PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN MEDIANTE PROCEDIMIENTO ABIERTO DEL SUMINISTRO DE PRODUCTOS Y PUESTA A DISPOSICIÓN DE EQUIPOS NECESARIOS PARA REALIZAR TÉCNICAS DE INMUNOHEMATOLOGIA Y SEGURIDAD TRANSFUSIONAL EN LA RED HEMOTERAPICA DE OSAKIDETZA

1.- ANTECEDENTES

El Plan Director de los Laboratorios de Osakidetza establece que los laboratorios hemoterápicos forman parte de la Red de Diagnóstico Biológico de Osakidetza.
En este contexto, se propone la contratación corporativa para la puesta a disposición de los productos y equipos necesarios para la realización de pruebas de inmunohematología, así como un sistema corporativo de seguridad transfusional en las diferentes Unidades que componen la Red Hemoterapia de Osakidetza

El presente documento consta de los siguientes Anexos:

ANEXO I Prescripciones técnicas de los laboratorios.

ANEXO II Actividad Anual prevista

ANEXO III Prescripciones técnicas relativas al desarrollo informático

ANEXO IV Atención a usuarios y acuerdos a nivel de servicio

.
Documento informativo de Directrices y especificaciones técnicas informáticas

2.- OBJETO DEL CONTRATO

El objeto del presente contrato consiste en la puesta a disposición , mediante procedimiento abierto, de los productos y equipos necesarios para realizar técnicas de Inmunohematología así como el material necesario para la utilización, desarrollo y mantenimiento de un sistema corporativo de seguridad transfusional en todos los Servicios Transfusionales (en adelante STs) de Osakidetza.

La Red hemoterápica de Osakidetza está compuesta por los siguientes servicios transfusionales;

ST Hospital Universitario Cruces Laboratorio de nodo principal
ST Hospital Universitario Basurto Laboratorio de nodo principal
ST Hospital Galdakao Laboratorio de nodo principal
ST Hospital Universitario Donostia. Laboratorio de nodo principal
ST Hospital Universitario de Álava (Sedes Txagorritxu y Santiago) Laboratorio de nodo principal
ST Hospital S Eloy. Laboratorio de respuesta Hospitalaria
ST Hospital Urduliz Laboratorio de respuesta Hospitalaria.
ST Hospital Bidasoa Laboratorio de respuesta Hospitalaria.
ST Hospital Mendaro Laboratorio de respuesta Hospitalaria.
ST Hospital Zumárraga. Laboratorio de respuesta Hospitalaria
ST Hospital Alto Deba. Laboratorio de repuesta Hospitalaria.

3.- DEFINICIÓN DEL CONTRATO

A efectos de este pliego se entiende por técnicas de Inmunohematología, y los procesos de seguridad transfusional, las pruebas relacionadas en el Anexo II.

El adjudicatario deberá:

a) Poner a disposición de Osakidetza, el equipamiento, la tecnología y los sistemas de información para su gestión, en régimen de disponibilidad, además de los consumibles necesarios para la realización de todas aquellas pruebas analíticas relacionadas en el Anexo II.
La actividad de los laboratorios indicada en el Anexo II se facilita a título orientativo, con el fin de que las empresas licitantes puedan dimensionar el equipamiento adecuado para los laboratorios. La empresa adjudicataria se compromete a adecuar el equipamiento ofertado inicialmente, para adaptarse a las necesidades que pudieran derivarse de cambios en la actividad, durante el periodo de vigencia del contrato.

b) Instalar y mantener el equipamiento y la tecnología, los sistemas de información, así como el material necesario, para que el personal técnico de los STs pueda realizar una gestión eficiente de la demanda.
Los sistemas de información deberán incluir, al menos, todas las conexiones y relaciones con los sistemas corporativos de Osakidetza que se definen más adelante con aplicaciones como Odolbide/eOdolbide y el sistema de gestión de laboratorio que en estos momentos es OMEGA 3000 de la empresa ROCHE y GESTLAB de la UTE COINTEC INDRA..

c) Instalar y mantener el equipamiento, la tecnología, y el sistema de información, así como el material necesario, para que el personal de los STs lleve a cabo todas las actividades y tareas que precisen los procesos analíticos descritos en el objeto del concurso.

d) Asegurar la renovación tecnológica durante el periodo de vigencia del presente contrato y para todos los servicios objetos del mismo.

e) Hacerse cargo de los reactivos y materiales para la puesta a punto de las técnicas y el acondicionamiento de los equipos. Así mismo, será a cargo del adjudicatario el consumo de reactivos, controles, y todos aquellos elementos necesarios para el mantenimiento preventivo y correctivo de los equipos.

f) Mantener y desarrollar, de acuerdo a las necesidades de Osakidetza, un sistema de seguridad transfusional que incluya todas las etapas del proceso, desde la identificación del paciente a transfundir y la obtención de la muestra pre transfusional hasta su vigilancia posterior a la transfusión.

4. OTRAS CONDICIONES DEL ADJUDICATARIO

4.1.- Formación

La entidad adjudicataria, previa conformidad del Comité de Hemoterapia Corporativo (en adelante CHC), determinará el programa formativo a seguir por el personal. La formación que se considere necesaria será financiada por el adjudicatario.

4.2.- Calidad

4.2.1.- Obligaciones generales

El adjudicatario estará obligado a que el objeto del contrato responda a los umbrales de calidad que determine el CHC.

Se deberá incluir en la oferta materiales y programas de control de calidad internos, a elegir entre uno propio y otro de reconocido prestigio por el CHC. Así como controles de calidad externos para todas las metódicas y equipos, que correrán a cargo del adjudicatario y serán también elegidos por el CHC.

