Junta de Andalucía

Consejería de Sanidad, Presidencia y Emergencias

Servicio Andaluz de Salud

PLIEGO DE PRESCRIPCIONES TÉCNICAS

SERVICIO DE DISPONIBILIDAD TECNOLÓGICA DEL SISTEMA DE PLANIFICACIÓN DOSIMÉTRICA, PRODUCTO SANITARIO, PARA TRATAMIENTO A PACIENTES MEDIANTE RADIOTERAPIA EXTERNA Y QUE OPERAN LOS SERVICIOS DE RADIOFÍSICA Y ONCOLOGÍA RADIOTERÁPICA DEL SERVICIO ANDALUZ DE SALUD.

Nº EXPEDIENTE: C.C. 5101/2025

1. OBJETO

El objeto del presente contrato es el servicio de disponibilidad tecnológica del sistema de planificación dosimétrica, producto sanitario, para tratamiento a pacientes mediante radioterapia externa y que operan los servicios de radiofísica y oncología radioterápica del Servicio Andaluz de Salud.

El servicio de disponibilidad tecnológica del sistema de planificación estará compuesto por aquellos componentes, equipamientos y recursos humanos necesarios para la realización de los procedimientos señalados anteriormente, de forma unificada y homogénea para los servicios de radiofísica y oncología radioterápica del Servicio Andaluz de Salud.

El contrato también incluirá la conexión sin coste de los nuevos equipos que sean adquiridos por el SAS durante el periodo de vigencia de la presente contratación.

2. ALCANCE.

Producto sanitario que consiste en un sistema de planificación de tratamientos radioterápicos, en servidores cuya ubicación determine el Servicio Andaluz de Salud, para la realización de los trabajos propios de preparación del tratamiento radioterápico, desde la importación de imágenes, delimitación de contornos y volúmenes, preparación del diseño del tratamiento, procesos de optimización, cálculo dosimétrico, procedimientos de verificación dosimétrica y preparación de los datos para su envío a tratamiento y otros sistemas asociados.

Para su ejecución la empresa adjudicataria aportará todos los medios materiales necesarios (por ejemplo, servidores de acceso remoto centralizado, equipamiento de conexión eléctrica, almacenamiento, licencia de producto de la plataforma, etc.) con los medios y licenciamiento universal, siendo obligación del contratista la realización de todas las tareas y operaciones y la activación de las licencias necesarias para su correcta operación desde los centros de destino, utilizando herramientas de acceso remoto desde las estaciones de trabajo del usuario. Los servidores de cálculo serán alojados en los centros CPD que determine el Servicio Andaluz de Salud según la solución propuesta, y manteniendo durante la duración del contrato el sistema actualizado a su última versión. Todo el equipamiento proporcionado para la puesta en marcha y funcionamiento de la solución deberá cumplir con las normativas TIC (https://ws001.sspa.juntadeandalucia.es/confluence/display/NORMATIVATIC).

Por tanto, la empresa adjudicataria se responsabilizará de disponer y mantener correctamente operativos, los medios materiales que necesita el SAS para realizar el servicio de planificación radioterápica, cuya realización será hecha por personal propio del SAS.

Se deberán llevar a cabo, entre otras, las siguientes actuaciones:

Instalación e integración con los sistemas existentes de una plataforma hardware y software para realizar las planificaciones de todos los tratamientos de radioterapia externa en cualquiera de los aceleradores lineales de los Servicios de Oncología Radioterápica del Sistema Sanitario Andaluz, que

son los que se detallan en el apartado 3 (CENTROS DESTINO Y VOLUMEN DE PACIENTES ESTIMADO) de la memoria justificativa de esta licitación. No obstante, las empresas adjudicatarias de cada uno de los lotes deberán incluir sin coste adicional para el Servicio Andaluz de Salud cualquier unidad de tratamiento que el comité de seguimiento del presente expediente considere necesario. Se estima la realización de 27.000 pacientes al año. El equipamiento hardware y los requerimientos de infraestructura necesarios para su alojamiento, serán proporcionados por el adjudicatario, con capacidad de integrarse en los CPD que se indiquen.

- **Garantía de cobertura completa de las necesidades de planificación de radioterapia externa, con una única plataforma.** El contratista incluirá el hardware, software y licencias necesarias para cubrir las necesidades totales de los Servicios de Oncología Radioterápica y Radiofísica, con relación al objeto del contrato.

- **Migración de los datos** (desde noviembre de 2015)**,** a cargo del contratista, desde el planificador con el que cuenta cada uno de los centros destino actualmente al planificador resultante del presente expediente en cada uno de los centros, o a formato DICOM-RT, con capacidad de importación de los mismo al planificador proporcionado. En caso de que para dicha migración fuera necesario realizar algún tipo de servicio por parte del anterior adjudicatario todos los costes deberán ser asumidos por el nuevo adjudicatario.

- **Exportación** de los tratamientos del planificador centralizado anterior (Philips Pinnacle) a formato DICOM RT, y la capacidad de importación al sistema de planificación proporcionado. Entrega de imágenes y resultados de la planificación al PACs Corporativos en formato DICOM RT.

- **Backup** de los modelos de máquina y planificaciones, con las medidas adecuadas para garantizar la accesibilidad y recuperación futura de todas las planificaciones. Correrá a cargo del contratista tanto el software como el hardware de almacenamiento necesarios, dimensionados adecuadamente para la carga de trabajo del servicio, estimadas en 27.000 planificaciones al año. El sistema de backup será autocontenido y gestionado por el contratista durante toda la vigencia del contrato.

- **Mantenimiento integral** del sistema software y hardware, incluyendo mantenimiento preventivo, correctivo, técnico-legal, y evolutivo de las actualizaciones de software. Este mantenimiento incluirá también la aplicación de todos los parches de seguridad de la solución prescritos por el SAS y las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos, de cara al cumplimiento de todas las políticas de seguridad necesarias.

  El alcance del contrato incluye también:

- **Formación continua** en el uso de las herramientas a los usuarios del sistema, adaptada a las características de las diferentes categorías profesionales de usuarios. Esta formación se llevará a cabo en castellano y dentro del horario laboral de cada hospital. Programa de formación inicial y continuada a nivel de: físicos, médicos y técnicos superiores en radioterapia y dosimetría.

- El **modelado** (incluyendo las medidas necesarias en los equipos) de los aceleradores lineales de cada Servicio de Oncología Radioterápica incluidos en el apartado 7. Centros de destino y volumen de pacientes estimados, de la memoria justificativa del presente expediente.

- Herramientas del tipo "comparar con el mejor" y de "centro de control" (*benchmarking* y *command center*), que reporten a los Servicios Centrales del SAS indicadores clave (como son el número de usuarios conectados, el número de licencias, de cada tipo, existentes y ocupadas en cada momento, y el desempeño a nivel de cálculo, consumo de memoria y disco, de los servidores o estaciones de cálculo).

- La ejecución de los trabajos cumplirá las prescripciones marcadas por la Dirección de cada uno de los hospitales implicados y sus Servicios de Ingeniería, Informática, Radiofísica y Protección Radiológica, Oncología Radioterápica.

3. OBLIGACIONES DEL CONTRATISTA DURANTE LA EJECUCIÓN DEL CONTRATO.

Este apartado describe las obligaciones del contratista durante la ejecución del contrato. La aplicación concreta de cada una de ellas al objeto de esta contratación depende directamente del entorno tecnológico en el que se encuadra.

Definición de entorno tecnológico.

Las condiciones generales que son de aplicación directa en conexión con el entorno tecnológico descrito a lo largo del presente documento son las siguientes:

3.1. Actuaciones, obligaciones y compromisos del contratista.

Los fundamentos operativos que han de ser tenidos en cuenta para llevar a cabo el presente servicio engloban todas las actuaciones necesarias, para su diseño y puesta en marcha, en particular, será necesario elaborar el DET (Documento de Entorno Tecnológico) y recibir la aprobación de la **USTIC** (Unidad de Seguridad en Tecnologías de la Información y Comunicaciones), en un plazo inferior a **4 meses** desde la firma de contrato, sin los cuales se entenderá que no se ejecuta la prestación.

De igual forma correrá por cuenta del contratista la integración con el sistema PACS corporativo implantado en el SAS, en formato DICOM RT, verificando la correcta entrega de las imágenes y datos dosimétricos en formato adecuado. Se deberá proveer un visor / interface DICOM RT para la visualización de los datos del PACs, de tal forma que dicha visualización pueda producirse sin necesidad de devolverlos al sistema de planificación. Dicha visualización debe comprender al menos los histogramas dosis volumen, imágenes de planificación, distribución de dosis y datos básicos de los campos de tratamiento.

Resolver, sin coste, las alertas sanitarias, o notas de seguridad del fabricante, que surjan con el equipamiento y softwares objeto del servicio.

Realizar encuestas de satisfacción del servicio entre los profesionales con acceso al sistema, de forma anónima y con periodicidad anual, en la que exista desagregación por centro y categoría profesional.

3.2. Almacenamiento de los estudios.

Los estudios serán enviados en formato DICOM-RT a la red de registro y verificación de radioterapia identificada para cada uno de los centros enumerados en el apartado 7. Centros de destino y volumen de pacientes estimados de la memoria del presente expediente, debiendo ser importados de forma correcta los datos del tratamiento y de dosis de referencia, las imágenes de verificación, y las posibles traslaciones que sean requeridas en las mismas, siendo responsabilidad del contratista, avisar de las posibles limitaciones o incompatibilidades existentes si no es posible solucionarlas técnicamente.
Se propondrá una política de backup en formato DICOM-RT indicando el flujo de información y el grado de automatización de la misma, proporcionando un diagrama de flujo con indicación de cada punto/tarea y si es ejecutada de forma automática o manual. Debe indicarse el consumo típico de espacio de tratamientos tipo (tratamiento de próstata 7 campos con un único CT, tratamiento de cabeza y cuello con 2 arcos VMAT y registro de 2 CT, y SBRT con 2 arcos VMAT y 8 juegos CT de imagen de ciclo respiratorio).

3.3. Verificaciones y controles de seguridad.

Después de cada intervención de asistencia técnica en los servidores o equipos se deberá verificar que se mantienen las características y estado de referencia inicial del sistema, así como las funcionales y esenciales para la seguridad y el funcionamiento del equipo, en la medida en que puedan haberse visto afectadas por las acciones de mantenimiento. Las intervenciones en el sistema deben ser previamente comunicadas y acordadas con el responsable de contrato que designe el órgano de contratación, y quedarán documentadas en cuanto a su alcance y posible repercusión en el funcionamiento del sistema, en particular si afecta a los cálculos dosimétricos.

Se deben realizar los controles de seguridad, de acuerdo con los plazos y el alcance determinados en las instrucciones de uso del equipo, exigidos por la legislación vigente.

Se elaborará calendario con las verificaciones de los equipos, que deberá ser aprobado por el responsable del Contrato, así como sus protocolos y resultados.

3.4. Ciberseguridad.

Este apartado aplica a todos los lotes que contienen dispositivos con capacidad de transmitir información a la red informática del centro sanitario donde se instale.

La empresa contratista deberá garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información según 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 sean objeto de la contratación.

El detalle de cómo el SAS va a requerir a los posibles licitadores todo aquello relativo a la ciberseguridad, queda recogido en el Anexo I y II de este documento.

Aquellas empresas licitadoras que estén certificadas en el ENS en la categoría ALTA, no tendrán que justificar ninguna de las medidas que se indican en el citado anexo I, ya que la propia certificación ofrece las garantías suficientes de cumplimiento de las normas de ciberseguridad.

Los requisitos normativos técnicos de obligado cumplimiento relativos a las Tecnologías de la Información y las Comunicaciones, adicionales a los ya indicados en este Pliego de Prescripciones Técnicas, pueden consultarse en Normativa TIC): (https://ws001.sspa.juntadeandalucia.es/confluence/display/NORMATIVATIC).

Todo software, sea producto sanitario o no, que no corra sobre el propio equipo suministrado, lo hará sobre hardware, siempre que este no deba ser producto sanitario, que el SAS proveerá.

En definitiva, para todas las tareas de montaje, instalación y puesta en servicio 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, siempre dentro de lo que suponga un esfuerzo razonable para el posible contratista dentro de las condiciones del contrato.

3.5. 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, 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 Dirección General de Sistemas de Información y Comunicación (en adelante DGSIC), 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, establecidas para los sistemas de categoría ALTA.

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:

a) La anonimización y el cifrado de datos personales;
b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico;
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 (en adelante 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:

a) Procedimiento de reporte de incidentes reales o sospechosos, detallando el escalado de la notificación.
b) 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.
c) Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.
d) Procedimientos para informar a las partes interesadas, internas y externas.
e) Procedimientos para:
    1. Prevenir que se repita el incidente.
    2. Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.
    3. 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.

El encargado de tratamiento prestará especial atención a las medidas de protección categorizadas en el ENS relacionadas con la protección de las aplicaciones informáticas (código [mp.sw] en el ENS) y desarrollo de aplicaciones (código [mp.sw.1] en el ENS).

1. El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de producción en el entorno de desarrollo.

2. Se usarán pautas de desarrollo documentadas en la plataforma CONFLUENCE de la DGSIC que:

a) Tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
b) Trate específicamente los datos usados en desarrollo y pruebas.
c) Permita la inspección del código fuente.

3. Los siguientes elementos serán parte integral del diseño del sistema:
   a) Los mecanismos de identificación y autenticación.
   b) Los mecanismos de protección de la información tratada.

4. La generación y tratamiento de pistas de auditoría. Las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

Aceptación y puesta en servicio (código [mp.sw.2] en el ENS):

1. Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación. Se verificará que:
   a) Se cumplen los criterios de aceptación en materia de seguridad.
   b) No se deteriora la seguridad de otros componentes del servicio.
2. Las pruebas se realizarán en un entorno aislado (pre-producción).
3. Las pruebas de aceptación no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.
4. Se realizarán las siguientes inspecciones previas a la entrada en servicio:
   a. Análisis de vulnerabilidades.
   b. Pruebas de penetración.

Protección de servicios y aplicaciones web (código [mp.s.2] en el ENS):

Los sistemas dedicados a la publicación de información deberán estar protegidos frente a las amenazas que les son propias.

a) Cuando la información tenga algún tipo de control de acceso, se garantizará la imposibilidad de acceder a la información sin autenticación, en particular tomando medidas en los siguientes aspectos:

a. Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.

b. Se prevendrán ataques de manipulación de direcciones de recursos de internet (más conocidos por el término URL por sus siglas en inglés).

c. Se prevendrán ataques de manipulación de fragmentos de información que se almacenan en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en inglés como «cookies».

d. Se prevendrán ataques del tipo inyección de código.

b) Se prevendrán intentos de escalado de privilegios conforme a lo estipulado en la plataforma Confluence de la DGSIC.

c) Se prevendrán ataques de «cross site scripting».

d) Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como «proxies» y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como «cache».

Firma electrónica [mp.info.4]

La firma electrónica es un mecanismo de prevención del repudio; es decir, previene frente a la posibilidad de que en el futuro el signatario pudiera desdecirse de la información firmada.

La firma electrónica garantiza la autenticidad del signatario y la integridad del contenido. Cuando se emplee firma electrónica solo se utilizarán medios de firma electrónica de los previstos en la legislación vigente.

a) Los medios utilizados en la firma electrónica serán proporcionados a la calificación de la información tratada. En todo caso:
1. Se emplearán algoritmos acreditados por el Centro Criptológico Nacional
2. Se emplearán, preferentemente, certificados reconocidos.
3. Se emplearán, preferentemente, dispositivos seguros de firma.

b) Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación:

1. Certificados.
2. Datos de verificación y validación.
3. Se protegerán la firma y la información mencionada en el apartado anterior con un sello de tiempo.
4. El organismo que recabe documentos firmados por el administrado verificará y validará la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad la información descrita en los epígrafes 1) y 2).
5. La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes 1) y 2).

