



Requerimientos técnicos STS OT14-2026 Láser para Oftalmología en HUN

Gesprona 52392



Índice de contenidos

1 REQUISITOS TÉCNICOS STS	3
1.1 Integraciones con los sistemas de información del SNS-O	3
1.1.1 Procedimiento	3
1.1.2 Requisito genérico para integraciones con productos del SNS-O que no implementan HL7	3
1.1.3 Requisito genérico para integraciones con productos del SNS-O que implementan HL7	4
1.2 Licenciamiento	4
1.2.1 Procedimiento	4
1.2.2 Requisito	4
1.3 Fuentes de los desarrollos realizados a medida para el SNS-O	5
1.4 Seguridad	5
1.5 Requisitos para la integración con Imagen Médica Digital	5
1.5.1 Conectividad	5
1.5.2 Estándar DICOM	6
1.5.3 Estudios DICOM	6
1.5.4 Servicio SCU	7
1.6 Retinógrafos	8
1.7 Coordinación de Integración con Imagen Digital	8
2 REQUISITOS TÉCNICOS DE INFRAESTRUCTURAS PARA PLIEGOS TÉCNICOS	9



1 REQUISITOS TÉCNICOS STS

1.1 Integraciones con los sistemas de información del SNS-O

1.1.1 Procedimiento

Si el Sistema de Información licitado requiere integrarse con productos SNS-O se incorporará al pliego este requisito. Además, se indicarán todas las integraciones requeridas desde un punto de vista funcional, no es necesario detallar el diseño ni la implementación de las integraciones. Si el Sistema de Información adquirido plantea integraciones con Laboratorio, Imagen Digital o Cuidados Intensivos se añadirán los requerimientos específicos recogidos en este documento.

Este requisito puede redactarse de dos formas distintas en función de si los productos del SNS-O con los que deberá integrarse el software licitado implementan o no HL7. Las características de interoperabilidad exigidas se detallarán más adelante en función de las necesidades del producto del SNS-O (por ejemplo, [capítulo 2.12.3](#)). A continuación, se proponen dos diferentes redacciones.

1.1.2 Requisito genérico para integraciones con productos del SNS-O que no implementan HL7

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.

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.

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 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.

1.1.3 Requisito genérico para integraciones con productos del SNS-O que implementan HL7

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.

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

1.2.1 Procedimiento

Deberá valorarse indicar en el pliego el número mínimo de usuarios concurrentes que el tipo de licenciamiento del Sistema de Información debe soportar. Por ejemplo: *“El Sistema de Información soportará 76 usuarios concurrentes, si bien se valorará positivamente un sistema de licencias que permitan un número ilimitado de usuarios.”*

1.2.2 Requisito

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 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 Requisitos para la integración con Imagen Médica Digital

Los requisitos incluidos en este apartado deberá cumplirlos cualquier equipo médico (equipo a partir de aquí), ya sean elementos hardware como software o la conjunción de ambos, que deba integrarse en el sistema de Imagen Médica Digital del SNS-O.

Las empresas licitantes de estos equipos deberán aportar como parte de su documentación técnica el documento “*DICOM Conformance Statement*”

El Adjudicatario asegurará la conectividad del equipo con la red corporativa de GN. El Adjudicatario entregará documentación técnica detallando la configuración TCP/IP y DICOM del equipo.

El Adjudicatario indicará en la oferta si el equipo puede dar servicio sin necesidad de conectarlo a la red corporativa de GN.

1.5.1 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.
- Los equipos móviles que dispongan de conectividad WIFI deberán cumplir Autenticación IEEE 802.1x WPA2-Enterprise y configurar un Usuario/Contraseña de Directorio Activo que se le proporcionará desde la DGTD.

1.5.2 Estándar DICOM

El equipo debe implementar el estándar DICOM versión 3.

Todos los parámetros de conexión con el PACS (HostName, IP, puerto, AET, StationName, Nodos Remotos, etc.) de los distintos servicios DICOM deberán poder ser configurados según las necesidades del SNS-O. La configuración DICOM inicial de los equipos será realizada por el adjudicatario con las instrucciones que le sean dadas desde la DGTD. La configuración DICOM de la modalidad deberá adecuarse a las prestaciones de especializada y primaria. La configuración DICOM será sin coste para el SNS-O y podrá volver a requerirse por parte del SNS-O a la empresa adjudicataria en cualquier momento después de la recepción del equipo.

Toda comunicación con nodos DICOM deberá establecerse con el AET configurado.

Salvo indicación expresa por parte de la DGTD, Hostname, StationName y AET tendrán el mismo valor.

Servicios DICOM

El SNS-O considera imprescindibles los siguientes servicios DICOM:

- DICOM WLM (DICOM worklist manager). Permite 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 QR (DICOM Query/Retrieve). Permite que el equipo consulte y descargue estudios desde el PACS.
- DICOM COMMITMENT. Permite verificar si un archivo, que fue enviando previamente al PACS, está almacenado correctamente.

Los servicios DICOM, al menos los imprescindibles, deben estar operativos y funcionales. No es aceptable:

- Requerir el pago de licencia, activación, o cualquier otro cargo para permitir su uso.
- Requerir el pago al servicio técnico del adjudicatario para su correcta configuración.

