1 REQUISITOS TÉCNICOS STS (SERVICIO DE TECNOLOGÍA DE SALUD)

1.1 Requisitos técnicos

El adjudicatario deberá instalar el equipo en el lugar que indique la propiedad y dejarlo en perfecto estado de funcionamiento. Para ello se entregarán todos los cables y elementos necesarios para ello.

Las estaciones que formen parte de la solución informática aportada por el adjudicatario deberán poder ajustarse al estándar de Gobierno de Navarra.

El software de control ofrecerá una interfaz para configurar, iniciar y supervisar los experimentos:

- La interfaz será intuitiva y fácil de usar.
- El equipo deberá registrar en todo momento las acciones realizadas por los diferentes usuarios.

Toda la configuración de conectividad de los dispositivos deberá quedar accesible y documentada para su consulta y/o modificación por parte de los técnicos especializados que la Dirección General de Transformación y Digitalización determine.

1.2 Requisitos de integración con los sistemas de información del SNS-O

En caso de que los sistemas de información que formen parte de la solución ofertada por el Adjudicatario requieran integrarse con los sistemas de información del SNS-O, será 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 construidos 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.

1.3 Soporte

1.3.1 Soporte técnico de atención al usuario de acuerdo a:

Atención telefónica inmediata a cargo de técnicos con conocimientos suficientes del producto y su infraestructura técnica para todos los centros con horario de 08:00 horas a 18:00 horas, todos los días del año.

También existirá la posibilidad de realizar acciones correctivas de forma remota.

La empresa deberá indicar en su oferta el procedimiento de activación de este soporte técnico (nº de teléfono, nº de fax, E-Mail, etc.) así como posibles variaciones en los horarios.

1.3.2 Soporte técnico in-situ

Dicho soporte se realizará en las instalaciones del gobierno de Navarra, por técnicos cualificados para la corrección de anomalías o mal rendimiento del sistema que no hayan podido arreglarse por otros medios.

Si el problema del sistema interfiere gravemente la actividad de la unidad que utiliza el sistema, deberá personarse el técnico en un plazo máximo de 24 horas.

1.3.3 Mantenimiento correctivo y preventivo

Este servicio incluye la actualización de versiones del software, si se incluye en la oferta.

También estarán incluidos los trabajos de configuración y puesta en marcha de los nuevos módulos que incorporen las aplicaciones en las nuevas versiones.

Estos trabajos se realizarán por la empresa de manera continuada a lo largo de la vigencia del contrato, de manera que los usuarios de los diferentes centros del Servicio Navarro de Salud – Osasunbidea que utilizan estos programas y los técnicos del Gobierno de Navarra tengan disponibles unos servicios técnicos para solicitar su atención cuando sea necesario.

El Adjudicatario se compromete a solucionar los errores de funcionamiento una vez hayan sido reportados.

1.3.4 Actualización de las aplicaciones

El proveedor se compromete a la actualización que sean necesarias para la renovación tecnológica que defina la DGTD, como puede ser: parches de seguridad, actualizaciones a Sistemas Operativos que tengan Soporte del Fabricante etc.

El equipo de trabajo designado por el proveedor trabajará in situ, en colaboración con el personal de Gobierno de Navarra, en las instalaciones del cliente mientras duren los trabajos de implantación y estabilización.

El proveedor proporcionara la formación en el software de forma que se asegure que los usuarios han adquirido los conocimientos necesarios para la configuración, puesta en marcha y uso del sistema.

El proveedor proporcionara la documentación técnica y funcional necesaria que le requiera Gobierno de Navarra.

1.3.5 Soporte de tercer nivel

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 Tecnología de Salud) 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.

1.4 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.

1.5 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.

1.6 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.

1.7 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.

1.7.1 Plan de instalación y puesta en marcha

Las empresas licitadoras deberán aportar un plan específico y cronograma de las actuaciones necesarias para la instalación y puesta en funcionamiento del equipamiento, servicios y software ofertados

Se aportará una propuesta metodológica para el desarrollo de las tareas de seguimiento y cumplimiento de los hitos y actuaciones necesarias que aseguren la correcta implantación del proyecto.

1.8 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 adjudicatario/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.

2 REQUISITOS TÉCNICOS DE SITYCS (SERVICIO DE INFRAESTRUCTURAS TECNOLÓGICAS Y CENTRO DE SOPORTE)

Todos los sistemas que requieran de conexión a la red de Gobierno de Navarra o internet deberán cumplir de forma general el Escenario Tecnológico del Gobierno de Navarra

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 (Si)
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 *appliance* 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 *extranet* con doble factor • VPN de sitio a sitio	
Los sistemas e información basados en sistemas operativos Microsoft 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 (SI)
El sistema de información se monitorizará con las herramientas que forman parte del escenario de monitorización: • Microsoft **SCOM**: Herramienta de monitorización de disponibilidad y rendimiento de infraestructuras y aplicaciones. • **Lookwise** de S21Sec: Herramienta de tipo SIEM orientada a la recolección y monitorización de eventos de seguridad que permite garantizar el cumplimiento de normativas de seguridad. • **NetScout Performance Manager**: Herramienta de monitorización y rendimiento de redes, infraestructura servidor y aplicaciones a partir del tráfico de red.	
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 *applets*.	
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.	

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 necesaria para soportar su propuesta.	
Dimensionamiento de los sistemas de información:	
CPU (nº de núcleos)	
Memoria (MB)	
Disco (GB)	
Sistema gráficos (resolución)	
Puertos de entrada y salida	
Periféricos	
Almacenamiento externo	
Latencia	
Rendimientos (*Throughputs*)	
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 *URLs* 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 cuatrimestral 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:** • Para servidores Linux que se encuentren en redes que ofrecen servicio *frontend* hacia Internet tendrán cadencia mensual de una distribución de las actualizaciones de seguridad (erratas) publicadas por el proveedor. • Para el resto de servidores Linux la cadencia es cuatrimestral. • 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:** Las actualizaciones de seguridad incluidas son: • Aquellas designadas por Microsoft como 'críticas' e 'importantes'. • Adobe Flash Player, Adobe Reader, Adobe Shockwave, IZArc, Java Runtime, Libreoffice. • Software adicional instalado por el proveedor. **Periodicidad mínima**: con una cadencia trimestral se realizará una actualización a las estaciones de trabajo 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 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 cuatrimestral. • 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)	