Datos de carácter personal [mp.info.1]:
Cuando el sistema trate datos de carácter personal, se estará a lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas por el Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
Lo indicado en el párrafo anterior también se aplicará, cuando una disposición con rango de ley se remita a las normas sobre datos de carácter personal en la protección de información.

3.6. 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 contratista autor material de los trabajos. La persona contratista 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.

3.7. 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/INTERPUB/01.+Normativa

Este portal recoge toda la regulación en cuanto a normas y procedimientos de trabajo que ha identificado la DGSIC 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.

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 de la DGSIC, así como la unidad de Seguridad TIC, siempre dentro de lo que suponga un esfuerzo razonable para el contratista dentro de las condiciones del contrato.

El contratista deberá incluir todos los servicios DICOM necesarios para garantizar el servicio ofertado.

Los requisitos normativos técnicos de obligado cumplimiento relativos a las Tecnologías de la Información y las Comunicaciones, adicionales a los ya indicados en este Pliego de Prescripciones Técnicas, pueden consultarse en el espacio Normativa TIC): (https://ws001.sspa.juntadeandalucia.es/confluence/display/NORMATIVATIC).

- Garantizar la interoperabilidad necesaria de los datos demográficos e identificadores de paciente entre el sistema de planificación y la red de gestión hospitalaria del Servicio Andaluz de Salud, incluyendo el envío del informe resumen de la planificación dosimétrica a la historia clínica del paciente.
- Interconexión e interoperabilidad del sistema con los equipos de imagen necesarios en cada centro, y los equipos de tratamiento disponibles en el Servicio Andaluz de Salud.
- Cada contratista de cada lote garantizará la interoperabilidad con la red de gestión de aceleradores asignada a dicho lote.

3.8. Rediseño funcional y simplificación de procedimientos administrativos

Con carácter general se deberá tener en consideración que la aplicación de medios electrónicos a la gestión de los procedimientos será precedida de la realización de un análisis de rediseño funcional y simplificación, en el marco del objetivo de simplificación de los procedimientos administrativos que persigue la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, lo dispuesto en su artículo 75.2 y en el artículo 37.1 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía.

Para ello se considerarán especialmente los criterios de simplificación y agilización establecidos en el artículo 6 del citado Decreto, así como el Manual y las herramientas para simplificación de procedimientos y agilización de trámites regulados en artículo 13. El Manual de Simplificación Administrativa y Agilización de Trámites de la Administración de la Junta de Andalucía, aprobado por Orden de 22 de febrero de 2010 (BOJA núm. 52 de 17 de marzo) está disponible en la siguiente dirección:

https://ws024.juntadeandalucia.es/ae/extra/manualdesimplificacion

3.9. Definición de procedimientos administrativos por medios electrónicos

La definición de los procedimientos deberá realizarse conforme a los conceptos y términos expresados en el documento Dominio Semántico del Proyecto w@ndA (ISBN 84-688-7845-6) disponible en la web de soporte de administración electrónica de la Junta de Andalucía. La citada web está accesible en la siguiente dirección:

http://www.juntadeandalucia.es/haciendayadministracionpublica/ae

3.10. 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.

3.11. 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.

3.12. 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 el ámbito de la Administración Electrónica. 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).

A. 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.

B. En el caso de que, en alguno de los sistemas, aplicaciones, herramientas, etc. objeto de contratación se gestionen trámites y actuaciones que se realizan con la Administración de la Junta de Andalucía por razón de la condición de empleado público.

El sistema deberá admitir, para los trámites y actuaciones que su personal realice con ella por razón de su condición de empleado público, el sistema de identificación de la plataforma de Gestión Unificada de Identidades de Andalucía (GUIA) de acuerdo con el artículo 25.1 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía.

3.13. Formación inicial y continuada.

El contratista debe impartir a los profesionales usuarios directos del equipamiento formación sobre su correcto uso, riesgos asociados y posibles incidencias. La formación se realizará según lo establecido en el PPT y en la oferta adjudicataria del contratista.

La formación constará de una formación inicial y continuada, llevada a cabo en castellano y dentro del horario laboral de cada hospital. Se considera un mínimo de 25 horas de formación por centro.

En todo caso, el plan de formación ofertado deberá cumplir:

- Dirigido a físicos, médicos, técnicos superiores en radioterapia y dosimetría y, en general, cualquier estamento relacionado con las prestaciones del servicio, para obtener el mejor uso y manipulación del mismo, en especial los servicios de STIC en tanto configuración y esquema del sistema.
- Deberá describir la metodología pedagógica y organizativa aplicada, usuarios a los que se dirige, número de horas presenciales y no presenciales, número de sesiones y formato de impartición de la formación.
- Deberá estar adaptado a las necesidades y contexto de los usuarios y del servicio.

El contratista debe garantizar la realización de las actividades de formación a sus empleados que sean necesarias para la correcta cualificación de los profesionales y el uso seguro de los equipos que son ámbito de su responsabilidad. Realizará actas de las actividades de formación impartidas que entregará al responsable del contrato con la periodicidad que se establezca o bajo demanda.

Además de la formación inicial y continuada, se requiere que la empresa adjudicataria proporcione un canal de contacto directo, ya sea mediante correo electrónico o telefónico, para resolver de forma ágil y eficiente cualquier duda o consulta que pueda surgir durante la duración del contrato.

3.14. Disponibilidad pública del software

De conformidad con lo establecido en la orden de 21 de febrero de 2005, sobre disponibilidad pública de los programas informáticos de la administración de la Junta de Andalucía y de sus organismos autónomos, el sistema de información desarrollado pasará a formar parte del repositorio de software libre de la Junta de Andalucía, en las condiciones especificadas en la citada orden. La persona adjudicataria deberá entregar el código fuente del sistema de información desarrollado, así como la documentación asociada y la información adicional necesaria, en un formato directamente integrable en el repositorio de software libre de la Junta de Andalucía. De esta obligación quedarán exentos todos aquellos componentes, productos y herramientas que, no habiéndose producido como consecuencia de la ejecución del contrato, estén protegidos por derechos de propiedad intelectual o industrial que no permitan la libre distribución o el acceso al código fuente.

La aplicación desarrollada será publicada en el repositorio de software libre de la Junta de Andalucía; viniendo acompañada, además, junto con el software, de la documentación completa, en formato electrónico, referente tanto al análisis y descripción de la solución, así como del correspondiente manual de usuario, con objeto de que este software pueda fácilmente ser usable.

3.15. Uso de infraestructuras TIC y herramientas corporativas.

En el marco de lo dispuesto sobre el impulso de los medios electrónicos en el art. 36.1 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía, se tendrán en cuenta todas las infraestructuras TIC (sistemas de información, tecnologías, frameworks, librerías software, etc.) que en la Junta de Andalucía tenga la consideración de corporativas u horizontales y sean susceptibles de su utilización. Se considerarán, entre otras, las siguientes:

- Para el modelado y tramitación de los flujos de trabajo ligados a procedimientos administrativos se deberá utilizar el tramitador TREW@ y herramientas asociadas (eximiéndose de esta obligación en el caso de flujos de trabajo que no estén ligados a procedimientos).
- @firma: la plataforma corporativa de autenticación y firma electrónica para los procedimientos administrativos, trámites y servicios de la Administración de la Junta de Andalucía.
- Autoridad de Sellado de Tiempo de la Junta de Andalucía.
- @ries: el registro unificado de entrada/salida.
- notific@: prestador de servicios de notificación.
- LDAP del correo corporativo para la identificación y autenticación de usuarios, hasta que se produzca la implantación definitiva del Directorio Corporativo de la Junta de Andalucía.
- port@firma: gestor de firma electrónica interna.
- Etc.

3.16. 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.

3.17. 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.

3.18. Desarrollo web: páginas web orgánicas del SAS y puntos de acceso electrónico permitidos en la administración andaluza

El Decreto 622/2019 de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía, establece la tipificación de puntos de acceso electrónico permitidos en la administración andaluza. En este sentido, los trabajos de desarrollo que tengan relación con páginas webs orgánicas del SAS se adecuarán a los dispuesto en este Decreto y, por tanto, se llevarán a cabo las acciones oportunas para la integración de los contenidos de las páginas web orgánicas del SAS en el punto de acceso electrónico general, el portal de la Junta de Andalucía.

3.19. Desarrollo web corporativa e intranet: apertura de datos

El diseño y desarrollo informático deberá facilitar el acceso y descarga de todos los datos existentes en la aplicación, así como posibilitar su publicación en el Portal de Datos Abiertos de la Junta de Andalucía. Los datos se proporcionarán en formatos estructurados, abiertos e interoperables, de acuerdo con la normativa vigente de publicidad y reutilización de información pública.

Los sistemas de información desarrollados deberán permitir la descarga de todos los datos en bruto y desagregados en varios formatos no propietarios como, por ejemplo, CSV, JSON, XML o también un estándar de facto como EXCEL (de las tablas que constituyan el núcleo de la aplicación, así como las tablas auxiliares para su interpretación) preferiblemente mediante API REST (interfaz de programación de aplicaciones), basado en estándares abiertos que permitirá el acceso automático a los datos y en tiempo real.

Si los anteriores conjuntos de datos contienen información de carácter personal, se realizarán la extracción de datos mediante un proceso de disociación o anonimización que garantice el cumplimiento de la Ley de Protección de Datos.

3.20. Cláusula sobre normalización de fuentes y registros administrativos

Con la finalidad de asegurar la compatibilidad e interoperabilidad con otras fuentes y registros administrativos, el tratamiento de variables demográficas (sexo, edad, país de nacimiento, nacionalidad, estado civil, composición del hogar), geográficas (país, región y provincia, municipio y entidad de población, dirección, coordenadas) o socioeconómicas (situación laboral, situación profesional, ocupación, sector de actividad en el empleo, nivel más alto de estudios terminado) que se haga en el sistema seguirá las reglas para la normalización en la codificación de variables publicadas por el Instituto de Estadística y Cartografía de Andalucía accesibles a través de la URL:

http://www.juntadeandalucia.es/institutodeestadisticaycartografia/ieagen/sea/normalizacion/ManNormalizacion.pdf

3.21. Censo de recursos informáticos (CRIJA)

Inventario de bienes: todos los bienes suministrados mediante el presente expediente requieren ser etiquetados tanto a nivel físico como lógico para su inventariado por parte de la Junta de Andalucía, de cara a cumplir con lo dispuesto en la Ley 4/86, de 5 de mayo, del Patrimonio de la Comunidad Autónoma de Andalucía en su artículo 14, así como la Orden de 23 de octubre de 2012 por la que se desarrollan determinados aspectos de la política informática de la Junta de Andalucía.

Etiquetado físico: el etiquetado físico se realizará mediante etiquetas que proporcionará la Junta de Andalucía. En caso de que el Organismo haya contratado la opción de etiquetado juntamente con el suministro del equipo, el proceso completo de etiquetado debe realizarlo la empresa suministradora, y los costes asociados a este proceso estarán incluidos dentro de los trabajos a realizar dentro de esta contratación. La empresa suministradora deberá realizar todos los pasos indicados en el procedimiento de inventariado de bienes vigente en la Junta de Andalucía para aquellos bienes del presente expediente contratados con la opción de etiquetado y tomar todas las medidas necesarias para garantizar que los bienes son entregados con la correspondiente entrada en el Censo de Recursos Informáticos de la Junta de Andalucía (CRIJA) y con la correspondiente etiqueta adherida al equipo en los términos que describe el procedimiento de inventariado. Dicho procedimiento se encuentra descrito en el archivo “02-ADA-PRO-CRIJA-Procedimiento de inventariado de bienes informáticos Junta de Andalucía. Proveedores.pdf”, el cual puede consultarse en la sección web de la Junta de Andalucía “Información de interés”, apartado “Procedimiento de Inventariado de Bienes Informáticos”, a través del enlace:

https://www.juntadeandalucia.es/haciendayadministracionpublica/apl/scc-frontpublico/InformacionUtilidades/recursosUtilidad

3.22. Condición de “no exclusividad”

Si alguna de las características establecidas en las especificaciones técnicas determinara una marca o modelo exclusivo, éstas serán tomadas únicamente como guía u orientación, sin que el hecho de no ajustarse exactamente sea causa de exclusión. Entendiendo este párrafo como condición de “no exclusividad”.

3.23. Especificaciones medioambientales.

3.23.1. Sistema de gestión de las sustancias químicas.

El contratista deberá haber implantado un sistema de gestión de las sustancias químicas con recursos específicos, el necesario grado de especialización y procedimientos e instrucciones documentados para garantizar la identificación de sustancias presentes en el producto adquirido en virtud de este contrato que hayan sido incluidas en la Lista de sustancias candidatas extremadamente preocupantes (SEP) identificadas con arreglo al artículo 57 del Reglamento (CE) nº 1907/2006 (Reglamento REACH), incluidas las posibles nuevas incorporaciones a dicha lista. Esto significa que el contratista tendrá que:

- Haber solicitado a los proveedores información sobre la presencia de las sustancias incluidas en esa lista, incluidas las nuevas incorporaciones a dicha lista (en el mes siguiente a la publicación de una lista revisada por la ECHA- *European Chemicals Agency*)
- Haber establecido un procedimiento sistematizado de recogida y registro de la información recibida sobre SEP incluidas en la lista de sustancias candidatas de REACH que estén presentes en los productos adquiridos en virtud de este contrato; es decir, procedimientos de registro y vigilancia (por ejemplo, inspecciones periódicas de documentación relativa al contenido de sustancias candidatas incluidas en la lista presentes en el producto, así como controles puntuales del contenido de sustancias químicas (informes de análisis de laboratorio) para evaluar la información recogida por si hubiera incoherencias.

Para verificar este apartado, los contratistas deberán confirmar que disponen de los procedimientos y las instrucciones anteriormente indicados y describir el sistema de documentación, vigilancia y seguimiento establecido, así como los recursos asignados al mismo (tiempo, personal y su especialización). Se podrán realizar controles puntuales de los informes descritos en el requisito anterior.

Reglamento (UE) 2019/424 de la Comisión, de 15 de marzo de 2019, por el que se establecen requisitos de diseño ecológico para servidores y productos de almacenamiento de datos de conformidad con la Directiva 2009/125/CE del Parlamento Europeo y del Consejo, y por el que se modifica el Reglamento (UE) n.° 617/2013 de la Comisión.

Reglamento (UE) 2023/826 de la Comisión de 17 de abril de 2023 por el que se establecen requisitos de diseño ecológico aplicables al consumo de energía en los modos desactivado y preparado, así como en el modo preparado en red, de los equipos eléctricos y electrónicos domésticos y de oficina con arreglo a la Directiva 2009/125/CE del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) nº 1275/2008 (CE) nº 107/2009 de la Comisión.

4. DESARROLLO OPERATIVO DEL SERVICIO.

La implantación incluida en la presente contratación deberá ser ejecutados en diferentes fases, que se detallan a continuación:

4.1. Fase I. Análisis de situación y consultoría.

El contratista realizará un despliegue de medios necesarios para poder evaluar la situación que le permita llevar a cabo la implantación posterior de la propuesta ofertada, para ello contará con el soporte del personal del SAS de la DGSIC.

Esta fase incluirá reuniones de seguimiento frecuentes e informes de las mismas, y de otras circunstancias que se puedan dar. Siendo responsabilidad directa del contratista la entrega de una propuesta de implantación realista según los plazos establecidos en los pliegos.