Todo el material y equipamiento ofertado deberá disponer de marcado CE

4.2.2.- Protocolos y Procedimientos de actuación

Con carácter enunciativo y no limitativo, la entidad adjudicataria deberá disponer y mantener actualizado la siguiente documentación:

Manual de procedimientos: (en idioma español)

Contendrá actualizados, al menos, los siguientes procedimientos :

- Procedimientos normalizados de los equipos en formato electrónico que detallen los métodos y protocolos que se utilizarán, con su fundamento, la descripción de la preparación de reactivos o medios, la realización de las técnicas, los métodos de medida y los instrumentos necesarios.
- Tratamiento y protección de datos, sistema de archivo y manual actualizado del sistema informático, así como un documento de procedimientos y medidas de seguridad de obligado cumplimiento para el personal con acceso a los datos de carácter personal en el que se establezcan las medidas, normas y procedimientos encaminados a garantizar el nivel de seguridad exigido en la normativa vigente con especial referencia a las medidas exigibles en el nivel alto de protección de datos.

Además, el adjudicatario deberá aportar, si se produjera un cambio de los lotes suministrados, un certificado con las especificaciones de calidad del nuevo lote

4.3.- Puesta en marcha

Los licitadores deberán elaborar un plan de puesta en marcha y/o adaptación de los STs , previa conformidad del CHC, que incluya todas las áreas y contendrá los aspectos recogidos en este Pliego.

Serán excluidas todas aquellas ofertas que no se comprometan a poner en funcionamiento las instalaciones en un plazo de **cuatro meses** a partir de la fecha de la firma del contrato.

4.4.-Sensibilidad y especificidad de los reactivos

Los licitadores incluirán en su oferta los datos de sensibilidad y especificidad garantizados para cada prueba. En los casos en que los resultados obtenidos sean inferiores a los establecidos en las especificaciones técnicas, la empresa adjudicataria suministrará reactivos adicionales sin coste para cubrir las diferencias siempre y cuando los resultados obtenidos no sean debidos al mal uso de los reactivos o de los equipos por parte del personal de las STs. Las empresas licitadoras deberán incluir en sus ofertas su compromiso en este sentido.

4.5.- Servicio técnico

El adjudicatario se encargará del mantenimiento y reparación de los equipos durante el periodo de vigencia del contrato, así como, a actualizar y/o reponer los mismos en el supuesto de cambio o mejora tecnológica, sin coste adicional.

El mantenimiento incluido en la oferta comprenderá todas las actuaciones de mantenimiento preventivo, correctivo y normativo.

El mantenimiento incluirá la sustitución de piezas, recambios, mano de obra, desplazamientos etc… y todos los elementos que garanticen el correcto funcionamiento de los equipos.

El adjudicatario deberá disponer de al menos un especialista, de presencia física, que apoye al personal de los STs en la puesta en marcha de técnicas, configuración de los sistemas y formación del personal.

4.6 Finalización del contrato

Una vez finalizado el contrato, los equipos deberán ser retirados por el adjudicatario, en un plazo no superior a 8 semanas.

5.-COMISION DE CONTROL Y EVALUACIÓN DE LA GESTIÓN DEL PRESENTE CONTRATO

El órgano de contratación, o la persona en quien delegue, y sin perjuicio de las facultades inspectoras de la Administración Sanitaria, podrá inspeccionar los servicios, instalaciones, locales, así como toda la documentación relacionada con el objeto del contrato. Para ello, la adjudicataria deberá facilitar la realización de sus tareas inspectoras, poniendo a su disposición cuanta información y documentos sean necesarios, así como facilitando el acceso a todas las dependencias e instalaciones.

Asimismo, en base al artículo 62 de la LCAP, se designa como responsables del contrato al Comité de Hemoterapia de la Red de Diagnóstico Biológico de Osakidetza

6.- DOCUMENTACIÓN TÉCNICA A PRESENTAR POR LOS LICITADORES

La DOCUMENTACION a incluir en los distintos sobres “A”, “B” y “C” deberá presentarse única y exclusivamente en formato digital a través de la Plataforma de Licitación Electrónica, cuyo acceso se indica en el Pliego de Cláusulas Administrativas Particulares

Los archivos digitales que contengan la documentación, ya sea en formato PDF, Word o Excel, RTF o cualquier otro, incluirán la información en texto seleccionable (excepto lógicamente en lo referido a imágenes, planos o similares).

En la documentación a enviar, se deberán aportar los estudios científicos contrastados que avalen la documentación técnica presentada.

La documentación aportada deberá seguir el orden propuesto en los criterios de valoración y los requisitos exigidos.

Con independencia de que el licitador o licitadores puedan presentar en su oferta cuanta información complementaria consideren de su interés, deberán presentar la exigida en cualquier apartado de este Pliego y, además la requerida en los siguientes puntos:

6.1 Equipos y reactivos

- Especificaciones de los equipos ofertados indicando su número y características técnicas detalladas
- Características de las técnicas ofertadas.
- Tecnología y funcionalidad del equipamiento propuesto.
- Características de la gestión de los reactivos.
- Gestión del mantenimiento de los equipos por el usuario.

6.2.- Servicios logísticos

- Características técnicas del material, ficha técnica o ruta informática de acceso al mismo
- Sistema de aseguramiento de la trazabilidad, la seguridad y las condiciones adecuadas en los envíos (tiempo de respuesta, mantenimiento de la cadena de frío, etc.).

6.3. .- Sistema de seguridad transfusional

- Deberán explicitarse los medios propuestos para la realización de todas las obligaciones recogidas en el Anexo III de este Pliego relativo al Desarrollo Informático.
- La planificación, organización del servicio, soporte de usuarios y niveles de acuerdo de servicio a partir del modelo basado en brazaletes identificativos (CIC de Osakidetza), dispositivos lectores así como la existencia de arquitectura multicentro localizada en SSCC..
- La solución de hardware requerida durante el período de vigencia del contrato a adoptar. En este sentido se seguirán las instrucciones suministradas por Osakidetza en relación a los dispositivos a utilizar en la asistencia cotidiana (PDAs, Tabletas, etc.).
- La estrategia de integración con los sistemas de información existentes, y planificación de las necesidades de integración con otros elementos utilizados en la asistencia cotidiana de hospitalización

6.4.- Pruebas adicionales

- Los licitadores deberán aportar la relación de todas las pruebas no relacionadas en el Anexo II que podrían realizarse en los mismos equipos ofertados,
  .
- Estas pruebas adicionales deberán estar valoradas económicamente, en la oferta económica, a título informativo en base a precio por prueba.

