



---

# **Requerimientos DGITIP para los pliegos de los expedientes de adquisición de un suministro**

V 5



# Índice de contenidos

<b>1</b>	<b>INTRODUCCIÓN</b>	<b>4</b>
1.1	Objetivos del documento	4
<b>2</b>	<b>CONDICIONES TÉCNICAS DE INFRAESTRUCTURAS INFORMÁTICAS5</b>	
2.1	Cláusulas generales a cualquier pliego	5
2.2	Cláusulas específicas en función de la tecnología	5
2.3	Cláusulas para la explotación de los sistemas de información	5
2.4	Cláusulas de seguridad	6
<b>3</b>	<b>REQUISITOS PARA LA INTEGRACIÓN EN EL SISTEMA DE IMAGEN MÉDICA DIGITAL DEL SNS-O</b>	<b>7</b>
3.1	REQUISITOS DE CONECTIVIDAD	7
3.1.1	Conectividad a nivel TCP/IP	7
3.1.2	Conectividad a nivel DICOM	7
3.2	REQUISITOS MODALIDAD DEPENDIENTE	8
3.2.1	Equipos que generan información en forma de gráficas	8
3.2.2	Equipos que emitan radiación ionizante	8
3.3	OTROS REQUISITOS	8
3.4	REQUISITOS ELECTROCARDIOGRAMAS (ECGs)	8
3.4.1	ECGs “puros” DICOM	8
3.4.2	ECGs DICOM con Integrador	8
3.5	REQUISITOS ECOCARDIÓGRAFOS	8
<b>4</b>	<b>REQUISITOS PARA LA INTEGRACIÓN EN EL SISTEMA DE INFORMACIÓN DE CUIDADOS CRÍTICOS Y ANESTESIA (SICCA)</b>	<b>10</b>
4.1	REQUISITOS DE CONECTIVIDAD	10
4.1.1	Conectividad a nivel TCP/IP	10
4.1.2	Conectividad a nivel Serie RS232	10
4.1.3	Otros tipos de Conectividad	10
4.2	REQUISITOS DE SOFTWARE	10
4.3	REQUISITOS DE DOCUMENTACIÓN	10
4.4	OTROS REQUISITOS	11
<b>5</b>	<b>ANEXO I. ESCENARIO TECNOLÓGICO</b>	<b>12</b>
<b>6</b>	<b>ANEXO II – MODELO DE SOPORTE DE REFERENCIA DEL SSIAS</b>	<b>13</b>
6.1	Responsables	13
6.2	Plan de soporte	13
6.2.1	Flujo general de incidencias - HGT	13
6.2.2	Equipo de soporte	17
6.3	Plan de operación	18
6.4	Plan de gestión de cambios	18
<b>7</b>	<b>ANEXO III – ESCENARIOS DE ACCESO REMOTO NORMALIZADO PARA PROVEEDORES</b>	<b>19</b>
7.1	Equipos gestionados exclusivamente por el proveedor	19
7.2	Equipos con software base de Gobierno de Navarra y sistema de información gestionado por el proveedor	20



### 7.3 Equipos completamente gestionados por Gobierno de Navarra



# 1 INTRODUCCIÓN

## 1.1 Objetivos del documento

El presente documento tiene como objetivo principal recoger todos los requisitos que deberían incluirse en todos los pliegos de condiciones de cualquier expediente de equipamiento donde se incluyan elementos hardware o software que deban conectarse a la red corporativa del GN.



# 2 CONDICIONES TÉCNICAS DE INFRAESTRUCTURAS INFORMÁTICAS

## 2.1 Cláusulas generales a cualquier pliego

- Los sistemas de información que se implanten deberán cumplir el [Escenario Tecnológico del Gobierno de Navarra](#).
- Antes de la puesta en explotación, la empresa adjudicataria entregará al GProy de la DGITIP, los documentos necesarios que permitan una explotación y soporte adecuado de los sistemas de información. Como mínimo deberá aportar los siguientes: Diseño Lógico y Físico, Plan de Explotación, Manual de Operación y Soporte y Modelo Administrativo y cualquier otro documento de planificación, implantación, etc.
- La empresa adjudicataria impartirá la formación técnica adecuada que permita el soporte y operación de los sistemas de información que implante y el soporte funcional a los usuarios y grupos de soporte que determine la DGITIP (CAU, OTSI's, OS2N, etc.).
- El coste de la integración con los sistemas de información del GdN correrá a cargo de la empresa adjudicataria.
- Cualquier sistema de información que genere imagen médica deberá cumplir el punto 3 *REQUISITOS PARA LA INTEGRACIÓN EN EL SISTEMA DE IMAGEN MÉDICA DIGITAL DEL SNS-O* salvo que explícitamente se indique en el pliego.

