



Requerimientos técnicos STS para ECG FIJOS y ECG PORTÁTILES en Atención Primaria

Gesprona 43092



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 Fuentes de los desarrollos realizados a medida para el SNS-O	3
1.4 Seguridad	4
1.5 Planificación	4
1.6 Plan de formación	4
1.7 Soporte de tercer nivel	5
1.7.1 Requisito concreto	5
1.7.2 Requisito genérico	5
1.8 Mantenimiento	6
2 REQUISITOS PARA LA INTEGRACIÓN CON IMAGEN MÉDICA DIGITAL	7
2.1 Conectividad	7
2.2 Estándar DICOM	7
2.3 Estudios DICOM	8
2.4 Electrocardiógrafos	8
2.4.1 Opción A	9
2.4.2 Opción B	9
3 DEMOSTRACIÓN	10
3.1.1 Entrega de documentación	10
3.1.2 Validación del circuito de conectividad	10
4 REQUISITOS TÉCNICOS DE INFRAESTRUCTURAS PARA PLIEGOS TÉCNICOS	11



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.

El licenciamiento deberá permitir soportar hasta 250 licencias concurrentes

1.3 Fuentes de los desarrollos realizados a medida para el SNS-O

El Adjudicatario entregará las fuentes, scripts, y cualquier otra documentación requerida que se desarrolle expresamente para el SNS-O.



1.4 Seguridad

El Sistema de Información deberá cumplir la normativa de seguridad aplicable.

Si el Adjudicatario suministra un Sistema de Información web, deberá cumplir con buenas prácticas de programación segura existentes (en un sentido amplio, pudiendo basarse en recomendaciones de entidades internacionales reconocidas como OWASP, WASC, etc.), reservándose la DGTD la facultad de realizar una auditoría al respecto para evaluar el grado de cumplimiento y detectar posibles deficiencias que pudiesen existir. En caso de detectarse incumplimientos y/o vulnerabilidades que puedan comprometer gravemente la seguridad del servicio prestado por la aplicación o de sus usuarios, el Adjudicatario se compromete a subsanarlas en tiempo y forma, antes de poner dicho servicio a disposición de los usuarios.

1.5 Planificación

Es necesario que los ofertantes presenten los cronogramas en los que se deben especificar los contenidos o tareas y su distribución en el tiempo.

La primera tarea del Adjudicatario será acordar un diseño de solución integrado y una planificación en detalle para su implantación con el equipo de la DGTD y del SNS-O.

1.6 Plan de formación

El adjudicatario estará obligado a realizar las acciones formativas que precise el órgano de contratación para asegurar el manejo del equipamiento y los sistemas de información, en su más óptima utilización, tanto desde el punto de vista operativo como funcional entendiéndose, en cualquier caso, que la amplitud y la calidad de la formación propuesta será precisa para el perfecto manejo y máximo rendimiento del equipamiento y los sistemas de información objeto del contrato.

Esta formación deberá ser especializada para cada tipo de usuario para utilizar el equipamiento y los sistemas de información en la forma prevista por el fabricante y efectuar adecuadamente las rutinas de servicio.

Cualquier modificación/actualización del equipamiento y los sistemas de información conllevará un periodo de formación del personal en los mismos términos señalados anteriormente.

Será, por tanto, de naturaleza obligatoria, que el/los adjudicatarios/s estén a disposición del SNS-O para realizar la formación y entrenamiento adecuado en el uso del equipamiento y los sistemas de información en las condiciones que se indiquen.

- Deberá formar al servicio en el uso de envío a la Historia clínica en cada una de las sedes donde se distribuyan los Electrocardiógrafos.
- Esta planificación para visitar las sedes de manera previa y con aviso de 30 días naturales, de manera coordinada con STS y la coordinación de ATT primaria.



1.7 Soporte de tercer nivel

1.7.1 Requisito concreto

El Adjudicatario habilitará un servicio de atención mediante teléfono, correo electrónico o herramienta de gestión de incidencias que registrará y solucionará las incidencias y consultas técnicas comunicadas por el segundo nivel de soporte del GN.

- El acceso a este servicio será, como mínimo, en días laborables, de lunes a viernes, de 8:00 a 15:00 horas.
- El tiempo de contestación por parte del Adjudicatario será de 24h desde la recepción para las incidencias y consultas técnicas.
- El Adjudicatario registrará todas las peticiones y dará respuesta telefónicamente o por e-mail con la consiguiente solución.
- El adjudicatario deberá garantizar la sustitución de piezas durante un mínimo de 10 años

Así mismo el Adjudicatario se compromete a disponer, bajo petición, de un técnico especialista que colabore en la resolución de aquellas incidencias que se consideren necesarias, en comunicación directa con los técnicos de soporte de segundo nivel de GN o con otros técnicos que GN decida. El Adjudicatario se compromete a servir en un mínimo de 48 horas el soporte online remoto por teléfono o videoconferencia.

