



Requerimientos técnicos STS OB22-2023 5 SALAS RX CON INTELIGENCIA ARTIFICIAL DE AYUDA AL DIAGNOSTICO EN HUN-A

GESPRONA 42358



Índice de contenidos

1 REQUISITOS TÉCNICOS STS	3
1.1 Integraciones con los sistemas de información SNS-O	3
1.2 Licenciamiento	3
1.3 Requisitos para la integración con Imagen Médica Digital	3
1.3.1 Conectividad	4
1.3.2 Estándar DICOM	4
1.3.3 Estudios DICOM	4
2 REQUISITOS TÉCNICOS DE INFRAESTRUCTURAS PARA PLIEGOS TÉCNICOS	6
2.1.1 Requerimientos específicos para solución "Housing"	11
2.1.2 Requerimientos específicos para solución en la nube	12
3 REQUISITOS ESPECÍFICOS DE INTELIGENCIA ARTIFICIAL	13



1 REQUISITOS TÉCNICOS STS

1.1 Integraciones con los sistemas de información SNS-O

Los sistemas de información que formen parte de la solución ofertada por el Adjudicatario deberán integrarse con los sistemas de información del SNS-O, siendo responsabilidad del Adjudicatario:

- El esfuerzo de integración desde sus sistemas de información.
- Las adecuaciones necesarias del software corporativo y propio del SNS-O que sean requeridas para garantizar las prestaciones actuales de los sistemas de información del SNS-O.

Estas adaptaciones no supondrán ningún coste directo ni repercutido a través de otros proveedores del SNS-O. El desarrollo será realizado por las empresas que la DGTD determine en cada momento, principalmente los adjudicatarios de sus contratos de mantenimiento.

No existe una plataforma de integración o bus de mensajería entre productos SNS-O. Todas las integraciones son punto a punto y deben diseñarse *ad-hoc*.

Los interfaces de comunicación con sistemas externos serán servicios web. De manera excepcional, justificando su utilización en base a criterios concretos relativos a necesidades de disponibilidad, asincronismo o interoperabilidad tecnológica y siempre con el acuerdo expreso del SNS-O se podrán utilizar los siguientes tipos de interfaces de comunicación con sistemas externo:

- Ficheros de intercambio.
- Interface de usuario. Desde un sistema de información es posible incrustar, abrir o redirigir a formularios web de otro sistema de información.
- Acceso directo a base de datos a través de tablas, vistas o procedimientos almacenados.

En el escenario de integración no se contempla el uso de HL7. Aquellos sistemas de información que implementen HL7 deberán adaptarse tanto al interface de comunicación como a la semántica del mensaje propio del sistema de información SNS-O con quien desean comunicarse.

Si fuese necesario GN dispone de plataformas para la ejecución desatendida de componentes contruidos para facilitar las integraciones. Estos componentes (tareas programadas o paquetes de transformación de datos) deben implementarse específicamente para cubrir aspectos tales como transformación de información o la monitorización del sistema para la notificación de eventos.

1.2 Licenciamiento

Las licencias de los softwares implantados serán propiedad de SNS-O de manera indefinida y SNS-O tendrá derecho a su actualización durante la vigencia del contrato.

El software (sistema operativo, aplicativos, drivers, etc.) incluido en el equipamiento tendrá un ciclo de vida equivalente al del equipamiento. Con el fin de garantizar el funcionamiento y el soporte del equipamiento, la fecha de fin de soporte del software deberá ser posterior a la vida útil estimada del equipamiento o garantizar su evolución a versiones del software que estén soportadas.

1.3 Requisitos para la integración con Imagen Médica Digital

Los requisitos incluidos en este apartado deberá cumplirlos cualquier equipo médico (equipo a partir de aquí), ya sean elementos hardware como software o la conjunción de ambos, que deba integrarse en el sistema de Imagen Médica Digital del SNS-O.

Las empresas licitantes de estos equipos deberán aportar como parte de su documentación



técnica el documento “*DICOM Conformance Statement*”

El Adjudicatario asegurará la conectividad del equipo con la red corporativa de GN. El Adjudicatario entregará documentación técnica detallando la configuración TCP/IP y DICOM del equipo.