4.2. Fase II. Aprovisionamiento del equipamiento e instalación de la herramienta.

El sistema de planificación dosimétrica para tratamiento a pacientes mediante radioterapia externa deberá cumplir los requisitos funcionales, técnicos y de licenciamiento que se recogen los apartados 7, 8 y 9 del presente pliego de prescripciones técnicas.

4.3. Fase III. Parametrización de la solución al ámbito tecnológico y funcional del proyecto.

Dado que la versión de origen del producto a implantar requiere de ciertas adaptaciones en el software para su adecuación al ámbito funcional y técnico del proyecto, la empresa contratista deberá realizar el análisis funcional, el diseño técnico y el desarrollo de las posibles adaptaciones, parametrizaciones e integraciones sobre el producto ofertado para su ajuste al alcance definido, según las funcionalidades ofrecidas por la herramienta propuesta, los requerimientos establecidos en el presente pliego y las decisiones tomadas durante las distintas reuniones de trabajo a mantener con los referentes funcionales que el SAS designe para esta finalidad. En lo que respecta a las integraciones, deberá hacerse hincapié en los datos, los servicios de integración y los requerimientos y modificaciones técnicas y funcionales a llevar a cabo en los sistemas de información con los que la solución ofertada deberá comunicarse.

Como resultado de estos trabajos, existirá una versión definitiva del sistema de información a implantar sobre un entorno de desarrollo, la cual deberá ser validada por el SAS ante el comité técnico de gestión del contrato.

4.4. Fase IV. Implantación

La DGSIC dispone de un modelo corporativo marco de implantaciones (en adelante MCMI), como documento maestro que recoge, estandariza y estructura el proceso de implantación de cualquier sistema de información en el ámbito del SAS. Es un modelo flexible y adaptable que define el conjunto de áreas de conocimiento, fases, procesos, actividades, usuarios y responsabilidades implicados en la ejecución de un proyecto de implantación.

La solución contratada deberá incluir una propuesta de plan de implantación, como adaptación de este modelo corporativo a la solución específica ofertada por el licitante y a las condiciones establecidas en los pliegos de esta contratación. Dicho plan deberá ser desarrollado en base al marco de trabajo definido y al entorno funcional, técnico y organizativo del proyecto, y podrá ser posteriormente concretado durante la etapa de lanzamiento y consultoría previa. En cualquier caso, el comité director estará facultado en todo momento para realizar los cambios que se estimen oportunos sobre el plan de implantación propuesto, con objeto de garantizar la correcta ejecución del proceso de implantación.

En el caso concreto de este proyecto, el plan de implantación deberá diseñarse en base a las siguientes directrices:

- Ha de estar orientado a asegurar el uso masivo del sistema de información propuesto, por parte de los distintos perfiles profesionales involucrados en cada centro implantado y deberá hacer hincapié en las áreas de conocimiento funcional, de migración o carga inicial de datos y formación diferenciada para dichos perfiles.
- Ha de incluir una propuesta de abordaje justificada y un calendario que deberá contemplar, dentro del plazo contractual establecido, la correcta implantación del 100% del proyecto.
- Se deberá perseguir como objetivo la homogeneización y uniformidad de los procesos de negocio involucrados en toda la organización. Es decir, la empresa contratista deberá trabajar de forma conjunta con la organización para que todos los centros involucrados hagan la misma tarea de la misma forma, admitiendo solo excepciones debidamente justificadas y aceptadas

por el comité director del proyecto.

Etapa I: lanzamiento.

Esta etapa se corresponde con las actividades definidas en las fases de análisis previo de situación y reingeniería de procesos del MCMI. En concreto, se deberán analizar las características funcionales detalladas del producto ofertado, así como su adaptación y personalización al ámbito funcional del proyecto, con objeto de homogeneizar y uniformizar los procesos de negocio involucrados en todo el SAS.

Para ello, será fundamental analizar la situación actual en cuanto a la gestión de la dosis de radiación de los estudios de imagen incluidos dentro del alcance del contrato, así como de los centros en que dichos equipos se ubiquen, lo que ayudará a justificar las decisiones a adoptar. Así, la empresa contratista deberá mantener reuniones de lanzamiento, visitando los distintos centros, mediante las cuales se realice la presentación del proyecto, se analice la situación de partida, se identifiquen y consulte a los interlocutores y grupos de trabajo del SAS cuya implicación pueda ser necesaria para la consecución de los objetivos especificados, y se propongan y consensuen los principales procesos de negocio que, de forma común, deban aplicarse a toda la organización.

Como consecuencia de la realización de esta etapa, la empresa contratista presentará:

- El plan de implantación definitivo, concretando y detallando el inicialmente presentado en su oferta técnica, así como las configuraciones y parametrizaciones de las plataformas tecnológicas involucradas en el proyecto, tanto desde un punto de vista técnico (hardware y software que soportarán el sistema de información ofertado), como desde un punto de vista funcional o de negocio.
- Acompañando al plan de implantación, la empresa contratista también deberá presentar una propuesta de abordaje y un calendario de implantación de las modalidades incluidas dentro del alcance del contrato, que deberá cubrir el 100% proyecto.
- Un análisis de la situación del equipamiento a conectar en cada centro.
- El conjunto de procesos de negocio cuya implantación debe ser común a todos los centros involucrados en el proyecto, convenientemente analizados y definidos.

Etapa II: monitorización del uso y generación de los primeros indicadores y sus resultados.

En esta etapa deberán llevarse a cabo las actividades definidas en las fases de implantación del MCMI.

El adjudicatario deberá participar en la instalación, configuración, parametrización e integración del sistema de información requerido. A su vez, deberá validar dicha instalación, garantizando la total compatibilidad e integración de todos los elementos que la componen.

Etapa III: puesta en producción y consolidación

En esta etapa deberán llevarse a cabo las actividades definidas en las fases de arranque, consolidación, extensión y paso a N3 del MCMI, para los centros incluidos dentro del alcance del contrato. Estas fases se abordarán teniendo en cuenta que la instalación de la infraestructura hardware y software asociada al proyecto está disponible, como consecuencia de la finalización exitosa en la instalación del centro piloto en la etapa anterior.

Tanto el SAS, como la empresa contratista, deberán asegurar que los distintos procesos de arranque de todos y cada uno de los centros incluidos dentro del alcance del presente contrato, finalicen con éxito. Este arranque se hará de forma paulatina, en base a la propuesta de abordaje y al calendario de implantación presentado junto con el plan de implantación asociado en la etapa I de lanzamiento y consultoría previa.

Las actuaciones correspondientes a los trabajos de implantación en un centro concreto se considerarán finalizadas tras la realización de las comprobaciones y diagnósticos necesarios que certifiquen la correcta integración en el sistema de las modalidades productoras de imagen mediante el uso de radiación del centro en cuestión, todo ello sin menoscabo de que cualquier defecto de ejecución detectado con posterioridad a la finalización del periodo de consolidación tras el arranque, deba ser resuelto sin cargo alguno en base a las condiciones de garantía estipuladas.

Los trabajos correspondientes a la etapa III de puesta en producción y consolidación, se realizarán de forma que se garantice la completa implantación del proyecto en el plazo establecido, proporcionando al personal de los centros el tiempo suficiente para colaborar con el adjudicatario en dichas implantaciones.

Etapa IV. Formación inicial en el uso sistema de planificación de radioterapia.

Se realizará formación dirigida a físicos, médicos, técnicos superiores en radioterapia y dosimetría y, en general, cualquier estamento relacionado con el adecuado uso de la nueva herramienta, para obtener el mejor uso y manipulación del mismo.

4.5. Fase V. Recepción del servicio.

Fase durante la cual el servicio se ha de seguir prestando por interés del servicio que presta, y durante el cual se verificarán que se han dado todas las circunstancias que permita la recepción del servicio, con especial atención a las propuestas y cuestiones mejoradas de la oferta del contratista.

Firma por ambas partes el acta de puesta a disposición del sistema de planificación dosimétrica para radioterapia. En dicha acta deberán de venir referidos los requisitos mínimos técnicos y funcionales exigidos, así como los valores reflejados en la oferta del licitador para cada uno de los criterios de adjudicación.

4.6. Generalidades a considerar.

Todo trabajo relacionado con la puesta en producción de sistemas de información, así como con su integración e interoperabilidad, deberá llevarse a cabo con la normativa publicada por el SAS a tal efecto en el espacio de la normativa TIC (https://ws001.sspa.juntadeandalucia.es/confluence/display/NORMATIVATIC). Será exigible seguir las normas más actualizadas que existan en el momento del inicio de cada una de las fases o trabajos a realizar.

Respecto a la gestión de la prestación de los productos software objeto de esta contratación, así como del proyecto de implantación asociado, la empresa contratista será corresponsable del correcto funcionamiento del sistema de información implantado, participando del:

- Proceso de gestión de incidencias, con objeto de restaurar los servicios TIC lo más rápidamente posible ante la aparición de cualquier incidente y/o malfuncionamiento y resolver aquellas solicitudes que necesiten de una capacidad o conocimiento experto para su resolución, cuando el grado de complejidad así lo requiera.
- Proceso de gestión de problemas, con objeto de gestionar las causas subyacentes de las incidencias que impacten sobre los sistemas de información del SAS y la infraestructura técnica que los soporta. El alcance va desde que se identifica un problema, ya sea de manera proactiva o reactiva, hasta la petición de cambio y gestión de cambios que dan solución al error identificado.

  Proceso de gestión de peticiones, con objeto de dar respuesta ágil y ordenada de todas las peticiones derivadas por el SAS.

En particular, se deberán resolver incidencias y problemas relacionados con:

- Defectos de construcción, parametrización, configuración o adaptación del sistema de información (errores de codificación, casos de prueba no contemplados, validaciones de datos no contempladas, etc.).
- Integraciones defectuosas, tanto entre las diversas partes o componentes del sistema de información como en su entorno de actuación (interfaces con otros sistemas, traspasos de información entre ellos, etc.).
- Disfunciones o desajustes entre las funcionalidades o características ofrecidas por el sistema de información en su puesta en explotación y la definición de dichas funcionalidades.
- Incompatibilidades de los productos contratados con otras herramientas o software de base (sistemas operativos, sistemas gestores de bases de datos, antivirus, etc.).
- Deficiencias en el rendimiento y uso adecuado de los recursos.

Asimismo, se deberán resolver peticiones relacionadas con:

- Consultas respecto de funcionalidades, parametrizaciones o configuraciones.
- Órdenes de trabajo necesarias para la correcta gestión de los accesos.
- Extracciones y/o modificaciones de datos, que no sean resolubles mediante herramientas específicas de explotación de datos.
- Asistencia para las revisiones de rendimiento y configuración de las infraestructuras que soportan los productos contratados, así como de los sistemas de información que usan los mismos.
- Colaboraciones y asesoramiento para la implantación de las posibles actualizaciones liberadas del producto instalado.
- Comprobaciones de que la resolución de incidencias se ha efectuado con el adecuado grado de optimización y con plena conformidad con las exigencias técnicas de los sistemas de información que emplean los productos contratados.
- Acceso a las bases de datos de conocimiento y a información sobre el software y la tecnología de los productos contratados.

- Adiestramiento en los productos contratados en la liberación de nuevas funcionalidades.

5. HERRAMIENTAS A EMPLEAR.

La persona adjudicataria se compromete a usar las herramientas de gestión que indique la DGSIC. El uso de otras herramientas de gestión distintas a las indicadas por propia iniciativa de la persona adjudicataria no lo exime de esta obligación, siendo de su cuenta la dotación de los medios técnicos necesarios para su integración.

A continuación, se definen las herramientas que se usarán para la gestión de todos los servicios definidos, sin menoscabo de incorporación o sustitución de alguna de ellas por indicación expresa de la TIC durante la vigencia del contrato. La persona adjudicataria se compromete al uso de dichas herramientas según las instrucciones que se detallan a continuación.

■ 1. NormativaTIC	■ 2. Servicios de integración con las herramientas de gestión TIC	■ 3. WT: Web Técnica
■ 4. JIRA y Confluence	■ 5. MTI-SSHH	■ 6. Repositorio de código fuente
■ 7. Repositorio de componentes	■ 8. Catálogos para el desarrollo software	■ 9. Sistema de integración continua
☐ 10. Sistema de gestión de la calidad del código fuente	■ 11. Sistema de Gestión de la Configuración (CMS)	■ 12. DMSAS
☐ 13. Endpoint Detection and Response (EDR) y Altiris Client Management Suite	☐ 14. Herramientas de gestión logística TIC	■ 15. JARVIS
☐ 16. Aplican todas las anteriores		

5.1. Compendio de la normativa TIC.

En el espacio NormativaTIC, apartado A), se enlazan todas las normas técnicas de la DGSIC. La persona contratista se comprometerá a prestar los servicios contratados de acuerdo con este compendio normativo:

https://ws001.sspa.juntadeandalucia.es/confluence/display/normativaTIC, apartado A).

Cualquier excepción al cumplimiento de esta cláusula deberá ser aprobada de forma previa al comienzo de las tareas por el SAS.

5.2. 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 contratista debe dotarse de los medios técnicos necesarios para hacer uso de los servicios de integración provistos por la DGSIC 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

5.3. 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

5.4. JIRA y Confluence

Son las herramientas del SAS destinadas a la gestión del ciclo de vida del software, proyectos y conocimiento, y encargadas de la gestión y coordinación de los contratos de servicios para el mantenimiento de aplicaciones a medida, proyectos y conocimiento.

La persona adjudicataria deberá conectarse a estos sistemas para la recepción y gestión de todas las solicitudes de servicio relacionadas con el objeto del contrato, corriendo por cuenta de la persona adjudicataria la dotación de los medios técnicos, y licenciamiento en caso de ser necesario, para su acceso, uso e integración en los citados sistemas.

5.5. 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 DGSIC estime otra cosa, se cerrarán los procesos de cálculo de los ANS.

5.6. Repositorio de código fuente

Es la herramienta del SAS destinada al almacenamiento del código fuente de los productos software desarrollados por el SAS.

La persona contratista deberá conectarse a este sistema para la entrega del código fuente de productos software desarrollados en el ámbito de esta contratación, según el procedimiento definido para ello en el espacio de NormativaTIC, apartado A), arriba mencionado.

5.7. Repositorio de componentes

Es la herramienta del SAS destinada al almacenamiento del código fuente de los productos software desarrollado por el SAS.

La persona adjudicataria deberá conectarse a este sistema para la entrega del código fuente de

productos software desarrollados en el ámbito de esta contratación, según el procedimiento definido para ello en el espacio de Normativa TIC, apartado A), arriba mencionado.

5.8. Catálogos para el desarrollo software

Existen tres catálogos principales que deben ser incluidos en todos los análisis que impliquen nuevas funcionalidades y/o modificaciones de productos software, con objeto de garantizar la coherencia interna de los datos y su alineamiento con la semántica de la organización.

- Catálogo de servicios de interoperabilidad: catálogo de servicios de interoperabilidad disponibles, ya sea a través de la plataforma SOA corporativa o directamente en las aplicaciones proveedoras.
- Catálogo de tablas maestras: catálogo de tablas que mantienen los datos maestros del SAS.
- Catálogo de componentes: catálogo de módulos y componentes disponibles para su reutilización en las distintas aplicaciones.

5.9. Sistema de integración continua

Es la herramienta del SAS destinada a la construcción automatizada del software a partir del código fuente entregado en el repositorio de código del SAS. La DGSIC será la responsable de la configuración de las tareas de construcción y empaquetado de cada entregable, según la información proporcionada a tal efecto por la persona adjudicataria.