1.7.2 Requisito genérico

El Adjudicatario se compromete a ofrecer un plan de soporte en el que se reflejarán los horarios de atención, los métodos de comunicación, el tipo de actuaciones (si son remotas o in situ). Como mínimo existirá un soporte de tercer nivel que atenderá las peticiones de los técnicos del GN

La empresa adjudicataria se integrará como tercer nivel de soporte en el modelo de soporte de referencia del STS (Servicio de Sistemas de Información del Área Sanitaria) de la DGTD.

La empresa deberá garantizar un soporte que comprenderá todo el horario potencial de funcionamiento del sistema de información en el que se establecerán sus condiciones de tiempos de atención, tiempos de respuesta, etc.

El Sistema de Información se implantará atendiendo a alguno de los escenarios de acceso normalizados para los proveedores.

La consideración de días festivos en relación al soporte, serán los determinados por las administraciones públicas de Navarra en las distintas localidades donde se utilice el sistema de información.

El adjudicatario estará obligado a realizar las acciones formativas que precise el órgano de contratación para asegurar el manejo del equipamiento y los sistemas de información, en su más óptima utilización, tanto desde el punto de vista operativo como funcional entendiéndose, en cualquier caso, que la amplitud y la calidad de la formación propuesta será precisa para el perfecto manejo y máximo rendimiento del equipamiento y los sistemas de información objeto



del contrato.

Esta formación deberá ser especializada para cada tipo de usuario para utilizar el equipamiento y los sistemas de información en la forma prevista por el fabricante y efectuar adecuadamente las rutinas de servicio.

Cualquier modificación/actualización del equipamiento y los sistemas de información conllevará un periodo de formación del personal en los mismos términos señalados anteriormente.

Será, por tanto, de naturaleza obligatoria, que el/los adjudicatarios/s estén a disposición del SNS-O para realizar la formación y entrenamiento adecuado en el uso del equipamiento y los sistemas de información en las condiciones que se indiquen.

1.8 Mantenimiento

El Adjudicatario se compromete a analizar y atender los errores de funcionamiento una vez hayan sido reportados, en un plazo inferior a 6 horas desde la notificación. Durante el periodo de garantía fijado en 10 años.

Según el apartado “2.4 Electrocardiógrafos” del presente documento. Si los electrocardiógrafos trabajan con algún elemento intermedio con la “Opción B”. Se deberá entregar una ficha con la siguiente información.

- Coste de mantenimiento anual del servidor, pasado el período de garantía de 10 años, indicando que incluye dicho mantenimiento.
- Coste de ampliación de licencias para soportar más de 250 ECGs.



2 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*” **como requisito imprescindible para la valoración de los requerimientos STS**

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 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.
- Tanto los electrocardiógrafos fijos como los electrocardiógrafos portátiles, deberán disponer de conectividad WIFI cumpliendo la Autenticación IEEE 802.1x WPA2-Enterprise y configurar un Usuario/Contraseña de Directorio Activo que se le proporcionará desde la DGTD.

2.2 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.

Servicios DICOM

El SNS-O considera imprescindibles los siguientes servicios DICOM:



- DICOM WLM (DICOM worklist manager). Permite la recepción de la lista de trabajo desde el PACS.
- DICOM Storage (Almacenamiento DICOM). Permite el envío de 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 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.

2.3 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, PatientID, ...) serán iguales en todos los objetos DICOM de una misma cita.
- Informes gráficos. Los informes gráficos que se envíen al PACS deben implementar DICOM WaveForm., compatible con tira de ritmo.

2.4 Electrocardiógrafos

Si el electrocardiógrafo implementa el estándar DICOM, deberá enviar directamente los electrocardiogramas (ECGs) al PACS.

Independientemente de que el electrocardiógrafo implemente el estándar DICOM o requiera de un componente externo, debe cumplir:

- Los ECGs deberán solicitar la lista de trabajo, simultáneamente con los tags DICOM AETitle y StationName, del propio aparato.
- El personal sanitario únicamente utilizará el electrocardiógrafo. La carga de la WorkList del PACS y el envío de los estudios al PACS deberá realizarse sin la interacción de un usuario, de la forma más desatendida posible.
- El ECG sea capaz de enviar varios estudios dentro de la misma prestación (WorkList).
- El ECG sea capaz de visualizar los ECGs realizados que están en la caché.
- El ECG sea capaz de enviar tiras de ritmo unidas a la prestación (WorkList).



- El ECG sea capaz de enviar estudios ECGs auto y tiras de ritmo en la misma prestación-cita (WorkList).
- El tiempo de retardo entre la finalización del estudio y la llegada al PACS no puede superar los 5 seg.

Las empresas que ofrezcan ECGs con la opción A, para realizar el envío de estudios directamente al PACS, obtendrán una puntuación adicional según los criterios valorables del PPT.