6.5.- Servicio técnico

- El adjudicatario proveerá de un plan de asistencia técnica personalizado para los STs con los requerimientos mínimos expresado en el Anexo IV. Este plan deberá detallar: recursos humanos, medios tecnológicos, horarios, tiempos de respuesta y tipos de soporte a disposición de la unidad.

6.6.- Plan de Formación-

- Plan de formación al personal sobre los equipos y sistemas que será continuado en el tiempo.

6.7.- Puesta en marcha

- El plan de apertura: actuaciones y cronograma para la puesta en funcionamiento del servicio objeto del contrato.

- Las fases de aceptación de los nuevos equipos: los plazos de instalación, sus verificaciones así como las pruebas de calibración.

7.- LUGAR Y ENTREGA DEL SUMINISTRO

- El contratista estará obligado a entregar los bienes objeto del suministro en el lugar que se designe por Osakidetza.

8.- DESARROLLO INFORMATICO

Las prescripciones técnicas relativas al desarrollo informático son las que se especifican en el Anexo III de este Pliego y en el documento informativo de Directrices y especificaciones técnicas informáticas generales.

.

ANEXO I

Prescripciones técnicas de los laboratorios

1.- INTRODUCCIÓN

Las características generales de los Laboratorios de Inmunohematología de los STs son:

- Calidad: las técnicas que se realicen han de cumplir holgadamente los estándares de calidad admitidos por la Comunidad Científica.

- Automatización: debe disponer de equipos y sistemas de automatización que permitan garantizar la seguridad del paciente y del profesional, una productividad adecuada, así como la eliminación de tareas y procesos que no aporten valor en un contexto de eficiencia.

- Contexto clínico y especialización: los sistemas de información y comunicación que den soporte al Laboratorio deben garantizar que éste se gestione en el contexto clínico del paciente, con los protocolos y guías que se definan y que se facilite la aportación de expertos tanto al informe final como a una mejor gestión de la demanda.

- Ergonomía: La arquitectura y distribución de los equipamientos y sistemas del laboratorio deben facilitar al máximo las condiciones de trabajo del personal tanto en el aspecto funcional como en el del espacio o en el del ruido.

2. CARACTERÍSTICAS TECNICAS *REQUISITOS EXIGIBLES*

2.1.- Equipos automáticos de Inmunohematología:

- Los equipos analíticos deberán ser de última generación, con capacidad de realizar las técnicas mencionadas en el Anexo II

- Los equipos ofertados deberán tener la suficiente flexibilidad para garantizar niveles adecuados de automatización y calidad técnica en los diferentes tipos de centros (Laboratorios de nodo principal y laboratorios de respuesta hospitalaria) autorizados para la actividad transfusional.

- La calidad analítica de las técnicas deberá ser como mínimo las especificadas por las recomendaciones nacionales e internacionales.

- Se deberá garantizar la transferibilidad de resultados entre los equipos y los sistemas de gestión del laboratorio.

- Los sistemas deberán ser redundantes, de forma que se garantice la prestación del servicio urgente en caso de fallo con mínima complicación, y que los sistemas dedicados a la prestación urgente puedan apoyar a la actividad ordinaria. La redundancia deberá ser con equipos y sistemas que puedan ser utilizados de forma indistinta por el personal, diferenciadamente en base al volumen de actividad de los servicios de transfusión.

- El número de equipos analíticos necesarios deberá ser el mínimo que garantice la redundancia citada manteniendo la simplicidad y practicabilidad.

- La practicabilidad general de los sistemas y su simplicidad deberían permitir su funcionamiento 24 horas y su manejo por personal a turnos.

- La gestión de reactivos debe permitir la carga y descarga fácil de los mismos.

- Los equipos permitirán la utilización de diferentes tipos de tubos.

- La tecnología de soporte será la de tarjetas con aglutinación en columnas.

- La gestión de los residuos estará adecuada a normativa, generando el menor volumen posible, fácil de gestionar, con dispositivos ligeros,

- Los equipos deberán conectarse de manera bidireccional al programa de gestión de laboratorio y al programa de gestión de Banco de Sangre, Odolbide/eOdolbide.

- Los equipos deberán disponer de sistema de alimentación ininterrumpida (SAI).

2.2.- Técnicas no automatizadas de Inmunohematología

La calidad analítica de las técnicas no automatizadas debe ser como mínimo iguales a las de las pruebas automatizadas.

- Se deberá garantizar el equipamiento necesario para la realización de las técnicas, la transferibilidad de resultados y la simplicidad en la gestión de reactivos y materiales.

- La practicabilidad general de los sistemas y su simplicidad deberán permitir su funcionamiento 24 horas y su manejo por personal a turnos.

2.3.- Sistema de seguridad transfusional:

- El sistema de seguridad transfusional incluirá todas las etapas del proceso, desde la identificación del paciente a transfundir y la obtención de la muestra pretransfusional hasta la vigilancia posterior a la transfusión.

- Ofrecerá la trazabilidad completa del proceso y la posibilidad de explotación de esa información.

- La descarga de datos debe ser a tiempo real.

- La empresa adjudicataria garantizará al menos, la funcionalidad y prestaciones del sistema informático actual y planificara la estrategia de mejora del sistema vigente.