La persona adjudicataria, por su parte, será la responsable de proporcionar las instrucciones y todos aquellos recursos software necesarios para la construcción y empaquetado de los entregables a partir de su código fuente. La construcción del ejecutable a partir del código fuente deberá poder realizarse únicamente en base a lo dispuesto por el SAS para sus entornos y tecnologías de desarrollo, así como en los elementos disponibles en los catálogos antes mencionados.

Previamente a cualquier entrega, la persona adjudicataria deberá verificar la correcta construcción y empaquetado del software, únicamente, a partir de los recursos disponibles a través del repositorio de componentes corporativo, siendo responsabilidad exclusivamente suya los retrasos derivados de los defectos detectados durante dicho proceso en las instalaciones del SAS.

5.10. Sistema de gestión de la calidad del código fuente

Es la herramienta del SAS destinada a la revisión de la calidad del código fuente entregado en el repositorio de código fuente del SAS.

El equipo de la Oficina de Calidad del SAS será el responsable de la medición de los indicadores y de la configuración de las tareas revisión de la calidad del código fuente proporcionado con cada entregable.

La persona adjudicataria, por su parte, será la responsable de asegurar el cumplimiento de los mínimos de calidad definidos para el código fuente proporcionado con cada entregable en el repositorio de código del SAS. Previamente a cualquier entrega, la persona adjudicataria deberá verificar la calidad del código fuente entregado según los mínimos exigibles por la Oficina de Calidad, siendo responsabilidad exclusivamente suya los retrasos derivados de los defectos detectados durante el proceso de revisión de la calidad del código fuente en las instalaciones del SAS.

5.11. Sistema de Gestión de la Configuración (CMS)

CMS es la herramienta de destinada a controlar y gestionar los componentes y activos TIC. El CMS mantiene las relaciones entre los componentes del servicio y cualquier incidencia, problema, error conocido, cambio y documentación asociada. Actualmente el CMS aglutina la información de varias fuentes distintas o CMS físicas, que accesibles mediante un único interfaz, constituyen una CMS integral y federada.

5.12. DMSAS

DMSAS es el directorio activo del SAS, que constituye la única fuente de identificación y autenticación normalizada de la organización y por ello todo sistema de información que se oferte deberá integrarse con dicho sistema.

5.13. Endpoint Detection and Response (EDR) y Altiris Client Management Suite

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 virus informáticos.

Para ello, la persona adjudicataria deberá usar las herramientas corporativas del SAS: Endpoint Detection and Response (EDR) y Altiris, para las cuales su personal estará convenientemente capacitado.

5.14. 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), SIGMA-MANSIS (gestión de activos), NWT (gestión de operación TIC), CMS (gestión de activos TIC), JIRA/Confluence (gestión de proyectos TIC), APOLO (gestión de almacenes TIC).

5.15. JARVIS

JARVIS es una aplicación realizada a medida para la recogida de peticiones de modificación y extracciones de datos desde Nueva Web Técnica y su lanzamiento automatizado y validado por la TIC a través de MS Orchestrator, alojando los resultados en un FTP corporativo al cual tienen acceso los resolutores de la petición.

De esta manera se agilizan las peticiones de lanzamiento (PL) de datos, se establece una trazabilidad concreta al respecto y se controlan las actuaciones en producción de los proveedores, incorporando adicionalmente una gestión de roles y permisos para cada uno de los actores involucrados.

Adicionalmente, a través del uso de plantillas y variables para las actuaciones, se asegura la flexibilidad y adaptabilidad a las necesidades demandadas, mejorando los tiempos de resolución y la percepción del usuario final, al eliminar elementos de gestión innecesarios.

Otros aspectos destacados de JARVIS son:

- Desde la aplicación se permite seleccionar la sentencia SQL autorizada, hora de lanzamiento y realizar seguimiento del resultado.
- La actuación debe estar asociada a una solicitud CGES que se válida para que esté abierta y asignada al proveedor.
- La aplicación mantiene una auditoría de quién realiza cualquier actuación.
- Se informa a CGES del resultado final.
- Se incluyen validaciones para detectar uso incorrecto del procedimiento
- El proveedor solo lanzará sentencias SQL aprobadas y autorizadas.

- La plantilla delimita la instancia de base datos que se pueden lanzar.
- Permite incorporar parámetros asociados.

5.16. Dotación actual del CPD regional

El equipamiento en cluster instalado en los distintos CPD regionales, y sus versiones de producto existentes son las siguientes, por lo que los dispositivos a instalar tienen que ser absolutamente compatibles con los mismos, la no evidencia de dicha compatibilidad supone el no cumplimiento de requisitos mínimos requeridos, y por tanto la propuesta no será válida:

- Cluster de 5 nodos LENOVO© ThinkAgile© HX650 V3 CN con CPU Intel(R) Xeon(R) © Gold 5415+ CPU @ 3.30GHz y RAM en módulos de memoria ThinkSystem© 64GB TruDDR5 4800MHz (2Rx4) 10x4 RDIMM.
- Hypervisor ACROPOLIS© (AHV).
- Sistema operativo ACROPOLIS© (AOS).

6. ESPECIFICACIONES TÉCNICAS SINGULARES.

6.1. Tecnología en el puesto cliente.

La aplicación estará diseñada en tecnología web en todos sus módulos. Los principales navegadores de Internet (Microsoft Internet Explorer, Microsoft Edge, Google Chrome, Safari y Firefox), deberán soportarla en la última versión disponible en el momento de la implantación, así como en dos versiones anteriores, sin requerir ninguno componentes software añadidos (plug in). No se aceptarán soluciones de puesto cliente basadas en tecnología Flash Player.

El funcionamiento de la aplicación en los puestos clientes seguirá la metodología denominada *zerofootprint* (ZFP) que implica que, además del requisito anterior de no requerir instalación de ningún elemento o complemento, requiere la ausencia de rastro alguno en el cliente una vez que se cierre la aplicación y el navegador de Internet.

6.2. Arquitectura de la instalación.

Aunque las modalidades productoras de imagen se encuentran repartidas por un gran número de centros del SAS, el equipamiento que se instale como consecuencia de la presente contratación estará centralizado en uno o ambos centros de procesamiento de datos.

No está prevista la instalación local de equipamiento en los centros, aunque en caso de ser necesario en algún punto concreto, el comité director de gestión del proyecto podrá aceptarlo. En caso de estimarse necesario y aceptarse, su suministro, instalación y mantenimiento será a cargo del adjudicatario.

6.3. Entorno tecnológico de la instalación.

En lo referente a infraestructura software, el SAS pondrá a disposición del proyecto cualquiera de los productos que constituyen su arquitectura tecnológica estándar:

- Sistema operativo: Oracle Enterprise Linux o Windows Server.
- Servidor de aplicaciones: Weblogic o IIS.
- Base de Datos: Oracle.

Las versiones de los productos indicados serán prescritas por la DGSIC en su momento de instalación.

Si el sistema de información ofertado no estuviera certificado para funcionar con alguno de estos productos, o si para su implantación y utilización se requiriese alguna licencia de software comercial adicional, éstas deben ser suministradas, instaladas, configuradas y soportadas por la empresa contratista.

El adjudicatario deberá proporcionar también la infraestructura hardware necesaria para el cumplimiento de las condiciones de funcionamiento requeridas en el presente pliego.

6.4. Integraciones

Las ofertas garantizarán un adecuado nivel de interoperabilidad técnica, semántica y organizativa, conforme a las estipulaciones del Esquema Nacional de Interoperabilidad. En concreto, se cumplirán las Normas Técnicas de Interoperabilidad establecidas por dicho esquema.

El producto ofertado proporcionará mecanismos de integración estándar, como mínimo API REST, Web Services (SOAP), así como el grado de cobertura de dichos mecanismos sobre las funcionalidades de la aplicación.

Además, todo intercambio de datos entre el sistema de información objeto de esta contratación y otros sistemas de información, se regirá por las normas de interoperabilidad publicadas por la Oficina Técnica de Interoperabilidad del SAS en el portal de Normativa TIC (https://ws001.sspa.juntadeandalucia.es/confluence/display/NORMATIVATIC) y por las directrices e indicaciones que aquella proporcione durante la ejecución del proyecto.

En caso de que para el correcto funcionamiento de las integraciones especificadas fuese necesario el desarrollo de nuevos servicios (o la modificación de los actuales) sobre los sistemas de información corporativos del SAS, estos trabajos serán gestionados por la Oficina Técnica de Interoperabilidad del SAS, con objeto de garantizar el correcto funcionamiento y comunicación de las aplicaciones involucradas en las distintas integraciones; el adjudicatario deberá asumir todos los gastos que pudieran generarse como consecuencia de los trabajos a realizar en el sistema de información ofertado o sus servicios de integración.

Todos los intercambios, interfaces e invocaciones entre la aplicación de la empresa contratista y otras aplicaciones, se deben presentar como solicitud a la Oficina Técnica de Interoperabilidad por los medios definidos en los procedimientos y la normativa del Servicio Andaluz de Salud para que las evalúen y, o bien se aprueben o bien se defina una solución alternativa. En todo momento se debe velar por el cumplimiento del Esquema Nacional de Interoperabilidad, así como la normativa establecida al

respecto por el Servicio Andaluz de Salud.

6.5. LDAP/Directorio activo

En virtud de lo establecido en artículo 17. Autorización y control de los accesos del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, el acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación de este real decreto deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas. Adicionalmente, de acuerdo con la medida de seguridad del marco operacional op.acc.1.4 del ENS cada cuenta (de entidad, usuario o proceso) estará asociada a un identificador único. En este caso, esta identificación y autenticación se realizará mediante integración con el directorio activo del SAS (DMSAS), que se constituye en fuente única de identificación y autenticación. Además, el sistema de información también deberá estar preparado para integrarse con dicho LDAP.

Se dispone de un componente Java para esta integración:

(https://ws001.juntadeandalucia.es/unifica/web/gobernanza/integracion-con-dmsas).

Además de la integración de las cuentas de usuario, los diferentes perfiles de trabajo en el sistema de planificación (facultativo especialista en radiofísica hospitalaria, facultativo especialista en oncología radioterápica y técnico especialista en radioterapia y dosimetría y otros profesionales que trabajen con la solución ofertada) iniciarán sesión mediante comprobación de la pertenencia de las cuentas personales a grupos de usuarios correspondientes a los perfiles profesionales citados. También será posible que, una vez validado el acceso mediante la consulta del directorio activo o el LDAP del SAS, sea la aplicación la que identifique los perfiles que cada usuario tendrá en la aplicación.

7. REQUISITOS FUNCIONALES MÍNIMOS.

Los requisitos funcionales mínimos vienen listados en la siguiente tabla, con su codificación, en modo general, se deberá incluir el cálculo dosimétrico, el contorneo, la delimitación de volúmenes, la optimización y en general todas las tareas relacionadas con el proceso de planificación radioterápica.

Será imprescindible cumplir con todos y cada uno de los requisitos funcionales mínimos. En caso contrario, la oferta no será admitida.

Lote 1

REQUISITOS FUNCIONALES MÍNIMOS LOTE 1		
REQUISITO	**DESCRIPCIÓN**	**Valor binario (SÍ/NO)**
Física (modelado)		

REQ OBL FUN. 1	Proporcionar herramientas para el modelado de las unidades de tratamiento y simulación por parte del usuario o bien proporcionar el modelado por parte de la casa comercial.	
Algoritmos		
REQ OBL FUN. 2	Algoritmo de cálculo convolución-superposición y/o Montecarlo y/o que resuelvan la ecuación de transporte de Boltzmann para fotones.	
REQ OBL FUN 3	Algoritmo de cálculo convolución-superposición y/o Montecarlo para electrones.	
REQ OBL FUN. 4	Optimización Multicriterio básico.	
Técnicas de tratamiento		
REQ OBL FUN. 5	3D, IMRT, arco dinámico conformado y VMAT.	
REQ OBL FUN. 6	Varian Halcyon © en el caso de que el centro posea una máquina de estas características.	
Adaptativa		
REQ OBL FUN. 7	Versatilidad para adaptativa offline. Integración de imagen a la hora de realizar la adaptativa offline.	
REQ OBL FUN. 8	Suma de planes calculados desde diferentes CT.	
Registro con otras modalidades de imagen		
REQ OBL FUN. 9	RM.	
REQ OBL FUN. 10	PET-CT.	
Herramientas de contorneo		
REQ OBL FUN. 11	Autocontorneo de órganos y volúmenes de interés con IA. (herramienta interna o externa al sistema principal)	
Evaluación de la robustez		
REQ OBL FUN.12	Evaluación de la robustez con fotones.	
Información relativa a la formación y soporte en la puesta en marcha		
REQ OBL FUN. 13	Programa formativo.	
REQ OBL FUN. 14	Servicio de consultoría clínica.	
Licencias		

REQ OBL FUN. 15	**Compromiso** de asumir los costes, en caso de ser necesarios, para activar las licencias necesarias en la red de registro y verificación para la importación de planes o la aplicación práctica de algún tipo de tratamiento.	

Lote 2

REQUISITOS FUNCIONALES MÍNIMOS DEL LOTE 2		
REQUISITO	**DESCRIPCIÓN**	**Valor binario (SÍ/NO)**
Física (modelado)		
REQ OBL FUN 1	Proporcionar herramientas para el modelado de las unidades de tratamiento o simulación por parte del usuario o bien proporcionar el modelado por parte de la casa comercial.	
Algoritmos		
REQ OBL FUN 2	Algoritmo de cálculo convolución-superposición y/o Montecarlo y/o que resuelvan la ecuación de transporte de Boltzmann para fotones.	
REQ OBL FUN 3	Algoritmo de cálculo convolución-superposición y/o Montecarlo para electrones.	
REQ OBL FUN 4	Optimización Multicriterio básico.	
Técnicas de tratamiento		
REQ OBL FUN 5	3D, IMRT, arco dinámico conformado y VMAT.	
Adaptativa		
REQ OBL FUN 6	Versatilidad para adaptativa offline. Integración de imagen a la hora de realizar la adaptativa offline.	
REQ OBL FUN 7	Suma de planes calculados desde diferentes CT.	
Registro con otras modalidades de imagen		
REQ OBL FUN 8	RM.	
REQ OBL FUN9	PET-CT.	
Herramientas de contorneo		
REQ OBL FUN 10	Autocontorneo de órganos y volúmenes de interés con IA. (herramienta interna o externa al sistema principal)	
Evaluación de la robustez		

REQ OBL FUN 11	Evaluación de la robustez con fotones.	
Información relativa a la formación y soporte en la puesta en marcha		
REQ OBL FUN 12	Programa formativo.	
REQ OBL FUN 13	Servicio de consultoría clínica.	
Licencias		
REQ OBL FUN. 14	**Compromiso** de asumir los costes, en caso de ser necesarios, para activar las licencias necesarias en la red de registro y verificación para la importación de planes o la aplicación práctica de algún tipo de tratamiento.	

