionamiento de la aplicación en relación con la arquitectura hardware / software montada.
- Esquema físico y lógico detallado incluyendo la conectividad entre equipos y entre aplicativos.
- Licenciamiento necesario.
- Resumen detallado de los procedimientos que ejecuta cada equipo 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.

1.9 Documentación a entregar a la finalización de la implantación

Una vez finalizada la implantación del Sistema, el adjudicatario deberá rellenar dos documentos que han sido definido por la STIC-COR:

1.- Plantilla del Proyecto, que contiene los siguientes epígrafes:

- Descripción del proyecto: descripción completa de la arquitectura física y lógica del sistema. Distintos componentes del sistema. Funcionalidades del sistema con detalle. Áreas funcionales a las que presta servicio. Diagramas, gráficos y toda la documentación estimada para definir de manera completa el proyecto.
- Contactos: lista completa de contactos asociados al proyecto. Contactos funcionales, contactos técnicos, contactos comerciales, etc. En caso de que durante la vigencia del contrato cambie alguno de estos contactos, se deberá notificar a STIC-COR a la mayor brevedad posible.
- Hardware / Equipamiento. Se solicita el detalle de todo el equipamiento instalado en el proyecto, incluyendo servidores, PCs, máquinas virtuales, etc. Para ello STIC-COR ofrecerá una plantilla que deberá ser rellenada para cada dispositivo.
- VPN: información de las VPNs asociadas al proyecto. Si la empresa dispone de VPNs de RCJA personales o Sede a Sede con las que ofrecerá el servicio, deberá aportar la información detallada sobre ellas (usuarios, IPs, etc.).
- Acceso a las aplicaciones cliente: apartado específico para recoger toda la documentación relativa al acceso de los usuarios. Descripción de aplicaciones (web, cliente pesado, etc.), formas de acceso, url, rutas de acceso, rutas del software, manuales de usuario, manuales de instalación, etc.
- Gestión de identidad: descripción de la gestión de la identidad del proyecto. ¿Utiliza DMSAS? ¿Grupos de usuarios DMSAS? ¿Utiliza IDENTIC? ¿Cuál es el flujo de gestión de altas/modificaciones/bajas de usuarios? Definición de responsabilidades de gestión de usuarios.
- Integraciones funcionales: detallar las integraciones que tiene el sistema con otros sistemas. Demográficos, informes, departamentales (MPA, Farmacia, etc). Descripción de la solución técnica del motor de integración.
- Soporte: detalle del soporte asociado al proyecto. Datos de contacto de soporte, horarios, acuerdos de nivel de servicio contratados, garantía del equipamiento dotado, etc.

- Documentación Adicional: toda la documentación adicional que se estime que pueda ser de interés para el conocimiento de la instalación (planos, manuales, documentación oficial del sistema, certificados, etc.).
  A modo de ejemplo se incluye el “DocumentoAnexo-I-PPT Plantilla del Proyecto”.

2.- Backups: toda la información necesaria sobre las copias de seguridad (detalle del procedimiento de copias de seguridad necesaria. Definición de responsabilidades. Restauraciones periódicas.)
A modo de ejemplo se incluye el “DocumentoAnexo-II Backups”
3.- Documentación Adicional: toda la documentación adicional que se estime que pueda ser de interés para el conocimiento de la instalación.

Estos documentos, completados por el adjudicatario, serán definitivos una vez que STIC-COR los haya validado, después de las revisiones que hayan sido necesarias.

1.10 Mantenimiento

Con independencia de lo que se establezca en el Pliego de Prescripciones Técnicas respecto al mantenimiento del objeto del contrato, para todo aquello que esté relacionado con soluciones del área TIC ofertadas por el adjudicatario (hardware, software, etc.), este ha de atenerse, además, a lo indicado en este anexo.

En la oferta, se indicará:

- Detalle del enfoque y planteamiento global del servicio de mantenimiento y soporte en cuanto al alcance, a la organización del mismo, la metodología y herramientas de seguimiento.
- Un plan de contingencias que tendrá que ser validado por la STIC-COR 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.

En caso de que lo ofertado por el adjudicatario sea un sistema de información, las nuevas versiones o revisiones del sistema de información 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 que se haya hecho a nivel de centro.