- La oferta del sistema de seguridad transfusional deberá incluir la seguridad del proceso mediante una etiqueta identificativa de la transfusión

Las principales funcionalidades que deberá contar son:

- Esquema único de BBDD multicentro con la actividad de los 12 centros transfusionales de Osakidetza.
- Parametrización a dos niveles: general y por centro transfusional.
- Proceso multicentro en todas sus fases: se inicia la petición en un centro y se transfunde en otro
- Pulsera transfusional adaptada a las necesidades de Osakidetza con control de seguridad en cada etiqueta, diferenciándose de las demás.
- Dos menús en PDA; enfermería y banco de sangre
- Incorporación del CIC en las lecturas con las dispositivos móviles disponibles.
- Validación del CIC entre la pulsera de identificación de pacientes y el volante electrónico de transfusión.
- Integración con la BB.DD de pacientes de Osakidetza, para obtener datos demográficos de un CIC.
- Validación con LDAP corporativo
- Envío de correos electrónicos a responsables del proceso transfusional en caso de incidencia transfusional
- Validación del DNI en las lecturas en los dispositivos móviles disponibles.
- Identificación de usuario en dispositivo móvil mediante lecturas de la TPE(Tarjeta Profesional de Electrónica)
- Integración con Osabide Global , Solicitud de Transfusión y Odolbide/eOdolbide
- Validación por estado de los procesos (correctos con incidencias, correctos sin incidencias, pendientes y con errores).
- Verificación de procesos anteriores completos.
- Alarmas en software y dispositivos móviles de tiempos de unidades fuera de banco, tiempo de transfusión excedido.
- Gestión autónoma de usuarios entre centros (permitir cambio de usuarios entre centros).
- Gestión del histórico de los procesos transfusionales.

Se incluirá la adaptación a los dispositivos asistenciales de identificación que Osakidetza implante o tenga en vigor, compatibilizándolos con los dispositivos específicos de la seguridad transfusional

Los requisitos técnicos de los dispositivos móviles son los siguientes;

Sistema operativo
Android 5.1.1 o superior
Banda
LTE cat4. 150M DL/50M UL
DC-HSPA+ 42M/5.7M
Dimensiones
214.8 mm × 124 mm × 7.8 mm (8 pulgadas)
Pantalla
8'' FHD 1200x1920 IPS
Batería
4800mAh Li-Po o superior
Memoria interna
2GB RAM + 16 GB ROM
Conectividad
WiFi 802.11a/b/g/n/ac (2.4/5Ghz)
Bluetooth 4.0 + EDR

Cámara

Frontal: 2MP // Trasera: 8MP AF Flash

PDA -Honeywell Dolphin 6000

- Dispositivo Smartphone con lector de barcodes
- Procesador 1GHz Single Core TI OMAP
- Memoria Interna 256 Mb + 512 Mb Flash
- S.O. Windows Windows® Mobile 6.5 Professional
- Wifi 802.11 b/g WAPI support y Bluetooth V2.1 con EDR
- Sistemas de seguridad WIFI soportados: WEP, WPA,WPA-PSK, WPA2, WPA2-PSK

PDA -Honeywell Dolphin 60S

- Dispositivo Smartphone con lector de barcodes
- Procesador TI AM3715 CortexA8 800 MHz
- Memoria Interna 256 Mb + 512 Mb Flash
- S.O. Windows Windows® Mobile 6.5 Professional
- Wifi 802.11 b/g/n WAPI support y Bluetooth V2.1 con EDR
- Sistemas de seguridad WIFI soportados : WEP, 802.1x, LEAP, TKIP, MD5, EAP-TLS, EAP-TTLS, WPA-PSK, WPA v2.0, and PEAP

ANEXO II

ACTIVIDAD ANUAL PREVISTA

LOTE 1	ACTIVIDAD ANUAL Nº Pruebas/Año	Txagorritxu	Donostia	Cruces	Basurto	Galdácano	Santiago
Grupo Hematico Sérico	86.500	16.000	18.800	13.900	15.500	9.500	3.250
Grupo Hematico Manual	107.430	30.000	3.000	45.000	3.000	10.000	1.000
Grupo Hematico Bolsa	91.400	6.700	20.100	25.000	13.000	14.200	2.100
Grupo Hematico Paciente	12.200	0	12.200	0	0	0	0
Grupo Hematico recien nacidos	15.400	3.000	4.500	4.850	1.100	0	0
Estudio Rh	13.760	1.040	5.200	2.000	2.400	1.160	200
Estudio Rh Kell	3.564	260	1.300	624	600	290	50
Escrutinio anticuerpos irregulares 3 celulas	123.290	16.000	31.000	33.000	15.000	14.350	3.000
Escrutinio anticuerpos irregulares enzimatico 3 celulas	12.496	1.480	200	0	0	2.690	673
Identificación de Anticuerpos	5.734	425	1.092	1.905	884	592	240
Identificación de anticuerpos enzimatico	918	108	273	0	221	148	59
Compatibilidad prueba cruzada	140.500	12.300	35.500	44.950	10.000	14.250	6.900
Coombs Directo	10.650	820	2.100	2.930	1.700	1.550	460
Coombs directo monoespecifico	6.015	250	3.000	1.400	30	1.050	20
Fenotipo extendido	1.748	194	419	440	255	220	**50**
Proyecto Seguridad transfusional	1						
Pulseras de seguridad Transfusional	60.000	6.529	15.677	13.200	11.855	4.500	1.800
		Bidasoa	Alto Deba	Zumárraga	Mendaro	San Eloy	Urdúliz
Grupo Hematico Sérico		1.500	1.250	2.000	1.400	2.300	1.100
Grupo Hematico Manual		900	430	3.000	1.100	1.000	9.000
Grupo Hematico Bolsa		2.000	800	1.600	2.500	2.800	600
Grupo Hematico Paciente		0	0	0	0	0	0
Grupo Hematico recien nacidos		0	600	800	550	0	0
Estudio Rh		120	240	280	120	400	600
Estudio Rh Kell		30	60	70	30	100	150
Escrutinio anticuerpos irregulares 3 celulas		1.500	1.080	2.160	2.000	3.200	1.000
Escrutinio anticuerpos irregulares enzimatico 3 celulas		821	0	0	2.732	3.900	0
Identificación de Anticuerpos		128	58	94	104	182	30
Identificación de anticuerpos enzimatico		15	0	23	26	45	0
Compatibilidad prueba cruzada		3.300	1.350	2.700	3.000	5.250	1.000
Coombs Directo		220	90	180	200	350	50
Coombs directo monoespecifico		50	0	65	100	0	50
Fenotipo extendido		**50**		**50**		**50**	**20**
Procesos Transfusionales							
Pulseras de seguridad Transfusional		1.375	620	1.248	1.156	1.740	300

ANEXO III

Prescripciones técnicas relativas al desarrollo Informático

1.- COORDINACIÓN Y DIRECCIÓN DEL PROYECTO

La empresa designará un jefe de proyecto en el ámbito informático, que será interlocutor único con Osakidetza y las UGCs. Dicho jefe de proyecto podrá acompañarse del personal técnico y funcional que estime conveniente en su relación con los homólogos de los hospitales y Osakidetza.
Se establecerán reuniones de seguimiento con la regularidad y contenido que en su momento se determinen.