2.4.1 Opción A

De forma nativa, sin requerir servidores ni otros productos intermedios. En la pantalla del electrocardiógrafo se mostrará la lista de trabajo (recuperada de la WorkList del PACS). Una vez seleccionado el paciente de la lista se realizará el ECG y al terminar el estudio se enviará al PACS en formato DICOM WaveForm

2.4.2 Opción B

En caso de que el electrocardiógrafo requiera de un componente o servidor adicional externo para enviar los ECGs al PACS:

- Tendrá capacidad para gestionar al menos 250 ECGs.
- Tendrá capacidad para gestionar varias listas de trabajo entregadas por el PACS. Deberá ser capaz de indicar la lista de trabajo asociada a uno o varios ECGs.
- Se valorará positivamente que sea capaz de gestionar varios PACS, tanto para las solicitudes de listas de trabajo como para el almacenamiento de ECGs. Esta capacidad permitirá cargar una o varias Worklist de un PACS en uno o varios electrocardiógrafos y enviar los estudios de estos electrocardiógrafos a ese mismo PACS. Ese mismo componente permitirá cargar otras Worklist de otros PACS en otros electrocardiógrafos y que éstos envíen los estudios a su respectivo PACS.
- El coste (licencia, implantación e integración) deberá estar incluido en la oferta.
- Incluirá el coste de mantenimiento, licenciamiento y atención de soporte durante 10 años desde la fecha de firma.
- Deberá disponer de un servidor durante las pruebas del concurso, según el siguiente punto.



3 DEMOSTRACIÓN

Durante el concurso, tras la solicitud de la documentación previa a la adjudicación, se realizarán pruebas para validar la conectividad. Entrega de documentación

La oferta deberá incluir los siguientes documentos

- Resumen de toda la Información actual
- Declaración Jurada STS del cumplimiento de los requerimientos STS
- Documento DICOM CONFORMANCE de los Electrocardiógrafos
- Dos ficheros con estudios DICOM: uno de tira de Ritmo y un electro.
- Si el producto ofertado requiere un servidor intermedio, según la opción B del apartado 2.4
 - Precio del Mantenimiento tras el periodo de garantía del servidor de 10 años
 - Características de Hardware y cumplimiento de la documentación del apartado 4 al completo, para un servidor que admita como mínimo 250 clientes ECG conectados.

3.1.1 Validación del circuito de conectividad

- 15 días antes de la realización de las pruebas, desde STS se facilitará una dirección IP para el ECG fijo y portátil por Ethernet, otra dirección IP para la interfaz Wifi, y si lo hubiera, otra dirección IP para el servidor de la Opción B, apartado 2.4.
- STS validará la conectividad de los ECG ofertados, tanto fijos como portátiles. Realizando las siguientes pruebas que entregarán un APTO al lote conjunto.
 - Validación de la conectividad ethernet
 - Validación de la conectividad wifi
 - Prueba de circuito de entrega de estudios al PACS Historia Clínica.
 - Envío de estudio al PACS
 - Envío tira de ritmo a PACS
 - Visualización de estudio en visor Raim Viewer
 - Visualización de estudio en Alma Workstation
- Si la validación de la integración de los ECG fuera la Opción A del apartado 2.4, sin necesidad de requerir un servidor intermedio, entregando los estudios de forma nativa, se aplicarán los criterios de puntuación indicados en el PPT.
- Si hubiera cualquier problema con la entrega de estudios según los criterios anteriores, desde STS solo se facilitará soporte para la conectividad, no para el desarrollo o evolución del producto del proveedor.



4 REQUISITOS TÉCNICOS DE INFRAESTRUCTURAS PARA PLIEGOS TÉCNICOS

En caso que la oferta del adjudicatario requiera la implantación de un servidor intermedio, el adjudicatario asumirá los costes y licenciamiento necesario para que funcione su producto.

Gobierno de Navarra facilitará una instancia virtual con los requerimientos de hardware indicados en la siguiente tabla.

El servidor deberá ser capaz de gestionar 250 ECGs de manera simultanea

El soporte y posibles problemas generados en la evolución del producto estará incluido durante los 10 años se servicio ofertado, garantizando la seguridad de los sistemas y la actualización de los mismos, aplicando parches para brechas de seguridad, etc.

Si hubiera un servidor intermedio, deberá estar montado 90 días desde la adjudicación del contrato y destinará todos los recursos necesarios para llevar a cabo su instalación, desde el momento en el que Gobierno de Navarra entregue la máquina virtual y acceso VPN.

Si la oferta incluye equipamiento (servidores, licencias, software, estaciones de trabajo, ...) que no son parte de la propia modalidad médica, deberán cumplir de forma general el Escenario Tecnológico de Gobierno de Navarra que está publicado en:

ANEXO STS - INFRAESTRUCTURAS Escenario Tecnológico GdN Junio 2024 **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)	
--	--