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

Cualquier intervención que requiera un corte de servicio, deberá realizarse en un horario pactado entre el adjudicatario y STIC-COR para que el impacto en el servicio sea mínimo.

1.10.1 Mantenimiento Preventivo

En la oferta se incluirá un plan detallado de mantenimientos preventivos de toda la configuración, tanto del hardware, como del software de base, software del sistema de información, etc. en el que se detalle qué actuaciones se realizarán y con qué periodicidad. A la finalización de cada actuación realizada, el adjudicatario deberá emitir un informe para la STIC-COR detallando todo lo realizado y su resultado.

La empresa adjudicataria tendrá siempre una visión proactiva para tratar de anticiparse a una eventual degradación progresiva del servicio, en cuyo caso, atenderá a los requerimientos que los técnicos de la STIC-COR soliciten.

1.10.2 Mantenimiento Evolutivo

En la oferta se detallarán todas aquellas acciones encaminadas a la mejora funcional y/o técnica y optimización del sistema. Se indicará la cadencia de implantación de nuevas versiones del producto, comunicando previamente a la STIC-COR el alcance, viabilidad y requerimientos de la misma, indicando, además, 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 desplegar las actualizaciones disponibles en el plazo máximo de un año (parches, subidas de versión, etc.) desde su liberación, para 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 STIC o STIC-COR.

1.10.3 Mantenimiento Correctivo. Definición del servicio de soporte

Las modalidades de soporte ofertadas serán las siguientes:

- Soporte telefónico
- Soporte por correo electrónico
- Soporte a través de control remoto / conexión remota, para lo que se habilitará un acceso remoto a la aplicación mediante VPN
- Soporte presencial

Los tiempos de respuesta, resolución y el tiempo máximo de indisponibilidad del servicio serán los definidos en los Acuerdos de Nivel de Servicio (en adelante ANS) establecidos en el apartado “Acuerdos de Nivel de Servicio”.

En la oferta deberá incluirse detalle del procedimiento de soporte que se proponga (horario y procedimiento de gestión de incidencias), durante la vigencia del contrato. Dicho procedimiento debe integrarse en el Centro de Gestión de Servicios TIC del SAS (en adelante **Ayuda Digital**), si así fuera requerido por la STIC-COR, en cuyo caso, el adjudicatario deberá utilizar la Web Técnica de Ayuda Digital para la atención y seguimiento de incidencias como resolutores. A través de ella recibirá incidencias directas de los usuarios o escalados por parte de los técnicos de la STIC-COR o por técnicos de Ayuda Digital.

El detalle de los servicios de integración con las herramientas de gestión TIC del SAS, sus actualizaciones y procedimientos, se encuentran disponibles en:

https://ws001.sspa.juntadeandalucia.es/confluence/display/SERVCGESP/API+REST+Servicios+CGES.

Escalados de incidencias

Una vez adjudicado el contrato, se pactará la matriz de escalados de incidencias entre el adjudicatario y la STIC-COR.

1.11 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 backup 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. Además, el adjudicatario deberá proveer la ampliación hardware necesaria en dicha infraestructura, de forma que sea suficiente para albergar todas las copias de seguridad durante la vigencia del contrato. Dicha ampliación deberá ser dimensionada y consensuada con la STIC-COR. 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 ejecute la realización de las copias diariamente (basándose en la definición hecha por el adjudicatario) y su traslado a ubicaciones remotas.

1.12 Datos “in-situ”

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

1.13 Metodología y Calidad

En relación con el desarrollo de software, existe un documento de Estándares y Normativa de Desarrollo, que el proveedor deberá conocer y aplicar en su medida en el caso de que lo ofertado sea un desarrollo de software. 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-COR.

1.14 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.

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.

