PLIEGO DE PRESCRIPCIONES TÉCNICAS

SUMINISTRO DE LOS PRODUCTOS Y PUESTA A DISPOSICION DE LOS EQUIPOS NECESARIOS PARA REALIZAR PRUEBAS DE ANALISIS CLINICOS CON TIEMPOS DE RESPUESTA URGENTE, PREFERENTE Y NO PREFERENTE EN LAS ORGANIZACIONES SANITARIAS INTEGRADAS DE DONOSTIALDEA, BIDASOA, BAJO DEBA, GOIERRI-ALTO UROLA Y TOLOSALDEA DE LA RED DE DIAGNÓSTICO BIOLÓGICO DE OSAKIDETZA

NÚMERO DE EXPEDIENTE 2025/00956

INDICE

INTRODUCCIÓN 4
1. OBJETO DEL CONTRATO 4
2. ÁMBITO Y ALCANCE DEL CONTRATO 4
2.1. Organizaciones implicadas o lugar de prestación y/o ejecución 4
3. LOTES 5
3.1. Justificación de la no división en lotes 5
3.2. Lotes: Objeto / Descripción / Códigos. 5
4. REQUISITOS NORMATIVOS Y ETIQUETAS O CERTIFICACIONES GENERALES 5
5. REQUISITOS NORMATIVOS Y ETIQUETAS O CERTIFICACIONES POR LOTES 5
5.1. Requisitos normativos por lote 5
6. REQUISITOS TÉCNICOS GENERALES 5
6.1. Requisitos técnicos generales: 5
6.2. Requisitos informáticos 6
6.3. Plan de diseño de instalaciones y equipamiento 6
7. REQUISITOS TÉCNICOS POR LOTES 7
7.1. Requisitos técnicos excluyentes por lote 7
LOTE 1: 7
7.2. Requisitos técnicos no excluyentes por lote 13
No procede. Todos los requisitos técnicos del lote son excluyentes. 13
7.3. Número máximo de lotes a los que licitar 13
7.4. Número máximo de adjudicatarios por lotes 14
8. VARIANTES TÉCNICAS 14
9. MUESTRAS / PRESENTACIÓN DE PRODUCTO / VISITA DE OBRA 14
9.1. Muestras 14
9.2. Presentación de producto: 14
9.3. Visita de obra 14
10. LUGAR Y PLAZOS DE ENTREGA / PLAN DE PUESTA DE MARCHA 14
10.1. Plazo de entrega: 14
10.2. Lugar de entrega 14

11. MODELO DE GESTIÓN 14
11.1. Equipo organizativo 14
11.2. Medios personales adscritos a la ejecución del contrato 14
11.3. Medios materiales adscritos a la ejecución del contrato 15
12. EJECUCIÓN / FACULTAD DE INSPECCIÓN / PLAN DE TRABAJO / PROGRAMA DE TRABAJO 15
12.1. Condiciones de ejecución 15
12.1.1 Indicadores gestión clínica 16
12.1.2 Formación 16
12.1.3 Calidad 16
12.1.4 Protocolos y Procedimientos de actuación 16
12.1.5 Rendimiento de los reactivos 17
12.1.6 Mantenimiento y Servicio técnico 17
12.1.7 Infraestructura auxiliar 17
12.1.8 Soporte a usuarios y mantenimiento de equipos informáticos del Middleware 18
12.2. Modelo de control y seguimiento 18
12.3. Programa de trabajo 18
13.- CONSULTAS AL PLIEGO 19
ANEXO I. ACTIVIDAD PREVISTA 20
ANEXO II. DIRECTRICES Y ESPECIFICACIONES TÉCNICAS INFORMÁTICAS 25

INTRODUCCIÓN

La Unidad de Gestión Clínica de los Laboratorios de Guipúzcoa (UGCLG) es una organización incluida en la Red de Diagnóstico Biológico de OSAKIDETZA (RDBO), que provee de todos los servicios de laboratorio a la Organización Sanitaria Integrada (OSI) Donostialdea, OSI Bidasoa, OSI Bajo Deba, OSI Goierri Alto Urola y OSI Tolosaldea, así como a los servicios socio sanitarios y de Salud Mental incluidos en sus áreas geográficas.

Los elementos organizativos estratégicos en la prestación de servicios de la UGCLG son el Laboratorio del Hospital Universitario Donostia (LHUD) y los Laboratorios de respuesta hospitalaria ubicados en los Hospitales del Bidasoa (LRHHB), de Mendaro (LRHHM) y de Zumárraga (LRHHZ) disponiendo de las especialidades de laboratorio necesarias para cubrir las necesidades de diagnóstico biológico de las OSIs descritas con anterioridad.

El LHUD es el laboratorio de referencia del Área Sanitaria de Gipuzkoa. En él está ubicada el Área organizativa Core desde donde se realiza la gestión extraanalítica y preanalítica de las solicitudes de pruebas procedentes de los diferentes puntos de obtención de muestras de la OSIs mencionadas previamente y desde donde se distribuyen las muestras a todos los laboratorios de la UGCLG. La gestión analítica de las pruebas del Core abarca las pruebas de respuesta rápida y las de alto volumen en un contexto de automatización total.

1. OBJETO DEL CONTRATO

El objeto del presente pliego de prescripciones técnicas consiste en el suministro de los productos y la puesta a disposición de los equipos necesarios para el procesamiento automático de pruebas analíticas con tiempo de respuesta urgente, no preferente y preferente en la UGCLG.

El objeto de la contratación se considera necesario para una prestación adecuada de la asistencia sanitaria en las organizaciones de servicio de Osakidetza.

No disponiendo de medios materiales para abastecerse, se considera idónea la contratación externa.

2. ÁMBITO Y ALCANCE DEL CONTRATO

2.1. Organizaciones implicadas o lugar de prestación y/o ejecución

El Plan Director de los Laboratorios de OSAKIDETZA establece que los laboratorios clínicos de la organización forman parte de la Red de Diagnóstico Biológico, una de cuyas competencias es la gestión de la compra corporativa para todos los laboratorios de la Red. Los laboratorios de la Red de Diagnóstico biológico destinatarios de estas pruebas son los incluidos en la UGCLG: LHUD, LRHHB, LRHHM, y LRHHZ.

3. LOTES

3.1. Justificación de la no división en lotes

Se propone un lote único al tratarse de una solución integral de suministro y cesión de equipamientos para diversos laboratorios con el objetivo de desarrollar una mayor eficiencia y coordinación en la ejecución de las prestaciones, así como el aprovechamiento de las economías de escala.