## 2.2 Cláusulas específicas en función de la tecnología

- Todos los sistemas de información de servidor serán virtualizables y alojados en la plataforma de virtualización VMWare con las características y condiciones descritas en el Escenario Tecnológico.
- Cualquier aparato que se quiera conectar a la red de datos deberá contar con conectividad RJ45.

## 2.3 Cláusulas para la explotación de los sistemas de información

- Las licencias de software 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 del sistema operativo o del servidor de aplicaciones.
- El sistema de información se monitorizará con las herramientas que forman parte del escenario de monitorización:
  - o Microsoft SCOM: Herramienta de monitorización de disponibilidad y rendimiento de infraestructuras y aplicaciones.
  - o Bitácora 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.
  - o NetScout Performance Manager: Herramienta de monitorización y rendimiento de redes, infraestructura servidor y aplicaciones a partir del tráfico de red.
- La empresa adjudicataria se integrará como tercer nivel de soporte en el [modelo de soporte de referencia del SSIAS](#) (Servicio de Sistemas de Información del Área Sanitaria).
- 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](#).



## 2.4 Cláusulas de seguridad

- El sistema de información deberá cumplir la normativa de seguridad aplicable.
- Si la empresa adjudicataria 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 DGITIP 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, la empresa adjudicataria se compromete a subsanarlas en tiempo y forma, antes de poner dicho servicio a disposición de los usuarios.



## 3 REQUISITOS PARA LA INTEGRACIÓN EN EL SISTEMA DE IMAGEN MÉDICA DIGITAL DEL SNS-O

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".

Así mismo, las empresas que resulten adjudicatarias se comprometen a integrarlos en el Sistema de Imagen Médica Digital del SNS-O.

Toda la configuración de conectividad, tanto TCP/IP como DICOM, deberá quedar accesible y documentada para su consulta y/o modificación por parte de los técnicos especializados que la DGITIP determine, y a ser posible, protegida por contraseña.

### 3.1 REQUISITOS DE CONECTIVIDAD

#### 3.1.1 Conectividad a nivel TCP/IP

- a) Conectividad Ethernet RJ45.
- b) Conectividad Ethernet inalámbrica para aquellos equipos que sean móviles. Cumplir los estándares: 802.11g, 802.11n, 802.1x (implementado TLS y se valorará la inclusión de SCEP).
- c) El equipo debe tener implementado y operativo el protocolo de comunicaciones TCP/IP.

#### 3.1.2 Conectividad a nivel DICOM

El equipo debe implementar el estándar DICOM versión 3.

Todos los parámetros de conexión con el PACS de los distintos Servicios DICOM (IP, puerto, AET, etc.) deberán poder ser configurados según las necesidades del Gobierno de Navarra. La configuración DICOM inicial de los equipos del adjudicatario será realizada por sus propios técnicos de conformidad con las instrucciones que le sean dadas desde la DGITIP.

**Los Servicios DICOM, al menos los imprescindibles, deben estar operativos y funcionales.** Esto implica que **no son aceptables** situaciones como las siguientes:

- Se requiera el pago de alguna licencia, activación, o cualquier otro cargo para permitir su uso.
- Se requiera el pago al servicio técnico de la casa para que lo configuren adecuadamente.
- Sólo soporta parte de los servicios y/o sólo parte de ellos estén operativos.

##### 3.1.2.1 Servicios DICOM imprescindibles

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

##### 3.1.2.2 Servicios DICOM recomendables

- a) **DICOM Print**. Permite imprimir imágenes en una impresora DICOM. Interesante sobre todo para preparar planes de contingencia.
- b) **DICOM QR** (DICOM Query/Retrieve). Consulta y recuperación DICOM. Permite que el equipo consulte y pida estudios a un PACS. Interesante sobre todo en aquellos equipos que integran software avanzado para la especialidad de que se trate (léase escáner, mamógrafos, etc.)



## 3.2 REQUISITOS MODALIDAD DEPENDIENTE

### 3.2.1 Equipos que generan información en forma de gráficas

El formato en el que se envíen al PACS tiene que ser DICOM WaveForm. Es el caso de Electrocardiogramas, Holter ECGs continuos, pruebas de esfuerzo, etc.

### 3.2.2 Equipos que emitan radiación ionizante

Generará Informe Estructurado de Dosis - SR (Structured Report).

Permitirá enviar los objetos SR al mismo PACS que las imágenes o a otro distinto a decisión de la DGITIP.

