PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE LA ADQUISICION DE UN SISTEMA AUTOMATIZADO DE ALMACENAMIENTO DE CONCENTRADOS DE HEMATIES EN EL CENTRO VASCO DE TRANSFUSIÓN Y TEJIDOS HUMANOS

1.- ANTECEDENTES

El CVTTH es la referencia en la asistencia transfusional de la Comunidad Autónoma Vasca (CAV). Es responsable de la promoción, extracción, estudio analítico, fraccionamiento primario, organización del fraccionamiento plasmático, distribución de componentes sanguíneos, así como la formación e investigación de medicina transfusional. Así mismo desarrolla las actividades de procesamiento analítico, criopreservación y distribución de tejidos humanos, y el banco de leche materna. La actividad del CVTTH como biobanco está integrada como nodo en el Biobanco Vasco para la Investigación O+EHUN.
Todo esto con arreglo a tres cuestiones clave:

1. **Autosuficiencia**, entendida como la responsabilidad primordial de asegurar la disponibilidad de componentes sanguíneos procedentes de la donación altruista y desinteresada de los ciudadanos de la CAV. La autosuficiencia es una responsabilidad específica de cada sistema sanitario que debe asegurar el abastecimiento de productos estratégicos para la asistencia y la salud pública, y limitados en cuanto a su obtención, por lo que es obligado no comprometer la organización de sistemas sanitarios vecinos más previsores.

2. **Seguridad**, entendida como el control para minimizar la aparición de efectos adversos, fundamentalmente los infecciosos, y su repercusión en la salud pública de la CAV.

3. **Calidad**, directamente relacionada con las anteriores y que incluye la obtención de componentes sanguíneos y tejidos y sustancias de origen humano (leche materna donada) de óptima seguridad y pureza.

El CVTTH está integrado en la *Red Transfusional y de Suministro de Tejidos Humanos y Sustancias de origen Humano del País Vasco*, de la que forman parte además los servicios de transfusión de los hospitales, los centros de obtención, implantación y bancos de tejidos humanos, y el Equipo de Coordinación de Trasplantes del País Vasco, y las Unidades de Neonatología. El CVTTH tiene una función coordinadora de la parte transfusional, y de las SOH de la Red y comparte con Coordinación de Trasplantes (cada uno en el área que es propia) la coordinación en el ámbito de suministro de tejidos.

El CVTTH dispone de una sede central situada en Galdakao (Vizcaya) en Barrio Labeaga 46 A, que alberga las oficinas centrales, los laboratorios, criobiología, donación, procesamiento, almacenamiento y distribución. Además, hay dos sedes territoriales. La territorial de Álava está situada en Vitoria-Gasteiz en la cuarta planta del edificio del Ambulatorio Olagibel, y la territorial de Gipuzkoa, se encuentra en Donostia-San Sebastián, en la calle Manuel Lekuona nº1 bajo. En ambas se desarrollan actividades de promoción, extracción y aféresis.

El CVTTH dispone de un sistema automatizado de almacenamiento de Concentrados de Hematíes que permite una gestión de este stock más eficiente, con interoperabilidad con el sistema de información eODOLBIDE, así como mejor ergonomía para los trabajadores. Este sistema (aparataje y software) debe ser renovado por su antigüedad.

El presente documento consta de los siguientes Anexos:

ANEXO I Relación de material

ANEXO II Prescripciones técnicas

ANEXO III Prescripciones técnicas relativas al desarrollo informático

ANEXO IV Atención a usuarios y acuerdos de nivel de servicio

ANEXO V Continuidad del servicio

2.- OBJETO DEL CONTRATO

El presente Pliego de Prescripciones Técnicas tiene por objeto definir el alcance y las condiciones que habrán de regir la contratación de los servicios necesarios para la retirada del actual sistema de almacenamiento automatizado de Concentrados de Hematíes (Kardex, gestionado por GRIFOLS) y la sustitución e instalación de un nuevo sistema, de acuerdo con las características que se indican en apartado 5. Definición del Contrato, en el que se detallan las necesidades técnicas para la realización de las mismas.

3.- ASPECTOS LEGALES

Los licitadores acreditarán, mediante la oportuna documentación, que el material ofertado cumple con la legislación y la normativa española y comunitaria vigente que sea de aplicación, siendo por cuenta del adjudicatario cualquier gasto que se derive de su aplicación. Asimismo, deberán acompañar a la ficha técnica de los productos la copia de los certificados de marcado CE de los productos.