Lote 3

REQUISITOS FUNCIONALES MÍNIMOS LOTE 3		
REQUISITO	**DESCRIPCIÓN**	**Valor binario (SÍ/NO)**
Física (modelado)		
REQ OBL FUN. 1	Proporcionar herramientas para el modelado de las unidades de tratamiento y simulación por parte del usuario o bien proporcionar el modelado por parte de la casa comercial.	
Algoritmos		
REQ OBL FUN. 2	Algoritmo de cálculo convolución-superposición y/o Montecarlo y/o que resuelvan la ecuación de transporte de Boltzmann para fotones.	
REQ OBL FUN 3	Algoritmo de cálculo convolución-superposición y/o Montecarlo para electrones.	
REQ OBL FUN. 4	Optimización Multicriterio básico.	
Técnicas de tratamiento		
REQ OBL FUN. 5	3D, IMRT, arco dinámico conformado y VMAT.	
REQ OBL FUN. 6	Planificación para Accuray Tomoterapia /radixact © en el caso de que el centro posea una máquina de estas características.	
Adaptativa		
REQ OBL FUN. 7	Versatilidad para adaptativa offline. Integración de imagen a la hora de realizar la adaptativa offline.	
REQ OBL FUN. 8	Suma de planes de diferentes CT.	
Registro con otras modalidades de imagen		
REQ OBL FUN. 9	RM.	
REQ OBL FUN. 10	PET-CT.	
Herramientas de contorneo		

REQ OBL FUN. 11	Autocontorneo de órganos y volúmenes de interés con IA. (herramienta interna o externa al sistema principal)	
Evaluación de la robustez		
REQ OBL FUN. 12	Evaluación de la robustez con fotones.	
Información relativa a la formación y soporte en la puesta en marcha		
REQ OBL FUN. 13	Programa formativo.	
REQ OBL FUN. 14	Servicio de consultoría clínica.	
Licencias		
REQ OBL FUN. 15	**Compromiso** de asumir los costes, en caso de ser necesarios, para activar las licencias necesarias en la red de registro y verificación para la importación de planes o la aplicación práctica de algún tipo de tratamiento.	

8. REQUISITOS TÉCNICOS MÍNIMOS.

Será imprescindible cumplir con todos y cada uno de los requisitos técnicos mínimos. En caso contrario, la oferta no será admitida.

Las siguientes tareas se consideran requisitos técnicos mínimos:

a) Activación de las licencias necesarias para cada uno de los centros que usaran el sistema, así como para cada uno de los equipos que se relacionan en el alcance, y trabajos de configuración, en las unidades de imagen relacionadas para el envío de las imágenes en los formatos requeridos por el sistema de planificación. Sin ser exhaustivos, el sistema deberá importar imágenes de forma correcta de al menos los sistemas CT, RM, y PET, PET/CT disponibles en los centros objeto del servicio.
b) Activación de las licencias necesarias, y trabajos de configuración, en las unidades de tratamiento y redes de registro y verificación, sistemas de verificación por imagen/superficie relacionadas, en los formatos requeridos por las mismas.
c) Mantener en condiciones de uso por parte de los usuarios el sistema de planificación.
d) Proporcionar una herramienta que configure un cuadro de mandos del sistema en el que se refleje el número de pacientes existentes, la etapa de trabajo en la que se encuentra, el espacio disponible en disco, usuarios conectados, licencias existentes y consumidas, y los parámetros que se consideren relevantes para la vigilancia del funcionamiento del sistema.
e) Garantizar la interoperabilidad necesaria de los datos demográficos e identificadores de paciente entre el sistema de planificación y la red de gestión hospitalaria del Servicio Andaluz de Salud, incluyendo el envío del informe resumen de la planificación dosimétrica a la historia clínica del paciente.

La capacidad de computación suministrada e instalada por el contratista, como parte del servicio, así como el espacio de almacenamiento, tendrán la dimensión suficiente para que en caso de que algún dispositivo hardware sufra una parada, el resto de elementos sean redundantes y suficientes para ser capaces de soportar el trabajo restante.

Se asegurará la alta disponibilidad del sistema (software y hardware), en los términos que se definen en el punto 13. “Modelo de seguimiento técnico del contrato”, del presente pliego técnico. Por ello, se deberá asegurar la respuesta inmediata a incidencias inesperadas y malos funcionamientos de los sistemas objeto de este contrato. Asegurar en todo momento la estabilidad y alta disponibilidad de la plataforma para, además de por la acción inmediata y coordinada ante incidencias, por una correcta actualización de la misma, un adecuado soporte preventivo y una monitorización continuada.

El contratista deberá proporcionar una licencia corporativa del mismo; es decir, no existirá limitación respecto del número y tipo de usuarios que podrán acceder y usar el sistema de información, así como en cuanto al número de centros a implantar o equipos a conectar al sistema de información ofertado. Además, tampoco habrá ningún tipo de limitación en cuanto al número de transacciones, integraciones, registros, documentos y/o expedientes de cualquier tipo o instancia.

El contrato también incluirá la conexión sin coste de los nuevos equipos que sean adquiridos por el SAS durante el periodo de vigencia de la presente contratación.

REQUISITOS TÉCNICOS MÍNIMOS		
REQUISITO	**DESCRIPCIÓN**	**Valor binario (SÍ/NO)**
Sistema de planificación de tratamientos		
REQ OBL TEC. 1	El sistema de planificación debe estar virtualizado a nivel de cliente. Es decir, las aplicaciones deben poderse ejecutar desde un ordenador convencional, con un sistema operativo convencional, que no exija ningún requerimiento especial de hardware en el cliente.	
REQ OBL TEC. 2	**En el caso del lote 1**. Deberán ofrecerse un total de 47 licencias que permitan el diseño de tratamiento y cálculo y optimización de forma concurrente y otras 55 licencias que permitan contorneo de volúmenes de interés y evaluación y exportación de planes de modo concurrente.	
REQ OBL TEC. 3	**En el caso del lote 2.** Deberán ofrecerse un total de 45 licencias que permitan el diseño de tratamiento y cálculo y optimización de forma concurrente y otras 52 licencias que permitan contorneo de volúmenes de interés y evaluación y exportación de planes de modo concurrente.	
REQ OBL TEC 4	**En el caso del lote 3**. Deberán ofrecerse un total de 18 licencias que permitan el diseño de tratamiento y cálculo y optimización de forma concurrente y otras 20 licencias que permitan contorneo de volúmenes de interés y evaluación y exportación de planes de modo concurrente.	
REQ OBL TEC 5	Incluir todo el hardware y servidores necesarios para la activación de esta solución, debiendo desglosarse la relación del mismo y su capacidad. Cálculo sobre tarjeta gráfica o GPU.	
REQ OBL TEC 6	Cada una de las licencias y funcionalidades ofertadas debe poder ser activada de forma individual a discreción única del Servicio Andaluz de Salud, de modo que las licencias o funcionalidades inactivas no incurran en gastos de mantenimiento.	

REQ OBL TEC 7	El contratista debe hacerse cargo de la copia de seguridad (incluyendo el hardware necesario para ella) de toda la información almacenada en el sistema de planificación. La capacidad de almacenamiento debe ser tal para cubrir un mínimo de todos los pacientes nuevos al año, para un sistema con un nivel de disponibilidad MEDIO, con RTO entre 4 horas < RTO < 1 día (RTO - Tiempo de Recuperación Objetivo)	
REQ OBL TEC 8	El sistema debe ser compatible con el software de seguridad (ENDPOINT DETECTION AND RESPONSE -EDR) del Servicio Andaluz de Salud.	
REQ OBL TEC 9	El tiempo que el sistema empleará en realizar la planificación, por tipología de tratamiento, y para un paciente que se tome como estándar, será el valor basal que se mantendrá a lo largo del expediente, siempre que sea por causas atribuibles a los medios aportados por el contratista. (Estos valores serán consignados en el acta de puesta disposición del sistema de planificación).	
Infraestructura		
REQ OBL TEC 10	Gestión de pacientes, Realización de backup de pacientes.	
REQ OBL TEC 11	Gestión de usuarios mediante directorio activo LDAP del SAS.	
Capacidades de exportación/importación/interoperatibilidad / compatibilidad		
REQ OBL TEC 12	Exportar a programas externos (verificación y dosimetría in vivo)	
REQ OBL TEC 13	Capacidad de modificación del nombre de las estructuras generadas por el contorneo automático para facilitar explotación de datos.	

Servicio de gestión de cambios y versiones.

La persona contratista, a través de la empresa desarrolladora y propietaria intelectual de los productos software objeto del contrato, se comprometerá a llevar a cabo una gestión de cambios y versiones de

las licencias software objeto de esta contratación. Quedará garantizada la capacidad para acceder a las actualizaciones y las nuevas versiones software de los productos contratados que se publiquen durante el período de garantía contratado, lo cual incluye las siguientes prestaciones:

- Acceso a nuevas versiones debido al mantenimiento correctivo, evolutivo, perfectivo y adaptativo del software.
- Acceso a actualizaciones de versiones y configuraciones que resulten de cambios introducidos por problemas de cualquier índole, tales como los de interoperabilidad con otros fabricantes y/o aplicaciones.
- Acceso a parches, actualizaciones menores y *hotfixes*.

La persona contratista, a través de la empresa desarrolladora y propietaria intelectual de los productos software objeto del contrato, será responsable de informar cada vez que se libere una nueva versión del producto, y deberá efectuar la entrega de las nuevas versiones por los medios electrónicos adecuados. Previamente, entregará una lista de las nuevas funcionalidades de la versión, que incluirán mejoras generales, nuevas funcionalidades y/o correcciones a "*bugs*".

Servicio de asistencia técnica multicanal.

La persona contratista, a través de la empresa desarrolladora y propietaria intelectual de los productos software objeto del contrato, se comprometerá a llevar a cabo un servicio asistencia técnica multicanal sobre las licencias software objeto de esta contratación, que se traducirá en las siguientes prestaciones:

- Atención y resolución de incidencias, problemas, dudas y consultas sobre los productos suministrados, participando del:

  - Proceso de gestión de incidencias, con objeto de restaurar los servicios TIC lo más rápidamente posible ante la aparición de cualquier incidente y/o mal funcionamiento, y resolver aquellas solicitudes que necesiten de una capacidad o conocimiento experto para su resolución, cuando el grado de complejidad así lo requiera.
  - Proceso de gestión de problemas, con objeto de gestionar las causas subyacentes de las incidencias que impacten sobre los sistemas de información del SAS y la infraestructura técnica que los soporta. El alcance va desde que se identifica un problema, ya sea de manera proactiva o reactiva, hasta la petición de cambio a gestión de cambios que da solución al error identificado.
  - Proceso de gestión de peticiones, con objeto de dar respuesta ágil y ordenada de todas las peticiones derivadas por el SAS y relacionadas con los productos suministrados.
  - Interacción on-line con técnicos especializados.
  - Acceso multicanal: telefónico, email, web de soporte.

- Informe sobre posibles incompatibilidades de los productos contratados con otras herramientas o software de base (sistemas operativos, sistemas gestores de bases de datos, antivirus, etc.).

- Acceso a las bases de datos de conocimiento y a información sobre el software y la tecnología de los productos contratados.

- Adiestramiento en los productos contratados o ante nuevas versiones que modifiquen sustancialmente el producto inicial.

9. REQUISITOS DE LICENCIAMIENTO.

Será imprescindible cumplir con todos y cada uno de los requisitos de licenciamiento. En caso contrario, la oferta no será admitida.

La solución propuesta, así como la configuración y tipo de licenciamiento ofertado, deberá cubrir la totalidad de requisitos recogidos en el presente pliego, así como las posibles mejoras propuestas por la empresa contratista, y permitir su instalación según las condiciones de disponibilidad, redundancia, necesidad de entornos, seguridad, etc.

Esta licencia corporativa tendrá un carácter permanente, es decir, transcurrido el período de garantía, deberá seguir usándose, sin otros costes adicionales.

La adquisición e implantación del sistema de planificación objeto de este contrato incluirá las siguientes capacidades durante el plazo de ejecución del contrato, en la medida que un centro correctamente implantado pasará a estar amparado por las prestaciones aquí definidas, y el periodo de garantía de esta contratación. Estas capacidades deberán ser desarrolladas por la empresa contratista a través de la empresa desarrolladora y propietaria intelectual de los productos software objeto del contrato, en el caso de que los productos software ofertados estén basado en tecnología propietaria, o a través de una empresa con soporte oficial o que participe activamente en el desarrollo de los productos propuestos, en el caso de que los productos software ofertados estén basados en fuentes abiertas.

En relación con la gestión de cambios y versiones de los productos software objeto de esta contratación, quedará garantizada la capacidad para acceder a las actualizaciones y las nuevas versiones software de los productos contratados que se publiquen en cualquiera de las plataformas en las que estén disponibles, lo cual incluye las siguientes prestaciones:

- Acceso a nuevas versiones debido al mantenimiento correctivo, evolutivo, perfectivo y adaptativo del software.
- Acceso a actualización de las versiones de los productos y configuraciones que resulten de cambios introducidos por problemas de cualquier índole, tales como los de interoperabilidad con otros fabricantes y/o aplicaciones.

Acceso a parches, actualizaciones menores y soluciones puntuales a los fallos de funcionamiento.

La empresa contratista será responsable de informar cada vez que se libere una nueva versión del producto, y deberá efectuar la entrega de las nuevas versiones por los medios electrónicos adecuados. Previamente, entregará una lista de las nuevas funcionalidades de la versión, que incluirán mejoras generales, nuevas funcionalidades y/o correcciones de errores.

El almacenamiento ofertado deberá garantizar la redundancia de los datos a través de técnicas de replicación del dato.

El servicio de disponibilidad tecnológica de las licencias software contemplarán las siguientes actividades:

- Servicio de gestión de cambios y versiones: actualización a nuevas versiones del software, acceso a parches y *hotfixes*, sin ningún tipo de limitación, del producto.
- Asistencia técnica multicanal.

10. MODELO DE SEGUIMIENTO TÉCNICO DEL CONTRATO.

La medida de la disponibilidad tecnológica se establece como el cociente entre el tiempo, en horas, que el equipo ha estado realmente operativo y el tiempo teórico que debería haber estado operativo, incluyendo fines de semana y festivos, en función de los requerimientos del equipo o instalación y descontando los mantenimientos preventivos, predictivos y legales, etc. Su formulación es:

PDE (%) = 100 x $PDE(\%) = 100 * \frac{\text{T.T.D.}-\text{T.M.N.}-\text{T.P.}}{\text{T.T.D.}-\text{T.M.N}}$

Donde:

- **Tiempo de Parada (TP)**: es el número de horas de parada del equipo medido para un periodo de tiempo dado y en una franja horaria diaria de 24 horas de lunes a domingo.

- **Tiempo Teórico Disponible (TTD)**: es el número de horas que una instalación o equipo debería estar funcionando o en condiciones de uso, en un determinado periodo de tiempo y en una franja horaria diaria como máximo de 24 horas de lunes a domingo.

- **Tiempo Mantenimiento No Correctivo (TMN)**: es el número de horas que una instalación o equipo se encuentra fuera de servicio, durante un determinado periodo de tiempo, por labores de mantenimiento preventivo, predictivo o por actualización o revisiones legales. Estos tiempos serán los declarados por la empresa contratista, conforme a la Planificación del mantenimiento correspondiente anual o con acuerdo previo de intervención entre el responsable del contrato y el prestador del servicio, pudiendo ser comprobados por el responsable de la Unidad clínica, Sección o Servicio de Electromedicina, y por el responsable del contrato. En los casos en los que las tareas de mantenimientos preventivos, predictivos o por actualización o revisiones legales, se realicen fuera del horario definido en el TTD, no serán considerados en el término TMN y por tanto, no contribuirán a disminuir el PDE.