## 3.3 OTROS REQUISITOS

Cuando el equipo incluya algún sistema hardware y/o software de almacenamiento de imágenes, postprocesado o similares tendrá que ser **compatible con el escenario tecnológico del Servicio Navarro de Salud y del Gobierno de Navarra**.

## 3.4 REQUISITOS ELECTROCARDIOGRAMAS (ECGs)

Deberá cumplir todos los puntos anteriores. Importante destacar que generarán los estudios en formato DICOM WaveForm.

Los ECGs, dependiendo del tipo de conexión DICOM, se pueden dividir en:

- ECGs “puros” DICOM. El propio ECG incluye la conectividad DICOM (Worklist y Storage).
- ECGs DICOM con Integrador. El ECG se comunica con un software “integrador” en formato propietario. El software integrador es el que realiza la conexión DICOM con el PACS.

### 3.4.1 ECGs “puros” DICOM

En la pantalla del ECG 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 el estudio en formato DICOM WaveForm.

No hay ningún software/servidor entre el ECG y el PACS.

### 3.4.2 ECGs DICOM con Integrador

El personal sanitario únicamente utilizará el ECG. No es admisible el requerimiento de una estación de trabajo.

Requerimientos del software “integrador”:

- Se instalará en un servidor y por tanto se aplicarán las [condiciones técnicas generales de infraestructuras informáticas](#).
- Capacidad para la gestión de un mínimo de 50 ECGs.
- Capacidad para gestionar varias WorkList pedidas al PACS e indicar qué WorkList está asociada a uno o varios ECGs.

Recomendable del software “Integrador”:

- Gestionar varios PACS tanto para la solicitud de WorkList como para el Storage. Esta capacidad permitirá definir una o varias Worklist asociadas a un PACS (PACS-a) a uno o varios ECGs y devolver los estudios de esos ECGs al PACS-a. En el mismo software “integrador” permitirá definir otras Worklist asociadas a otro PACS (PACS-n) a otros ECGs y que éstos devuelvan los estudios a su respectivo PACS-n.

## 3.5 REQUISITOS ECOCARDIÓGRAFOS

Cumplir los requisitos del punto 3.1 REQUISITOS DE CONECTIVIDAD.

Compatibilidad con uno de los sistemas de diagnóstico: XCelera o EchoPac.



## Licencia XCelera o EchoPac



## **4 REQUISITOS PARA LA INTEGRACIÓN EN EL SISTEMA DE INFORMACIÓN DE CUIDADOS CRÍTICOS Y ANESTESIA (SICCA)**

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 Sistema de información de Cuidados Críticos y Anestesia (SICCA a partir de aquí).

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 SICCA.

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 DGITIP determine.

El producto SICCA se basa en el producto comercial Metavision con una conexión de los dispositivos generalmente 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 contra el servidor de integración de Metavision.
- Gasómetros: Conectividad Ethernet directa con servidor de integración de Metavision

### **4.1 REQUISITOS DE CONECTIVIDAD**

#### **4.1.1 Conectividad a nivel TCP/IP**

- a) Conectividad Ethernet RJ45.
- b) El equipo debe tener implementado y operativo el protocolo de comunicaciones TCP/IP.

#### **4.1.2 Conectividad a nivel Serie RS232**

- a) Conectividad Serie / RS232.
- b) El equipo debe tener implementado y operativo el protocolo de comunicaciones Serie / RS 232.
- c) Por cada unidad del equipo suministrado se aportarán 2 conectores/conversores Serie / RJ45

#### **4.1.3 Otros tipos de Conectividad**

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

### **4.2 REQUISITOS DE SOFTWARE**

- a) El licitador debe certificar que el fabricante del producto Metavision dispone del driver de conexión de su dispositivo o, en caso contrario, asumir los costes de su desarrollo para ser usados en el momento de una futura integración con SICCA.
- b) El adjudicatario podrá ser requerido a colaborar con personal de la DGITIP o el fabricante del producto Metavision durante una posible integración del dispositivo con SICCA en algunas extensiones de este producto en el SNS-O

### **4.3 REQUISITOS DE DOCUMENTACIÓN**

- a) Deben suministrarse las credenciales de acceso al dispositivo para acceder y administrar la configuración del protocolo de comunicación.
- b) Incluir manual de configuración TCP/IP o RS232 del dispositivo.