Esta configuración de no división en lotes permite que la solución planteada sea homogénea y armónica, así mismo, ocasiona que los analizadores, los sistemas de automatización y los sistemas informáticos sean iguales, lo cual facilita ampliamente la gestión y formación de usuarios. La no división en lotes conlleva una interlocución única, un soporte técnico integral y permite que los resultados entre diferentes laboratorios sean homogéneos independientemente del laboratorio donde se haya realizado la prueba.

3.2. Lotes: Objeto / Descripción / Códigos.

Ver Anexo I.

4. REQUISITOS NORMATIVOS Y ETIQUETAS O CERTIFICACIONES GENERALES

Los licitadores acreditarán, mediante la documentación oportuna, que el material ofertado cumple la legislación vigente.

Los reactivos ofertados en el lote a licitar deberán contar con marcado CE de acuerdo con lo establecido en el RD 1662/2000 de 29 de septiembre por el que se regulan los productos sanitarios para diagnóstico “in vitro”. El licitador acreditará el cumplimiento de este requisito.

5. REQUISITOS NORMATIVOS Y ETIQUETAS O CERTIFICACIONES POR LOTES

5.1. Requisitos normativos por lote

Al existir un único lote los requisitos normativos se aplican a dicho lote.

5.1.1. Lote 1: Requisitos normativos y etiquetas

No procede.

6. REQUISITOS TÉCNICOS GENERALES

6.1. Requisitos técnicos generales:

Las características generales de este laboratorio son:

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

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

Contexto clínico y expertización: los sistemas de información y comunicación que den soporte al CORE 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 CORE 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.

6.2. Requisitos informáticos

Los requisitos informáticos y las especificaciones técnicas necesarias pueden consultarse en el documento adicional Directrices y especificaciones técnicas informáticas.

6.3. Plan de diseño de instalaciones y equipamiento

Los licitadores deberán elaborar un plan de diseño de instalaciones y equipamientos de LHUD, LRHHB, LRHHM, y LRHHZ a partir de la información contenida en este Pliego ajustado a los requisitos técnicos exigidos. Se suministrarán planos de ubicación de los diferentes laboratorios.

El plan de diseño de instalaciones y equipamientos contendrá una memoria desarrollada que explique y justifique la solución propuesta, tanto en relación con la estructura como con las instalaciones y su funcionalidad.

Se deberá especificar la huella de todos los equipos analíticos y preanalíticos, así como la servidumbre de uso de los mismos.

Asimismo, aportará:

Planos que expresen las soluciones propuestas, esquemas de principio, diagramas de recorridos y sistemas. Se desarrollarán las diversas instalaciones con la localización de los elementos que lo componen.

Perspectivas foto-realistas del conjunto y cuanta información gráfica quiera añadir el licitador para la mejor comprensión de la propuesta.

El plan incluirá planos de las fases propuestas para la transición de la situación actual a la propuesta del licitador.

El proyecto incluirá los planes de contingencia que contemplen las circunstancias de fallos en los sistemas de alimentación, en los equipos, en los sistemas de automatización o en los sistemas de información para garantizar la continuidad del servicio con el mínimo impacto en el mismo.

Un Plan de apertura que detalle las actuaciones y cronograma para la puesta en funcionamiento del servicio objeto del contrato incluyendo toda la estrategia de transición de los sistemas actuales a los sistemas adjudicados.

Las actuaciones a detallar serán: fases, obras de adecuación, necesidad de espacios temporales, instalación y pruebas de equipos, verificación de métodos y formación del personal. Toda la puesta en marcha ha de hacerse con el mínimo impacto en la actividad asistencial normal.

7. REQUISITOS TÉCNICOS POR LOTES

7.1. Requisitos técnicos excluyentes por lote

LOTE 1:

7.1.1. Lote 1: Requisitos técnicos

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

Los equipos ofertados deberán tener la suficiente flexibilidad para garantizar niveles adecuados de automatización y calidad técnica en los diferentes tipos de Laboratorios: LHUD, LRHHB, LRHHM, y LRHHZ.

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 de todos los laboratorios de la UGCLG.

Se deben ofertar los equipos básicos que los Laboratorios de la UGCLG considere necesarios; 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 laboratorios.

La practicabilidad general de los sistemas y su simplicidad deberían permitir su funcionamiento 24 x7x365 y su manejo por personal a turnos.

La gestión de los residuos estará adecuada a normativa, generando el menor volumen posible, fácil de gestionar.

7.1.2. Requisitos técnicos del Laboratorio CORE del HUD.

El CORE, área organizativa del LHUD, se ubica en las plantas 1 y 2 del Edificio ARANZAZU del Hospital Universitario Donostia y tiene las siguientes funciones:

Gestión de la fase extraanalítica y preanalítica de todas las muestras recibidas de HUD y de todos los Centros de extracción asociados a UGLG:

- Recepción
- Centrifugación
- Clasificación
- Alicuotación y distribución de muestras

- Gestión de archivos de muestras

Gestión de todas las pruebas de tiempo de respuesta urgente (menor a 40min) las 24 x7x365:

- Procesamiento
- Validación
- Archivo de muestras

Gestión de la mayoría de las pruebas hospitalarias con tiempo de respuesta preferentes (menor a 2 horas):

- Procesamiento
- Validación
- Archivo

Gestión de las pruebas de rutina susceptibles de ser automatizadas en gran escala garantizando la calidad y la eficiencia. El 99% de las pruebas que gestione tendrán un tiempo de respuesta inferior a 24 horas:

- Procesamiento
- Validación
- Archivo de muestras

Los equipos serán redundantes para garantizar un servicio ininterrumpido 24x7x365.

Requisitos del Sistema de Automatización Total para el laboratorio CORE del LHUD.

La oferta incluirá sistemas de automatización total para los tubos de suero, orina, suero (serología), plasma citrato y sangre total EDTA, al menos uno para cada uno de los sistemas ofertados.

Los sistemas funcionarían 24x7x365 y gestionarían las muestras urgentes, preferentes y no preferentes. Las entradas de todas las muestras y el puesto de control de los sistemas deberán ser próximas para facilitar la gestión de las muestras y el trabajo del personal.

La oferta incluirá también equipos redundantes de recepción/clasificación /centrifugación y alicuotación con elevada capacidad de procesamiento de muestras. Estos equipos permitirán realizar el registro de presencia de la muestra, su preclasificación, destaponado en su caso, alicuotación y retaponado, así como la detección de errores de etiquetado, registro u otros.