El Adjudicatario indicará en la oferta si el equipo puede dar servicio sin necesidad de conectarlo a la red corporativa de GN.

1.3.1 Conectividad

Para asegurar la conectividad del equipo con la red corporativa del GN se requiere:

- Interfaz física: RJ45.
- Estándar de red de área local: Ethernet.
- Protocolo de red: TCP/IP.
- Los equipos móviles deberán cumplir Autenticación IEEE 802.1x WPA2-Enterprise y configurar un Usuario/Contraseña de Directorio Activo.

1.3.2 Estándar DICOM

El equipo debe implementar el estándar DICOM versión 3.

Todos los parámetros de conexión con el PACS (HostName, IP, puerto, AET, StationName, Nodos Remotos, etc.) de los distintos servicios DICOM deberán poder ser configurados según las necesidades del SNS-O. La configuración DICOM inicial de los equipos será realizada por el adjudicatario con las instrucciones que le sean dadas desde la DGTD. La configuración DICOM de la modalidad deberá adecuarse a las prestaciones de especializada y primaria. La configuración DICOM será sin coste para el SNS-O y podrá volver a requerirse por parte del SNS-O a la empresa adjudicataria en cualquier momento después de la recepción del equipo.

Toda comunicación con nodos DICOM deberá establecerse con el AET configurado.

Salvo indicación expresa por parte de la DGTD, Hostname, StationName y AET tendrán el mismo valor.

Servicios DICOM

El SNS-O considera imprescindibles los siguientes servicios DICOM:

- DICOM WLM (DICOM worklist manager). Permite el envío al equipo de la lista de trabajo desde el PACS.
- DICOM Storage (Almacenamiento DICOM). Se encarga de enviar las imágenes que genera el equipo al PACS.

El SNS-O recomienda desplegar los siguientes servicios DICOM:

- DICOM Print. Permite imprimir imágenes en una impresora DICOM.
- DICOM QR (DICOM Query/Retrieve). Permite que el equipo consulte y pida estudios al PACS.
- DICOM COMMITMENT. Permite verificar si un archivo, que fue enviando previamente al PACS, está almacenado correctamente.

Los servicios DICOM, al menos los imprescindibles, deben estar operativos y funcionales. No es aceptable:

- Requerir el pago de licencia, activación, o cualquier otro cargo para permitir su uso.
- Requerir el pago al servicio técnico del adjudicatario para su correcta configuración.

1.3.3 Estudios DICOM

- Utilizará el set de caracteres ISO_IR 100 para los servicios DICOM WLM SCU y Storage SCU.
- Los objetos DICOM tienen que llegar al PACS con los tags DICOM correctos para que la visualización en los visores del SNS-O sea óptimo.



- Todos los objetos DICOM enviados al PACS, tendrán los tags DICOM Station Name (0008,1010) e Institution Name (0008,0080), según los parámetros indicados por la DGTD.
- Los campos identificativos del estudio (AccessionNumber, StudyInstanceUID, StudyDate, StudyTime, PatientID, ...) serán iguales en todos los objetos DICOM, de un mismo estudio, enviados al PACS.
- Informes gráficos. Los informes gráficos que se envíen al PACS deben implementar DICOM WaveForm.
- Equipos con radiación ionizante deben enviar la información de dosis radiológica al Sistema de Dosis del SNS-O. La forma preferente es la primera de cada tipo de modalidad.
 - Equipos CT (TAC).
 - Radiation Dose Structured Report (RDSR) con SOP Class UID: "1.2.840.10008.5.1.4.1.1.88.67".
 - CT Dose Report con SOP class UID: "1.2.840.10008.5.1.4.1.1.7".
 - Equipos MG (Mamógrafo).
 - Cabecera DICOM.
 - Radiation Dose Structured Report (RDSR) con SOP Class UID: "1.2.840.10008.5.1.4.1.1.88.67". Si es validado que no incluya la fuerza de compresión de la mama.
 - Equipos DX (Radiología general).
 - Radiation Dose Structured Report (RDSR) con SOP Class UID: "1.2.840.10008.5.1.4.1.1.88.67".
 - Cabecera DICOM.
 - Resto de equipos.
 - Radiation Dose Structured Report (RDSR) con SOP Class UID: "1.2.840.10008.5.1.4.1.1.88.67".