Para el cálculo del Porcentaje de Disponibilidad Efectiva (PDE) se considerará disponible un equipo o sistema cuando esté funcionando y cuando se encuentre en condiciones de funcionar. El contador de este parámetro se pone en marcha cuando existe una comunicación en la herramienta GMAO de equipo parado, y se paraliza el mismo cuando se realiza un cierre técnico de dicho aviso. Si existen evidencias que el cierre técnico no debería haberse producido porque el equipo no está funcional, se pondrá en marcha de nuevo el contador de parada de equipo y el cierre, cuando el equipo esté funcional, será dado por el centro como cierre administrativo o definitivo. La fuente de cálculo será el software de gestión de activos, en adelante GMAO, del Centro. Los tiempos de paradas por causas ajenas al contratista (corte en el suministro eléctrico, en las comunicaciones, por uso indebido intencionado probado y documentado) no computarán a efectos de disponibilidad.
Para calcular el tiempo de parada se restará el tiempo que transcurra entre el momento del aviso dado por el personal autorizado del Centro, y la fecha y hora del restablecimiento del funcionamiento normal del equipo o sistema. Cuando un equipo se encuentre parado se identificará en la

herramienta GMAO como parado cuando se cree su aviso correspondiente. Y el cierre de la orden de trabajo se realizará en el momento que el equipo ha sido restituido a su estado para la contabilización real del tiempo de parada. No podrán imputarse retrasos en los valores consignados en el GMAO sobre actuaciones finalizadas, como por ejemplo la falta de recursos humanos para cerrar dicha orden de trabajo. Los tiempos de parada por preventivos, técnicos legales, predictivos, actualizaciones serán los declarados por el contratista.

En el denominador de la fórmula del PDE pueden reflejarse otros tiempos como contingencias no relacionadas con el contratista como catástrofes, sabotajes, robos (estos dos últimos deben quedar suficientemente acreditados para que puedan ser admitidos).

En los casos que se le solicite, el contratista estará obligado a presentar los datos, en formato digital, que obran en su propiedad de las horas y fechas de parada y restitución de los equipos.

El control y seguimiento de este indicador se realizará mensualmente, salvo que se determine otro periodo por la Dirección de cada Centro.

El PDE de las instalaciones descritas en el PPT se medirá mensualmente sobre los datos obtenidos del mes natural anterior cumplido a la fecha de análisis, se realizará para el primer mes natural completo tras la incorporación de la información de equipos y sistemas en el GMAO, 30 días después que el contratista disponga de la licencia del mismo. Este informe será desarrollado para cada uno de los Centros objeto del presente contrato, y entregado en formato digital a la Dirección de Gestión del Centro o persona en quien delegue, de cada Centro, y al Responsable del Contrato.

El tiempo esperado de disponibilidad se calcula para un periodo de **14 h/día** en cada uno de los días del periodo de **lunes a sábado**. De esta forma en un trimestre con posee 13 semanas el tiempo de disponibilidad esperado sería de 14 horas/día, 6días/semana, daría un Tiempo Teórico Disponible (TTD) es de: **1.092 horas/trimestre**.

El tiempo de disponibilidad real será el tiempo esperado de disponibilidad expresado en horas descontando la duración de la interrupción de prestación del servicio contada desde su primera comunicación en **Ayuda Digital** hasta la conformidad de solución por parte del usuario o el responsable del contrato, descontando en dicho cómputo el horario de 22:00h a 8:00h. De esta forma una incidencia comunicada a las 18:00h y confirmada su resolución a las 10:00h del día siguiente descontaría un total de 6 horas a la disponibilidad. Y una incidencia comunicada a las 8:00h y solucionada a las 10:00h del día siguiente descontaría un total de 16 horas de la disponibilidad esperada.

El valor exigido de PDE mínimo es del 98 %, o el ofertado por el contratista.

10.1. Control y seguimiento del contrato.

10.1.1. Informe mensual.

El contratista emitirá los siguientes informes, con periodicidad mensual, antes del décimo día del mes siguiente al del análisis, sobre el uso y paradas del sistema de planificación junto con la estadística del uso de licencias y simultaneidad del uso de las mismas, y dirigirlo al responsable del Contrato:
En particular, y como mínimo, se señalarán:

- Número máximo diario de accesos/usuarios concurrentes al sistema.
- Número de veces en los que se genere una cola de pacientes en espera de optimización y cálculo.
- Tiempo medio de optimización por paciente (incluyendo cálculo de dosis)
- Tiempo medio de cálculo por paciente (exclusivamente cálculo de dosis).
- Número de pacientes existentes en el sistema de planificación y espacio ocupado en disco, desagregados por centro si procede.

10.1.2. Informe anual.

El contratista emitirá los siguientes informes, con periodicidad anual, antes del día trigésimo del mes de enero del año siguiente al del informe, sobre el desarrollo del Programa llevado a cabo durante el año finalizado, y dirigirlo al responsable del Contrato, con la agrupación de los informes mensuales del año en evaluación, el listado y análisis de las intervenciones realizadas, el número total de pacientes planificados por centro, el volumen ocupado de backup y archivado.

10.1.3. Gestión de la documentación.

Toda la documentación generada para este servicio, y regula este PPT, será alojada en un servidor de información que dispondrá el SAS, y será el contratista el que remita, por un medio verificable, la información que sea de su obligación, denominando los archivos con un descriptivo que declare de forma general el contenido del archivo seguido de la fecha de creación de dicho archivo en el formato de AÑOMESDIA. Por ejemplo, el informe mensual del desarrollo del programa en formato Openoffice®, sería 'Informe enero TPSRT 20200224.odt'.

10.2. Disponibilidad pública del software

De conformidad con lo establecido en la orden de 21 de febrero de 2005, sobre disponibilidad pública de los programas informáticos de la administración de la Junta de Andalucía y de sus organismos autónomos, el sistema de información desarrollado pasará a formar parte del repositorio de software libre de la Junta de Andalucía, en las condiciones especificadas en la citada orden. La persona contratista deberá entregar el código fuente del sistema de información desarrollado, así como la documentación asociada y la información adicional necesaria, en un formato directamente integrable en el repositorio de software libre de la Junta de Andalucía. De esta obligación quedarán exentos todos aquellos componentes, productos y herramientas que, no habiéndose producido como consecuencia de la ejecución del contrato, estén protegidos por derechos de propiedad intelectual o industrial que no permitan la libre distribución o el acceso al código fuente.
La aplicación desarrollada será publicada en el repositorio de software libre de la Junta de Andalucía; viniendo acompañada, además, junto con el software, de la documentación completa, en formato electrónico, referente tanto al análisis y descripción de la solución así como del correspondiente manual de usuario, con objeto de que este software pueda fácilmente ser usable.

10.3. Documentación y notificación.

1. El contratista mantendrá una documentación detallada para el seguimiento y registro de todas las actualizaciones aplicadas, incluyendo la fecha, el contenido de las actualizaciones y los dispositivos afectados.
2. Se notificará e informará a los usuarios y al personal relevante sobre las actualizaciones realizadas y cualquier cambio esperado en el funcionamiento del dispositivo.

3. 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.

10.4. Control y supervisión de la prestación del servicio.

El SAS designará un responsable del Contrato (art. 62 de la LCSP), así como los recursos humanos que estime necesarios para la supervisión, control y comprobación de la correcta prestación del objeto del contrato, entre los cuales cabe destacar, al menos:

a) Un responsable del Contrato que coordinará la ejecución de acuerdo con este pliego de prescripciones técnicas.
b) Una Comisión de Seguimiento del Programa (CSP).

La comunicación se establecerá principalmente entre los interlocutores nombrados por ambas partes. Debiendo, para ello, el contratista nombrar, de forma fehaciente, y comunicar al responsable del contrato del SAS, un responsable técnico del contrato.

10.5. Seguimiento de la ejecución del contrato.

Para verificar el cumplimiento del objeto de esta contratación se establecerá un sistema de gestión de la calidad de la prestación del servicio que podrá motivar, en cualquier momento, declaraciones de cumplimiento defectuoso del contrato, y por tanto provocar el inicio de expediente de penalización, a juicio de las diferentes comisiones de seguimiento o del responsable del contrato.

Para el seguimiento del cumplimiento de la prestación del servicio se establece el siguiente a nivel regional:

El órgano de contratación del servicio constituirá una comisión regional para el seguimiento (CSP) del propio contrato. La misma estará constituida por el responsable del contrato, por representante de la Dirección General de Asistencia Sanitaria y Resultados en Salud, un representante de la Dirección de

Tecnologías de la Información y las Comunicaciones del SAS, dos FEA Radiofísica Hospitalaria así como el personal que designe la Dirección Gerencia del SAS.

La CSP se reunirá, con la periodicidad que ésta establezca, para analizar el grado de cumplimiento del objeto de esta contratación a través de los informes de incidencias o evidencias de incumplimiento recibidos de los distintos integrantes de la propia comisión.

10.6. Adopción de decisiones del responsable del contrato.

El artículo 62 de la ley de contratos Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, dice literalmente "…los órganos de contratación deberán designar un responsable del contrato al que corresponderá supervisar su ejecución y adoptar las decisiones y dictar las instrucciones necesarias con el fin de asegurar la correcta realización de la prestación pactada". En concordancia con el citado artículo, el responsable del contrato podrá adoptar las decisiones que considere, con el único objetivo de asegurar la correcta realización de la prestación pactada, y siempre teniendo en cuenta el mutuo acuerdo entre las partes, Administración y empresa contratista.

Relación, no exhaustiva, de decisiones que podrían ser tomadas por el responsable del contrato:

- Cambio de servidores físicos por virtuales.
- Configuraciones de conexión de equipos informáticos.
- Distribución de licencias y enclavamiento de las mismas.
- Nomenclaturas y estandarización.

10.7. Parámetros de calidad

Por la importancia que tienen en el objetivo final pretendido, esto es, la planificación de tratamientos de radioterapia, los parámetros que tendrán la consideración de especial relevancia en cuanto a la calidad del servicio prestado, son los que se describen a continuación:

- Redundancia del sistema que maximice la ausencia de paradas del sistema.
- Estabilidad del tiempo de cálculo.
- Trasparencia de la gestión de colas de cálculo (p.e. mostrando el número de cálculos en espera o el tiempo esperado hasta iniciar)
- Estabilidad de la accesibilidad al sistema.

10.7.1. Acuerdos de nivel de servicio de la garantía.

Como medio para garantizar la calidad de la garantía, se establecerán unos ANS y el compromiso por parte de la persona contratista de cumplirlos. Estos ANS podrán evolucionar a lo largo de la ejecución del contrato con el fin de conseguir una mejora continua en la calidad del servicio efectivamente proporcionado. Los recursos, tanto humanos como de otra índole, disponibles para el servicio de garantía, deberán ser dimensionados de forma cualitativa y cuantitativa como mínimo para garantizar los ANS vigentes en cada momento.

Los ANS se basarán en la definición de unos indicadores de calidad que reflejen de forma objetiva la calidad del servicio 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. Se han elaborado atendiendo a los siguientes criterios:

- El establecimiento de indicadores de calidad del servicio de garantía prestado, de manera que el SAS pueda realizar una evaluación objetiva de los servicios y que la persona contratista de esta licitación tenga una base para la corrección de las eventuales deficiencias en la prestación y para la mejora de sus procesos y organización.
- La automatización del seguimiento y control de los indicadores de calidad del servicio de garantía recogidos en los ANS. Los datos para la revisión de los indicadores del ANS se obtendrán de las distintas herramientas ya implantadas en el SAS.
- La persona contratista se comprometerá a realizar todas las acciones organizativas necesarias para permitir un adecuado control de todos los ANS identificados como mínimos en este pliego.

El SAS, a través del responsable del contrato, podrá proponer cambios en la estructura de los ANS mínimos requeridos, que en todo caso deberán ser consensuados con la persona contratista. Los cambios podrán afectar tanto a los elementos del servicio objeto de medición como a la frecuencia, la unidad de medición y el nivel de servicio.

Condiciones de medida

En el cálculo de los indicadores no se contabilizarán los tiempos que se indican a continuación:

- No contabilizarán como tiempo de indisponibilidad las paradas programadas que se realicen en las condiciones preestablecidas y acordadas.
- 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.).
- Pérdidas de servicio debidas a causa de fuerza mayor (incendios, inundaciones, etc.), aunque en este caso se aplicarán los acuerdos alcanzados en el proceso de continuidad.

La persona contratista garantizará el tiempo máximo de diagnóstico (definición de la naturaleza y origen/causa de la incidencia mediante el uso de la información disponible) y, en su caso, de resolución o indicación de las medidas a adoptar para su resolución, en función de la prioridad de la incidencia.

PRIORIDAD	**SIGNIFICADO**
Muy alta	Todas las funciones, o una proporción substancial de las funciones de las licencias, no están disponibles y no hay un “workaround” posible, o va tan lento que los tiempos de respuesta lo hacen inutilizable, y/o hay un problema que ha causado o tiene el potencial de provocar una interrupción significativa del funcionamiento de los sistemas
Alta	Las funciones o una proporción substancial de las funciones de las licencias no están disponibles y hay un “workaround” posible, o ha disminuido su rendimiento de tal forma que los tiempos de respuesta hacen muy difícil el uso de los sistemas y/o hay un problema que causa o tiene potencial de provocar una interrupción significativa del funcionamiento de la red.
Normal	Alguna función de las licencias no está disponible o ha disminuido su rendimiento, de tal forma que impacta en la reducción de eficiencia de

	usuarios finales pero que un “workaround” puede ser aceptable para el cliente y se propone e implementa por la persona contratista.

Indicadores

El seguimiento de los niveles de servicio se realizará en base a indicadores. 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 el espacio de Normativa TIC.

La persona contratista garantizará que el tiempo máximo de diagnóstico y resolución de la incidencia, en función de la prioridad de la misma, será de:

PRIORIDAD	TIEMPO DE RESOLUCIÓN
MUY ALTA	TRmax1: 24 horas desde el momento de notificación de la incidencia.
ALTA	TRmax2: 48 horas desde el momento de notificación de la incidencia.
NORMAL	TRmax3: 72 horas desde el momento de notificación de la incidencia.

Donde:

- TRmax1 es el tiempo máximo de diagnóstico y resolución de incidencias de prioridad MUY ALTA.
- TRmax2 es el tiempo máximo de diagnóstico y resolución de incidencias de prioridad ALTA.
- TRmax3 es el tiempo máximo de diagnóstico y resolución de incidencias de prioridad NORMAL.

La persona contratista deberá definir la naturaleza y origen/causa de la incidencia mediante el uso de la información disponible y, en su caso, indicar las medidas a adoptar para su resolución.

11. NORMATIVA.

En el desarrollo de la prestación del servicio, el contratista deberá cumplir toda la normativa aplicable, tanto nacional, como autonómica y local, sea de índole técnica, laboral, social, administrativa, etc., incluyendo también la que pudiera producirse durante el período de vigencia del contrato. Debido a la naturaleza del objeto del contrato, se deberá prestar una especial atención al Real Decreto 192/2023, de 21 de marzo, por el que se regulan los productos sanitarios.

Además, el contratista deberá cumplir la normativa interna del Servicio Andaluz de Salud y las de régimen interior del centro de destino que pudiera afectarle, en particular las relativas a las actuaciones a realizar en el mismo.

ANEXO I. MEDIDAS SOBRE CIBERSEGURIDAD

Régimen de la seguridad de la información

El artículo 2 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad ("ENS") dispone que los pliegos de prescripciones administrativas o técnicas de los contratos, que celebren las entidades del sector público incluidas en el ámbito de aplicación del ENS, contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con éste de los sistemas de información en que se sustenten los servicios prestados por los contratistas, como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS

En consecuencia, el Servicio Andaluz de Salud considera necesario que los proveedores que vayan a concurrir a la licitación deben estar en condiciones de exhibir, con carácter previo a la formalización del contrato, la correspondiente Certificación de Conformidad con el ENS, o una Declaración de Conformidad con el ENS únicamente cuando se haya declarado categoría BÁSICA del sistema para el que concurren.

Así pues, en base a lo anterior y al análisis de los riesgos a que están expuestos los servicios objeto de la licitación, el Servicio Andaluz de Salud establece que el contratista esté en condiciones de exhibir la correspondiente Declaración o Certificación de Conformidad con el ENS para la categoría de seguridad ALTA, así como mantener la conformidad en vigor durante la vigencia del contrato. Esta Declaración o Certificación de Conformidad con el ENS se entiende que debe incluir en su alcance, como mínimo, el ámbito objeto de la contratación.