1.15 Tratamiento de datos de carácter personal

De acuerdo con lo establecido en el artículo 32 del 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) en adelante RGPD, la figura del responsable del tratamiento, que recae en el Director Gerente del Servicio Andaluz de Salud (en adelante SAS), representado por cada Dirección Gerencia de los centros, realizará la evaluación de riesgos que determinen las medidas apropiadas para garantizar la seguridad de la información y los derechos de las personas usuarias. Asimismo, y como se detalla en el acuerdo correspondiente, el encargado del tratamiento, representado por la persona contratista, también evaluará los posibles riesgos derivados del tratamiento, teniendo en cuenta los medios utilizados (tecnologías de acceso, recursos utilizados, etc.) y cualquier otra contingencia que pueda incidir en la seguridad. La determinación de las medidas de seguridad que deben ser aplicadas por la persona contratista podrá realizarse mediante la remisión de toda la información a la plataforma Confluence corporativa de la STIC, donde se albergan las medidas de seguridad de tratamiento de información de ámbito general o para escenarios de tratamiento o cesión de información específicos. Como mínimo, se incorporarán las medidas establecidas en Real Decreto 311/2022, de 3 de mayo,

por el que se regula el Esquema Nacional de Seguridad, en adelante ENS, conforme a la categoría del sistema y la declaración de aplicabilidad.

El encargado del tratamiento, junto con el responsable del tratamiento, establecerán las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad según lo identificado en la Evaluación de Riesgos que, en su caso, incluirán, entre otros:

1. a) La anonimización y el cifrado de datos personales;

2. b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

3. c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico;

4. d) Un proceso de verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

El encargado del tratamiento asistirá al responsable del tratamiento para que éste pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III del RGPD. Se incluirán las funcionalidades necesarias que permitan atender los derechos de los titulares de los datos: acceso, rectificación, supresión, oposición, portabilidad, limitación y decisiones automatizadas.

El encargado del tratamiento pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En caso de violación de la seguridad de los datos personales, el encargado del tratamiento notificará sin dilación indebida y en un plazo máximo de 24 horas al responsable del tratamiento, las violaciones de la seguridad de los datos personales de las que tenga conocimiento. La notificación de las violaciones de la seguridad de los datos se realizará obligatoriamente mediante correo electrónico a los buzones del Delegado de Protección de Datos (DPD) y a la Unidad de Seguridad TIC (USTIC), junto con una comunicación al Centro de Gestión de Servicios TIC (Ayuda Digital) del SAS a través de sus canales.

Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, incluyendo:

1. Procedimiento de reporte de incidentes reales o sospechosos, detallando el escalado de la notificación.
2. Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.
3. Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.
4. Procedimientos para informar a las partes interesadas, internas y externas.
5. Procedimientos para:
    a. Prevenir que se repita el incidente.
    b. Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.
    c. Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidencias.

La gestión de incidentes que afecten a datos de carácter personal tendrá en cuenta lo dispuesto en el Reglamento Europeo de Protección de Datos (RGPD), en lo que corresponda.

1.16 Interoperabilidad

Las ofertas garantizarán un adecuado nivel de interoperabilidad técnica, semántica y organizativa, conforme a las estipulaciones del Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (ENI). En concreto, se cumplirán las Normas Técnicas de Interoperabilidad establecidas por dicho esquema. Se cuidarán especialmente los aspectos de interoperabilidad orientados a la ciudadanía, de tal forma que se evite la discriminación a los ciudadanos por razón de sus elecciones tecnológicas. El sistema implantará los protocolos ENIDOCWS y ENIEXPWS para que los documentos y expedientes electrónicos que se gestionen en el mismo puedan, a partir de sus códigos seguros de verificación, ser puestos a disposición e interoperar de manera estandarizada con otros sistemas y repositorios electrónicos de la Junta de Andalucía, así como remitirse a otras Administraciones si procede.

También se atenderá a los modelos de datos sectoriales relativos a materias sujetas a intercambio e información con la ciudadanía, otras Administraciones Públicas y entidades, publicados en el Centro de Interoperabilidad Semántica de la Administración (CISE) que resulten de aplicación.

Además, y en virtud del artículo 11.2 del RD 4/2010 por el que se establece el ENI, se hará uso de los siguientes formatos no incluidos en el catálogo de estándares del ENI para dar cobertura, en caso de que aplique, a funcionalidades y aplicaciones de ámbito sanitario:

- ISO/HL7 27931 – HL7 v2.x – FHIR DSTU2 – FHIR STU3
- ISO 12052 – DICOM, para el caso de imagen electrónica

La aplicación que se desarrolle/provea deberá integrarse con los sistemas de información corporativos siguiendo las pautas, normas y procedimientos definidos por la Oficina Técnica de Interoperabilidad del SAS, que actuará de asesor y coordinador de los diferentes circuitos a definir para que se pueda verificar la corrección de los flujos de información, accesibles a través de la página correspondiente del portal Confluence del SAS:
https://ws001.sspa.juntadeandalucia.es/confluence/display/normativaTIC , apartado A).