Permitirá enviar los objetos RDSR o CT Dose Report al mismo PACS al que se envía la imagen asociada al objeto o a otro distinto a decisión de la DGTD.



2 REQUISITOS TÉCNICOS DE INFRAESTRUCTURAS PARA PLIEGOS TÉCNICOS

Requerimiento SI la oferta incluye equipamiento (servidores, licencias, software, estaciones de trabajo, ...) que no son parte de la propia modalidad.

Todos los sistemas deberán cumplir de forma general el Escenario Tecnológico de Gobierno de Navarra, según el documento anexo en el pliego:

ANEXO STS II - Escenario Tecnológico GdN Noviembre 2023 v1.0.pdf

Además, deberán cumplir los siguientes requisitos específicos para lo cual en cada oferta se entregará esta tabla completada junto a la propuesta técnica:

Requisitos	Aceptación (Sí)
Todos los sistemas de información de servidor serán virtualizables y alojados en la plataforma de virtualización VMware de Gobierno de Navarra con las características y condiciones descritas en el Escenario Tecnológico del mismo.	
Los parámetros de red de los sistemas de información tanto para equipos servidor como cliente o equipo tipo <i>appliance</i> serán asignados por Gobierno de Navarra. Incluidos dirección IP (fija o DHCP), máscara de red, DNS y puerta de enlace. • Interfaz física: 1Gb mediante RJ45 o 10Gb mediante fibra óptica. • Estándar de red de área local: Ethernet. • Protocolo de red: TCP/IP.	
Los dispositivos que hagan uso de la red wifi utilizarán alguno de los siguientes estándares dependiendo de las características de los APs que doten de cobertura la ubicación: IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac o IEEE 802.11ax. A su vez, los dispositivos deberán soportar el método de autenticación WPA2/WPA3 Enterprise que utiliza el estándar IEEE 802.1X para autenticación de red basados en la estructura EAP (Protocolo de Autenticación Extensible) con un servidor RADIUS.	
Los cambios necesarios en los parámetros de red de los sistemas de información serán posibles durante toda la vida útil de los sistemas de información y estará debidamente documentada la ejecución de los mismos por parte del fabricante, instalador o proveedor. Los cambios en los parámetros de red de los sistemas de información necesarios durante el periodo de soporte, serán realizados por el proveedor del soporte sin ocasionar gastos a Gobierno de Navarra.	
Los sistemas de información estarán colocados en una VLAN asignada por Gobierno de Navarra, detrás de un cortafuegos aportado por Gobierno de Navarra y los cuales están descritos en el escenario tecnológico. La VLAN asignada podrá estar compartida con otros equipos del mismo u otros fabricantes.	



El acceso remoto a los sistemas de información únicamente será posible mediante las opciones tecnológicas que provee Gobierno de Navarra y que son: • Acceso VPN SSL mediante <i>extranet</i> con doble factor • VPN de sitio a sitio	
Los sistemas e información basados en sistemas operativos Microsoft y RedHat Linux deberán disponer de un software Antimalware/antivirus instalado, licenciado y que se actualice automáticamente durante todo el tiempo que dure el soporte del mismo. Aun en los casos en que la operación y soporte del equipamiento la proporcione el proveedor, Gobierno de Navarra ofrece la inclusión de su sistema antivirus corporativo.	
Obligación de notificar al Responsable de Explotación de Gobierno de Navarra las vulnerabilidades, parches existentes o brechas de seguridad que puedan afectar a los sistemas de información según normativa vigente.	

