



Valoración Ecógrafo Neurología HUN-A

Gesprona: 45301

Valoración ofertas

Versión 1.0



Control de cambios

Fecha	Autor	Descripción	Versión
03/10/2024	Javier Trías	Creación documento y valoración de ofertas	1.0



Índice de contenidos

1 INTRODUCCIÓN	4
2 REQUERIMIENTOS	5
2.1 Requisitos para la integración con Imagen Médica Digital	5
2.1.1 Conectividad	5
2.1.2 Estándar DICOM	5
2.1.3 Estudios DICOM	6
2.1.4 Ecocardiógrafos	6
2.2 Requisitos técnicos de Infraestructuras para pliegos técnicos	6
3 LICITANTES	13
3.1 ESAOTE (A60785573)	13
3.2 GE (A28061737)	14
3.3 PHILIPS (A28017143)	15
4 VALORACIÓN	16



1 INTRODUCCIÓN

Éste documento realiza la valoración del pliego OT04-2024 en lo concerniente a los requerimientos STS incluidos en el pliego para la adquisición de Ecógrafo de Neurología de HUN-A:



2 REQUERIMIENTOS

2.1 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.

2.1.1 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.

Interfaz wifi: Los equipos móviles deberán cumplir con los estándares requeridos en el punto 2: [43564 Requerimientos técnicos STS - ANEXO II REQUERIMIENTOS INFRAESTRUCTURAS - Febrero 2024.pdf](#)

■ .

2.1.2 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.

2.1.3 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.

2.1.4 Ecocardiógrafos

El ecocardiógrafo deberá ser compatible con el sistema de información del SNS-O utilizado para el diagnóstico: IntelliSpace CardioVascular..

2.2 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 que está publicado en el documento:

[43564 Requerimientos técnicos STS - ANEXO II REQUERIMIENTOS INFRAESTRUCUTURAS - Febrero 2024.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 parchado. 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)	
--	--



3 LICITANTES

3.1 ESAOTE (A60785573)

Cumple los requisitos.

Entrega el documento "doc150330-DCS_MyLab_F12XX_C716W-1.pdf" donde describe correctamente todos los criterios indicados en los requerimientos.

Table 1 provides an overview of the network services supported by the MyLab devices.

Table 1
NETWORK SERVICES

SOP Classes	User of Service (SCU)	Provider of Service (SCP)
Transfer		
Ultrasound Image Storage	Yes (*)	Yes (*) (***)
Ultrasound Multiframe Image Storage	Yes (*)	Yes (*) (***)
Secondary Capture Image Storage	Yes (*)	Yes (*) (***)
Comprehensive SR Storage	Yes (*) (**)	No
Query/Retrieve		
Study Root Information Model FIND	Yes (*) (***)	No
Study Root Information Model MOVE	Yes (*) (***)	No
Workflow Management		
Modality Worklist	Yes (*) (****)	No
Storage Commitment Push Model	Yes (*) (**) (****)	No
Modality Performed Procedure Step	Yes (*) (**) (****)	No
Print Management		
Basic Grayscale Print Management	Yes (*)	No
Basic Color Print Management	Yes (*)	No

(*) Enabled by the purchasable DICOM option.

Table 6
SOP CLASSES FOR AE STORAGE

SOP Class Name	SOP Class UID	SCU	SCP
Ultrasound Image Storage	1.2.840.10008.5.1.4.1.1.6.1	Yes	No
Ultrasound Multiframe Image Storage	1.2.840.10008.5.1.4.1.1.3.1	Yes	No
Secondary Capture Image Storage	1.2.840.10008.5.1.4.1.1.7	Yes	No
Comprehensive SR Storage ¹¹	1.2.840.10008.5.1.4.1.1.88.33	Yes	No
Storage Commitment Push Model ¹²	1.2.840.10008.1.20.1	Yes	No
Verification	1.2.840.10008.1.1	Yes	Yes ¹³

Table 33
BROAD WORKLIST QUERY MATCHING KEYS

Tag	Attribute	Contents
(0008,0005)	Specific Character Set	Can be "ISO_IR 100", "ISO_IR 144", "ISO_IR 101", "ISO_IR 192" or "GB18030" ²⁴
(0008,0050)	Accession Number	empty, can be set



3.2 GE (A28061737)

Cumple los requisitos.