Los productos y accesorios deberán estar conformes, en el momento en que se realice su suministro, con las condiciones que les sean de aplicación, constando la declaración conforme del fabricante que acredite el cumplimiento de las normas técnicas de aplicación obligada para cada uno de los equipos que oferten.

4.- BASES GENERALES PARA LA CONTRATACION DEL SUMINISTRO DEL MATERIAL

El valor estimado del presente expediente es:

Presupuesto máximo	**300.000,00 €**
Presupuesto SIN IVA	**300.000,00 €**
Valor estimado del expediente sin IVA	**300.000,00 €**

5.- DEFINICIÓN DEL CONTRATO

La empresa adjudicataria realizará, en síntesis, los servicios de desmontaje del equipo obsoleto, instalación de equipo, adecuación y cierre de la cámara frigorífica, instalación del equipamiento informático y software de gestión, puesta en marcha, formación del personal y mantenimiento del sistema.

Las Especificaciones se detallan en el Anexo II.

6.-OTRAS CONDICIONES DEL ADJUDICATARIO

6.1.- Formación

La entidad adjudicataria, previa conformidad del equipo directivo del CVTTH, determinará el programa formativo a seguir por el personal. La formación que se considere necesaria será financiada por el adjudicatario.

Deberá permitir y facilitar a los responsables del CVTTH el acceso permanente a las aplicaciones informáticas y sistemas de información empleados para la prestación del servicio.

6.2.- Calidad

6.2.1.- Obligaciones generales

El adjudicatario estará obligado a que el objeto del contrato responda a los umbrales de calidad que determine el CVTTH, acordes siempre a la legislación y a Estándares, Guías reconocidas por la comunidad científica.

Todo el material y equipamiento ofertado deberá disponer de marcado CE.

6.2.2.- Protocolos y Procedimientos de actuación

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

Guías de Uso, Manual de procedimientos, para operadores y administradores: en idioma español

Si procediera: Tratamiento y protección de datos, sistema de archivo y manual actualizado del sistema informático, 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.

6.3.- Puesta en marcha

Los licitadores deberán elaborar un plan de puesta en marcha, previa conformidad del CVTTH, que incluya todas las áreas afectadas 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.

6.4.- Servicio técnico

El adjudicatario se encargará del mantenimiento y reparación de los equipos mecánicos y sistemas informáticos asociados durante el periodo de vigencia de garantía del contrato, así como, a la actualización del software, 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.

7.-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.

8.- DESARROLLO INFORMATICO

Las prescripciones técnicas relativas al desarrollo informático son las que se especifican en el Anexo III de este Pliego.

ANEXO I Relación de material

Lote	Art.	Denominación	Nº unidades	Precio Unitario Licitación SIN IVA	IVA%	Obligatorio Lote Entero	Adjudicación Compartida	Procede entregar muestras
1	1	Sistema automatizado de almacenamiento de concentrados de hematies	1	300.000,00	21	SI	NO	NO

ANEXO II Prescripciones técnicas

1.- INTRODUCCIÓN

Se distinguen dos elementos:
A) EQUIPO. El equipo armario debe estar constituido básicamente por un sistema rotatorio de contenedores a diferentes niveles con bandejas en los que almacenar las unidades de Concentrados de hematíes, según orden establecido por configuración de distintos parámetros (caducidad, grupo sanguíneo, código de producto, máximo de unidades por bandeja…) El equipo es gestionado por un software integrado con el sistema informático principal del CVTTH.

B) SOFTWARE. El programa informático de gestión del equipo armario se instalará en un ordenador con maqueta de Osakidetza proporcionado por el CVTTH según las especificaciones del Anexo IV, donde la aplicación se alojará en un servidor virtualizado en el CPD de Osakidetza. Debe integrarse con los siguientes sistemas del CVTTH: LDAP corporativo, Eodolbide (producto comercial e-Delphyn de la empresa Hemasoft) y si fuese necesario, con la NAS(Network Attached Storage) corporativa.

2. CARACTERÍSTICAS TECNICAS *REQUISITOS EXIGIBLES*

Respecto al EQUIPO:

- El equipo debe tener un volumen útil de almacenamiento aproximado de 5,6 m^3. Y unas medidas aproximadas de 2700 mm de altura, 3500 mm de anchura y 1700 mm de fondo.
- El equipo debe ser instalado en una cámara de 4ºC, existente y en funcionamiento.
- El equipo debe ser capaz de almacenar hasta 6000 unidades de Concentrados de hematíes.
- El elemento frontal de la cámara dispondrá de una ventana lo suficientemente amplia para acceder con facilidad y comodidad al equipo, con apertura mecánica y manual, y con cierres que garanticen las condiciones de almacenamiento de los componentes sanguíneos.
- El acceso a los mandos /accesorios/ interruptores del equipo por parte del usuario debe ser fácil.