Requisitos	Aceptación (Sí)
El sistema de información se monitorizará con las herramientas que forman parte del escenario de monitorización: • Centreon: Herramienta de monitorización de disponibilidad y rendimiento de infraestructuras y aplicaciones. • QRadar de IBM: Herramienta de tipo SIEM orientada a la recolección y monitorización de eventos de seguridad que permite garantizar el cumplimiento de normativas de seguridad.	
El sistema de información no podrá usar <i>applets</i> de Java. El sistema de información no podrá usar la arquitectura de plugin de plataforma cruzada NPAPI en la que se basa entre otros el plugin de Java para exploradores web, ya que los navegadores modernos no soportan esta arquitectura. Esta restricción no afecta a las aplicaciones Java Web Start, solo afecta a los <i>applets</i>.	
Licenciamiento del software base. Las licencias de software base se adquirirán a nombre del Gobierno de Navarra con una duración ilimitada. Cuando el sistema de información se despliegue en los servidores corporativos, compartidos con varias aplicaciones más y con acceso restringido por parte del proveedor, no será necesario que se adquieran las licencias del sistema operativo, del servidor de aplicaciones o del gestor de base de datos. Si el sistema de información se despliega en servidores exclusivos, la empresa adjudicataria deberá aportar las licencias del sistema operativo, servidor de aplicaciones y gestor de base de datos (así como cualquier otro elemento software específico necesario) que se adapten a la infraestructura existente en Gobierno de Navarra, y siempre en las versiones, ediciones, y dimensionamiento (número de usuarios, procesadores, servidores, etc. licenciados) que se definan desde la DGTD como necesarias y adecuadas, siempre de	



acuerdo al Escenario Tecnológico.	
Licenciamiento del producto. Las licencias del producto, si existe la posibilidad, serán de tipo software. Anteponiéndose estas a las de tipo mochila/hardware.	
Usuarios y contraseñas: • Las cuentas de usuario de los sistemas de información deben ser nominales. No se permiten cuentas genéricas. • Si es posible los sistemas de información se integrarán en el Directorio Activo de Gobierno de Navarra y utilizarán usuarios dentro del mismo. • Política de contraseñas a aplicar en los sistemas de información y requerimientos de seguridad para todos los usuarios (está política no se aplica a usuarios de servicio, genéricos o de pruebas): ○ La contraseña debe tener una longitud mínima de ocho caracteres. ○ Deben combinarse tres tipos distintos de caracteres elegidos entre mayúsculas, minúsculas, números y caracteres especiales: @ \$. ○ Se obliga a un cambio de contraseña inicial tanto cuando se realice la primera conexión a la red de Gobierno de Navarra como tras la restauración de la contraseña (cuando por olvido se solicite un cambio de contraseña y sea asignada una provisionalmente, esta deberá ser sustituida inmediatamente para que cumpla los requisitos anteriores). ○ Se obliga al cambio de contraseña cada 30 días. El equipo integrado en dominio avisa al usuario cinco días antes de que caduque la contraseña. ○ No se pueden reutilizar las últimas 24 contraseñas. ○ La cuenta de usuario será desactivada si no se utiliza durante 90 días. Para volver a entrar a la red debe solicitar la activación de la cuenta. ○ No se permitirán palabras en cualquier idioma, secuencias lógicas deducibles, permutaciones sencillas, ni secuencias de teclado.	



Además, la propuesta que se presente en la oferta contendrá la respuesta a los siguientes apartados:

Requerimientos	
Necesidad de adquisición de Infraestructura. El proveedor deberá detallar la infraestructura servidora y puesto cliente necesaria para soportar su propuesta.	
Dimensionamiento de los sistemas de información:	
CPU (nº de núcleos)	
Memoria (GB)	
Disco (GB)	
Sistema gráficos (resolución)	
Puertos de entrada y salida	
Periféricos	
Almacenamiento externo	
Latencia	
Rendimientos (<i>Throughputs</i>)	
Sistema operativo	
Software específico	
Se detallarán al máximo los requisitos y especificaciones en cuanto a previsión de crecimiento y se entregará un plan de capacidad durante la vigencia del contrato. (Especificar documento y página de la oferta donde se especifica)	
Se definirá la necesidad de realizar copias de seguridad de los sistemas de información indicando los parámetros necesarios de tipo de copia, periodicidad y retención. Tendrá en cuenta lo siguiente: - Se realizan sobre la infraestructura servidora de Gobierno de Navarra. Las estaciones de los usuarios no se respaldarán (aunque pueden existir excepciones tras un estudio previo entre gestión de copias y el responsable de la información de la estación). - Sistemas operativos vigentes en el escenario tecnológico de Gobierno de Navarra. - Software base vigente en el escenario tecnológico de Gobierno de Navarra (Especificar documento y página de la oferta donde se especifica)	
El acceso a Internet de los sistemas de información se verá limitado sólo a aquello estrictamente necesario y justificado (listas blancas). Se deberán definir los accesos necesarios a Internet, especificando las <i>URLs</i> de destino y los puertos necesarios. Gobierno de Navarra se reserva el derecho a no aceptar accesos a Internet de los sistemas de información si los considera un riesgo innecesario. (Especificar documento y página de la oferta donde se especifica)	
Los accesos de los sistemas de información a los recursos de la red corporativa de Gobierno de Navarra se verán limitados a sólo a aquello estrictamente necesarios y justificados (listas blancas). Se deberán definir los accesos necesarios a los recursos internos en la propuesta. (Especificar documento y página de la oferta donde se especifica)	
No se permitirá la conexión a Internet de los sistemas de información por métodos distintos a los autorizados por Gobierno de Navarra. Se definen estos métodos de conexión en equipos como encaminadores 3G/4G,	