La conformidad con el ENS se establece como una obligación esencial de este contrato, de manera que en caso de que el contratista no pueda mantener la conformidad con el ENS durante la vigencia del contrato -por pérdida, retirada o suspensión de la Certificación de Conformidad o imposibilidad de mantener la Declaración de Conformidad- deberá comunicar esta circunstancia, de forma inmediata y sin dilación indebida, al Servicio Andaluz de Salud, quien considerará el impacto de esta circunstancia en la prestación objeto del contrato, pudiendo suponer una causa de resolución del contrato.

En este sentido, el contratista será responsable de la seguridad y el buen uso de la información y los medios electrónicos requeridos para la ejecución del contrato. A tal efecto, además del ENS y los requisitos de seguridad aplicables de las guías CCN-TIC, el contratista deberá conocer y aplicar la normativa interna de seguridad de la entidad del **Anexo I**, que irá reflejada la declaración de aplicabilidad del contratista del **Anexo II**.

Se deja expresa constancia que en el caso que el contratista trate con datos personales por cuenta de el Servicio Andaluz de Salud como consecuencia de la ejecución del contrato objeto de licitación deberá suscribirse el correspondiente acuerdo de encargado de tratamiento de datos personales que se adjunta en el contrato.

El contratista se obliga a que los productos que lleven incorporados programas informáticos, para los programas informáticos que constituyan productos por sí mismos o cualquier producto que se conecte a las redes de los centros sanitarios, se desarrollen y fabriquen basándose en el estado actual de la técnica, teniendo en cuenta los principios de ciclo de vida del desarrollo, gestión de los riesgos, incluida la seguridad de la información, validación y verificación.

Asimismo, el contratista deberá cumplir con las siguientes obligaciones relativas a la seguridad de la información:

Designación de un Punto o Persona de contacto (POC)
Comunicar al Servicio Andaluz de Salud el nombre y los datos de la persona designada como punto de contacto del adjudicatario, quien podrá ser el propio Responsable de Seguridad del adjudicatario, alguien que forme parte de su área o bien tenga comunicación directa con ésta. Esta persona tendrá la obligación de garantizar el cumplimiento de esta cláusula, así como canalizar las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes derivados de la ejecución del contrato.

En caso de que el Servicio Andaluz de Salud haya designado a un Delegado de Protección de Datos ("**DPD**"), ésta facilitará sus datos de contacto.

Personal cualificado

Contar con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios contratados y, a tal efecto, formar e informar a su personal sobre sus deberes, obligaciones y responsabilidades en materia de seguridad.
Vigilancia continua

Aplicar medidas que permitan la evaluación permanente del estado de la seguridad de los activos de manera que se permita al contratante medir su evolución, detectar vulnerabilidades, comportamientos anómalos o deficiencias de configuración, así como su oportuna respuesta.

Certificaciones:

Que los productos de seguridad o los servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser utilizados en los sistemas de información del Servicio Andaluz de Salud se encuentren en el *Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación* (CPSTIC) del Centro Criptológico Nacional o bien tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, de acuerdo con el artículo 19 del ENS.

Interconexión:

No intercambiar información y prestar servicios con otros sistemas, salvo que previamente haya sido autorizado expresamente por la entidad contratante.

Asimismo, en caso de que se autorice una interconexión, colaborar con la entidad contratante en el análisis de riesgos derivados de la misma y, en concreto, documentar las características de la interfaz, los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada.

ANEXO II. MEDIDAS DE SEGURIDAD MÍNIMAS PARA LOS PRODUCTOS QUE LLEVEN INCORPORADOS PROGRAMAS INFORMÁTICOS, PARA LOS PROGRAMAS INFORMÁTICOS QUE CONSTITUYAN PRODUCTOS POR SÍ MISMOS O CUALQUIER PRODUCTO QUE SE CONECTE A LAS REDES DE LOS CENTROS SANITARIOS

Se relacionan a continuación las medidas y controles de seguridad mínimos incluidas en el RD 311/2022 Esquema Nacional de Seguridad ENS que debe cumplir el contratista del concurso público para la adquisición de Dispositivos Médicos que incorporen programas informáticos (software) o para los programas informáticos que constituyan dispositivos médicos por sí mismos. Estas medidas de seguridad deben estar activas en el momento del despliegue o implantación de los dispositivos adquiridos en los centros sanitarios.

Será el contratista el responsable de establecer las medidas y controles de seguridad relacionados a continuación. Estas se aplicarán siempre de forma que no afecten a la disponibilidad y rendimiento de los dispositivos médicos implicados.

1. Política de Gestión de Vulnerabilidades

1. Cláusula: Proceso de Identificación y Gestión de Vulnerabilidades

1. El contratista deberá implementar y mantener un proceso continuo y proactivo para la identificación y gestión de vulnerabilidades a lo largo del ciclo de vida de todos sus productos. Este proceso incluirá la consulta regular a bases de datos públicas de vulnerabilidades reconocidas internacionalmente, así como el uso de fuentes de inteligencia de amenazas como informes de ciberseguridad y bases de datos de vulnerabilidades.

2. Cláusula: Análisis Regular de Vulnerabilidades

1. El contratista realizará análisis de vulnerabilidades periódicos en los dispositivos médicos objeto del contrato, utilizando herramientas avanzadas de escaneo y pruebas de penetración.
2. Los análisis podrán ser realizados en las instalaciones del adjudicatario, del fabricante del dispositivo, o cualquier otra ubicación adecuada, y podrán ser llevados a cabo directamente por el contratista o por terceros autorizados.
3. El contratista documentará de manera exhaustiva las vulnerabilidades conocidas y potenciales identificadas en cada dispositivo, asegurando una transparencia total en los resultados.

3. Cláusula: Notificación y Plan de Corrección

1. El contratista notificará debida y regularmente a la *Servicio Andaluz de Salud* los resultados de los análisis de vulnerabilidades llevados a cabo, proponiendo además un plan de corrección y priorización de las debilidades en los dispositivos médicos para ser aplicado sobre los dispositivos desplegados en las instalaciones de la *Servicio Andaluz de Salud*.
2. Los dispositivos médicos adquiridos deberán implantarse en los centros sanitarios inicialmente libres de vulnerabilidades conocidas. En todo caso, si por razones técnicas o legales no fuera posible llevar a cabo un despliegue inicial libre de vulnerabilidades conocidas, el contratista

deberá entregar el último análisis de vulnerabilidades donde se identificarán las vulnerabilidades conocidas hasta la fecha de los dispositivos médicos a desplegar en los centros sanitarios, así como el plan correspondiente plan de corrección y priorización de estas.

4. Cláusula: Implantación Inicial Libre de Vulnerabilidades

1. Los dispositivos médicos adquiridos deberán ser implantados en los centros sanitarios libres de vulnerabilidades conocidas en el momento de la instalación.
2. En caso de que, por razones técnicas o legales, no sea posible un despliegue inicial completamente libre de vulnerabilidades conocidas, el contratista deberá proporcionar al cliente el último informe de análisis de vulnerabilidades. Este informe debe identificar las vulnerabilidades conocidas hasta la fecha y presentar un plan de corrección y priorización correspondiente. En este caso el contratista especificará los mecanismos habilitados para la remediación continua de todas las vulnerabilidades no corregidas en el momento de la puesta en producción del dispositivo.

2. Auditoría y Registro de Actividad:

5. Cláusula: Registros de Seguridad y Configuración de Logs

1. Los sistemas de información asociados a los dispositivos médicos, así como, en su caso, los propios dispositivos médicos, deberán permitir la activación y configuración de registros de seguridad. Estos sistemas deben ser capaces de registrar eventos de seguridad importantes de manera detallada y continua.
2. Se mantendrán logs detallados de todas las actividades de acceso a los dispositivos y sistemas, incluyendo accesos exitosos, intentos fallidos, cambios en la configuración, y cualquier otra actividad relevante.
3. La configuración de los dispositivos debe permitir establecer políticas de retención de logs adecuadas para asegurar que los registros estén disponibles para auditoría durante un período determinado, de acuerdo con las mejores prácticas y regulaciones aplicables.

6. Cláusula: Monitorización Continua y Revisión de Auditoría

1. Los dispositivos médicos y sus sistemas de información relacionados deberán permitir la monitorización continua mediante sistemas automatizados desplegados por la *Servicio Andaluz de Salud para la* detección de intrusiones, accesos no autorizados, actividades sospechosas o no autorizadas.
2. Los dispositivos médicos y sus sistemas de información relacionados dispondrá de la capacidad necesaria para que la *Servicio Andaluz de Salud* pueda llevar a cabo revisiones periódicas de los registros de auditoría para identificar cualquier acceso no autorizado o actividad sospechosa.

3. Autenticación y Autorización:

7. Cláusula: Sistemas de Control de Acceso y Autenticación

1. Los dispositivos médicos y sus sistemas de información relacionados deberán disponer de un sistema de control de acceso robusto que garantice que solo el personal autorizado pueda acceder a los datos personales de los pacientes.
2. Se establecerán controles de acceso basados en roles que aseguren que solo el personal con las credenciales apropiadas pueda realizar acciones específicas dentro del sistema, limitando el acceso a funciones críticas según las responsabilidades de cada usuario.

8. Cláusula: Procedimientos de Autorización de Acceso

1. Los mecanismos de control de acceso deben estar alineados con los procedimientos establecidos por la *Servicio Andaluz de Salud* para las autorizaciones de acceso a los dispositivos y sus sistemas de información relacionados.
2. Las políticas de acceso y autorización serán revisadas y actualizadas periódicamente por el contratista para reflejar cambios en el personal y las necesidades de seguridad, garantizando que solo el personal necesario tenga acceso a información sensible.
3. La *Servicio Andaluz de Salud* podrá llevar a cabo auditorías regulares para asegurar el cumplimiento de los procedimientos de autorización de acceso y para identificar y corregir cualquier desviación.

4. Configuración Segura

9. Cláusula: Configuración Inicial Segura

1. El contratista garantizará que todos los dispositivos médicos sean configurados inicialmente con una configuración segura, evitando el uso de configuraciones predeterminadas inseguras.
2. La configuración de seguridad inicial seguirá las recomendaciones del fabricante del dispositivo y las mejores prácticas de la industria.
3. Todas las credenciales predeterminadas serán cambiadas inmediatamente después de la instalación del dispositivo y antes de su primer uso, garantizando así que no se utilicen credenciales de fábrica.

10. Cláusula: Deshabilitación de Servicios y Configuración de Firewalls

1. El contratista deshabilitará todos los servicios y puertos no necesarios en los dispositivos médicos para minimizar la superficie de ataque, asegurando que solo permanezcan funcionales los estrictamente necesarios para el funcionamiento del dispositivo.
2. Se configurarán firewalls con políticas de acceso estrictas para controlar el tráfico entrante y saliente, permitiendo exclusivamente las comunicaciones imprescindibles necesarias para el funcionamiento del dispositivo.

3. El contratista informará a la *Servicio Andaluz de Salud* de las actualizaciones necesarias en las reglas de los firewalls para mantenerlos al día con las últimas firmas de amenazas y asegurar una protección continua.

11. Cláusula: Protección Física de los Dispositivos

1. Para la instalación física de los dispositivos, se seguirán estrictamente las directrices del fabricante, garantizando que los componentes que actúen como servidores (como sistemas de gestión de bases de datos, servidores web o de aplicaciones) estén protegidos contra manipulaciones no autorizadas.
2. Estos componentes deberán estar ubicados exclusivamente en infraestructuras físicas que cumplan con las medidas de seguridad físicas establecidas por las políticas de seguridad de la *Servicio Andaluz de Salud*.
3. En todo caso, la ubicación y protección de estos componentes deberán cumplir con el marco de medidas de protección mp.if del Esquema Nacional de Seguridad para la protección de instalaciones e infraestructuras.

5. Política de actualizaciones del software

12. Cláusula: Políticas de Actualización

1. El contratista deberá establecer y mantener políticas claras y documentadas para la actualización de hardware y software de los dispositivos médicos, garantizando que todos los dispositivos estén equipados con los últimos parches de seguridad y firmware antes de ser puestos en producción.
2. Se implementará un proceso regular y sistemático de actualización y parcheo para corregir vulnerabilidades de seguridad conocidas y mejorar la funcionalidad de los dispositivos.

13. Cláusula: Actualizaciones Automáticas

1. Siempre que sea factible y no represente un riesgo para el funcionamiento o el rendimiento del dispositivo, el contratista habilitará procesos de actualización automáticos. Estos procesos permitirán que los dispositivos se actualicen automáticamente para aplicar parches de seguridad y mejoras.
2. El contratista garantizará que las actualizaciones automáticas sean configurables para permitir al usuario definir horarios de actualización y así minimizar interrupciones en el servicio.

14. Cláusula: Mecanismos Seguros de Actualización

1. El contratista deberá implementar mecanismos seguros para la actualización de software, asegurando la autenticidad e integridad de las actualizaciones.
2. Dispondrá de un plan de actualización regular que incluya la aplicación de actualizaciones y parches.

15. Cláusula: Evaluación de Impacto y Pruebas

1. El contratista llevará a cabo evaluaciones de impacto exhaustivas para evaluar el efecto de las actualizaciones en el funcionamiento del dispositivo y la seguridad del paciente antes de su implementación.
2. Todos los parches y actualizaciones serán revisados y probados en un entorno de pruebas antes de su aplicación en el entorno de producción, siguiendo procedimientos estandarizados para minimizar los riesgos de interrupciones.

6. Medidas de seguridad para la Protección de LOS Datos

16. Cláusula: Medidas de Seguridad para la Protección de Datos

1. Los dispositivos médicos y sus sistemas de información relacionados, objeto de este contrato, deberán estar en disposición de asegurar el cumplimiento con las regulaciones de protección de datos como Reglamento (UE) 2016/679 RGPD y Ley 3/2018 LOPDGDD que protegen la privacidad de los datos del paciente y la confidencialidad de los datos sensibles. En particular, en aquellos casos que se considere necesario, debido a la sensibilidad de la información tratada por los dispositivos, o en sistemas categorizados en categoría ALTA de acuerdo con el ANEXO I "Categorías de seguridad de los sistemas de información" del Esquema Nacional de Seguridad, tendrán la capacidad para el cifrado de datos en tránsito y en reposo, utilizando mecanismos de cifrado fuertes para proteger los datos tanto en tránsito como en reposo, asegurando la confidencialidad de la información.

7. Política de auditoría y pruebas de seguridad

17. Cláusula: Requisitos de Pruebas de Seguridad

1. La *Servicio Andaluz de Salud* establecerá los requisitos mínimos de pruebas de seguridad para todos los productos adquiridos, basándose en el umbral de riesgo aceptable definido por la organización.
2. Se podrán realizar pruebas de penetración y auditorías periódicas de seguridad para validar la configuración y el rendimiento de los dispositivos antes de su despliegue en producción.
3. Para ello, se requerirá el establecimiento de un entorno de pruebas que refleje el entorno de producción, permitiendo una evaluación precisa y detallada de los dispositivos médicos.

18. Cláusula: Capacidad para Pruebas de Seguridad y Auditorías

1. Los dispositivos médicos adquiridos deberán tener la capacidad de ser sometidos a pruebas de seguridad y auditorías que verifiquen al menos los siguientes aspectos:

- Auditorías de seguridad sobre el registro de actividades de los dispositivos médicos y los sistemas de información relacionados.
- Revisiones de auditoría para identificar accesos no autorizados o actividades sospechosas, incluyendo la monitorización en tiempo real mediante herramientas automatizadas y el envío de telemetría a herramientas de correlación de datos.
- Revisión y evaluación del cumplimiento y la efectividad de las políticas de seguridad de la *Servicio Andaluz de Salud,* incluyendo la necesidad de ajustes según sea necesario.