Respecto al SOFTWARE, debe permitir para los distintos aspectos relacionados:

- **Accesibilidad:**
  - Acceso con integración del directorio activo (LDAP), controlado mediante usuario y contraseña, con validación de contraseña a través del LDAP corporativo.

- **Configuración General y funcionalidades troncales:** Opción de Consultar y Modificar los datos relacionados con:
  - Seguridad: La longitud mínima, caducidad y vigencia de las contraseñas de usuario.
  - Validación LDAP: Activación del servicio de directorio activo (LDAP) para la validación de usuarios en la aplicación
  - Conexión: Datos de conexión del sistema con el servicio de directorio activo (LDAP)
  - Entradas y Salidas:
    • Posibilidad de confirmación automática/manual de albaranes

    • Número máximo de horas transcurridas desde que una unidad es retirada del armario automatizado por una salida de estudio temporal hasta el momento en que ésta misma unidad retorna de nuevo al armario.

  - Gestión de unidades RFID: Al activarse, debe permitirse gestionar de forma particular las unidades que dispongan de etiquetas RFID. Las unidades que dispongan de etiqueta RFID pueden ser almacenadas en cajetines separados, no mezclando estas unidades con aquellas que no tengan esta característica.

  - Códigos especiales inventario: Códigos de barras (Code 128: Subtipo A, B o C) asignados a la ejecución de comandos concretos durante la ejecución de inventarios

  - Listado de contingencia: Exportación automática de las existencias del armario, tras la finalización de cualquier albarán de entrada, salida, inventario o solicitarlo expresamente. Debe permitirse la configuración de la ruta de salida y el nombre del fichero resultante.

- **Integración con los sistemas de información del CVTTH** siendo éstos: LDAP corporativo, eODOLBIDE, producto comercial e-Delphyn de la empresa Hemasoft y si fuese necesario, con la NAS(Network Attached Storage) corporativa., siguiendo los estándares de interoperabilidad del Anexo IV.

- **Gestión de usuarios mediante perfiles de usuario:** Gestionar **e**l acceso de los usuarios a las funciones del programa mediante la utilización de perfiles de usuario.
  - • Crear, modificar, inactivar o eliminar perfiles.
  - • Gestionar accesos directos a las funcionalidades más utilizadas.
  - • Posibilidad de impresión de listados de perfiles.
  - • Crear un perfil de administración.

- **Gestión del sistema de almacenamiento:** Gestionar las características de los equipos de almacenamiento desde la aplicación.
  - Gestión de los cajetines de almacenamiento:
    • Alta, modificación, inactivación y/o eliminación de cajetines
    • Asignación de cajetines a los armarios automáticos.
    • Posibilidad de generación de listados de cajetines

  - Gestión de los armarios automáticos:
    • Alta, modificación, inactivación y/o eliminación de armario
    • Asignación de peso máximo por bandeja y peso máximo diferencial entre bandejas
    • Gestión de la estructura de armario: cestas / bandejas / cajetines.
    • Opción de copia de estructura de armario.

- **Gestión de productos:** Gestionar las características de los productos almacenables desde la aplicación web.
    - Procesos básicos soportados:
        - Alta, modificación, inactivación y/o eliminación de productos
        - Configuración del tiempo máximo permitido para la salida de estudio temporal
    - Productos alternativos o equivalentes: Funcionalidad que permita la configuración de productos que pueden entregarse indistintamente ante una solicitud de salida.
    - Gestión de grupos sanguíneos:
        - Alta, modificación, inactivación y/o eliminación de grupos sanguíneos
        - Asignación de grupo a los productos.
    - Gestión de fenotipos:
        - Alta, modificación, inactivación y/o eliminación de fenotipos
        - Asignación de fenotipo a las unidades.
    - Gestión de familias de productos:
        - Alta, modificación, inactivación y/o eliminación de familias de productos
        - Asignación de familia a los productos.
- **Gestión de inventarios:** Disponer de la funcionalidad de comprobación de las existencias físicas respecto a las existencias lógicas en los armarios automáticos.
    - Gestión diferenciada de cinco tipos de inventarios:
        - Inventario por Producto
        - Inventario por Familia
        - Inventario por Ubicación
        - Inventario por Caducidad
        - Inventario por Cajetín Vacío
    - Exportación del resultado del inventario: Generación manual o automática de fichero de interface con los resultados de los procesos de inventario.