encaminadores ADSL, tarjetas SIM, etc. En cada caso se deberá evaluar y autorizar la solución por lo que se deberá especificar en la propuesta si existe alguno de estos dispositivos junto con una evaluación de riesgos para poder ser evaluado y autorizado si corresponde. (Especificar documento y página de la oferta donde se especifica, en caso de que existan)	
Por regla general no se permite el <i>autologon</i> en los sistemas de información y los servicios de aplicación de los sistemas de información tienen que poder ejecutarse sin haber iniciado sesión. En caso de que el sistema de información requiera <i>autologon</i>, se deberá especificar en la oferta y Gobierno de Navarra evaluará si se autoriza según los riesgos que se encuentren. (Especificar documento y página de la oferta donde se especifica, en caso de que existan)	

Requerimientos	
Es obligatorio realizar actualizaciones de seguridad y seguir una política al respecto. Como referencia se seguirá la política de Gobierno de Navarra. En caso de justificar no poder seguir esta política se deberá presentar una política alternativa de actualizaciones de seguridad. La política de actualizaciones de seguridad de Gobierno de Navarra consiste en: Actualizaciones de seguridad en servidores Windows: - Las actualizaciones de seguridad incluidas son aquellas designadas por Microsoft como 'críticas' e 'importantes'. - Periodicidad mínima: con una cadencia trimestral se realizará una actualización a los servidores Windows de las actualizaciones de seguridad (parches) publicadas por el proveedor desde la última iteración del ciclo de parcheado. Como norma general, dentro del paquete de actualizaciones se excluyen aquellas con una fecha de publicación inferior a un mes para garantizar la estabilidad de los equipos. - Adicionalmente se establece la posibilidad de ejecutar actualizaciones extraordinarias sin atender a la cadencia cuatrimestral establecida en el apartado anterior en el caso de la publicación de actualizaciones críticas cuyo impacto real en caso de explotación maliciosa pueda ser alto. Actualizaciones de seguridad en servidores Linux: - Periodicidad mínima: con una cadencia es trimestral. El parcheo completo de un servidor Linux nuevo es parte obligatoria del despliegue. - Adicionalmente, se establece la posibilidad de ejecutar actualizaciones extraordinarias sin atender a la cadencia mensual o cuatrimestral establecidas en los apartados anteriores en el caso de la publicación de actualizaciones críticas cuyo impacto real en caso de explotación maliciosa pueda ser alto. Actualizaciones de seguridad de puesto de trabajo: - Con una cadencia trimestral, se realizará una distribución de software en los puestos de trabajo de las últimas actualizaciones de seguridad (parches) publicadas por los proveedores, con la particularidad de los productos Microsoft, que se incluirán aquellas publicadas en el mes anterior, para garantizar la estabilidad de las estaciones cliente. - Adicionalmente, se establece la posibilidad de ejecutar actualizaciones extraordinarias, sin atender a la cadencia trimestral establecida en el apartado anterior, en el caso de la publicación de	



actualizaciones críticas cuyo impacto real en caso de explotación maliciosa pueda ser alto. Actualizaciones de seguridad en <i>appliances</i> o con sistemas embebidos: • Para <i>appliances</i> que se encuentren en redes que ofrecen servicio <i>frontend</i> hacia Internet, la cadencia es mensual de la distribución de las actualizaciones de seguridad (erratas) publicadas por el proveedor. • Para el resto de <i>appliances</i> la cadencia es trimestral. • Adicionalmente, se establece la posibilidad de ejecutar actualizaciones extraordinarias sin atender a la cadencia mensual o cuatrimestral establecidas en los apartados anteriores en el caso de la publicación de actualizaciones críticas cuyo impacto real en caso de explotación maliciosa pueda ser alto. (Indicar la aceptación de la política de Gobierno de Navarra, o especificar la política de actualización detallando el documento y página de la oferta)	
--	--