2.- UBICACIÓN FÍSICA

El equipamiento dedicado a la realización de los servicios objeto del contrato se ubicará en dependencias de las UGCs, distribuido en:

Área de gestión de los ST. Residirán en ella los equipos directamente relacionados con la actividad propia del ST y los puestos informáticos necesarios para su control y gestión, en dependencias de las UGCs

Para los equipos destinados a servidores de aplicaciones, de bases de datos y procesos. En función de la solución propuesta se decidirá si se alojan en el Centro de Proceso de Datos (CPD) de SSCC o en el CPD del centro donde se ubica el Laboratorio.

3.- INSTALACIONES E INFRAESTRUCTURA BÁSICA

La empresa adjudicataria utilizará las instalaciones e infraestructura básica de las UGCs, en concreto, el cableado de datos y los servicios de electricidad y refrigeración, tanto los generales como los del CPD.
Si la inclusión del equipamiento del adjudicatario implicase la necesidad de incrementar o reconfigurar las infraestructuras propias del hospital, el coste económico de estas modificaciones será asumido por la citada empresa.

4.- EQUIPAMIENTO INFORMÁTICO Y ARQUITECTURA

El adjudicatario aportará el hardware y software necesarios para la prestación del servicio, y se encargará de su instalación, configuración, puesta en producción, mantenimiento y adecuación, así como de dar el adecuado soporte al usuario y a las incidencias que pudieran surgir.
Los puestos informáticos necesarios para su control y gestión del Laboratorio estarán configurados con la maqueta de Osakidetza.

El equipamiento físico y lógico que tenga que interactuar o integrarse con otros sistemas de información del Departamento de Salud, de las UGCs, de Osakidetza o de sus Organizaciones de Servicios cumplirá los estándares definidos por éstos, tal y como viene establecido en este Anexo III. Estos estándares actuales podrían ser modificados por las UGCs u Osakidetza durante el contrato.
Actualmente, la versión de maqueta que se instala en los equipos de Osakidetza, es la 2.6; aunque convive con versiones anteriores instaladas.

Hardware

Procesador con un mínimo de tecnología de 45nm, caché L2 de 3 Mb y FSB de 1.066 Mhz.
Memoria RAM 2 Gb.
Disco duro 250 Gb

Monitor 19 pulgadas con resolución 1440x900 mayoritaria o 1280x1024.

Sistema operativo

Windows 7 Enterprise N (32 Bit) SP1 + Windows media feature Pack

Asimismo, la arquitectura de los sistemas a instalar en el CPD cumplirá los estándares definidos en dicho Anexo III. Estos estándares actuales podrían ser modificados por las UGCs u Osakidetza durante el contrato.

La configuración de toda la infraestructura informática, en especial la electrónica (de comunicaciones y seguridad) y el equipamiento instalado en el CPD, seguirá los criterios establecidos por Osakidetza, las UGCs, y será supervisado por los hospitales y los SSCC.

5.- COMUNICACIONES Y CONECTIVIDAD

El equipamiento informático del adjudicatario, tanto el situado en el área de gestión del ST como en el área de CPD, estará conectado a la red local del hospital.

En el área de gestión del ST el adjudicatario proveerá las infraestructuras necesarias para conectar los equipos de trabajo necesarios si las ya existentes no fuesen suficientes o tuviesen que plantearse cambios de ubicación de las mismas. En caso de ser necesaria la ampliación de cableado (puntos de red) y/o electrónica de comunicaciones, la adquisición e implantación de las citadas infraestructuras deberá atenerse a los criterios marcados por Osakidetza, y las UGCs.

En el área de CPD el adjudicatario proveerá las infraestructuras adecuadas para la arquitectura que se defina si las ya existentes no fuesen suficientes siguiendo los estándares de Osakidetza y de las UGCs en esta materia, incluyendo cableado, electrónica de comunicaciones (switches), balanceadores, equipos de seguridad y tantos dispositivos como sean necesarios para interconectar, de forma segura y con capacidad y disponibilidad suficientes, todo el equipamiento.
Las comunicaciones externas se realizarán a través de la red corporativa de Osakidetza

CAPA SEGURIDAD Y CONFIGURACION/POLITICA SEGURIDAD SOBRE APPS

Las aplicaciones que son diseñadas ad-hoc y entregadas para ser registradas en la plataforma MDM (in-house) al ser transmutadas recibirán una capa de seguridad la cual se modifica con parámetros de configuración y política de tal forma que habrá que tener en cuenta dichas posibilidades.
Las configuraciones a tener en cuenta y básicas desplegadas en las configuraciones de seguridad de la plataforma en lo que concierne a las APPS y al dispositivo propiamente dicho:

- No se pueda acceder a la memoria externa del dispositivo (con todo lo que ello implica).
- Uso de la cámara no podrá acceder a memoria física.
- Denegar la interacción entre aplicaciones Seguras y No seguras.
- Bloqueo de transferencia de datos (corta y pega (portapapeles) entre APPS.
- Imposibilidad uso de micrófono.

Bloqueo de la posibilidad de Captura de Pantalla. Dado que haría uso de memoria externa

6.- SERVICIO DE DIRECTORIO

Tanto los Servidores del área de CPD como los PCs del área de gestión del ST estarán integrados en el dominio que indiquen las UGCs del Directorio Activo (Microsoft) de los hospitales.