El sistema debe ser capaz de manejar preparar y enrutar todo tipo de tubos y muestras mediante sistemas automatizados a través de su conexión al Sistema Informático del Laboratorio (SIL).

El equipamiento debe estar diseñado de tal manera que se minimice al máximo la manipulación de la muestra y debe incluir dispositivos que garanticen la no contaminación cruzada o ambiental de las mismas.

Los tubos se guardarán tapados en los archivos automatizados.

Requisitos del sistema de automatización total del área de suero y orina para el Laboratorio Core del LHUD

Sistema integrado de alto rendimiento con un mínimo de capacidad para procesar 13.000 determinaciones/hora de bioquímica (método fotométrico), 5400 determinaciones/hora (iones) y

1.500 determinaciones /hora de inmunoquímica con la cartera de servicios mencionada en el Anexo I. El sistema debe disponer de:

- Sistemas de entrada de muestras lo más flexible posible.
- Sistemas de centrifugación.
- Sistemas de verificación de tipo de tubo y calidad de la muestra.
- Sistemas destaponadores.
- Sistemas clasificadores.
- Sistemas alicuotadores.
- Sistemas analíticos.
- Sistemas re taponadores.
- Sistemas archivadores de muestras en línea con capacidad mínima de 27.000 muestras. Los tubos se guardarán tapados.
- Sistemas de deshecho automático de muestras.
- Sistema de respuesta rápida (menos de 40 minutos/muestra), para pruebas de respuesta urgente, con funcionamiento 24x7x365.

El sistema deberá disponer de los elementos necesarios que permitan la priorización de las muestras de forma individual en función del tipo de petición de forma ágil y transparente para el usuario.

La disposición física de los sistemas debe facilitar al máximo la funcionalidad y la comodidad para el personal, de forma que rutina y urgencia estén integradas favoreciendo un entorno ergonómico de trabajo adecuado.

El sistema permitirá en cualquier momento la localización de la muestra en caso de que se necesite.

La gestión de las muestras deberá ser lo más ágil posible, con altas capacidades de entrada y gestión de las muestras y mínima retención de las mismas por parte de los equipos.

El sistema permitirá definir reglas que prioricen la entrada en determinados equipos en función de las pruebas solicitadas.

Requisitos técnicos específicos de los equipos analíticos de bioquímica e inmunoquímica del Laboratorio Core del LHUD

Los equipos analíticos deberán ser de última generación, con posibilidad de realizar configuraciones híbridas y con capacidad de realizar las técnicas mencionadas en el Anexo I.

Los equipos bioquímicos serán capaces de medir índices séricos (ictericia, hemólisis, lipemia).

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

Se debe garantizar la transferibilidad de resultados entre los diferentes equipos y la simplicidad en la gestión de reactivos.

Los sistemas deben ser redundantes de forma que se garantice la prestación del servicio urgente en caso de fallo con mínima complicación. La redundancia debería ser con equipos y sistemas similares que puedan ser utilizados de forma indistinta por el personal.

El número de equipos analíticos necesarios debería ser el mínimo que garantice la redundancia manteniendo la simplicidad y practicabilidad. Los equipos serán en lo posible iguales por línea, al menos en cuanto al manejo y la gestión de reactivos.

La practicabilidad general de los sistemas y su simplicidad deberían permitir su funcionamiento 24x7x365 y su manejo por personal a turnos.

La gestión de las muestras debe garantizar la no contaminación de las mismas. Los módulos de inmunoquímica deben incluir dispositivos que garanticen la no contaminación cruzada o ambiental con antígenos, anticuerpos o ácidos nucleicos en caso de tener que realizar técnicas susceptibles de contaminación.

Los sistemas deberán disponer de sensores de muestra, así como detección de fibrina y coágulos. La gestión de reactivos debe permitir la carga y descarga fácil de los mismos.

Los sistemas de bioquímica deben disponer de canales abiertos que permitan incorporar otras técnicas.

El sistema permitirá la realización de las pruebas mediante el sistema de automatización o directamente en los equipos.

Los sistemas ofertados tendrán la menor huella posible, incluyendo el espacio de servidumbre necesario para trabajar con los equipos.

Para LRHHB, LRHHM, y LRHHZ, se aplicarán los mismos criterios técnicos y de redundancia que para el LHUD explicados anteriormente en este apartado. Los sistemas ofertados dispondrán la misma tecnología con el fin de que los resultados sean intercambiables. El conjunto tendrá una capacidad mínima de 1500 determinaciones/hora (bioquímica más iones) y 240 determinaciones/hora de Inmunoquímica.

Requisitos técnicos del sistema de automatización total del Área de serología para el Laboratorio Core del LHUD

Sistema integrado de alto rendimiento con un mínimo de capacidad para procesar 600 determinaciones/hora con la cartera de servicios mencionada en el Anexo I. El sistema debe disponer de:

- Sistemas de entrada de muestras lo más flexible posible.
- Sistemas de verificación del tipo de tubo y calidad de la muestra.
- Sistemas destaponadores.
- Sistemas clasificadores.
- Sistemas alicuotadores que garanticen la no contaminación cruzada o ambiental de las mismas con antígenos, anticuerpos o ácidos nucleicos en caso de tener que realizar técnicas susceptibles de contaminación de la misma.
- Sistemas analíticos.
- Sistemas retaponadores.

Requisitos técnicos específicos de los equipos analíticos del Área de Serología del Laboratorio Core del LHUD

Los equipos analíticos deberán ser redundantes, de última generación, con capacidad de realizar las técnicas mencionadas en el Anexo I.

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

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

El sistema permitirá la realización de las pruebas mediante el sistema de automatización o directamente en los equipos.

La gestión de las muestras debe garantizar la no contaminación de las mismas y debe incluir dispositivos que garanticen la no contaminación cruzada o ambiental con antígenos, anticuerpos o ácidos nucleicos en caso de tener que realizar técnicas susceptibles de contaminación.

El sistema deberá disponer de canal de respuesta rápida para muestras urgentes de serología infecciosa (ej. donantes biológicos), con tiempos de respuesta rápida (menos de 60 minutos/muestra) y funcionamiento 24x7x365.

Para LRHHB, LRHHM, y LRHHZ, se aplicarán los mismos criterios técnicos y de redundancia que para el LHUD explicados anteriormente en este apartado. Los sistemas ofertados dispondrán la misma tecnología con el fin de que los resultados sean intercambiable.