- Revisión y evaluación del cumplimiento normativo para asegurar el cumplimiento con normativas y estándares relevantes.
- Evaluación de los controles técnicos y los procedimientos de seguridad del proveedor.

2. Las auditorías y pruebas de seguridad, incluidas pruebas de penetración, se llevarán a cabo de manera periódica, después de cambios significativos en los dispositivos o sus sistemas de información, o ante la sospecha de incidentes de seguridad, para asegurar el cumplimiento de políticas, la detección de vulnerabilidades y posibles brechas de seguridad, y evaluar la resistencia de los dispositivos a ataques maliciosos.
3. La *Servicio Andaluz de Salud* podrá contratar a auditores externos para realizar evaluaciones independientes de la seguridad de los dispositivos médicos (Auditorías de Terceros).

19. Cláusula 3: Pruebas de Validación Post-Despliegue

1. La *Servicio Andaluz de Salud* llevará a cabo pruebas de validación post-despliegue o pruebas de aceptación para confirmar que los dispositivos funcionan según lo esperado y cumplen con los requisitos de seguridad establecidos.
2. Estas pruebas asegurarán que las configuraciones y controles de seguridad se hayan aplicado correctamente y que no existan vulnerabilidades significativas antes de que los dispositivos entren en operación.

8. Política para licitaciones que utilizan servicios en la nube

20. Cláusula: Cumplimiento Regulatorio

1. Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información deberán cumplir con el Esquema Nacional de Seguridad (ENS) y el Reglamento General de Protección de Datos (RGPD), así como los requisitos de auditoría de pruebas de penetración, transparencia, cifrado, gestión de claves y jurisdicción de los datos.
2. Se deberá garantizar la conformidad con las normativas específicas para servicios en la nube, incluyendo las guías CCN-TIC correspondientes para SaaS, PaaS e IaaS.

21. Cláusula: Cumplimiento con Guías CCN-TIC

1. En función del modelo de servicio en la nube proporcionado, el contratista deberá cumplir con lo establecido en la guía CCN-TIC correspondiente (SaaS, PaaS o IaaS).

22. Cláusula: Localización y Ubicación Geográfica de los Datos Personales

1. El contratista deberá informar a la *Servicio Andaluz de Salud* sobre la ubicación geográfica de los datos, incluidas copias de seguridad y almacenamiento de logs, antes y durante el desarrollo del servicio.
2. Si los dispositivos médicos o sus sistemas relacionados manejan datos personales ubicados en la nube, se deberá asegurar en todo momento que la localización de los servidores donde se almacenan estos datos están ubicados en Europa, así como notificar cualquier cambio respecto a dicha localización.

3. Se deberá cumplir con la Ley 3/2018 LOPDGDD y demás normativa relacionada en materia de protección de datos.
4. Se deberá colaborar con el responsable del tratamiento en garantizar el ejercicio garantizará el ejercicio de los derechos de protección de datos conforme a las normativas aplicables.

23. Cláusula: Devolución y Destrucción de Datos

1. El contratista deberá disponer de mecanismos que regulen la devolución de la información en el formato de datos y los plazos especificados, o en su defecto, la destrucción de los mismos, proporcionando evidencias certificadas de la realización. Establecerá un protocolo estandarizado para la devolución y destrucción de datos que incluya pasos detallados y verificables.

24. Cláusula: Política de Respaldo y Recuperación

1. El contratista deberá disponer de mecanismos para una política de respaldo y pruebas de recuperación que incluya:

- Identificación del alcance de los respaldos.
- Política de copias de seguridad.
- Medidas de cifrado de información en respaldo.
- Procedimiento de solicitud de restauraciones de respaldo.
- Realización de pruebas de restauración.
- Traslado de copias de seguridad (si aplica).

25. Cláusula: Plan de Recuperación ante Contingencias

1. Para garantizar la continuidad de los servicios, el proveedor deberá disponer y presentar un plan de recuperación ante contingencias que incluya:

- Identificación y descripción de medios alternativos para la provisión de servicios.
- Realización de al menos una prueba de recuperación anual con un informe detallado.
- Actualización de la documentación del plan de recuperación según sea necesario.

26. Cláusula: Transferencia de Conocimiento e Información al Finalizar el Contrato

1. Al finalizar el contrato, el contratista deberá desarrollar las acciones precisas para la transferencia de conocimiento e información, incluyendo la devolución de toda la información en el formato y plazo especificados, utilizando medios seguros.
2. Establecerá un período de transición definido y planificado para asegurar una transferencia de conocimiento sin interrupciones.

27. Cláusula: Planificación de la Restitución y Transferencia Tecnológica

1. El contratista presentará una planificación detallada para la restitución y transferencia tecnológica, contemplando medios, acciones de contingencia y riesgos potenciales.

2. Cuando sea necesario, se incluirá un período de transición para la gestión organizada del proceso de transferencia.
3. Documentará un plan detallado de transición que incluya todas las etapas del proceso de transferencia, asegurando la coordinación efectiva entre todas las partes involucradas.

9. Política de Acceso Remoto Seguro para servicios de mantenimiento y resolución de incidencias

28. Cláusula: Autorización Previa para Herramientas de Acceso Remoto

1. El contratista deberá obtener autorización previa y expresa por parte de la *Servicio Andaluz de Salud* para la instalación de cualquier herramienta de acceso remoto destinada a la prestación de servicios de mantenimiento y resolución de incidencias en dispositivos médicos y sus sistemas de información relacionados.
2. Ninguna herramienta de acceso remoto para servicios de mantenimiento estará preautorizada sin esta aprobación explícita.

29. Cláusula: Uso de Servicios VPN

1. Para el acceso remoto a los dispositivos médicos y la prestación de servicios de mantenimiento y resolución de incidencias, se utilizarán preferentemente los servicios corporativos de VPN sede a sede proporcionados por la *Servicio Andaluz de Salud.*
2. Todas las comunicaciones realizadas a través de esta VPN deberán estar cifradas y autenticadas adecuadamente.

30. Cláusula: Autenticación Multifactor

1. Es obligatorio el uso de autenticación multifactor (MFA) para todos los accesos remotos a los dispositivos médicos y sus sistemas de información relacionados.
2. Se implementarán mecanismos avanzados de autenticación multifactor (MFA) para verificar la identidad de los usuarios que acceden al dispositivo.

31. Cláusula: Autorización de Usuarios

1. Solo los usuarios previamente autorizados por la *Servicio Andaluz de Salud* a propuesta del contratista tendrán los derechos de acceso necesarios para la prestación de servicios de mantenimiento y resolución de incidencias mediante acceso remoto.

32. Cláusula: Propuesta de Herramientas de Acceso Remoto por el Adjudicatario

1. Por razones operativas, el contratista podrá proponer herramientas específicas para el acceso remoto a los dispositivos y sus sistemas de información relacionados para la prestación de servicios de mantenimiento y resolución de incidencias.
2. Estas herramientas deben respetar la arquitectura de seguridad de la *Servicio Andaluz de Salud,* incluyendo la arquitectura de protección de perímetro tipo 6 (APP-6) según la Guía de Seguridad TIC CCN-TIC 811.

33. Cláusula: Evaluación Excepcional de Herramientas de Acceso Remoto

1. En casos donde la herramienta propuesta por el contratista no soporte la arquitectura de seguridad APP-6 o no pueda utilizar servicios de VPN, el Servicio Andaluz de Salud podrá evaluar excepcionalmente el uso de otras herramientas propuestas por el adjudicatario.
2. Las herramientas podrán ser autorizadas si cumplen con las condiciones de seguridad necesarias y no incrementan el riesgo para la seguridad de las infraestructuras de la *Servicio Andaluz de Salud*.
3. Corresponderá al contratista demostrar el cumplimiento de las condiciones de seguridad necesarias mediante análisis y pruebas de seguridad realizadas por terceros independientes acreditados.
4. Las herramientas propuestas por el contratista no podrán contar en ningún caso con vulnerabilidades conocidas.

10. Comunicación y Respuesta a Incidentes

34. Cláusula: Proceso Integral de Gestión de Incidentes

1. El contratista dispondrá de un proceso integral para hacer frente a los incidentes ocurridos en sus propias instalaciones que puedan tener impacto en la seguridad de los sistemas o servicios que presta a la *Servicio Andaluz de Salud*.
2. Este proceso incluirá procedimientos claros y detallados para la detección, análisis, contención, erradicación y recuperación de incidentes de seguridad.
3. Se asignarán roles y responsabilidades específicas a miembros del equipo de seguridad del contratista para garantizar una gestión eficaz de los incidentes, incluyendo la capacidad de asignar recursos para investigar las causas, analizar las consecuencias y resolver el incidente.

35. Cláusula: Procedimientos de Contención y Recuperación

1. El contratista implementará procedimientos de contención rápidos para limitar el alcance y el impacto de los incidentes de seguridad ocurridos en sus propias instalaciones que puedan afectar los sistemas o servicios que presta a la *Servicio Andaluz de Salud*.
2. Se incorporarán estrategias para erradicar las amenazas y recuperar el funcionamiento normal de los dispositivos y servicios afectados lo más rápido posible.

36. Cláusula: Notificación de Incidentes

1. El contratista notificará sin dilación a las partes interesadas y a las autoridades competentes sobre los incidentes de seguridad ocurridos en sus propias instalaciones, según lo requieran las normativas aplicables.
2. Cuando el incidente pudiera afectar a los servicios prestados por el contratista a la *Servicio Andaluz de Salud* o este pudiera repercutir de alguna forma en sus infraestructuras tecnológicas , el contratista informará de las actuaciones llevadas a cabo para la resolución del incidente a los responsables de la información, responsables de los servicios afectados, al CERT de referencia, así como al responsable de los sistemas de información, el responsable de seguridad y el delegado de protección de datos de la *Servicio Andaluz de Salud*.

3. Se definirán claramente las cadenas de mando y las responsabilidades de comunicación durante un incidente para asegurar una respuesta coordinada y eficiente entre el contratista y la *Servicio Andaluz de Salud*.

37. Cláusula: Canales de Comunicación para Incidentes

1. Para una comunicación ágil de los incidentes, se podrán utilizar múltiples canales de comunicación, como correo electrónico, mensajería instantánea y reuniones informativas, para asegurar que la información llegue a todos los involucrados.
2. El contratista establecerá canales claros para el reporte y seguimiento de incidentes de seguridad mediante protocolos de comunicación definidos, asegurando que todas las partes interesadas sean informadas adecuadamente durante un incidente.
3. Esto incluirá la comunicación con el personal interno de la *Servicio Andaluz de Salud,* otros proveedores, autoridades y pacientes, en su caso.

11. Protección contra código dañino

38. Cláusula: Uso de software antivirus y de Detección y Respuesta ante amenazas.

1. Siempre que las especificaciones del fabricante del dispositivo y sus sistemas relacionados lo permitan, se utilizará software para la protección contra código dañino y otras amenazas que impidan el uso de los dispositivos por intrusos o agentes maliciosos.
2. Tendrán siempre preferencia los sistemas de protección contra código dañino propios de la Servicio Andaluz de Salud, ya que sus alertas son monitorizadas y supervisadas por la propia entidad y/o sus CERT de referencia.
3. En aquellos casos en que el fabricante del dispositivo imponga una determinada herramienta para la protección contra código dañino, el contratista deberá especificar quién o qué organismo o empresa y de qué forma se monitorizan las alertas ocurridas en los dispositivos objeto de adjudicación, así como de qué forma se comunicarán estas al CERT de referencia de la Servicio Andaluz de Salud.
4. Los productos o servicios de seguridad propuestos por el fabricante deberán figurar en el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPTIC) del Centro Criptológico Nacional o bien tener certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, de acuerdo con el artículo 19 del ENS.
5. En aquellos casos contemplados en la cláusula anterior, el tiempo de comunicación de alertas será siempre inmediato, es decir, en tiempo real.
6. En todo caso, si el sistema relacionado con el dispositivo presta un servicio web, este deberá ser protegido frente a ataques de manipulación, inyección de código e inyección SQL al menos mediante validación y saneamiento de entradas, uso de funciones seguras, control de accesos y privilegios, filtros y escapes de caracteres especiales, manejo adecuado de errores, etc.

39. Cláusula: Evaluación de Terceros Proveedores relacionados con la adjudicación.

1. El contratista dispondrá de mecanismos y criterios de seguridad rigurosos para la evaluación y selección de sus propios proveedores que tengan relación con esta adjudicación. Estos criterios deben incluir la revisión de las políticas de seguridad, prácticas de manejo de datos, y medidas de ciberseguridad implementadas por los proveedores.

2. El contratista dispondrá de la capacidad para llevar a cabo auditorías periódicas de seguridad de sus proveedores para asegurar que cumplen con los requisitos de seguridad establecidos. Las auditorías deben incluir evaluaciones de vulnerabilidades, revisiones de cumplimiento normativo y pruebas de penetración. En su defecto podrán exigir las certificaciones de seguridad equivalentes de acuerdo con la normativa aplicable.

40. Cláusula: Contratos y Acuerdos

1. El contratista incluirá cláusulas de seguridad específicas en todos los contratos y acuerdos con sus proveedores relacionados con esta adjudicación. Estas cláusulas deben cubrir aspectos como la protección de datos, la respuesta a incidentes, la gestión de acceso y la obligación de mantener actualizadas las medidas de seguridad.
7. Estos contratos se revisarán periódicamente con sus proveedores para asegurar que las cláusulas de seguridad sigan siendo relevantes y efectivas. Las revisiones deben tener en cuenta cambios en las normativas, avances tecnológicos y lecciones aprendidas de incidentes de seguridad pasados.

12. Concienciación y Formación en Ciberseguridad

La concienciación y la formación en ciberseguridad son fundamentales para asegurar que todo el personal relacionado con los dispositivos médicos esté preparado para identificar y responder adecuadamente a las amenazas cibernéticas.

41. Cláusula: Programas de Formación

1. El contratista contará con programas de formación en ciberseguridad para todos sus empleados. Esta formación debe cubrir los fundamentos de la ciberseguridad, la protección de datos, el reconocimiento de amenazas comunes y las políticas de seguridad de la organización.
2. Los programas ofrecerán una formación continua y actualizaciones periódicas sobre nuevas amenazas y mejores prácticas de seguridad.

42. Cláusula: Concienciación de Seguridad

1. De igual forma, el contratista mantendrá campañas de concienciación regulares para mantener la seguridad cibernética en la mente de todo el personal.

13. Resolución de conflictos en la aplicación de las cláusulas de seguridad

43. Cláusula: Equilibrio Funcionalidad y Seguridad

1. Siempre que el contratista entienda que la aplicación de alguna de las cláusulas de seguridad de este anexo pueda afectar a la disponibilidad de los servicios que presta el dispositivo, pueda suponer un perjuicio para el rendimiento del mismo o se pueda poner en peligro la seguridad del paciente deberá comunicarlo a la *Servicio Andaluz de Salud* de forma inmediata.
2. El Servicio Andaluz de Salud atenderá las razones expuestas por el contratista y evaluará la pertinencia o no de las excepciones propuestas por el contratista siempre que la solicitud se acompañe de la justificación adecuada y se propongan medidas compensatorias alternativas.

3. El Servicio Andaluz de Salud podrá aceptar las medidas compensatorias alternativas siempre que estas sean equivalentes a las medidas excepcionadas y no supongan un incremento en el riesgo para la seguridad de la Servicio Andaluz de Salud.