Este portal recoge toda la regulación en cuanto a normas y procedimientos de trabajo que ha identificado la STIC como imprescindibles para el aseguramiento de la calidad de los servicios de intercambio de información prestado a sus clientes, así como de calidad de la semántica corporativa necesaria para mantener la coherencia de los procesos.

Se cuidarán especialmente los aspectos de interoperabilidad orientados a la ciudadanía, de tal forma que se evite la discriminación a los ciudadanos por razón de sus elecciones tecnológicas. También se atenderá a los modelos de datos sectoriales relativos a materias sujetas a intercambio de información con la ciudadanía, otras Administraciones Públicas y entidades, publicados en el Centro de Interoperabilidad Semántica de la Administración (CISE) que resulten de aplicación.

Para la práctica de la verificación, mediante un código generado electrónicamente, de documentos firmados electrónicamente en la Administración de la Junta de Andalucía, para el contraste de su autenticidad y la comprobación de su integridad, en el marco de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. y su normativa de desarrollo, y el apartado VIII (Acceso a documentos electrónicos) de la Norma Técnica de Interoperabilidad de Documento Electrónico, se utilizará la Herramienta Centralizada de Verificación, de acuerdo con el protocolo técnico disponible en el apartado correspondiente de la web de soporte de administración electrónica de la Junta de Andalucía.

1.17 Uso de certificados y firma electrónica

Para la identificación y firma electrónica mediante certificados electrónicos se atenderán las guías y directrices indicadas en el apartado correspondiente a la plataforma @firma en la web de soporte de administración electrónica de la Junta de Andalucía, en particular en lo relativo a la no utilización de servicios y componentes obsoletos, de custodia de documentos en la plataforma o cuya desaparición esté prevista para futuras versiones, a formatos de firma electrónica y la realización de firmas electrónicas diferenciadas y verificables para cada documento, realizándose en su caso las

oportunas actuaciones de adecuación de las funcionalidades actualmente existentes en los sistemas incorporados en el objeto de la contratación. La citada web está accesible en la siguiente dirección: http://www.juntadeandalucia.es/haciendayadministracionpublica/ae

Se utilizarán los servicios provistos por la implantación corporativa de la plataforma @firma gestionada por la Consejería competente en materia de administración electrónica.

1.18 Práctica de la verificación de documentos firmados electrónicamente

Para la práctica de la verificación, mediante un código generado electrónicamente, de documentos firmados electrónicamente en la Administración de la Junta de Andalucía, para el contraste de su autenticidad y la comprobación de su integridad, en el marco del artículo 27.3.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, el artículo 42.b) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y el apartado VIII (Acceso a documentos electrónicos) de la Norma Técnica de Interoperabilidad de Documento Electrónico, se utilizará la Herramienta Centralizada de Verificación, de acuerdo con el protocolo técnico disponible en el apartado correspondiente de la web de soporte de administración electrónica de la Junta de Andalucía..

1.19 Gestión de usuarios y control de accesos

En todo lo relativo a la implementación de la funcionalidad de gestión de usuarios y control de accesos del sistema de información a desarrollar, se tendrán en cuenta las estipulaciones que sobre seguridad hace la legislación vigente en materia de tratamiento de datos personales, 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) así como de la legislación nacional vigente en materia de protección de datos y el Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad. En particular, se perseguirá:

- la correcta identificación de los usuarios (medida op.acc.1 del anexo II del ENS).
- la adecuada gestión de derechos de acceso (medida op.acc.4).
- la correcta selección e implantación de los mecanismos de autenticación (medida op.acc.5 y op.acc.6).

En relación con las directrices corporativas que se creen en materia de gestión de identidades:

En todo lo relativo a la implementación de la funcionalidad de gestión de usuarios y control de accesos del sistema de información a desarrollar (roles, gestión de login y password...) se deberán respetar las directrices que la Junta de Andalucía elabore en lo referente a la gestión de identidades y en su caso, adaptándose a la solución de single sign-on que la Junta haya provisto. Dichas Directrices se proporcionarán con la suficiente antelación, aportando la documentación técnica existente para tal fin.