Requisitos técnicos del sistema de automatización total para el área de sangre total EDTA del Laboratorio Core del LHUD

El sistema será capaz de gestionar 800 muestras/hora, con un número suficiente de equipos que realicen reticulocitos.

Cada sistema de automatización deberá incluir de forma integrada los siguientes componentes:

- Dispositivos de entrada.
- Equipos analizadores de hematimetría.
- Equipos extensores/teñidores.
- Equipos clasificadores.
- Sistema de morfología digital que permita un recuento diferencial leucocitario, morfología eritrocitaria extendida y recuento plaquetar.

El sistema gestionará las determinaciones mencionadas según los criterios de priorización que se establezcan permitiendo su uso para pruebas preferentes, no preferentes o urgentes.

El sistema debe permitir la generación de test reflejos o repeticiones basados en reglas predefinidas en los analizadores y/o en el sistema middleware de gestión.

El sistema deberá permitir el procesamiento de muestras mediante el sistema de automatización total o directamente en los analizadores.

Requisitos técnicos específicos de los equipos analíticos del Área de sangre total EDTA del Laboratorio Core del LHUD

Las características generales de los equipos analíticos serán:

Los equipos analíticos deberán ser de última generación, con capacidad de realizar las técnicas mencionadas y con velocidad igual o superior a las 100 muestras/hora.

Los analizadores ofertados para realizar los hemogramas deberán como mínimo permitir la medida de los siguientes parámetros sanguíneos:

- Serie roja: recuento de eritrocitos, hemoglobina, hematocrito, VCM, HCM y CHCM y ADE.
- Serie blanca: recuento de leucocitos y su diferenciación porcentual y absoluta, en al menos cinco poblaciones (neutrófilos, linfocitos, monocitos, eosinófilos y basófilos).
- Recuento de plaquetas por impedancia y por fluorescencia. VPM.

- Recuento de reticulocitos en porcentaje y número absoluto.

Los sistemas deben ser redundantes incluido el sistema de morfología digital de forma que se garantice la prestación del servicio urgente en caso de fallo y que la parte urgente apoye también la ordinaria. La redundancia debe ser con equipos y sistemas iguales que puedan ser utilizados de forma indistinta por el personal y que garanticen la transferibilidad de los resultados.

El número de equipos analíticos necesarios debe ser el óptimo que garantice la redundancia incluida la cadena de trasporte de los tubos que una los componentes descritos en el apartado anterior, manteniendo la simplicidad y practicabilidad.

La practicabilidad general de los sistemas y su simplicidad debe permitir su funcionamiento 24 x7x365.

La capacidad de trabajar con micro muestras (pediatría). A tal efecto las empresas licitadoras deberán facilitar en su oferta datos acerca de la cantidad mínima de muestra requerida en modo manual.

Esta área debe incluir un software para gestión remota del sistema de morfología digital que permita acceso desde los puestos de validación clínica.

Se incluirán Equipos dedicados para recuento de líquidos biológicos en al menos tres áreas de trabajo dependientes del Core.

Para LRHHB, LRHHM y LRHHZ, se aplicarán los mismos criterios técnicos y de redundancia que para el LHUD explicados anteriormente en este apartado. Los sistemas ofertados dispondrán de la misma tecnología con el fin de que los resultados sean intercambiables. El conjunto tendrá una capacidad mínima de 200 determinaciones/hora con posibilidad de utilizar el modo de trabajo de líquidos biológicos en todos los analizadores ofertados.

Requisitos técnicos del sistema de automatización total del Área de coagulación (tubo de Plasma-citrato) del Laboratorio Core del LHUD

El sistema será capaz de gestionar un mínimo de 800 determinaciones/hora con tubos de plasma-citrato incluyendo rutina y urgencia. Estará compuesto al menos de:

- Sistemas de entrada de muestras lo más flexible posible.
- Sistemas de centrifugación.
- Sistemas de verificación del tipo de tubo, calidad de la muestra y chequeo automático de volumen de llenado en módulos preanalíticos o sistemas analíticos.
- Sistemas clasificadores.
- Sistemas analíticos.
- Sistemas archivadores de muestras en línea con capacidad mínima de 800 muestras tapadas.

Requisitos técnicos específicos de los equipos analíticos del Área de coagulación del Laboratorio Core del LHUD.

Las características generales de los equipos analíticos serán:

Los equipos analíticos deberán ser de última generación y de alta capacidad.

Los equipos serán capaces de medir índices plasmáticos (ictericia, hemólisis, lipemia) y chequeo de obstrucción por presencial de microcoágulos.

Deberán contemplar la posibilidad de realizar otras pruebas de coagulación (el licitador especificará qué otras pruebas de la cartera de servicios es posible realizar).

Los coagulómetros deben ser automáticos, foto-ópticos, selectivos para procesamiento de muestras programadas, y capaces de realizar las técnicas diagnósticas de coagulación y fibrinólisis, utilizando para ello métodos coagulométricos por turbidimetría, cromogénicos por absorbancia e inmunológicos por inmunoturbidimetría.

Los coagulómetros dispondrán de carga continua de reactivos, muestras y consumibles en cualquier momento y sin necesidad de que el analizador interrumpa ninguna de sus actividades.

Los sistemas deben ser redundantes de forma que se garantice la prestación del servicio 24 x7x365. El número de equipos analíticos necesarios debería ser el óptimo que garantice la redundancia manteniendo la simplicidad y practicabilidad.

Para los laboratorios de LRHHB, LRHHM y LRHHZ, se aplicarán los mismos criterios técnicos y de redundancia que para el LHUD explicados anteriormente en este apartado. Los sistemas ofertados dispondrán la misma tecnología con el fin de que los resultados sean intercambiables. El conjunto tendrá una capacidad mínima de 200 determinaciones/hora.

Requisitos técnicos. Middleware.

El sistema deberá disponer de un middleware que permita una gestión integral del laboratorio Core y los laboratorios de respuesta hospitalaria, permitiendo una máxima personalización.

El sistema proporcionará la trazabilidad total de las muestras del sistema. Presentará al menos las siguientes funcionalidades:

- La gestión del control de calidad.
- La incorporación de reglas automáticas en relación a la priorización de muestras o pruebas, test reflejos., gestión de alertas, control de calidad, diluciones, etc.
- La gestión remota del equipo y gestión de resultados y alarmas: revisión y validación técnica y facultativa, permitiendo la realización de acciones directas sobre los analizadores.
- La gestión de las situaciones contingentes (fallo de un equipo, etc.) ofreciendo alternativas sencillas.
- La explotación de la información para la mejora del proceso.