2.1.1 Requerimientos específicos para solución “Housing”

Infraestructura Virtual del GdN:

- No está permitido el uso/instalación de GPUs.

Infraestructura propietaria del adjudicatario (Housing):

- Todo el equipamiento debe ser enrackable, o en su defecto incorporar un kit que permita la instalación sobre un rack de 19”.
- Las guías, bandejas, kits, etc., deben ser compatibles para su instalación sobre perfiles de rack con orificios redondos o cuadrados.
- Todo el equipamiento debe disponer de doble fuente de alimentación.
- El flujo de refrigeración será:
 - “front to back” para el equipamiento que disponga de conexiones de comunicaciones en la parte trasera.
 - “back to front” para el equipamiento que disponga de conexiones de comunicaciones en la parte frontal.
 - “back to front” para la electrónica de red. Todo el cableado se realizará por la parte trasera del rack para evitar cruzar cables desde el frontal.
- Debe disponer de al menos 1 interface de red para gestión fuera de banda en caso de caída de la LAN de servicio.
- Debe disponer de al menos 2 interfaces de red para servicio en alta disponibilidad.
- No se permitirá la conexión de mochilas USB u otros dispositivos en la parte frontal que comprometan el correcto cierre de la puerta del rack.
- Si es ofertado/requerido el producto en Alta Disponibilidad es necesario replicar todo el sistema para implantarlo en ambos CPDs del GdN.
- El adjudicatario proveerá de un firewall de capa 3 que les aisle de la red del GdN. El GdN proveerá de una IP.
- El adjudicatario proveerá de todas las licencias necesarias: S.O., VMWare, SQL Server, ...
- La solución proporcionada debe contar con todos los sistemas necesarios para mantener su funcionamiento, soporte y recuperación ante problemas: copias de seguridad, monitorización, antivirus comercial para empresas, ...
- El proveedor es responsable de mantener unas políticas de seguridad, contraseñas y configuración, acordadas con Infraestructuras del GdN, para garantizar el funcionamiento del producto y la seguridad del mismo y sus datos.



2.1.2 Requerimientos específicos de protección de datos.

Tanto si la solución ofertada por los licitantes es una solución en la red de Gobierno de Navarra, como si fuera una solución en “la nube”. Deberá cumplir con los siguientes requisitos:

- Rellenar el documento “ANEXO III - Contrato encargado tratamiento nivel MEDIO v3.doc”
- Respecto a la protección de datos: La solución propuesta, tanto on premise como en su caso en nube, deberá cumplir con la normativa vigente estatal y europea, en cuanto a protección de datos, en la actualidad Reglamento (UE) 2016/679 y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, respectivamente. Además, se deberá firmar el correspondiente Acuerdo de Encargo entre el Servicio Navarro de Salud – Osasunbidea, como Responsable del tratamiento, y el adjudicatario del mismo, como Encargado del Tratamiento.
- Respecto a la seguridad de la información: La propuesta deberá cumplir con las medidas de seguridad establecidas por el SNS-O, de acuerdo al escenario tecnológico del mismo, según ANEXO STS II - Escenario Tecnológico GdN Noviembre 2023 v1.0.pdf.



3 REQUISITOS ESPECÍFICOS DE INTELIGENCIA ARTIFICIAL

A nivel informático, el alcance de la solución presentada por los licitantes, debe disponer de un motor de Inteligencia Artificial como como mínimo, tenga la capacidad de ayudar al diagnóstico para Patología Torácica, en todas las salas; también tener la funcionalidad de realizar el cálculo de Edad Ósea, como mínimo, en una de las salas de HUN-B.