En concreto, la autenticación de usuarios y gestión de permisos se debe de realizar mediante el Directorio Activo Corporativo (DMSAS) bajo el marco de Gestión de Identidades (IDENTIC) establecido por el Sistema Sanitario Público de Andalucía (en adelante **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.

1.20 Desarrollo web: accesibilidad

Todos los sitios webs y aplicaciones para dispositivos móviles desarrollados o que sean mejorados de manera significativa en el marco del presente contrato deberán ser accesibles para sus personas usuarias y, en particular, para las personas mayores y personas con discapacidad, de modo que sus contenidos sean perceptibles, operables, comprensibles y robustos. La accesibilidad se tendrá presente de forma integral en el proceso de diseño, gestión, mantenimiento y actualización de contenidos de los sitios web y las aplicaciones para dispositivos móviles.

En este ámbito se deberán cumplir lo establecido por el Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público. En particular, se deberán cumplir los requisitos pertinentes de la norma UNE-EN 301-549:2019, de Requisitos de accesibilidad de productos y servicios TIC, o de las actualizaciones de dicha norma, así como de las normas armonizadas y especificaciones técnicas en la materia que se publiquen en el Diario Oficial de la Unión Europea y/o hayan sido adoptadas mediante actos de ejecución de la Comisión Europea.

Por último, como obliga la normativa se deberá realizar al menos una revisión anual de la accesibilidad de los sitios web y sistemas desarrollados o mejorados de manera significativa en el marco del contrato, así como actualizar y en su caso, elaborar, la correspondiente Declaración de accesibilidad de conformidad con el modelo europeo establecido Decisión de Ejecución (UE)

2018/1523 de la Comisión de 11 de octubre de 2018 por la que se establece un modelo de declaración de accesibilidad de conformidad con la Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público.

1.21 NWT: Nueva Web Técnica

Es la herramienta del SAS destinada a la gestión de solicitudes, incidencias, peticiones, problemas y configuración, los cuales se registrarán en este sistema informático, y se utilizarán como prueba documental para valorar el grado de cumplimiento del contrato.

La persona adjudicataria deberá conectarse a este sistema para la recepción de todos los avisos de solicitudes, corriendo por cuenta de la persona adjudicataria la dotación de los medios técnicos necesarios para su integración en el citado sistema.

El registro de incidencias y sus datos son confidenciales. La persona adjudicataria no divulgará su contenido a terceros sin la aprobación expresa del SAS.

El detalle del manual de la puede consultarse en

https://ws001.sspa.juntadeandalucia.es/confluence/pages/viewpage.action?pageId=26935915.

1.22 MTI-SSHH

Es la herramienta del SAS que representa la única fuente de información válida para el análisis de datos y para el cálculo de los ANS del contrato, así como para la comprobación de su cumplimiento.

Los ANS estarán disponibles y habrá un periodo en el que se actualicen en función de los datos que arrojen las herramientas operacionales que son fuentes para su cálculo. Llegado el día 10 del mes siguiente al del periodo de prestación del servicio, salvo que la STIC estime otra cosa, se cerrarán los procesos de cálculo de los ANS.

1.23 Protección puesto de trabajo y distribución de software

El adjudicatario deberá adaptarse en todo momento a los procedimientos de resolución remota del SAS, entre los que cabe destacar, sin ser exhaustivos:

- Gestión de inventario, de la configuración y de activos.
- Administración y despliegue de software.
- Ejecución de las políticas de actualización de parches establecidas.

- Gestión y despliegue de imágenes y maquetas definidas para cualquier elemento de la configuración.
- Control remoto de los equipos de puesto de trabajo digital.
- Ejecución de las políticas de protección y eliminación de malware.

Para ello, la persona adjudicataria deberá usar las herramientas corporativas del SAS: Crowdstrike, Altiris, etc. para las cuales su personal estará convenientemente capacitado.

1.24 Extracción de información

El adjudicatario deberá proporcionar los mecanismos necesarios (réplica de la base de datos, usuarios de sólo lectura, creación de vistas, etc.), así como, la información y formación necesaria para que el equipo de la STIC-COR pueda explotar las bases de datos del sistema de información, para la elaboración de cuadro de mandos de seguimiento que demande la Dirección del Hospital. En este sentido, si el adjudicatario no proporciona información/formación del modelo de datos del sistema de información deberá proporcionar las vistas de la base de datos necesarias para las explotaciones de información que sean necesarias durante la vigencia del contrato. La creación y documentación, del tipo de cada uno de los campos o columnas de la vista, tendrá la calificación de una solicitud con prioridad normal en los acuerdos de nivel de servicio.