- c) En el caso de conexiones basadas en conectividad Serie /SR232 deberá aportarse el esquema de conversión de conector serie a RJ45
- d) En el caso de conexiones basadas en conectividad Serie /SR232, por cada unidad de equipo suministrado se aportarán 2 conectores/conversores Serie / RJ45

## 4.4 OTROS REQUISITOS

Cuando el equipo incluya algún sistema hardware y/o software necesario para la integración del dispositivo tendrá que ser **compatible con el escenario tecnológico del Servicio Navarro de Salud y del Gobierno de Navarra**.

El proveedor correrá con todos los gastos necesarios para la correcta integración del equipamiento con SICCA, si hubiera que hacer algún desarrollo deberá también financiarlo el proveedor. La DGITIP determinará el proveedor autorizado para realizar los desarrollos correspondientes.



## **5 ANEXO I. ESCENARIO TECNOLÓGICO**

Publicado en el portal del Gobierno de Navarra:

[http://www.navarra.es/home\\_es/Gobierno+de+Navarra/Organigrama/Los+departamentos/Presidencia+justicia+e+interior/Publicaciones/Publicaciones+propias/Modernizacion/Escenario/](http://www.navarra.es/home_es/Gobierno+de+Navarra/Organigrama/Los+departamentos/Presidencia+justicia+e+interior/Publicaciones/Publicaciones+propias/Modernizacion/Escenario/)



# 6 ANEXO II – MODELO DE SOPORTE DE REFERENCIA DEL SSIAS

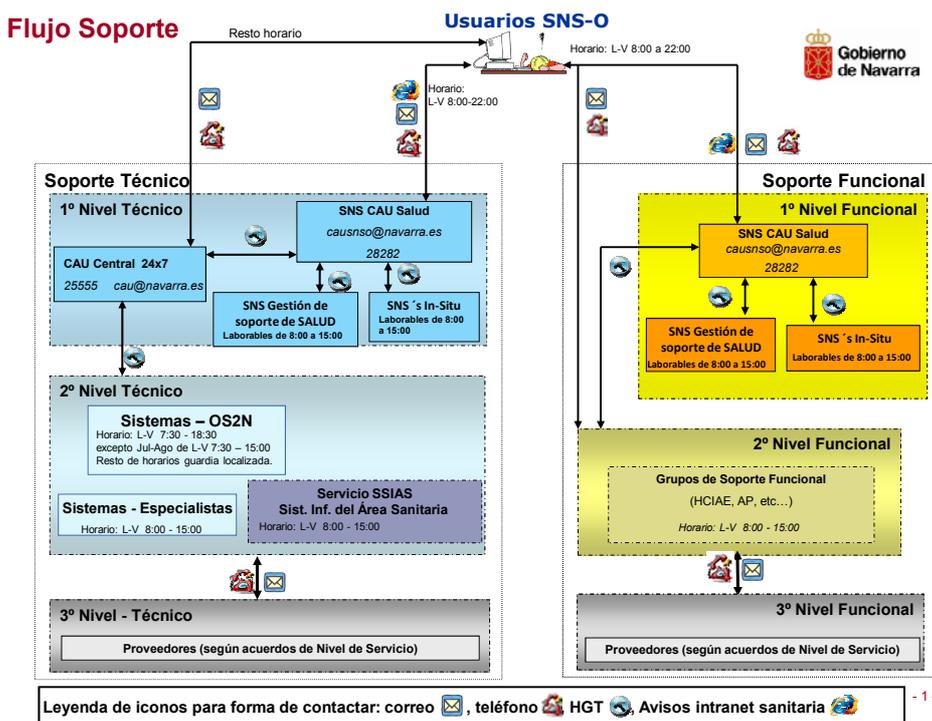
## 6.1 Responsables

En este apartado se deben identificar los responsables del servicio una vez este se encuentre en producción.

- **Responsables de Negocio (RNeg):** persona de la unidad propietaria del sistema de Información, que se responsabiliza internamente en la unidad de obtener el adecuado nivel de servicio, solicitándose a la DGITIP como proveedor.
  - Nombre, email y teléfono
  
- **Responsable Técnico (RTec):** persona dentro de la DGITIP, generalmente de las unidades gestoras de los departamentos, que vela por el cumplimiento global del nivel de servicio deseado por el cliente, promoviendo las acciones y proyectos de mejora oportunos.
  - Nombre, email y teléfono
  
- **Responsable de Explotación (RExp):** persona siempre del Servicio de Infraestructuras, o colaboradores, que se encarga, mediante la adecuada coordinación de los técnicos disponibles, de proporcionar el nivel de servicio de las infraestructuras y el sistema de Información implantado.
  - Nombre, email y teléfono

## 6.2 Plan de soporte Flujo general de incidencias - HGT

La siguiente figura esquematiza el flujo de las incidencias Técnicas a través de los diferentes niveles:



Con carácter general, de lunes a viernes y de 8:00 a 22:00, la primera atención al usuario (la canalización de la incidencia) siempre la realizará el CAU SNS-O (compuesto por los grupos



SNS CAU Salud, SNS's In Situ y SNS Gestión de soporte de salud) para las incidencias técnicas. Fuera de este horario, será el CAU-CENTRAL<sup>1</sup> quien canalice las incidencias técnicas (no las funcionales).