Requisitos técnicos Gestión automatizada de stocks.

El licitador deberá proporcionar un sistema de gestión y almacenamiento automático de reactivos con capacidad de gestionar todos los reactivos del laboratorio CORE a mantener en frio, conectados al sistema de gestión económica de OSAKIDETZA (SAP).

7.2. Requisitos técnicos no excluyentes por lote

No procede. Todos los requisitos técnicos del lote son excluyentes.

7.3. Número máximo de lotes a los que licitar

No procede. Un único lote.

7.4. Número máximo de adjudicatarios por lotes

Un único adjudicatario por lote.

8. VARIANTES TÉCNICAS

No se admiten.

9. MUESTRAS / PRESENTACIÓN DE PRODUCTO / VISITA DE OBRA

9.1. Muestras

No se admiten.

9.2. Presentación de pro

No procede.

9.3. Visita de obra

Con objeto de facilitar la conveniente preparación de las ofertas, se comprende la opción de se pueda concertar cita previa para visitar las instalaciones.

10. LUGAR Y PLAZOS DE ENTREGA / PLAN DE PUESTA DE MARCHA

10.1. Plazo de entrega:

Plazo de entrega del suministro: 4 días hábiles desde la fecha de pedido remitido por el departamento de compras correspondiente.

10.2. Lugar de entrega

El contratista estará obligado a entregar los bienes objeto del suministro en el lugar que se designe por las Organizaciones de Servicio de OSAKIDETZA determinadas en el ámbito y alcance del objeto del contrato.

11. MODELO DE GESTIÓN

11.1. Equipo organizativo

No procede.

11.2. Medios personales adscritos a la ejecución del contrato

No procede.

11.3. Medios materiales adscritos a la ejecución del contrato

La empresa adjudicataria pondrá a disposición del hospital, en condición de cesión temporal, y por un tiempo igual a la duración del presente concurso, el equipamiento necesario para la obtención del resultado final de las unidades analíticas ofertadas, en las condiciones descritas en el punto 12.1.

12. EJECUCIÓN / FACULTAD DE INSPECCIÓN / PLAN DE TRABAJO / PROGRAMA DE TRABAJO

12.1. Condiciones de ejecución

El adjudicatario deberá:

- En el caso de cambio de adjudicatario deberá presentar un plan de trabajo y de contingencia para garantizar la continuidad del funcionamiento a pleno rendimiento de la actividad del laboratorio mientras dura la implantación del nuevo equipamiento, tecnología y sistemas de información que se adjudiquen y deberá indicar y poner los medios necesarios para llevar a cabo la transición.
- Suministrar el equipamiento, la tecnología y los sistemas de información para su gestión, en régimen de cesión, además de los consumibles necesarios para la realización de todas aquellas pruebas analíticas relacionadas en el Anexo I. La actividad de los laboratorios indicada en el Anexo I se facilita a título orientativo, con el fin de que las empresas adjudicatarias 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.
- Instalar y mantener el equipamiento y la tecnología, así como el material necesario, para que la UGCLG realice los procesos preanalíticos; recepcione, prepare, distribuya, procese y conserve las muestras.
- Instalar y mantener el equipamiento, la tecnología y el Middleware necesario para la gestión del proceso analítico, así como dotar del material preciso, para que la UGCLG incorpore al sistema de información del laboratorio los resultados analíticos y la información generada, por vía electrónica de acuerdo a las necesidades de los hospitales incluidos y de OSAKIDETZA, que es el producto Laborabide basado en Gestlab de Clinisys.
- Instalar equipos (redundantes en LHUD) para el tratamiento y acondicionamiento del agua necesaria para el funcionamiento de los laboratorios objeto del contrato, así como el sistema de monitorización remota de la instalación de acuerdo a las especificaciones del servicio de mantenimiento de cada OSI. Los gastos de mantenimiento, recambios y fungibles para los sistemas de tratamiento y acondicionamiento del agua serán a cargo de la empresa adjudicataria.
- Instalar y mantener en caso necesario los sistemas de alimentación ininterrumpida necesarios para garantizar el funcionamiento de las instalaciones de acuerdo a los estándares de equipamiento y monitorización del Servicio de Mantenimiento de cada OSI.
- Ofertar equipos en redundancia para asegurar el servicio ante incidencias en los laboratorios del UGCLG.
- Asegurar la renovación tecnológica durante el periodo de vigencia del presente contrato. El adjudicatario se compromete a actualizar el equipamiento durante la vigencia del concurso, así como a adecuarlo ante nuevas actividades no previstas inicialmente.
- Hacerse cargo de los reactivos y materiales para la puesta a punto de las técnicas y el acondicionamiento de los equipos, anterior a la puesta en producción de los analizadores y resto de

equipos. Asimismo, será a cargo del adjudicatario el consumo de reactivos, controles, calibradores y todos aquellos elementos necesarios para el mantenimiento preventivo y correctivo.

12.1.1 Indicadores gestión clínica

El adjudicatario deberá proveer los sistemas de información que permitan realizar un seguimiento continuado de indicadores, la detección de los fallos y la aplicación de medidas correctoras, así como su evaluación externa por parte de la UGCLG o de personas o entidades en la que deleguen. Los indicadores deberán estar integrados en el sistema de información de Gestión Clínica que la UGCLG utilice.

La adjudicataria deberá poner a disposición de la UGCLG todos los datos relativos a rendimientos para cada una de las técnicas para facilitar el análisis relativo a los mismos.

12.1.2 Formación

La entidad adjudicataria, previa conformidad del laboratorio, determinará el programa formativo a seguir por el personal. La formación relacionada con el funcionamiento de los equipos y técnicas que se considere necesaria será financiada por el adjudicatario.

12.1.3 Calidad

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

Se deberá incluir en la oferta materiales y un programa de control de calidad interno-externo, a elegir entre uno propio y otro de reconocido prestigio por el laboratorio. También se incluirá inscripción y participación en Programas Externos de la calidad gestionados por las Sociedades Científicas Nacionales y/o Internacionales, elegidos por el Laboratorio para todas las metódicas y equipos, que correrán a cargo del adjudicatario hasta un importe máximo de 25.000 euros.

12.1.4 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).
- 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.