Entrega el documento “10 GEHC-DICOM-Conformance_Vivid-EchoPACv206_DOC2652554_Rev3.pdf” donde describe correctamente todos los criterios indicados en los requerimientos.

TABLE 0.1 NETWORK SERVICES

SOP Classes	User of Service (SCU)	Provider of Service (SCP)
Transfer		
Ultrasound Multi-frame Image Storage	Yes	Yes
Ultrasound Image Storage	Yes	Yes
Ultrasound Multi-frame Image Storage (Retired)	Yes	Yes
Ultrasound Image Storage (Retired)	Yes	Yes
Secondary Capture Image Storage	Yes	Yes
Comprehensive SR	Yes	No
CT Image Storage *	No	Yes
Enhanced CT Image Storage *	No	Yes
Query/Retrieve		
Study Root Query/Retrieve Information Model – FIND	Yes	No
Study Root Query/Retrieve Information Model – MOVE	Yes	No
Print Management		
Basic Grayscale Print Management Meta SOP Class	Yes	No
Basic Color Print Management Meta SOP Class	Yes	No
Workflow Management		
Storage Commitment Push Model SOP Class	Yes	No
Modality Performed Procedure Step SOP Class	Yes	No
Modality Worklist Information Model – FIND SOP Class	Yes	No

Option*: This means that this service can be purchased separately and may be available

Basic Color Print Management Meta SOP Class	1.2.840.10008.5.1.1.18
Study Root Query/Retrieve Information Model – FIND	1.2.840.10008.5.1.4.1.2.2.1
Study Root Query/Retrieve Information Model – MOVE	1.2.840.10008.5.1.4.1.2.2.2
Comprehensive Structured Report Storage	1.2.840.10008.5.1.4.1.1.88.33

Option *: The DICOM Worklist network service is not available within the EchoPAC Software Only

s supported.

**TABLE 2.7.1
SUPPORTED SPECIFIC CHARACTER SETS**

Defined Term	Character Set Description
ISO_IR 100	Latin alphabet No. 1



3.3 PHILIPS (A28017143)

Cumple los requisitos.

Entrega declaración jurada con el cumplimiento de los requerimientos solicitados: "6 4
Declaracion cumplimiento requisitos PPT .pdf"

y completo de todos los requerimientos solicitados en el Pliego de Prescripciones Técnicas.

Que el equipo ofertado por la empresa a la que representan, PHILIPS IBÉRICA, S.A. (Sociedad Unipersonal), para el presente expediente de contratación, cumple con los Requerimientos mínimos de conectividad necesaria, según lo estipulado en el documento " 43564 Requerimientos técnicos STS Ecógrafo Neurología HUN-A (OT04-2024) v0.3" y "43564 Requerimientos técnicos STS Anexo II Requerimientos Infraestructuras" que se adjuntan en el pliego.

Describe en varios de sus documentos la conectividad DICOM.

Dispone de **NetLink/DICOM 3.0** que proporciona impresión y almacenamiento en red, commitment, worklist, MPPS y Q&R. Generación de informes estructurados para eco en adultos, eco pediátrica y aplicaciones vasculares: DICOM verification SCU/SCP, DICOM Storage, DICOM Query/Retrieve, DICOM StC (Storage Commitment), DICOM Worklist SCU, Basic Greyscale Print SCU, DICOM MPPS (Modality Performed Procedure Step).

La plataforma tiene la capacidad de almacenar datos e imágenes en disco duro, en DVD/CD o medio USB.

Posibilidad de exportar imágenes y vídeos tanto en formato PC como DICOM.

Posibilidad de enviar estudios vía DICOM de forma inalámbrica (Seguridad WEP).

Permite el Multi-Modality Query/Retrieve para visualización en tiempo real con imágenes importadas a la plataforma COMPACT 5000, previamente grabadas en MRI, CT, mamografía o ultrasonido utilizando el protocolo DICOM.

Es capaz de almacenar imágenes en datos brutos.

Posibilidad de acceso remoto para diagnóstico y atención inmediatos a través del Philips.

Remote Service mediante una conexión LAN (incluido durante garantía).

Sistema de autodiagnóstico que permite una rápida identificación de errores de software y su corrección mediante un back-up de restauración del sistema.



4 VALORACIÓN

Las ofertas **cumplen** los requisitos Técnicos STS de conectividad DICOM a Imagen Digital.