- **Gestión de los movimientos de entrada/salida:**
  - Gestión diferenciada por tipo de albaranes de salida:
    - Albarán de salida por Fecha de Extracción
    - Albarán de salida por Fecha de Caducidad Mínima
    - Albarán de salida por Fecha de Caducidad
    - Albarán de salida por Preselección de Unidades
    - Albarán de salida por Código de Donación

  - Gestión de unidades con reserva: Permitir a los usuarios con el permiso correspondiente, reservar ciertas unidades para evitar la salida.
  - Gestión de albaranes de entrada:
    - Importación de albaranes de entrada
    - Previsualización y ejecución de albaranes de entrada
    - Opción de reserva de unidades asociada a albaranes de entrada

  - Funcionalidad de salidas/entradas temporales: Soportar la funcionalidad de salidas temporales de unidades, controlando el tiempo transcurrido entre la salida y la subsiguiente entrada.

- **Búsqueda de unidades:** Proporcionar una utilidad para localizar unidades en el sistema de almacenamiento a partir de una serie de filtros configurables por el usuario.
  - Posibilidad de descarga y exportación de los resultados.

- **Generación de informes:** Permitir la generación de diferentes informes, que reflejan los resultados de la operativas y el estado de la instalación. Los informes se deben poder visualizar, imprimir y/o exportar.
    - Existencias: Mostrar las unidades existentes en el sistema que cumplan los criterios de filtro que el usuario haya introducido, con opciones simple/detallado.

    - Unidades fuera de stock: Mostrar las unidades que se encuentran fuera del sistema debido a la realización de salidas temporales y que cumplan los criterios de filtro introducidos, con opciones simple/detallado.

    - Cajetines con existencias: Mostrar las ubicaciones que cumplen el filtro introducido, así como la información de las unidades contenidas en ellas: producto, grupo sanguíneo (en aquellos productos que lo gestionen), donación, fecha de extracción, fecha de caducidad, si la unidad está reservada y observaciones (si la unidad tuviera observaciones).
    - Cajetines vacíos: Mostrar los cajetines vacíos en la instalación, con opciones simple/detallado

    - Distribución ocupación disponible: Mostrar la ocupación del sistema de almacenamiento, con opciones simple/detallado.

    - Donaciones: Mostrar histórico de albaranes e inventarios referente a una donación concreta y/o un tipo de producto, indicando la ubicación y la fecha en la que se han realizado.
- **Gestión para la prevención de desequilibrios y/o sobrecarga del equipo armario automatizado.**

El adjudicatario deberá:

a) Retirar el equipo obsoleto, instalar el equipo armario automatizado, adecuar la cámara 4ºC, y licencias de software, facilitar el material complementario (bandejas, lectores de códigos de barras, …)

b) Proceder a la configuración del ordenador y su conexión con la impresora de red del área de distribución del CVTTH, configuración del software, desarrollo de interfaces nuevos cuyo coste correrá a carga del licitador y conexiones con el sistema principal del CVTTH eODOLBIDE y la integración con el LDAP corporativo.

c) **Facilitar un Plan de Puesta en marcha.** Los licitadores deberán elaborar un plan de puesta en marcha y/o adaptación, con cronograma, agentes involucrados… intentando que el tiempo de parada (armario automatizado no operativo por el CVTTH) sea el menor posible. 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 adjudicación.

d) Facilitar la documentación necesaria para la cualificación inicial del equipo, tales como DQ/IQ/OQ/PQ, y certificados CE en su caso.

e) Facilitar Manual de Uso de aparatos y aplicativos, Protocolos e Instrucciones de Trabajo en castellano, en soporte pdf.

f) **Facilitar un Plan de Asistencia Técnica y Soporte.** Este plan deberá detallar la atención de consultas e incidencias y sobre el mantenimiento, tales como periodos de mantenimiento, recursos humanos, medios tecnológicos, canales y horarios, tiempos de respuesta, tipos de soporte a disposición del CVTTH e indicadores de seguimiento de este soporte (asignación de prioridad o gravedad, tiempo de resolución…). Debe tenerse en cuenta que cualquier incidencia que afecte al servicio de forma crítica será considerada inicialmente como Urgente. El adjudicatario se encargará del mantenimiento y reparación del equipo y sistemas informáticos asociados durante el periodo de vigencia del contrato. El mantenimiento incluido en la oferta comprenderá todas las actuaciones de mantenimiento preventivo, correctivo y normativo, incluidas calibraciones (si procede). El mantenimiento incluirá la sustitución de piezas, recambios, mano de obra, desplazamientos… y todos los elementos que garanticen el correcto funcionamiento de los equipos. El soporte telefónico deberá ser continuo 24x7x365.

g) **Facilitar un Plan de Formación.** El adjudicatario deberá disponer de al menos un especialista dedicado que apoye al personal del centro en la puesta en marcha de la configuración de los sistemas y formación del personal. Este Plan deberá detallar los recursos y medios asignados.