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

12.1.5 Rendimiento de los reactivos

A efectos de este pliego se consideran determinaciones analíticas efectivas, las que son informadas, las que son procesadas con materiales de control de calidad y las utilizadas en procesos de calibración recomendados en la ficha técnica.

Se considerarán determinaciones no efectivas, las utilizadas en calibraciones adicionales necesarias, no incluidas en ficha técnica. Asimismo, se considerarán como tal las determinaciones achacables a errores o fallos de los equipos y/o de los reactivos.

El adjudicatario se comprometerá a suministrar información de las determinaciones realizadas desglosadas en pacientes, controles, calibraciones y repeticiones con el fin de evaluar las determinaciones efectivas. Con carácter mínimo semestral se revisarán las determinaciones efectivas y no efectivas. El adjudicatario suministrará sin cargo reactivos por la cantidad de determinaciones no efectivas en el periodo analizado, siempre y cuando la desviación no sea debido al mal uso de los reactivos o del equipamiento por parte de los Laboratorios.

Las empresas licitadoras deberán incluir en sus ofertas su compromiso en este sentido, teniendo en cuenta que las determinaciones objeto de este pliego se realizarán en su mayoría con carácter diario.

12.1.6 Mantenimiento y 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.

En caso de que la reparación del equipo no pueda realizarse en el propio laboratorio o suponga la inutilización del mismo, el adjudicatario estará obligado a sustituirlo, de modo inmediato, mientras dure la reparación.

El adjudicatario se compromete a mantener informada a la Dirección de la UGCLG de las actividades de mantenimiento llevadas a cabo por los medios electrónicos que se acuerden.

El adjudicatario se compromete a mantener personal técnico/aplicativo in situ en el laboratorio del HUD como soporte a las actividades de mantenimiento y configuración de los equipos de la UGCLG, al menos en jornada laborable de 8 a 18 horas, así como un servicio de localización fuera de este horario que garantice la asistencia técnica in situ 24x7x365 en caso de avería con necesidad de intervención urgente.

12.1.7 Infraestructura auxiliar

El adjudicatario deberá de proveer de la siguiente infraestructura auxiliar para dar soporte al sistema: Sistema de gestión de almacenes (frío y temperatura ambiente) para dar soporte a todo el CORE integrado con el sistema de gestión de suministros corporativo (SAP).

Sistema de gestión de los residuos generados cumpliendo la normativa vigente.

Instalación y mantenimiento del sistema de desmineralización redundante de agua para servicio de todo el laboratorio CORE de LHUD, así como en LRHHB, LRHHM, y LRHHZ.

Instalación y mantenimiento de sistemas de presión o vacío que requiera el equipamiento en el caso de que no fueran suficientes los suministros del hospital.

Instalación y mantenimiento de los sistemas de alimentación ininterrumpida necesarios ajustándose a los estándares que defina el departamento de mantenimiento de los centros.

Consultoría para la optimización de los procesos y adecuación de los espacios en el laboratorio CORE de LHUD, así como en LRHHB, LRHHM, y LRHHZ para garantizar la máxima funcionalidad. La adecuación de los espacios correrá a cargo del adjudicatario.

Adecuación de las instalaciones de fontanería y conexiones eléctricas e informáticas necesarias de las instalaciones necesarias para garantizar un entorno de trabajo confortable, minimizando el ruido generado por los instrumentos.

Asimismo, el adjudicatario se comprometerá a diseñar e instalar un sistema de disipación del calor generado por los analizadores.

12.1.8 Soporte a usuarios y mantenimiento de equipos informáticos del Middleware

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.

12.2. Modelo de control y seguimiento

El Comité de laboratorios de la Red de Diagnóstico Biológico, 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 empresa 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.

12.3. Programa de trabajo

No procede.

13.- CONSULTAS AL PLIEGO

Las consultas técnicas o aclaraciones al pliego sobre los aspectos técnicos del Pliego de Bases Técnicas podrán dirigirse a la siguiente dirección:

contrata@osakidetza.eus Tfno. 945006042

Las consultas jurídicas o administrativas podrán dirigirse a la siguiente dirección:

contrata@osakidetza.eus Tfno. 945006042

ANEXO I. ACTIVIDAD PREVISTA

Denominación prueba	Total pruebas 5 años	Total pruebas año
Acetaminofeno	4.500	900
ACTH	10.040	2.008
ADA	8.100	1.620
ALBUMINA	1.094.725	218.945
ALFA 1 ANTITRIPSINA	25.500	5.100
Alfa fetoproteina	43.500	8.700
Amikacina	5.625	1.125
AMILASA	255.000	51.000
Amonio	26.070	5.214
Androstenodiona	13.000	2.600
Anfetaminas	59.000	11.800
Anticuerpos TPO	75.000	15.000
Anticuerpos receptor TSH	21.000	4.200
Anticuerpos tiroglobulina	12.500	2.500
Antígeno carcinoembrionario	137.000	27.400
APOLIPOPROTEINA A1	17.500	3.500
APOLIPOPROTEINA B	15.750	3.150
APTT mezcla	5.500	1.100
ASLO (Antiestreptolisina)	12.000	2.400
Benzodiacepinas	36.000	7.200
Beta 2 microglobulina	59.500	11.900
Beta amiloide 1-42 LCR	6.000	1.200
Beta-Crosslaps	6.500	1.300
Bilirrubina directa	297.500	59.500
Bilirrubina total	1.782.000	356.400
CA 125	43.500	8.700
CA 15.3	63.000	12.600
CA 19.9	61.500	12.300
Calcio	1.986.385	397.277
Cannabis	63.000	12.600
Carbamazepina	9.500	1.900
Ceruloplasmina	18.000	3.600