7.- GESTIÓN, ADMINISTRACIÓN DE LOS SISTEMAS

Corresponde al adjudicatario la gestión y administración de las máquinas y los sistemas de información (servidores, PCs, dispositivos periféricos, bases de datos, aplicaciones, etc.) dedicados a la prestación de este servicio, así como la atención de usuarios e incidencias con relación al software y hardware aportado por el adjudicatario.

Las tareas de gestión y administración se llevarán a cabo desde puestos situados en el área de gestión del ST y en el servicio de informática del Hospital.
Si para actividades de monitorización, mantenimiento u otras similares, el adjudicatario considera necesario disponer de un acceso externo, podrá dotarse de una conexión VPN (accesible desde Internet), con las condiciones y requisitos que para este tipo de enlaces tienen establecidos Osakidetza y las UGCs. En cualquier caso se garantizará siempre el acceso a cualquier dato de carácter personal de una forma segura, cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

La empresa facilitará al hospital documentación detallada acerca de la configuración de las máquinas, en especial electrónica (si la hubiera) y servidores, y la mantendrá permanentemente actualizada.

8.- MONITORIZACIÓN Y AUDITORÍA

Las UGCs y los SSCC dispondrán de capacidad de monitorización de los equipos informáticos de la empresa adjudicataria, con el suficiente nivel de autorización para cumplir al menos dos objetivos:

Comprobar que la instalación se adecua a lo establecido previamente.

Disponer de información sobre la disponibilidad o indisponibilidad del servicio.

Más allá de esta exigencia, las UGCs y los Servicios Centrales de Osakidetza se reservan el derecho de efectuar auditorias tan extensas, profundas y detalladas como consideren oportuno para comprobar:

La calidad de las instalaciones.

La adecuación a lo comprometido y acordado.

El cumplimiento de estándares de seguridad y LOPD, así como la normativa aplicable en este ámbito.

Para todo ello la empresa proveerá los medios, herramientas y elementos de conectividad necesarios.

9.- INTEGRACIÓN Y ADECUACIÓN CON RESPECTO A LOS SISTEMAS DE INFORMACIÓN CON LAS UGCS, OSAKIDETZA Y DE SUS ORGANIZACIONES DE SERVICIOS

Los estándares de obligado cumplimiento en cuanto a integración de sistemas se detallan en el documento de descripción de requisitos técnicos para publicadores y subscriptores de eventos. Estos estándares actuales podrían ser modificados por las UGCs u Osakidetza durante el contrato.
Las adaptaciones requeridas en los Sistemas de Información del Departamento de Salud, de las UGCs, de Osakidetza y de sus Organizaciones de Servicios derivadas de la adopción de la solución propuesta deberán ser asumidas por el adjudicatario. El desarrollo será realizado por las empresas que Osakidetza, y las UGCs determinen en cada momento, principalmente los adjudicatarios de sus contratos de mantenimiento.

Así mismo, el coste de las conexiones y/o las licencias que sean necesarias para conectarse a OMEGA 3000, de la empresa ROCHE y GESTLAB de la empresa COINTEC serán asumidas por el adjudicatario durante todo el periodo que dure el contrato y también las necesarias para Odolbide/eOdolbide.

Los cambios de arquitectura e infraestructuras que fueran requeridos para mantener las funcionalidades actuales y futuras en los Sistemas de Información relatados, así como el desarrollo, pruebas unitarias y de integración, paso a producción, y expansión a todos los centros de las nuevas versiones de los Sistemas de Información en este apartado descritos deberán ser igualmente asumidos por el adjudicatario.

La captura de demográficos de pacientes se realizará en el HIS corporativo, utilizando los catálogos corporativos de Osakidetza que se precise. Además, se mantendrán actualizados dichos datos, según la información enviada por el HIS.

10.- NORMATIVA Y ESTÁNDARES

En todas las instalaciones del hospital, incluyendo el laboratorio, la empresa actuará con conocimiento y supervisión de las UGCs. En las interconexiones físicas y lógicas con el resto del hospital o de otros nodos de la red corporativa de Osakidetza y en cualquier actuación que implique a personas o equipos de las UGCs, de Osakidetza o de sus Organizaciones de Servicios la empresa cumplirá los estándares y normativa que estos determinen; entre otros:

La gestión de las muestras.
Normativa de seguridad.
Especificaciones técnicas de infraestructura.
Estándares de arquitectura de sistemas y desarrollo.
Estándares de arquitectura y configuración de CPDs.
Normativa y estándares de conectividad.
Normativa y estándares de conectividad. Requisitos técnicos para publicadores y subscriptores de eventos. Gestor de Eventos Event Manager.
Normativa para puesta en producción de aplicaciones en CPDs.
Normativa para relación con el centro de atención a usuarios (CAU).
Estos estándares podrían ser modificados por las UGCs u Osakidetza durante el contrato.

11 NORMATIVA Y OPERATIVA PARA CONECTAR UN EQUIPO A LA RED

Este punto contiene un conjunto de **medidas organizativas y técnicas** que conforman la Normativa, Operativa y Necesidades que se detalla a continuación.
Tienen como objetivo **garantizar la seguridad** de la RED de datos de Osakidetza, y se deberán **aplicar** a los equipos que se conecten a la red.

1. CONOCIDO e INVENTARIADO.

1.1. Primero acudir a Informática
1.2. Inventariar –> (Definiendo *Grupo Inventario*)

2. CUMPLIR ESTANDARES DE CONECTIVIDAD (Cable y Wifi).

2.1. Estándares de conectividad vía Wifi / Dispositivos inalámbricos:

Seguridad:
- Utilización del estándar IEEE 802.11 b/g/n
- Capacidad de asociarse a un SSID de la red WIFI correspondiente
- Soporte SSID oculto
- Soporte WPA2 Enterprise
- Cifrado de datos AES
- Autenticación EAP basada en certificado de máquina
- Soportar certificados:
  - Los certificados emitidos son de 1024 bits
  - El certificado de la CA raíz es de 4096
  - Soporten certificados con hash SHA-2
  - El tipo de certificado: x.509
  - Protocolo: RSA

2.2. Estándares de conectividad vía cable:

- Soporte velocidad de transmisión mínima 100/1000 funcionando en full dúplex (fibra o cobre; preferiblemente cobre)
- Soporte para protocolo de conectividad segura 802.1X
- Soporte para protocolo DHCP

2.3. Además de cumplir los estándares de conectividad indicados anteriormente, el fabricante deberá realizar la adecuación oportuna, en caso de evolución de los mismos.