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 el CVTTH.
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 del CVTTH. Los equipos destinados a servidores de aplicaciones, de bases de datos y procesos, se alojan en el Centro de Proceso de Datos (CPD) de Osakidetza.

• 3.- INSTALACIONES E INFRAESTRUCTURA BÁSICA

La empresa adjudicataria utilizará las instalaciones e infraestructura básica del CVTTH, 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 estarán configurados con la maqueta de Osakidetza.

El equipamiento físico y lógico que tenga que interactuar o integrarse con otros sistemas de información, del CVTTH y de Osakidetza cumplirá los estándares definidos por éstos, tal y como viene establecido en este Anexo IV. Estos estándares actuales podrían ser modificados por el CVTTH u Osakidetza durante el contrato.

Actualmente, la versión de maqueta que se instala en los equipos de Osakidetza, son la 1709 y la 1909 con sistema operativo Windows10-Professional 64 bits.

Las especificaciones técnicas de los equipos son:

Hardware:
Procesador i5
Memoria RAM 8 Gb.
Disco duro 500 Gb.
Monitor 19 pulgadas con resolución 1440x900 mayoritaria o 1280x1024.

Asimismo, la arquitectura de los sistemas a instalar en el CPD cumplirá los estándares definidos en este anexo. Estos estándares actuales podrían ser modificados por el CVTTH 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 y será supervisado por el CVTTH.

• 5.- COMUNICACIONES Y CONECTIVIDAD

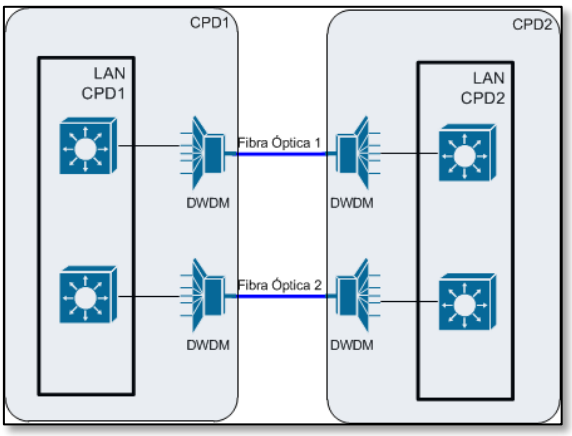
El equipamiento informático del adjudicatario estará conectado a la red local del hospital.

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 el CVTTH.

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 del CVTTH 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, cuyos elementos principales son:

Datacenter

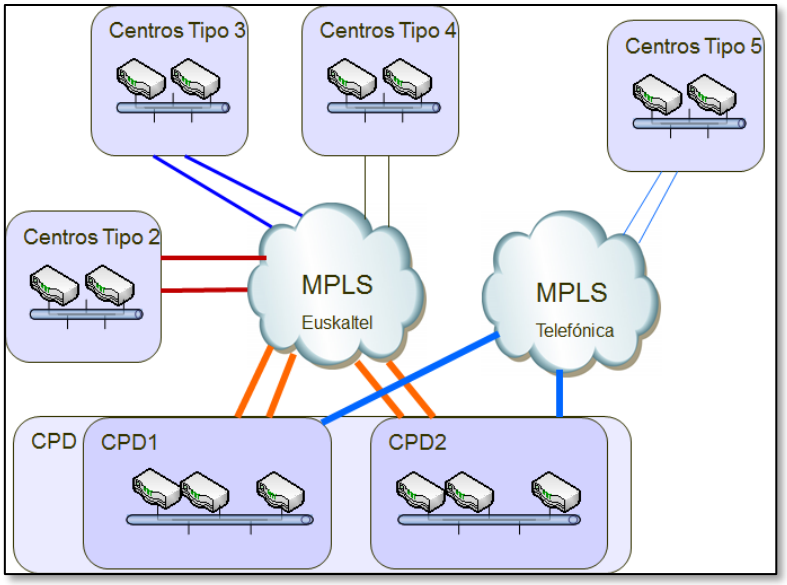
La infraestructura de Datacenter de **Osakidetza** está formada por dos sedes interconectadas entre ellas mediante una conexión redundada de fibra óptica oscura dedicada. De manera gráfica sería como sigue:



Red WAN

Actualmente **Osakidetza** dispone de **dos redes WAN MPLS**. Una de ellas operada por Euskaltel y la otra por Telefónica.