Datos clínicos generados por IA

El SNS-O considerará como datos clínicos pertenecientes a la historia clínica del paciente cualquier información clínica que el sistema de información o hardware potenciado por IA genere. Esto incluye cualquier valoración pre-diagnóstica, diagnóstica, medición o predicción que pueda servir para describir la clínica del estudio, priorizar una lista de trabajo o apoyar la decisión clínica de un profesional sanitario. El adjudicatario deberá ofrecer un mecanismo para integrar dichos datos clínicos generados por IA en los sistemas de información del SNS-O, cumpliendo los requerimientos de integración detallados a continuación:

1. Los datos estructurados deben ser interpretables por parte de los sistemas de información del SNS-O, para así poder ofrecer funcionalidades en base a los mismos: orquestación de procesos, priorización de listas de trabajo, generación de informes, automatización de tareas repetitivas, explotación de datos poblacionales, etc.
2. Los licitantes presentarán documentación técnica detallada relativa al software de inteligencia artificial, su comportamiento, instalación, requerimientos de hardware, licencias necesarias, para el algoritmo de IA.
3. Proyecto de validación del algoritmo. El fabricante presentará un proyecto que describa la validación clínica necesaria para verificar el correcto funcionamiento de los algoritmos de IA procesando estudios realizados a pacientes del SNS-O por parte de técnicos del SNS-O. Este entregable deberá contener una descripción detallada del volumen y el tipo de pruebas a realizar. Así mismo, describirá quién y cómo valorará las salidas del algoritmo de IA.
4. Durante el periodo del concurso, es requerido la realización de una video llamada Demostrativa por cada licitante, cada una con un máximo de 2 horas, donde presentará la solución técnica a SNS-O, referente a los puntos anteriores, y desde donde se realizarán consultas técnicas relativas a la tecnología de IA. Esta video llamada se realizará de forma coordinada entre licitante y SNS-O
5. Tras la adjudicación, durante los 90 días desde la firma del contrato, y tras la instalación de la primera sala RX, el adjudicatario, participará junto al Equipo de Inteligencia Artificial NaIA e Imagen Digital y los Radiólogos de SNS-O, en una prueba de concepto de los puntos anteriores. SNS-O se reserva el derecho a anular la funcionalidad de IA si desde STS valorase algún tipo de incompatibilidad. En este caso, la sala RX deberá tener la capacidad de trabajar de manera autónoma sin IA.

Validación previa

El adjudicatario deberá ofrecer un mecanismo que le permita al SNS-O validar que los algoritmos de IA tendrán un desempeño adecuado en el circuito asistencial objetivo. El cumplimiento de este requerimiento es obligatorio.

Este proyecto de validación previa tendrá las siguientes características:

- Su diseño estadístico se presentará como parte de la documentación a aportar en el pliego. Incluirá un tamaño de muestra necesario, métricas a medir y un plan detallado para su ejecución.
- En caso de que no sea posible o necesaria una validación estadística del desempeño, se motivará, y se presentará un mecanismo de validación alternativo.
- Se realizará en el SNS-O, no se admitirán estudios de otros hospitales, y se realizará de forma coordinada con el SNS-O.



- Se realizará de forma que los algoritmos de IA --todavía sin validar en el SNS-O-- no influyeran en las decisiones de los profesionales sanitarios que participan en el circuito asistencial.
- El SNS-O podrá decidir no hacer uso de la IA en caso de tener resultados que valore como negativos. En tal caso, el adjudicatario devolverá al SNS-O el importe que haya podido pagar por la funcionalidad potenciada por IA, o podrá presentarle un plan para la mejora del algoritmo (sin repercutir ningún coste al SNS-O).

Monitorización

El adjudicatario deberá ofrecer un mecanismo que supervise y garantice que el algoritmo de IA mantiene el desempeño adecuado durante todo el ciclo de vida su producto. El adjudicatario deberá describir de forma detallada el proyecto de monitorización en la documentación que aporta al pliego. El cumplimiento de este requerimiento es obligatorio.

Este mecanismo de monitorización de IA, incluirá como mínimo:

- Evaluaciones periódicas de una muestra de los estudios por parte de expertos.
- Alertas automáticas en caso de que se identifique una degradación del desempeño.

Un responsable del SNS-O estará al tanto de los resultados de la monitorización y de las posibles alertas que genere.