## 6.2.1.1 Soporte de primer nivel

### 6.2.1.1.1 Técnico

El equipo de atención de **primer nivel**<sup>2</sup> es 24x7 y está compuesto por:

- SNS CAU Salud (Lunes a viernes de 08:00 a 22:00)

Entre las responsabilidades del primer nivel, se destaca:

- Registrar las incidencias técnicas o funcionales dependiendo de lo que notifique el usuario del SNS-O en horario de 8:00 a 22:00.
- Realizar tareas de complejidad media tanto técnicas como funcionales procedimentadas por el nivel 2.
- Como norma general no pueden hacer nada "nuevo" sin coordinarse con el nivel 2.
- Hacer las tareas rutinarias sobre la infraestructura.
- Solucionar los problemas que surjan en los puestos de trabajo de los usuarios del SNS-O
- Escalar las incidencias al soporte del segundo nivel y/o tercer nivel según lo establecido en sus procedimientos.
- Cierre de la incidencia, si ha sido resuelta en este primer nivel, y forma de subsanación.
- Tareas de operación de gestión de los usuarios de las aplicaciones del SNS-O
- Tareas de explotación de datos para el usuario del SNS-O.
- Gestión de peticiones de servicio a la DGITIP del SNS-O.

Desde el SNS CAU Salud, vía HGT se pueden derivar las incidencias al grupo SNS's In Situ que aglutina a los OTSIs in situ ubicados en los centros del SNS-O

De igual manera pueden derivar los tickets al Grupo de Gestión del Soporte de Salud y a los Grupos de Soporte Funcional

- CAU-CENTRAL, (Lunes a viernes de 22:00 a 8:00 y fines de semana y festivos 24x7) grupo de técnicos ubicados en el CPD de Gobierno de Navarra.

Entre las responsabilidades del primer nivel, se destaca:

- Registrar las incidencias, así como las solicitudes de actuación para los administradores.
- Realizar tareas de complejidad media procedimentadas por el nivel 2.
- Como norma general no pueden hacer nada "nuevo" sin coordinarse con el nivel 2.
- Hacer las tareas rutinarias sobre la infraestructura.
- Solucionar los problemas que surjan en los puestos de trabajo
- Escalar las incidencias al soporte del segundo nivel y/o tercer nivel según lo establecido en sus procedimientos.
- Cierre de la incidencia, si ha sido resuelta en este primer nivel, y forma de

<sup>1</sup> Los medios para comunicarse con el CAU-CENTRAL están descritos en la intranet de Gobierno de Navarra (<http://catalogoservicios.admon-cfn Navarra.es/C3/CAU/default.aspx>).

<sup>2</sup> Los técnicos de este nivel tienen acceso al entorno de Preproducción y Producción. Los enlaces a la aplicación pueden servir para que el CAU pueda verificar que la aplicación está operativa.



subsanción.

### 6.2.1.1.2 Funcional

De momento el SNS CAU Salud no atiende todas las incidencias funcionales. Lo que hará si detecta que una incidencia es funcional, y no la sabe resolver, será derivarla al Grupo de Soporte Funcional correspondiente.

### 6.2.1.2 Soporte de segundo nivel - HGT

#### 6.2.1.2.1 Técnico

El horario de atención del **segundo nivel** es de 8:00 a 15:00 los días laborables y está compuesto por:

- **Soporte segundo nivel (OS2N):** grupo de técnicos ubicados en el CPD de Gobierno de Navarra en horario de Lunes a Viernes de 7:30 a 18:30, excepto Julio y Agosto que será de 7:30 a 15:00. Es contactado por el primer nivel de soporte técnico (CAU-CENTRAL) y realizará todas aquellas tareas técnicas más específicas y para las cuales han recibido una formación e intentará darle una solución. En caso de no poder resolverla escalará la incidencia al grupo de especialistas de sistemas.
- **Especialistas sistemas:** grupo de técnicos ubicados en el CPD de Gobierno de Navarra en horario laboral de 8:00 a 15:00 horas. Son especialistas en las áreas que participan. Ejemplos:
  - Estaciones de trabajo: darán soporte especializado a los puestos de trabajo de los usuarios.
  - Directorio Activo: darán soporte especializado a los servicios de Directorio Activo, políticas globales sobre los puestos de trabajo, DNS, servidores radius de la red inalámbrica, etc.
  - Servidores Web y de aplicaciones: darán soporte especializado a los servidores de la aplicación.
  - Gestor BBDD: darán soporte especializado a la infraestructura de SQL Server 2005 y de Reporting.
  - Resto de grupos de personas que se encargan de dar soporte a otras infraestructuras como pueden ser la del correo electrónico, antivirus, etc.
- **Grupo de Soporte SSIAS:** grupo que realiza el soporte técnico en horario laborable de 8:00 a 15:00, compuesto por:
  - **Responsables del Grupo**
    - **PATRICIA ARBELOA**
    - **Dirección:** Calle Cabárceno 6, 3ª Planta SARRIGUREN - 31621
    - **Teléfono 1:** 848 425723
    - **E-Mail:** [patricia.arbeloa.marco@navarra.es](mailto:patricia.arbeloa.marco@navarra.es)
  - **Técnico**
    - **Nombre, email y teléfono**
- Es contactado por el primer nivel de soporte técnico (CAU-CENTRAL) a través de HGT.

#### 6.2.1.2.2 Funcional

Entre las responsabilidades del segundo nivel, se destaca:

Atender las consultas sobre funcionamiento que les trasladan desde el primer nivel de soporte. Su mayor nivel de conocimiento les permite diferenciar si la consulta es por una deficiente utilización del usuario o por un problema de funcionamiento del programa.



### **6.2.1.3 Soporte de tercer nivel**

#### **6.2.1.3.1 Técnico**

Completar

#### **6.2.1.3.2 Funcional**

Completar



## 6.2.2 Equipo de soporte

### 6.2.2.1 Técnico

Nivel	Horario	Asignación	Contacto	Responsable
1º	8:00-22:00 (L a V)	CAU SNS-O	Teléfono: 848 <b>428282</b> Correo: <a href="mailto:causnso@navarra.es">causnso@navarra.es</a>	Nombre: Enrique Lorenzo Vello Teléfono: 848 <b>429326</b> <a href="mailto:elorenzov@cfnavarra.es">elorenzov@cfnavarra.es</a>
1º	22:00-8:00 (L a V, fin de semana y festivos)	CAU-CENTRAL	Teléfono: 848 <b>425555</b> Correo: <a href="mailto:cau@navarra.es">cau@navarra.es</a>	Nombre: Roberto Liberal Teléfono: 848 <b>425629</b> Correo: <a href="mailto:rliberao@navarra.es">rliberao@navarra.es</a>
2º	08:00-18:30 Verano: 08:00 a 15:00	Soporte y operación segundo nivel (OS2N)	Teléfono: 848 <b>425845</b> Correo: <a href="mailto:sistemas11@navarra.es">sistemas11@navarra.es</a>	Nombre: Juan Antonio Rozas Teléfono: 848 <b>428824</b> Correo: <a href="mailto:jrosazar@navarra.es">jrosazar@navarra.es</a>
2º	8:00-15:00 (L a V)	Especialistas sistemas		Nombre: Eduardo Zariquiegui Teléfono: 848 <b>428942</b> Correo: <a href="mailto:ezarigua@navarra.es">ezarigua@navarra.es</a>
2º	8:00-15:00 (L a V)	Grupo de Soporte SSIAS	Teléfono: 848 <b>425723</b> Correo: <a href="mailto:soportessias@navarra.es">soportessias@navarra.es</a>	Nombre: Patricia Arbeloa Teléfono: 848 <b>425723</b> Correo: <a href="mailto:patricia.arbeloa.marco@navarra.es">patricia.arbeloa.marco@navarra.es</a>
3º	Proveedor	Proveedor	Proveedor	Proveedor



### 6.2.2.2 Funcional

Nivel	Horario	Asignación	Información de Contacto	Responsable
1º	8:00 – 22:00 (L a V)	CAU SNS-O	Teléfono: 848 428282 Correo: <a href="mailto:causnso@navarra.es">causnso@navarra.es</a>	Nombre: Enrique Lorenzo Vello Teléfono: 848 429326 <a href="mailto:elorenzov@cfnavarra.es">elorenzov@cfnavarra.es</a>
2º	08:00-15:00	Grupo de Soporte Funcional	Depende de cada aplicación	Nombre: Julio Morán Teléfono 848 427227 <a href="mailto:julio.moran.pi@cfnavarra.es">julio.moran.pi@cfnavarra.es</a>
3º	Proveedor	Proveedor	Depende de cada aplicación	Proveedor

## 6.3 Plan de operación

## 6.4 Plan de gestión de cambios



# 7 ANEXO III – ESCENARIOS DE ACCESO

## REMOTO NORMALIZADO PARA

### PROVEEDORES

#### 7.1 Equipos gestionados exclusivamente por el proveedor

Estos equipos son aquellos físicos o virtuales desplegados dentro de la red de Gobierno de Navarra pero que únicamente son gestionados por el proveedor, tanto a nivel de software base (sistema operativo, antivirus, etc.) como a nivel de sistema de información.

