1. ANEXO 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.

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 Huelva 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 Infanta Elena de Huelva 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 Huelva (en adelante **STIC-HUE**).

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.

Los documentos que se generen desde el software de gestión deben poder abrirse con Libre Office, al ser esta es 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 Software Corporativo

La autenticación de usuarios se debe de realizar mediante Directorio Activo (LDAP) corporativo (DMSAS) bajo el marco de Gestión de Identidades 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-HUE 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 servidores 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 servidor 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.

  - Como 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

- 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.

En el caso de los equipos multifunción, la seguridad deberá estar integrada en el dispositivo cumpliendo como mínimo los siguientes requisitos:

- Encriptación de las comunicaciones.
- Encriptación de los discos duros de las máquinas.
- Cualquier software que se desee instalar en las máquinas deberá ser supervisado previamente por el equipo provincial TIC.

1.8. Integraciones

Las integraciones necesarias deberán ser pactadas entre el adjudicatario, el responsable del contrato y la STIC-HUE.

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-HUE.

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-HUE 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-HUE 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-HUE en el horario más oportuno. Las actuaciones en este sentido serán coordinadas por la STIC-HUE 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-HUE 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 a través de Ayuda Digital.

1.10.3.2. Soporte de segundo nivel

Cuando el adjudicatario haya determinado que la incidencia no puede ser resuelta por él mismo, escalará la incidencia a través de Ayuda Digital al Equipo Provincial TIC, quien hará un segundo diagnóstico para determinar cómo y quién debe resolver la incidencia.

1.11. Datos “in-situ”

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

1.12. 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.

1.13. 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.

1.14. 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 (CGES) 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.

1.15. 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.

1.16. 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.

1.17. 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.

1.18. 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.

1.19. 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.

1.20. Servicios de integración con las herramientas de gestión TIC

Para optimizar los esfuerzos de gestión relacionados con las solicitudes que se registran y resuelven a través de las herramientas de gestión TIC, la persona adjudicataria debe dotarse de los medios técnicos necesarios para hacer uso de los servicios de integración provistos por la STIC y mantener actualizadas dichas integraciones en todo momento. Estas actualizaciones pueden ser motivadas por la evolución o incorporación de nuevos servicios de integración.

El detalle de estos servicios de integración, sus actualizaciones y procedimientos, se encuentran disponibles en:

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

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 SAS enrolará a la persona adjudicataria en los actuales procedimientos de resolución remota, 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: microCLAUDIA, Crowdstrike y Altiris, para las cuales su personal estará convenientemente capacitado.

1.24. Herramientas de gestión logística TIC”

El SAS dispone de diversas herramientas que dan cobertura a distintos aspectos de la gestión logística TIC y a las cuales la persona adjudicataria deberá integrarse para dar cobertura a todo el proceso: SIGLO (herramienta corporativa de gestión logística), NWT (gestión de operación TIC), CMS (gestión de activos TIC), JIRA/Confluence (gestión de proyectos TIC), APOLO (gestión de almacenes TIC).