Denominación prueba	Total pruebas 5 años	Total pruebas año
Chagas	12.000	2.400
Ciclosporina	10.500	2.100
Cistatina C	5.000	1.000
Citomegalovirus IgG	31.280	6.256
Citomegalovirus IgM	27.000	5.400
CK	350.680	70.136
CK MB masa (Método inmunológico)	61.500	12.300
Cloro	3.793.160	758.632
CO2 total bicarbonato	134.520	26.904
Cocaina	52.000	10.400
Colesterol	2.352.500	470.500
Colinesterasa	3.250	650
Complemento C3 C	46.500	9.300
Complemento C4	45.655	9.131
Coriogonadotropina (HCG total)	55.000	11.000
Cortisol ORINA	10.500	2.100
Cortisol SUERO	38.500	7.700
Creatinina	4.970.000	994.000
Creatinina enzimática	150.000	30.000
Cyfra 21,1	9.000	1.800
DHEA S	16.500	3.300
Digoxina	48.000	9.600
Dimero D	155.750	31.150
Enolasa Neuronal Específica	12.000	2.400
Epstein barr EBNA IgG	28.500	5.700
Epstein barr VCA IgG	31.500	6.300
Epstein barr VCA IgM	27.000	5.400
Estradiol 17 beta	58.500	11.700
Etanol	189.000	37.800
Etilglucuronido	25.000	5.000
Factor X activado	6.930	1.386
Factor reumatoide	89.390	17.878
Fenitoina	8.000	1.600
Fenobarbital	8.000	1.600
Ferritina	1.369.565	273.913
Fibrinógeno Von Claus	110.000	22.000

Denominación prueba	Total pruebas 5 años	Total pruebas año
Fólico	615.065	123.013
Folitropina (FSH)	61.500	12.300
Fosfatasa alcalina	1.684.625	336.925
Fósforo	550.000	110.000
Frotis digitalizados	281.500	56.300
Gamma GT	2.607.865	521.573
Gentamicina	4.000	800
Glucosa	4.022.470	804.494
GOT AST	1.951.905	390.381
GPT ALT	3.137.100	627.420
Haptoglobina	36.760	7.352
HDL colesterol	1.862.400	372.480
HE4	27.500	5.500
Hemoglobina glicosilada	1.075.000	215.000
Hemograma	4.280.000	856.000
Hepatitis A virus IgG ó Ac.totales	76.640	15.328
Hepatitis A virus IgM	27.000	5.400
Hepatitis B virus anti-Hbe	12.000	2.400
Hepatitis B virus anti-HBs cuantificado	190.500	38.100
Hepatitis B virus core IgG ó Ac.totales	184.000	36.800
Hepatitis B virus core IgM	15.000	3.000
Hepatitis B virus HBe Ag	7.500	1.500
Hepatitis B virus HBs Ag (Ag Australia)	216.500	43.300
Hepatitis C virus IgG	172.500	34.500
Herpes simple 1 IgG	63.000	12.600
Herpes simple 2 IgG	63.500	12.700
Hierro	1.260.180	252.036
Homocisteina	15.000	3.000
Hormona antimulleriana	5.500	1.100
Hormona de crecimiento (HGH)	19.500	3.900
HTLV I/II	19.500	3.900
IGF I	18.000	3.600
IGFBP3	7.500	1.500
Inmunoglobulina IgA	197.500	39.500
Inmunoglobulina IgG	137.500	27.500
Inmunoglobulina IgM	142.500	28.500

Denominación prueba	Total pruebas 5 años	Total pruebas año
Insulina	10.000	2.000
Interleukina 6	4.000	800
LDH	648.665	129.733
Lipasa	261.400	52.280
Lipoproteina A	16.000	3.200
Litio	47.000	9.400
Lutropina (LH)	61.500	12.300
Magnesio	345.000	69.000
Metadona	25.000	5.000
metotrexato	8.400	1.680
Micofenolato	2.000	400
Microalbúmina	795.000	159.000
Opiaceos	45.000	9.000
Paratirina intacta (PTH i)	163.500	32.700
Péptido C	9.500	1.900
Péptido natriurético (BNP o Pro BNP)	482.500	96.500
Plaquetas (Fluorescencia)	100.000	20.000
PLGF	3.500	700
Potasio	3.845.545	769.109
Prealbúmina	115.500	23.100
Procalcitonina	535.000	107.000
Procolageno I propeptido aminoterminal	7.500	1.500
Progesterona	13.500	2.700
ProGRP	5.500	1.100
Prolactina	60.000	12.000
Proteina C reactiva	1.742.500	348.500
Proteinas totales	1.951.250	390.250
Proteinas totales en LCR	32.715	6.543
Proteinas totales en orina	283.750	56.750
PSA libre	88.500	17.700
PSA total	361.000	72.200
Recuento celular líquidos biológicos	59.775	11.955
Reticulocitos	130.000	26.000
Rubeola virus IgG cuantitativa	52.500	10.500
Salicilato	2.250	450
SCC	5.500	1.100

Denominación prueba	Total pruebas 5 años	Total pruebas año
SFLT1	3.500	700
SHBG	27.000	5.400
Sodio	3.863.995	772.799
Tacrolimus	39.000	7.800
Tau fosforilada LCR	6.500	1.300
Tau Total LCR	6.500	1.300
Teofilina	2.000	400
Testosterona total	61.500	12.300
Tiempo protrombina TP	1.334.500	266.900
Tiempo trombina	9.000	1.800
Tiempo tromboplastina parcial activ APTT	1.230.000	246.000
Tiroglobulina	12.000	2.400
Tirotropina (TSH)	1.640.000	328.000
Tiroxina libre (fT4)	470.000	94.000
Tobramicina	3.000	600
Toxoplasma IgG cuantitativa	39.000	7.800
Toxoplasma IgM	22.500	4.500
Transferrina	1.177.500	235.500
Treponema Pallidum IgG + IgM	141.000	28.200
Triglicéridos	1.965.000	393.000
Triyodotironina libre (fT3)	43.500	8.700
Troponina ultrasensible	370.000	74.000
Urato	1.237.500	247.500
Urea	2.547.500	509.500
Valproato	19.000	3.800
Vancomicina	27.000	5.400
VIH 1-VIH 2 Anticuerpos + Ag VIH	225.000	45.000
Vitamina B12	601.500	120.300
Vitamina D 25(OH) total	472.500	94.500
TOTAL	**75.581.630**	**15.116.326**

ANEXO II. DIRECTRICES Y ESPECIFICACIONES TÉCNICAS INFORMÁTICAS

En las siguientes páginas se presenta el documento que contiene las especificaciones técnicas que deben cumplir los dispositivos y tecnologías que se ponen a disposición de Osakidetza Servicio Vasco de Salud.