1.5.3 Estudios DICOM

- Utilizará el set de caracteres ISO_IR 100 para los servicios DICOM WLM SCU y Storage



SCU.

- Los objetos DICOM tienen que llegar al PACS con los tags DICOM correctos para que la visualización en los visores del SNS-O sea óptimo.
- Todos los objetos DICOM enviados al PACS, tendrán los tags DICOM Station Name (0008,1010) e Institution Name (0008,0080), según los parámetros indicados por la DGTD.
- Los campos identificativos del estudio (AccessionNumber, StudyInstanceUID, StudyDate, StudyTime, PatientID, ...) serán iguales en todos los objetos DICOM de un mismo estudio.
- Informes gráficos. Los informes gráficos que se envíen al PACS deben implementar DICOM WaveForm.
- Deberá ser compatible con el sistema de información del SNS-O utilizado para el diagnóstico: IntelliSpace CardioVascular.
- Los equipos que emitan radiación ionizante deben poder enviar la información de dosis radiológica al Sistema de Gestión de Dosis del SNS-O.
 - La forma preferente es:
 - Radiation Dose Structured Report (RDSR) con SOP Class UID: "1.2.840.10008.5.1.4.1.1.88.67".
 - Permitirá enviar los objetos RDSR al mismo PACS al que se envían las imágenes del estudio y a otro distinto a decisión de la DGTD.

1.5.4 Servicio SCU

Para que una modalidad pueda integrarse con el ecosistema DICOM del SNS-O, es imprescindible que actúe como SCU al menos para los servicios DICOM Storage y DICOM WLM, conforme a lo indicado en el apartado 1.1.1.

El SNS-O requiere que esta capacidad SCU esté disponible según una de las siguientes modalidades, en orden de preferencia:

- Opción A — SCU nativo: la modalidad implementa de forma nativa el servicio SCU, sin requerir software adicional ni hardware externo para establecer comunicación DICOM con el PACS y demás nodos del SNS-O.
- Opción B — Estación adjunta SCU: en caso de que la modalidad no disponga de servicio SCU nativo, el adjudicatario deberá suministrar e integrar un ordenador externo que asuma esta función. Este ordenador:
 - Formará parte integrante de la modalidad a todos los efectos del contrato.
 - Será mantenido íntegramente por el adjudicatario durante toda la vigencia del contrato, incluyendo actualizaciones de sistema operativo, software DICOM y cualquier incidencia derivada de su funcionamiento.
 - Deberá tener instalada y activa una solución antivirus gestionada, conforme a las políticas de seguridad del SNS-O.
 - No podrá ser utilizado para funciones distintas a las de intermediación DICOM de



la modalidad. No se permitirá su uso como estación de trabajo clínica, de administración, ni para ningún otro fin no vinculado directamente a la integración de la modalidad.

No es aceptable que el SNS-O asuma la provisión, mantenimiento o soporte del ordenador SCU bajo ningún concepto.

1.6 Retinógrafos

El estudio contendrá tantas series como imágenes. Cada serie solamente contendrá una imagen.

- En caso de aplicar prestaciones similares a retinografía al láser, se aplicará el mismo criterio.

1.6.1 Láser oftalmológico

El adjudicatario deberá declarar en la oferta las SOP Classes DICOM que genera el equipo, indicando para cada una:

- Identificador de la SOP Class (SOP Class UID).
- Tipo de objeto generado (imagen, informe estructurado, waveform, etc.).
- Servicios DICOM asociados (Storage SCU, WLM SCU, etc.).

El SNS-O se reserva el derecho de validar la compatibilidad de las SOP Classes declaradas con el PACS y los visores clínicos del SNS-O antes de la recepción definitiva del equipo.

1.7 Coordinación de Integración con Imagen Digital

- La integración y configuración del equipo con los Sistemas de Información del SNS-O se realizará de forma coordinada con el Servicio de Tecnologías de Salud (STS), en concreto con el equipo de Imagen Médica Digital (IMD), que supervisará y validará el proceso.
- Una vez conocidos los plazos de entrega del equipo, el Adjudicatario comunicará al Servicio de Infraestructuras con suficiente antelación y junto al montaje/desmontaje del equipamiento actual, pueda planificar las tareas de red y conectividad necesarias. El Adjudicatario no iniciará ninguna tarea de integración o configuración sin haber coordinado previamente los plazos y el plan de trabajo con el equipo IMD.



2 REQUISITOS TÉCNICOS DE INFRAESTRUCTURAS PARA PLIEGOS TÉCNICOS

Si la oferta incluye equipamiento (servidores, licencias, software, estaciones de trabajo, etc.) que no forma parte de la propia modalidad médica, es decir, que no será soportado por el adjudicatario, o que requiera la instalación de software en estaciones de trabajo del Gobierno de Navarra, dicho equipamiento deberá cumplir el Escenario Tecnológico del Gobierno de Navarra, publicado en:

Anexo STS EscenarioTecnologico GdN 12-2025 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)
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 (Si)
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 adquirieran 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.	



- | | |
|--|--|
| <ul style="list-style-type: none">○ 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 (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 <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)	
--	--