1.25 Formación Personal TIC

Se deberá incluir en la oferta un plan de formación y transferencia de conocimiento para el personal técnico de la STIC-COR, con el objetivo de conocer en detalle la solución ofertada (arquitectura hardware/software, modelo de explotación de información, etc.). Se deberá consensuar este plan de formación con la STIC-COR antes de su ejecución.

No obstante, lo anterior, si el personal técnico de la STIC-COR necesitara alguna formación adicional durante la vigencia del contrato, el adjudicatario deberá impartirla, previo acuerdo con la STIC-COR, sin coste adicional.

1.26 Desinstalación del equipamiento TIC

A la finalización del contrato, y una vez que la STIC-COR determine que el sistema puede ser retirado, todo el equipamiento TIC (software, hardware, etc.) aportado por el proveedor será retirado por este, corriendo por su cuenta la desinstalación, el desmontaje, la retirada del cableado y desconexión de la red informática, la retirada y reciclaje de los residuos y elementos no utilizables que el desmontaje origine, su transporte, etc. Asimismo, será obligación del contratista la eliminación

de cualquier dato que haya podido quedar almacenado en los equipos y elementos auxiliares de estos. Ninguna actuación debe ser realizada (apagado del sistema de información, retirada de hardware/software, etc.) sin un documento de autorización expresa emitido y firmado por la STIC-COR.

1.27 Exportación de datos y transferencia de conocimiento.

En el caso de la finalización del contrato y de no continuidad del adjudicatorio, este deberá hacer una exportación (sin coste adicional) de toda la información almacenada en su sistema a fin de que STIC-COR pueda utilizarla para incorporarla en un nuevo sistema de información (migración de datos) o para consulta de histórico. **Dicha exportación deberá cumplir con el formato establecido por STIC-COR.**

En caso necesario, el adjudicatario deberá proporcionar una transferencia de conocimiento sobre la exportación realizada.

1.28 Electrónica de red.

Si el número de puertos de comunicaciones necesarios implica la ocupación de 20 puertos o más en los switches, se exigirá al adjudicatario la provisión de la electrónica de red necesaria para cubrir las necesidades de conectividad.

Por estandarización, compatibilidad de los equipos existentes y aprovechamiento de espacio en los RACK disponibles, antes de que el adjudicatario adquiera los switches y sus componentes adicionales (transceivers, latiguillos, cables de stacking, etc.), sus características deberán ser consensuadas con la STIC-COR.

1.29 Acuerdos de Nivel de Servicio

Si la STIC-COR, en función de la naturaleza del contrato, así lo estimara, podrá exigir el cumplimiento de los ANS que se definen en este apartado, como medio para garantizar la calidad del funcionamiento del sistema de información. La definición de estos ANS podrá redefinirse (siempre a un nivel de exigencia menor) a lo largo de la ejecución del contrato con el fin de conseguir una mejora continua en la calidad del servicio efectivamente proporcionado. Todos los recursos disponibles para el servicio deberán ser organizados para garantizar los ANS vigentes en cada momento.

Los ANS se basan en la definición de unos indicadores de calidad que reflejan de forma objetiva la calidad del servicio TIC real proporcionado, con especial atención a los aspectos más críticos del mismo, y en el establecimiento de un umbral o valor mínimo de calidad para cada uno de ellos.

El concepto de incidencia, prioridad en la clasificación de incidencias, intervención, tiempo de respuesta, etc., y los procesos que guían su gestión, se encuentran definidos en Confluence, en la siguiente dirección Web:

https://ws001.sspa.juntadeandalucia.es/confluence/pages/viewpage.action?pageId=10388046

Condiciones de medida

En el cálculo de los indicadores se tendrán en cuenta dos decimales y no se contabilizarán las demoras que estén completa y exclusivamente en el ámbito de las responsabilidades de terceros (otros proveedores externos, el propio SAS, etc.), ni se contabilizarán las pérdidas de servicio debidas a causa de fuerza mayor (incendios, inundaciones, etc.).

