



Requerimientos técnicos STS (IBE008-2024 2 máquinas de anestesia HRS)

Gesprona 42283



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 la plataforma de integración de dispositivos médicos SILAGUN	3
1.3.1	Interfaz de comunicación	3
1.3.2	Requisitos para integración con SILAGUN	4
1.3.3	Documentación técnica a presentar	4
2	REQUISITOS TÉCNICOS DE INFRAESTRUCTURAS PARA PLIEGOS TÉCNICOS	5



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*.

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 la plataforma de integración de dispositivos médicos SILAGUN

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 genere datos a ser recogidos por el producto SILAGUN, y que requieran ser trasladados a terceros productos del SNS-O para la persistencia de los mismos (SICCA, QREA, Irati+, etc.)

Las conexiones de SILAGUN con los equipos generalmente se realizan a través de concentradores Serie RS232/Ethernet de marca DIGI (Connect ES) a excepción de:

- Monitores multiparamétricos: Deben implementarse con una solución basada en Gateway TCP/IP con la que interactuara SILAGUN.
- Bombas de perfusión: Deben implementarse con una solución basada Gateway o rack de comunicaciones que recoja los datos de cada dispositivo y disponga de un interfaz ethernet para su conexión a servidor de integración de SILAGUN vía TCP/IP

1.3.1 Interfaz de comunicación

Conectividad TCP/IP

- Interfaz física: RJ45



- Estándar de red de área local: Ethernet.
- Protocolo de red: TCP/IP

Conectividad Serie

- Interfaz física: RS232 DB9 o similar
- Protocolo de comunicaciones RS232.

Otros tipos de Conectividad

- Para cualquier otro tipo de conector (USB, etc.), el adjudicatario deberá aportar el hardware necesario para la conversión a RS232 con conector RJ45.

1.3.2 Requisitos para integración con SILAGUN

Todos los equipos deben tener habilitada la exportación de datos sin requerir de licencias o costes adicionales para ello.

Las ofertas para equipos basados en Gateway deben incluir el propio Gateway (hardware y software) o, en caso de ya existir el mismo en SNS-O, asegurar que el Gateway existente puede asumir la integración de los nuevos equipos sin requerir costes adicionales de licencias.

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, a excepción de los que requieren un tráfico broadcast entre los equipos y el servidor ya que estarán ubicados en VLAN diferenciadas.

El adjudicatario podrá ser requerido a colaborar con personal de la DGTD durante la posible integración del dispositivo con SILAGUN. El plan del trabajo de la integración del equipo estará condicionado por la priorización del mismo por el Responsable de Negocio de SILAGUN y el plan de otros trabajos ya existente en el Programa del mismo.

1.3.3 Documentación técnica a presentar

Las empresas licitantes de estos equipos deberán aportar como parte de su documentación técnica las diferentes propuestas de arquitectura necesarias para la posible integración de su producto con la SILAGUN.

En el caso de comunicaciones por el estándar RS232 debe incluir:

- Esquema de transformación de pines RS232 a conector RJ45,
- Documentación técnica con el protocolo de comunicación entre el equipo y terceros
- Documentación técnica de las secuencias que el equipo emite como datos.
- Instrucciones de acceso a la configuración del equipo para configuración de los parámetros RS232.
- Ejemplo sencillo y claro de los comandos necesarios para la explotación de la información del equipo y un esquema temporal detallado de todos los comandos necesarios a enviar y las respuestas recibidas por el dispositivo, cómo interpretar/trasformar dichas respuestas a una codificación UTF-8 y, si se usa un sistema de control CHK, ejemplo de cálculo del mismo.

En el caso de comunicaciones HL7 vía Ethernet debe incluir:

- Documentación técnica con el protocolo de comunicación entre el Gateway y terceros.
- Documentación técnica de las secuencias que el equipo emite como datos.
- Ejemplo sencillo y claro de la mensajería HL7 necesarias para la explotación de la información del equipo.



2 REQUISITOS TÉCNICOS DE INFRAESTRUCTURAS PARA PLIEGOS TÉCNICOS

Requerimiento SI la oferta incluye equipamiento (servidores, licencias, software, estaciones de trabajo, ...) adicionales a los equipos.

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

42283 ANEXO II - Escenario Tecnológico Gobierno de Navarra Febrero 2024 v1.1.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)
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 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 applets 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 *autologon* 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 *autologon*, 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 *appliances* o con sistemas embebidos:

- Para *appliances* que se encuentren en redes que ofrecen servicio



frontend hacia Internet, la cadencia es mensual de la distribución de las actualizaciones de seguridad (erratas) publicadas por el proveedor.

- Para el resto de *appliances* 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)