En el siguiente diagrama se ve de manera esquemática:



En el esquema anterior se observa que los centros están divididos por tipo, en función de su tamaño con el siguiente detalle de caudales:

	CAUDAL POR ACCESO	NÚMERO DE ACCESOS	OPERADOR
TIPO 1	2 Gbps	2	EUSKALTEL
TIPO 2	300Mbps	2	EUSKALTEL
TIPO 3	80Mbps	2	EUSKALTEL
TIPO 4	30Mbps	2	EUSKALTEL
TIPO 5	4Mbps*	2	TELEFÓNICA

** Caudal variable en función de la cobertura de operador.*

Las características principales de la Red de comunicaciones de **Osakidetza** son las siguientes:

- **Cifrado** de los datos que transitan por la red WAN.
- **Alta Disponibilidad y Redundancia** de la solución de modo que se asegure la continuidad de las comunicaciones en todos los centros ante eventuales incidencias.
- **Utilización máxima** de las capacidades solicitadas de modo que se obtenga el aprovechamiento máximo de los accesos y caudales totales de cada centro (**Balanceo de Carga**). Ambos accesos se utilizan de forma simultánea.
- Se permite la comunicación **any-to-any** (spoke-to-spoke) entre todos los centros.
- **Calidad de Servicio**: Mediante la configuración de **Clases de Servicio (CoS)** soportadas sobre la Red MPLS.

• 6.- SERVICIO DE DIRECTORIO

Tanto los Servidores del área de CPD como los PCs estarán integrados en el dominio que indique el CVTTH del Directorio Activo (Microsoft) de Osakidetza,

• 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 Distribución de Componentes sanguíneos del CVTTH.

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 el CVTTH. 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 CVTTH la 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

El CVTTH y los Servicios Centrales de Osakidetza 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, el CVTTH 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 EL CVTTH Y OSAKIDETZA

Los estándares de obligado cumplimiento en cuanto a integración de sistemas se detallan a continuación y podrían ser modificados por el CVTTH u Osakidetza durante el contrato.

Las adaptaciones requeridas en los Sistemas de Información del CVTTH, de Osakidetza derivadas de la adopción de la solución propuesta deberán ser asumidas por el adjudicatario. El desarrollo será realizado por las empresas que Osakidetza, y el CVTTH determinen en cada momento, principalmente los adjudicatarios de sus contratos de mantenimiento.

Así mismo, el coste de las nuevas conexiones y/o las licencias que sean necesarias para conectarse a eOdolbide, producto comercial e-Delphyn de la empresa Hemasoft serán asumidas por el adjudicatario durante todo el periodo que dure el contrato

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.

Los Sistemas de Información corporativos a integrar susceptibles de conexión son:

Sistema de Información para la gestión del Centro Vasco de Transfusión, eOdolbide
LDAP corporativo
NAS-Isilon Datalake

Interoperabilidad:

Los requisitos de integración de diversos sistemas de información de **Osakidetza** se realizarán de acuerdo a una arquitectura orientada a servicios (SOA) sobre la plataforma Oracle SOA Suite (Oracle BPEL Process Manager, Oracle Service Bus (OSB), Oracle Business Rules, ...).

Dicha arquitectura proporciona una forma bien definida de exposición e invocación de **Servicios Web**, lo cual facilita la interacción entre diferentes sistemas propios o de terceros.

Sobre la misma arquitectura SOA, **Osakidetza** implementa una solución de integración orientada a **Eventos**; es un diseño a medida que gestiona un conjunto de sistemas que publican eventos y un conjunto de aplicaciones que se suscriben a determinados eventos. Dicha solución se denomina Gestor de Eventos-Event Manager y es responsable de recibir los eventos publicados, ejecutar las validaciones adecuadas y almacenar los eventos para su envío a los subscriptores que estén asociados a cada uno de los elementos recibidos.