Los indicadores que se utilizarán en el presente contrato son los siguientes:

INDICADOR	DEFINICIÓN	UNIDAD	OBJETIVO
Porcentaje de solicitudes resueltas en plazo Según la tipología, impacto, urgencia y **características** de la solicitud, se establece una prioridad a la misma. Se calcularán los siguientes indicadores según la prioridad asignada, del total de solicitudes resueltas en plazo entre todas las solicitudes resueltas por el proveedor para la misma prioridad.			
I0_01	**Porcentaje de solicitudes resueltas en plazo, con prioridad muy alta:** el tiempo máximo de resolución será de 4 horas hábiles de servicio desde la asignación de la solicitud.	Porcentaje	IO_01 >= 90%
I0_02	**Porcentaje de solicitudes resueltas en plazo, con prioridad alta:** el tiempo máximo de resolución será de 12 horas hábiles de servicio desde la asignación de la solicitud.	Porcentaje	IO_02 >= 80%

I0_03	**Porcentaje de solicitudes resueltas en plazo, con prioridad normal:** el tiempo máximo de resolución será de 30 horas hábiles de servicio desde la asignación de la solicitud.	Porcentaje	IO_03 >= 70%
Tiempo medio de resolución de solicitudes Según la tipología, impacto, urgencia y características de la solicitud, se establece una prioridad a la misma. Se calculará el tiempo medio de solicitudes para la misma prioridad que ha resuelto el adjudicatario en el periodo.			
IO_04	**Tiempo medio de resolución de solicitudes, con prioridad muy alta**	Horas hábiles	IO_04 <= 4
IO_05	**Tiempo medio de resolución de solicitudes, con prioridad alta**	Horas hábiles	IO_05 <= 12
IO_06	**Tiempo medio de resolución de solicitudes, con prioridad normal**	Horas hábiles	IO_06 <= 30
IO_07	**Porcentaje de solicitudes asignadas al adjudicatario con incumplimiento en el plazo de resolución que son reclamadas** Porcentaje de solicitudes asignadas al adjudicatario que, con incumplimiento en el plazo de resolución según su prioridad, son reclamadas respecto del total de solicitudes asignadas al adjudicatario.	Porcentaje	IO_07 <= 1%
IO_08	**Porcentaje de solicitudes resueltas por el adjudicatario que son reabiertas** Porcentaje de solicitudes resueltas por el adjudicatario que son reabiertas respecto del total de solicitudes resueltas por el adjudicatario. Se entiende resuelta por el adjudicatario aquella solicitud en la que es el propio adjudicatario el que hace la propuesta de cierre de la solicitud.	Porcentaje	IO_08 <= 1%
IO_09	**Número de problemas abiertos** Hace referencia al número de problemas que tiene asignado el adjudicatario en estado “Abierta” en un momento	Problemas	IO_09 <=10

IO_10	**Tiempo medio de resolución de problemas**	días	IO_10<=20

1.30 Conformidad con los marcos metodológicos de desarrollo de software de la Junta de Andalucía

Durante la realización de los trabajos se tendrán en cuenta los recursos proporcionados por los marcos metodológicos vigentes de desarrollo de software en la Junta de Andalucía, así como las pautas y procedimientos definidos en éstos.

1.31 Propiedad intelectual del resultado de los trabajos

Todos los estudios y documentos, así como los productos y subproductos elaborados por el contratista como consecuencia de la ejecución del presente contrato serán propiedad del Servicio Andaluz de Salud, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello la persona adjudicataria autor material de los trabajos. La persona adjudicataria renunciará 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 Servicio Andaluz de Salud, específicamente todos los derechos de explotación y titularidad de las aplicaciones informáticas y programas de ordenador desarrollados al amparo de esta contratación, corresponden únicamente al Servicio Andaluz de Salud.

La presente cláusula no será de aplicación a los productos y herramientas preexistentes empleados para la ejecución del contrato protegidos por derechos industriales o de propiedad intelectual.

Firmado:

DELGADO OSUNA JOSE ANTONIO - 30962940H

Firmado digitalmente por DELGADO OSUNA JOSE ANTONIO - 30962940H
Fecha: 2025.05.26 13:58:39 +02'00'

José Antonio Delgado Osuna

Subdirector Provincial SIC de Córdoba