Operativa y Líneas de trabajo a Futuro/**Necesidades**

o Los estándares de conectividad figurarán en los expedientes de contratación (Nota: en los expedientes de la Subdirección de Informática de la Dir. General se indican los estándares WIFI) -> Ver el documento **DET** en IKT – Normativa,

o Se verificará que las ofertas cumplan con dichos estándares para poder ser adjudicatarios.

o Informática dispondrá de dichos estándares para que los equipos que les soliciten conectar a la red, y que no se hayan adquirido atendiendo a las indicaciones anteriores, puedan chequear con el proveedor si cumplen los estándares de conectividad; en caso de no cumplir lo elevarán jerárquicamente en su centro **(*)** y al Comité/Comisión de Seguridad que se establezca (se menciona más adelante).

o Si hay algún caso conocido de equipamiento que ya está conectado a la red y que no cumple con dichos estándares, se elevará jerárquicamente en el centro donde esté, para que la jerarquía / quien los adquirió contacte con el proveedor y tome las medidas oportunas para cumplir con dichos estándares (adaptar / sustituir / renovar el equipamiento, lo que proceda según el caso).

Necesidades:

Crear un Comité/Comisión de Seguridad.

o Regular “elevar jerárquicamente en el centro”.

(*) *Propuesta: según el caso, Informática determinará a quién/quienes elevará jerárquicamente: Gerencia, Dir. Económica, Dir. Asistencial, Jefe del servicio afectado, Subdirector Informática de OSI, etc…*

3. CUMPLIR CON LOS SIGUIENTES ESTANDARES DE SEGURIDAD

3.1. El **software** del equipo estará **libre de vulnerabilidades** de seguridad, conocidas hasta la fecha

Operativa:

- Meterlo en el Dominio de Osakidetza: se le dará un nombre de según la nomenclatura de Osakidetza.
- Instalar el agente de antivirus
- Instalar el agente de actualización de parches de MS

3.2. **Compromiso del fabricante/proveedor** en el mantenimiento de software actualizado libre de vulnerabilidades de seguridad.

 Sistemas operativos generalistas: (windows, linux), Soportarán la incorporación del equipamiento a los sistemas corporativos de actualización (sccm, rh satelite) **aplicándoles las mismas políticas**. En caso de no poder incorporarse a dichos sistemas, aplicarán unas políticas de actualización similares que deberá conocer y validar la organización

Operativa y Líneas de trabajo a Futuro/**Necesidades**

o Crear un Comité/Comisión de Seguridad

o Solución a los casos en que no se pueden aplicar parches de seguridad.

o Dotar a los Centros de ARQUITECTURA de Pruebas (HA, Entornos, Snapshot, etc…, diversas soluciones para utilizar según el caso.)

El proveedor certificará el parche a aplicar / se dotará de entorno de pruebas **(*)** para probar / verificar la aplicación del/los parche/s correspondientes, antes de aplicarlos en PRO.

(*) *Según ARQUITECTURA de pruebas (HA, PRE, Snapshot, etc)*

Si el proveedor no certifica la aplicación de los parches, se elevará jerárquicamente en el centro y al Comité/Comisión de Seguridad para tomar las medidas oportunas.
 Sistemas operativos propietarios: deberá existir un calendario de actualizaciones anual.
Operativa

 Los equipamientos serán sometidos a análisis de vulnerabilidades periódicos debiéndose atender a los resultados de los informes cuando muestre vulnerabilidades de seguridad.

Operativa y Líneas de trabajo a Futuro/**Necesidades**
o Dotar de las licencias necesarias para poder analizar todo el equipamiento.

Analizar una vez al mes todo lo que esté "encendido" en Dir. General y Centros.
En caso de no dotarnos de los recursos necesarios para analizar todo el equipamiento, el número de IPs sobre los que se puede hacer análisis es limitado, de modo que se plantea la siguiente operativa:
- se definirán equipos críticos que estarán continuamente monitorizados y tendrán un seguimiento especial de la evolución de sus vulnerabilidades, y
- se dispondrá de un pool de IPs para lanzar escaneos puntuales a ciertos equipos, entre ellos a equipos de nueva implantación antes de su puesta en producción.
 En caso de ocurrir una nueva vulnerabilidad critica, el proveedor aplicará los parches correspondientes a la mayor brevedad (sin esperar al siguiente ciclo de actualización, para que no quede comprometida la seguridad)

Operativa:
Informática contactará con el proveedor para indicarle que debe aplicar el/los parches indicándole la criticidad del mismo y que por tanto ha de hacerse sin esperar al siguiente ciclo de actualización.
3.3. ***Acceso mínimo:*** Deberán documentar los accesos que requieren los equipos de modo que se habilitará el acceso **sólo** a lo necesario (puertos/comunicaciones).

Operativa y Líneas de trabajo a Futuro/**Necesidades**
- Dir. General: Se hace vía el *Procedimiento de Alta de maquina*
- CENTROS: No se hace; haremos una sesión concreta para revisar la ficha de Alta de máquina de Dir. General, y adaptar/reutilizar para los Centros.

3.4. ***Acceso remoto***: El acceso remoto al equipamiento se realizará siempre según los estándares corporativos.

Operativa y Líneas de trabajo a Futuro/**Necesidades (*)**
- VPN Site2Site o VPNSSL
- CENTROS: "Segmentación?, otros?, …**",**

(*) Caso/Ejemplo Wanna Cry: Equipo del proveedor que entra por VPN correctamente, **pero** si tenía el Wanna Cry **nos podría haber infectado** porque no se audita/verifica que este securizado y no infectado.