Relación de estándares de comunicación soportados:

- Protocolos a nivel de mensaje:
  - SOAP 1.1 y SOAP 1.2,
  - WSDL 1.1 y WSDL 1.2 Binding,
  - SOAP con Attachments
- Protocolos de seguridad a nivel de mensaje:
  - WS-Security 1.0/1.1,
  - WS-SecurityPolicy,
  - WS-Policy,
  - WSPolicyAttachment,
  - WS-Security: Username Token Profile 1.0/1.1,
  - WS-Security: X.509 Token Profile 1.0/1.1,
  - WSSecurity: SAML Token Profile 1.0/1.1,
  - WS-Security: KerberosToken Profile 1.1,
  - WS-Reliable Messaging 1.0,
  - WS-Addressing,
  - WS-I Basic Profile 1.1
- Protocolos a nivel de transporte:
  - HTTP 1.0, HTTP 1.1,
  - TLS, SSL
  - Interoperabilidad con registros UDDI v3-compliant
  - Sistemas middleware basados en JMS/MQ.

Servicios Web

Los Servicios Web se implementarán de acuerdo con las especificaciones WSDL v1.1, SOAP v1.1, v1.2, UDDI v2.XX y XML v1.0, con el objetivo de incorporar las recomendaciones de la WS-I definidas en la especificación Basic Profile v1.0, v2.0 y de esta manera asegurar la interoperabilidad entre los sistemas.

El estándar de codificación que se utiliza en los mensajes XML es UTF-8.

La seguridad aplicada a los servicios web cubrirá los siguientes aspectos:

- **Autenticación**: Verificar que el cliente (usuario o aplicación) es quien dice ser. La identidad de un usuario se realizará en base a la información presentada por el usuario (usuario/contraseña, certificado, token SAML)

- **Autorización**: Otorgar acceso a los servicios en base a la identidad del cliente o a los roles asignados.
- **Confidencialidad, privacidad**: Mantener la información secreta mediante el uso de algoritmos de encriptación estándar de elementos XML.
- **Integridad, no repudio**: Asegurar que un mensaje permanece inalterado durante la transmisión mediante la firma digital. La firma también valida la identidad del remitente y proporciona una marca de tiempo para garantizar que una transacción no puede ser repudiada más tarde ni por el remitente ni por el destinatario.

Osakidetza usa **Oracle Web Service Manager** (OWSM) para gestionar y aplicar políticas a los servicios web publicados en la plataforma SOA.

La política estándar que **Osakidetza** ha definido para los servicios proporciona:

- Autenticación mediante certificado x509
- Protección del mensaje mediante firma (sin encriptado)

Existen dos versiones de la política en OWSM, una para servicios y otra para clientes. Para garantizar la interoperabilidad, cada política tiene su versión compatible con tecnología .NET y Java.

- oracle_wss10_x509_token_with_message_sign_service_policy
- oracle_wss10_x509_token_with_message_sign_service_policy_net
- oracle_wss10_x509_token_with_message_sign_client_policy
- oracle_wss10_x509_token_with_message_sign_client_policy_net

Los clientes y aplicaciones que acceden a través de internet entran a la DMZ a través del firewall de aplicaciones (WAF). El WAF aplica reglas contra ataques y define patrones de seguridad.

- Es responsabilidad de cada aplicación publicada en la DMZ controlar el acceso y autorizar a los usuarios.
- El OSB de internet publica los servicios a los que pueden acceder las aplicaciones de internet.
- El OSB de internet audita todas las llamadas a los Servicios Web mediante una política propietaria de **Osakidetza** gestionada por OWSM.
- En el OSB de internet se protegen todos los servicios con la política oracle_wss10_x509_token_with_message_sign_service_policy. Esta política autentica a las aplicaciones mediante certificado x509 y firma el mensaje de petición y respuesta.
- El OSB de internet delega la ejecución a servicios publicados en la Intranet.
- En la intranet, se despliegan instancias independientes de servicios web para dar servicio a las peticiones que llegan desde el OSB de Internet.
  Nota: OSB -> Oracle Service Bus 11.1.1.7

Gestor de Eventos

A continuación, se describen los requisitos técnicos que tienen que cumplir las aplicaciones para publicar y/o recibir eventos.

- Estándares de comunicación

La mensajería del Servicio **Osakidetza** se implementará de acuerdo con las especificaciones del estándar HL7 versión 2.XX o con cualquier otro formato propio de **Osakidetza**; de esta manera se asegura la interoperabilidad entre los sistemas de información.

- Relación de tecnologías soportadas para la publicación y subscripción a eventos.