Para poder tener acceso desde el exterior el PC debe cumplir las siguientes condiciones:

El equipo debe estar en la VLAN independiente. Si el equipo existe ya y no está en esta VLAN requerirá cambio de dirección IP.

Para equipos de electromedicina (EMED), es decir, PC's de control de analizadores, los propios analizadores y Sistemas de tratamiento clínico y diagnóstico, existen VLAN específicas para equipos médicos en el entorno del CHN, equipos médicos o estaciones de la Fundación Miguel Servet y para máquinas virtuales en el CPD de Orcoyen. Asimismo, en el Hospital García Orcoyen de Estella y en el Hospital Reina Sofía existen VLANes con el mismo propósito.

Para los equipos de domótica, aire acondicionado y alarmas se va a crear una VLAN independiente.

El acceso se podrá hacer a través de dos servicios diferentes que permiten abrir una VPN entre el proveedor y el Gobierno de Navarra. Una vez establecida la VPN podrán acceder con RDP (escritorio remoto), ssh, http, CIFS y otros protocolos, siempre que no supongan un problema de seguridad.

- a. Acceso a través del Portal VPN: Para ello necesitan contar con un usuario de directorio activo. El acceso por http y CIFS entre otros se puede hacer únicamente ingresando en el portal y permite tener las URLs/rutas publicadas en el mismo. El acceso por RDP y ssh requiere establecer un túnel SSL pulsando sobre el botón Conectar. Esta opción tiene menos usabilidad para los proveedores que una VPN sitio a sitio.
- b. Acceso a través de una VPN sitio a sitio: Se trata de establecer una VPN a nivel de equipos de electrónica entre el proveedor y Gobierno de Navarra. Es necesario que el equipo de electrónica del proveedor permita este tipo de conexión y que firme un contrato con Gobierno de Navarra. Esta opción es la más usable para el proveedor.

Se recomienda que el equipo disponga de un antivirus para no contagiar a otros equipos de la misma red.

El equipo podrá acceder a recursos de red, al Directorio Activo, copias de seguridad, monitorización y otros servicios horizontales siempre que se cumplan las normas de acceso seguro en cada caso.

El responsable de explotación se deberá encargar, con la periodicidad que establezca el procedimiento de instalación de parches (actualmente cada 3 meses), de que el proveedor mantenga actualizados los parches en el equipo.



## 7.2 Equipos con software base de Gobierno de Navarra y sistema de información gestionado por el proveedor

Estos equipos son aquellos físicos o virtuales desplegados dentro de la red de Gobierno de Navarra, con software base (sistema operativo, antivirus, etc.) gestionado por Gobierno de Navarra y sistema de información (servidor de aplicaciones, base de datos, etc.) gestionados por el proveedor.

El acceso del proveedor a los sistemas se dará en las siguientes condiciones:

El acceso se podrá hacer a través de dos servicios diferentes que permiten el acceso a los sistemas de información de Gobierno de Navarra.

- a. Acceso a través del Portal VPN: Para ello necesitan contar con un usuario de directorio activo. Se puede acceder ingresando en el portal VPN y permite tener las URLs/rutas publicadas en el mismo. Esta opción tiene menos usabilidad para los proveedores que una VPN sitio a sitio.
- b. Acceso a través de una VPN sitio a sitio: Se trata de establecer una VPN a nivel de cortafuegos entre el proveedor y Gobierno de Navarra. Es necesario que el cortafuegos del proveedor permita este tipo de conexión y que firme un contrato con Gobierno de Navarra. Esta opción es la más usable para el proveedor.