3.5. ***Acceso a Internet:*** El equipamiento que requiera conectividad a Internet deberá utilizar y soportar los mecanismos de conectividad a Internet corporativos.

Operativa y Líneas de trabajo a Futuro/**Necesidades (*)**
- Soportar Navegación a través de PROXY (hay diferentes perfiles)

Se habilita bajo demanda, y durante el periodo de tiempo necesario/ventana (tareas de instalación, etc…).
(*) Caso/Ejemplo: Solución de Lencería: requiere acceso a Internet porque utilizan/acceden a los Servidores del proveedor de Lencería.
3.6. ***Entorno Antimalware***: Los sistemas operativos que soporten productos antimalware, se incorporarán al entorno de protección corporativo. En caso de no poder incorporarse, aplicarán medidas de seguridad equivalentes y deberán ser conocidas por la organización.

Operativa y Líneas de trabajo a Futuro/**Necesidades**
o Sistemas operativos propietarios

Si el proveedor indica que no soporta la instalación del antivirus de Mcafee o su sustituto, deberá indicar qué producto instala para su evaluación. Se le exigirá un software antimalware si es un sistema operativo susceptible y existen soluciones de antivirus.
3.7. ***Usuarios administradores***: Las operaciones realizadas por los usuarios administradores estarán auditadas.

Líneas de trabajo a Futuro/**Necesidad (*)**
(*) Cuando dispongamos de la solución a esta necesidad habrá que detallar la **Operativa**.
3.8. ***Usuarios genéricos:*** Se debe evitar el uso de este tipo de usuarios.

El uso de este tipo de usuarios impide identificar a quién accede (*login* al equipo), lo que dificulta la localización del origen de los problemas en caso de incidencia.
Así mismo, a los usuarios **(*)** se les permitirá acceso únicamente a los recursos y servicios requeridos, restringiendo a su vez el nivel de acceso y permisos al mínimo suficiente para el funcionamiento correcto.
(*) usuarios identificados con DNI o no/genéricos
Operativa y Líneas de trabajo a Futuro/**Necesidades (*)**
- Promover el uso de DA

(*) Casos/Ejemplos: **a_local** (que tenga acceso a lo minino que deberían tener, y hacer lo mínimo que deberían hacer, etc..); uso de **carpetas compartidas** con permisos escritura a everyone en estaciones y hasta servidores.
3.9. ***Dispositivos móviles corporativos(tablets, portátiles, móviles):*** Este tipo de equipamiento debe estar sometido a medidas adicionales de seguridad para verificar su estado antes de conectar a la red debido a la exposición que haya podido sufrir en conexiones externas al entorno corporativo.

12. INFORMACIÓN DE SEGUIMIENTO Y CONTROL DEL SERVICIO

La empresa adjudicataria elaborará y remitirá a Osakidetza y las UGCs información relativa a la prestación del servicio, con la regularidad que se determine y con el contenido y detalle necesarios, tanto para la comprobación del cumplimiento de los niveles de servicio como para facilitar las decisiones de gobierno de la actividad.

Asimismo, la empresa pondrá a disposición de las UGCs la capacidad para acceder a los sistemas y aplicaciones en base a su función auditora.
Para llevar a cabo estas exigencias, la empresa dispondrá los elementos técnicos necesarios, conforme a los procedimientos y estándares determinados por Osakidetza y/o las UGCs

ANEXO IV

Atención a usuarios y acuerdos del nivel de servicio

1.- SOPORTE A USUARIOS Y MANTENIMIENTO DE EQUIPOS Y SEGURIDAD TRANSFUSIONAL

El adjudicatario ofrecerá soporte de usuarios (atención de consultas e incidencias) y mantenimiento con relación al software y hardware aportado por el mismo en base a esta licitación.

Las herramientas de gestión a utilizar en este contrato , en relación al soporte a usuarios de seguridad transfusional, serán las siguientes:

- La herramienta utilizada por el 1º nivel de CAU de Osakidetza, para registro y gestión de las consultas e incidencias técnicas y funcionales de los aplicativos, es el producto HP-Service Manager
  .
- La herramienta utilizada en Osakidetza para la Gestión de la Demanda y el flujo de Mantenimiento, es el producto HP-PPM (Project and Portfolio Management).

El servicio de Atención a Consultas y Soporte, actuará como soporte de 2ª nivel de los servicios contratados, pudiendo realizarse el acceso al servicio por los siguientes canales:

- Vía derivación del CAU de 1º nivel, previo registro en HP-Service Manager
- Vía HP-PPM: Incidencia registrada en HP-PPM, por la Subdirección de informática de Osakidetza
- Vía teléfono: derivado del CAU Osakidetza o de la Subdirección de informática de Osakidetza

En caso de que el proveedor disponga de una herramienta para la gestión del CAU, deberá integrarse con las herramientas actuales y futuras de Osakidetza, siendo a cargo del adjudicatario los costes derivados de esta integración correrán a cargo del adjudicatario.

El soporte de los equipamientos deberá estar conformado por tres tipos de apoyo. El primer nivel estará disponible telefónicamente. El segundo será de acceso remoto y el tercero, será presencial en los casos en los que sea necesario. Ambos niveles de soporte se ofrecerán en los horarios descritos más adelante.

2.- HORARIO DE PRESTACIÓN DE SERVICIOS DE SOPORTE

Para los servicios de soporte, el horario de prestación debe cubrir suficientemente las necesidades de asistencia de los diferentes entornos. Deberá ofertarse como mínimo:

- De 08:00 a 20:00 horas, de forma ininterrumpida (Lu-Vi)
- De 08:00 a 19.00h de forma ininterrumpida (Sábados).
- Fuera de este horario debe existir al menos un buzón de avisos para dejar constancia de incidencias y reclamar servicio prioritario para el siguiente día.

Las averías de equipos que exijan un soporte presencial deberán ser resueltas en un plazo no superior a 24h (salvo festivos) desde la comunicación de la incidencia.

En Vitoria-Gasteiz, a 24 de enero de 2019

Fdo: Iñaki Unzaga Basauri

Red Diagnóstico Biológico de Osakidetza