Tecnologías que soporta el gestor de eventos para la publicación y subscripción a eventos, así como si la modalidad soporta transaccionalidad y las opciones de seguridad disponibles:

Modalidad	Tecnología	Transaccional	Orden	Seguridad
Publicación	Mensajería JMS	Sí	Sí, si el publicador establece el parámetro UnitOfOrder	Autenticación (user/pass)
Publicación	Servicio web	No	No	Ninguna, Autenticación (user/pass) y WS-Security
Subscripción	Mensajería JMS	Sí	Sí. Event Manager garantiza la entrega en el mismo orden que ha recibido los mensajes	Autenticación (user/pass)
Subscripción	Servicio OSB	Sí	Sí. Event Manager garantiza la entrega en el mismo orden que ha recibido los mensajes	Ninguna
Subscripción	Servicio web	Sí	Sí. Event Manager garantiza la entrega en el mismo orden que ha recibido los mensajes	Ninguna, Autenticación (user/pass) y WS-Security

Por cada modalidad y tecnología se deben cumplir unos requisitos técnicos que serán indicados al adjudicatario para la implementación de esta forma de integración.

Mensajería. Definición de Evento

Un evento es un documento XML definido mediante un XSD, donde:

- **id:** Es el identificador del tipo de evento. Se genera durante el proceso de alta del evento en el sistema de administración de Event Manager. Durante el procesamiento de un evento se verifica que el id sea válido.
- **correlation:** Es un campo libre en el que el publicador del evento indica un número correlativo relativo a su sistema.
- **source:** Es el identificador del publicador. Se genera durante el proceso de alta de un publicador en el sistema de administración de Event Manager. Durante el procesamiento de un evento se verifica que el source sea válido.
- **timestamp:** Lo establece el publicador del evento en el momento del envío.
- **metadata**: Puede contener un xml que ayude a describir el contenido del evento. Event Manager puede utilizar esta información para tomar decisiones de enrutado.
- **payload:** Es el contenido del evento. Puede ser cualquier cadena de texto o XML.

El resultado devuelto cuando se publica un evento en Event Manager es un XML definido por un XSD, donde:

- **uuid:** Es un identificador único que se asigna a cada evento procesado por Event Manager.
- **processed:** true o false, si el evento se ha procesado correctamente o con errores.
- **errorCode:** Si se ha producido un error, aquí se informa el código del error.
- **errorDescription:** Si se ha producido un error contiene la descripción de éste.

Se realiza gestión de errores: codificación de errores y descripción de los mismos.

• 10.- NORMATIVA Y ESTÁNDARES

En todas las instalaciones del hospital, la empresa actuará con conocimiento y supervisión del CVTTH. 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 del CVTTH, de Osakidetza la empresa cumplirá los estándares y normativa que estos determinen; entre otros:

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 el CVTTH 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 via 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 ó VPNSSL

(*) 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 el CVTTH 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 del CVTTH 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 el CVTTH

ANEXO IV Atención a usuarios y acuerdos de nivel de servicio

• 1.- SOPORTE A USUARIOS Y MANTENIMIENTO DE EQUIPO ARMARIO Y SOFTWARE

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, 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.

Tras la gestión de cada comunicación de incidencia o actuación de mantenimiento, el adjudicatario elaborará un informe que deberá ser proporcionado al CVTTH.

• 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 un servicio 24 x 7 x 365

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.

ANEXO V Continuidad del servicio

El adjudicatario, como proveedor de servicios tecnológicos, deberá disponer y mantener un plan de continuidad y de contingencias sobre las infraestructuras que soportan sus servicios prestados. Por su parte, OSAKIDETZA indicará los niveles de servicio, tiempos de respuesta objetivo y tiempos de vuelta a la normalidad para cada uno de los servicios que, por su parte, el adjudicatario deberá asegurar estas exigencias mediante la adopción de las medidas necesarias.

Los niveles exigidos por OSAKIDETZA estarán condicionados por los que tuviese históricamente asociados a su servicio. Se debe asegurar la colaboración del adjudicatario en el mantenimiento de estos niveles, además de asegurarlo también en la realización del plan de pruebas y simulacros ya definidos en los servicios que OSAKIDETZA presta a la ciudadanía.

Si bien se entiende que el modelo de recuperación ante desastres, planes de continuidad y planes de contingencia de las dos organizaciones (el adjudicatario y OSAKIDETZA) no han de ser homólogos, el compromiso aquí reconocido establecerá las bases para la consecución de una línea común que permita mantener de manera coherente ambos modelos. Queda el detalle de su definición como una tarea a abordar de manera conjunta tras la firma de la presente contratación para lo que se dispone, como punto de partida, el anexo de “Medidas de seguridad aplicables”.