Los accesos permitidos son:

- Al servidor web por http/s
- A un recurso compartido por CIFS
- A los logs de las aplicaciones. A estudiar en cada implantación cómo resolverlo mientras no se tenga una solución corporativa.
- A la base de datos en modo lectura. La autenticación integrada no está disponible y se tendrá que hacer por usuario local de base de datos.
- En productos con software de cliente pesado se permite el acceso por RDP o ssh, siempre y cuando el usuario de acceso no tenga permisos de administración. Este equipo deberá estar obligatoriamente en una de las VLANes independientes.
- A los servidores de desarrollo que no pertenezcan a la Plataforma de Desarrollo/Integración del Software RDP o ssh siempre y cuando se encuentre en la VLAN de desarrollo.
- A los servidores que forman parte de la Plataforma del Desarrollo de Software según lo establecido en el perfil de desarrollador en cada momento.

Los accesos no permitidos son:

- Por motivos de seguridad, a cualquier puesto de trabajo estándar de Gobierno de Navarra. No se puede utilizar TeamViewer o herramientas similares. Gobierno de Navarra no tiene estandarizada una herramienta que permita este tipo de accesos.
- Por defecto se deniegan el resto de accesos. A estudiar en cada caso.

El equipo debe estar en el estándar de Gobierno de Navarra en cuanto a sistema operativo, antivirus, copias, etc.



El proveedor no tendrá permisos de administración sobre el servidor. Únicamente dispondrá de los permisos estrictamente necesarios para poder dar el soporte técnico.

Cualquier incidencia en la que esté trabajando el proveedor debe quedar registrada en la HGT a través del CAU-SNS o del **CAU-Central dependiendo de la hora en que se produzca la incidencia** y escalada al proveedor de la manera que se determine en el Modelo Administrativo, pudiendo ser reescalada a otros grupos de soporte internos GdN (también de la manera que se establezca en el Modelo Administrativo).

El acceso remoto al servidor se otorgará únicamente una vez abierto el ticket y se denegará nuevamente este acceso una vez se finalice el ticket. **El CAU-SNS solo puede hacer estas tareas si el usuario con el que se hace el acceso remoto está dentro de la OU de Salud de DA para acceso externo.**

Toda actuación que implique parada de servicio requerirá que el proveedor envíe una Notificación al CAU de SNS para que éste a su vez gestione la comunicación con los usuarios afectados.

## 7.3 Equipos completamente gestionados por Gobierno de Navarra

Estos equipos son aquellos físicos o virtuales desplegados dentro de la red de Gobierno de Navarra, con software base (sistema operativo, antivirus, etc.) y sistema de información (servidor de aplicaciones, base de datos, etc.) gestionado por Gobierno de Navarra.

El acceso del proveedor a los sistemas se dará en las siguientes condiciones:

El acceso se podrá hacer a través de dos servicios diferentes que permiten el acceso a los sistemas de información de Gobierno de Navarra.

- a. Acceso a través del Portal VPN: Para ello necesitan contar con un usuario de directorio activo. Se puede acceder ingresando en el portal VPN y permite tener las URLs/rutas publicadas en el mismo. Esta opción tiene menos usabilidad para los proveedores que una VPN sitio a sitio.
- b. Acceso a través de una VPN sitio a sitio: Se trata de establecer una VPN a nivel de cortafuegos entre el proveedor y Gobierno de Navarra. Es necesario que el cortafuegos del proveedor permita este tipo de conexión y que firme un contrato con Gobierno de Navarra. Esta opción es la más usable para el proveedor.

Los accesos permitidos son:

- Al servidor web por http/s
- A un recurso compartido por CIFS
- A los logs de las aplicaciones. A estudiar en cada implantación cómo resolverlo mientras no se tenga una solución corporativa.
- A la base de datos en modo lectura. La autenticación integrada no está disponible y se tendrá que hacer por usuario local de base de datos.
- A los servidores de desarrollo que no pertenezcan a la Plataforma de Desarrollo/Integración del Software RDP o ssh siempre y cuando se encuentre en la VLAN de desarrollo.
- A los servidores que forman parte de la Plataforma del Desarrollo de Software según lo establecido en el perfil de desarrollador en cada momento.



Los accesos no permitidos son:

- Por motivos de seguridad, a cualquier puesto de trabajo estándar de Gobierno de Navarra. No se puede utilizar TeamViewer o herramientas similares. Gobierno de Navarra no tiene estandarizada una herramienta que permita este tipo de accesos.
- No se permite el acceso por RDP o ssh.
- No se permite la instalación de software que envíe información de monitorización.
- Por defecto se deniegan el resto de accesos. A estudiar en cada caso.

El equipo debe estar en el estándar de Gobierno de Navarra en cuanto a sistema operativo, antivirus, copias, etc.

El proveedor no tendrá permisos de administración sobre el servidor. Únicamente dispondrá de los permisos estrictamente necesarios para poder dar el soporte técnico.