Vitoria-Gasteiz, 2025eko ekainaren 16a Vitoria-Gasteiz, a 16 de junio de 2025

(*)IZ./FDO.: **Dra. Mercedes Sota Busselo**

Red Diagnóstico Biológico Osakidetza
Osakidetzako Diagnostiko Biologikoko Sarea

(*) La firma electrónica se encuentra al final de este documento



Osakidetza

DET - Directrices y Especificaciones Técnicas

HOJA DE CONTROL

Título	DIRECTRICES Y ESPECIFICACIONES TÉCNICAS		
Entregable			
Nombre del Fichero	DET DyM_IOC v06.1.docx		
Autor	Osakidetza		
Versión/Edición	V6.1	**Fecha Versión**	15/07/2022
Aprobado por		**Fecha Aprobación**	
		Nº Total Páginas	

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
v01	Primera Versión	Osakidetza		07/03/2016
V02	Soluciones Móviles	Osakidetza		22/08/2016
V03	Revisión Evolución tecnologías IOC	Osakidetza		22/02/2017
V04	Requisitos Dispositivos Inalámbricos	Osakidetza		10/11/2017
V05.1	Adaptación a estándares Batera (en proceso)	Osakidetza		21/07/2021
V06.0	Nuevo modelo de aplicaciones	EJIE		20/06/2022
V06.1	Actualizaciones API REST y tecnologías de desarrollo de apps móviles.	Osakidetza		15/07/2022

ÍNDICE

1 Objeto

2 Especificaciones para Desarrollo

2.1 Arquitectura de Referencia

2.1.1 Vista lógica

2.2 Directrices de Desarrollo

2.2.1 Construcción de Aplicaciones por Capas

2.2.2 Capa de Presentación

2.2.3 Capa de Negocio

2.2.4 Capa de Persistencia

3 Modelo de aplicaciones modernas

3.1 Especificaciones de desarrollo

3.2 Entorno tecnológico

3.2.1 Contenedores

3.2.2 Orquestación de contenedores

3.2.3 Plataforma operativa y seguridad

3.2.4 Plataformas horizontales

4 Directrices tecnológicas de IOC

4.1 Entorno tecnológico

4.2 ESPECIFICACIONES DEL CLIENTE (MAQUETA)

4.3 Dispositivos de entrada/salida

4.4 Seguridad, acceso, autenticación y autorización

4.5 Monitorización

4.6 Backup/Restore

5 Interoperabilidad

5.1 Servicios Web

5.2 Gestor de Eventos

5.2.1 Estándares de comunicación

5.2.2 Mensajería. Definición de Evento

5.3 Arquitectura API REST

6 Explotación Información- Business Intelligence

7 Soluciones Móviles

7.1 Tecnologías Cliente

7.1.1 Angular

7.1.2 Ionic Framework 5 o superior

7.2 Tecnologías Servidor

7.2.1 Nginx

7.2.2 Node.js

7.2.3 MongoDB

8 Calidad de uso

1 OBJETO

Este documento, DET (**Directrices y Especificaciones Técnicas),** contiene las Directrices y Especificaciones Técnicas de los Sistemas de Información de Osakidetza en el ámbito TIC.

El objeto es incluirlo en los Pliegos de Bases Técnicas (PBTs) de los expedientes de contratación para la adquisición, mejora, evolución o adaptación de las soluciones (producto/aplicación/desarrollo) que conforman los Sistemas de Información de Osakidetza y/o cualquier otra contratación que requiera recursos TIC que sean competencide Informática de la Dirección General de Osakidetza.

2 ESPECIFICACIONES PARA DESARROLLO

Este apartado refleja los principales aspectos del diseño técnico de la arquitectura de referencia para aplicaciones web, definida por Osakidetza.

Una arquitectura de referencia es un conjunto de patrones diseñados y probados para ser usados en un contexto específico, en nuestro caso, en los sistemas de misión crítica de Osakidetza. Es una guía de ayuda para ser usada por los arquitectos y desarrolladores, que permite conceptualizar nuevas aplicaciones rápidamente reutilizando un diseño suficientemente probado.

La arquitectura de referencia refleja las decisiones y aspectos técnicos de diseños basados en la experiencia de Osakidetza en el desarrollo, mantenimiento y evolución de aplicaciones web. El principal propósito de la arquitectura de referencia para aplicaciones web es, por lo tanto, homogeneizar el desarrollo, despliegue y explotación en producción de las aplicaciones.

En este sentido, la implementación de la arquitectura de referencia aportará los siguientes beneficios perseguidos por Osakidetza:

- Mejorar el rendimiento de las aplicaciones.
- Garantizar la escalabilidad y la tolerancia a fallos.
- Facilitar las integraciones entre sistemas.
- Aprovechar las tecnologías estándares y capacidades proporcionadas por los recursos hardware y software existentes en la organización.
- Reducir el coste del mantenimiento (evolutivo y correctivo) mediante la simplificación del diseño de la solución y la implementación del mismo.

2.1 Arquitectura de Referencia

Una de las características generales de los proyectos con éxito es que existe un diseño previo bien fundamentado que define la arquitectura general del sistema, las soluciones de infraestructura y plataforma (por ejemplo, alta disponibilidad, recuperación frente a desastres, copia de seguridad y restauración, monitorización), y realiza un mapeo de requerimientos a elementos de la arquitectura.

Desde el punto de vista de sistemas de información, este requerimiento estratégico debe tener una base de arquitectura y diseño previo que permita cumplirlo durante la evolución del ciclo de vida.

Los **principios de la arquitectura de referencia**, describen los principios fundamentales que se han considerado para el diseño de dicha arquitectura. Los principios representan los preceptos o reglas básicas que guían el proceso de diseño.

La arquitectura de referencia se describe usando tres vistas diferentes:

- **Vista lógica** o conceptual, en la que se presenta la arquitectura mediante una visión de alto nivel que permite entender los diferentes componentes que intervienen y las interacciones existentes entre ellos.
- **Vista de implementación**, en la que se proporcionan detalles adicionales sobre la tecnología y productos para la construcción de los diferentes componentes.
- **Vista de despliegue**, en la que se describe de forma pormenorizada la información del sistema relativa a la instalación y explotación que se realiza por entornos.

2.1.1 Vista lógica

El propósito de la vista lógica es permitir un entendimiento de alto nivel de la arquitectura de referencia y de las diferentes capas y componentes en las que está estructurada. También se define la integración con otros sistemas.

Sobre esta vista lógica se deberían plasmar todos los elementos que deben ser considerados cuando se diseña una nueva aplicación.

Las aplicaciones deben de tomar este diseño como referencia e indicar:

Las capas de la arquitectura de referencia que se implementarán

Servicios externos con los que interactúa la aplicación

Clientes que usarán la aplicación

Servicios de persistencia de datos

En la siguiente figura se muestra la vista lógica de la arquitectura de referencia para aplicaciones web.

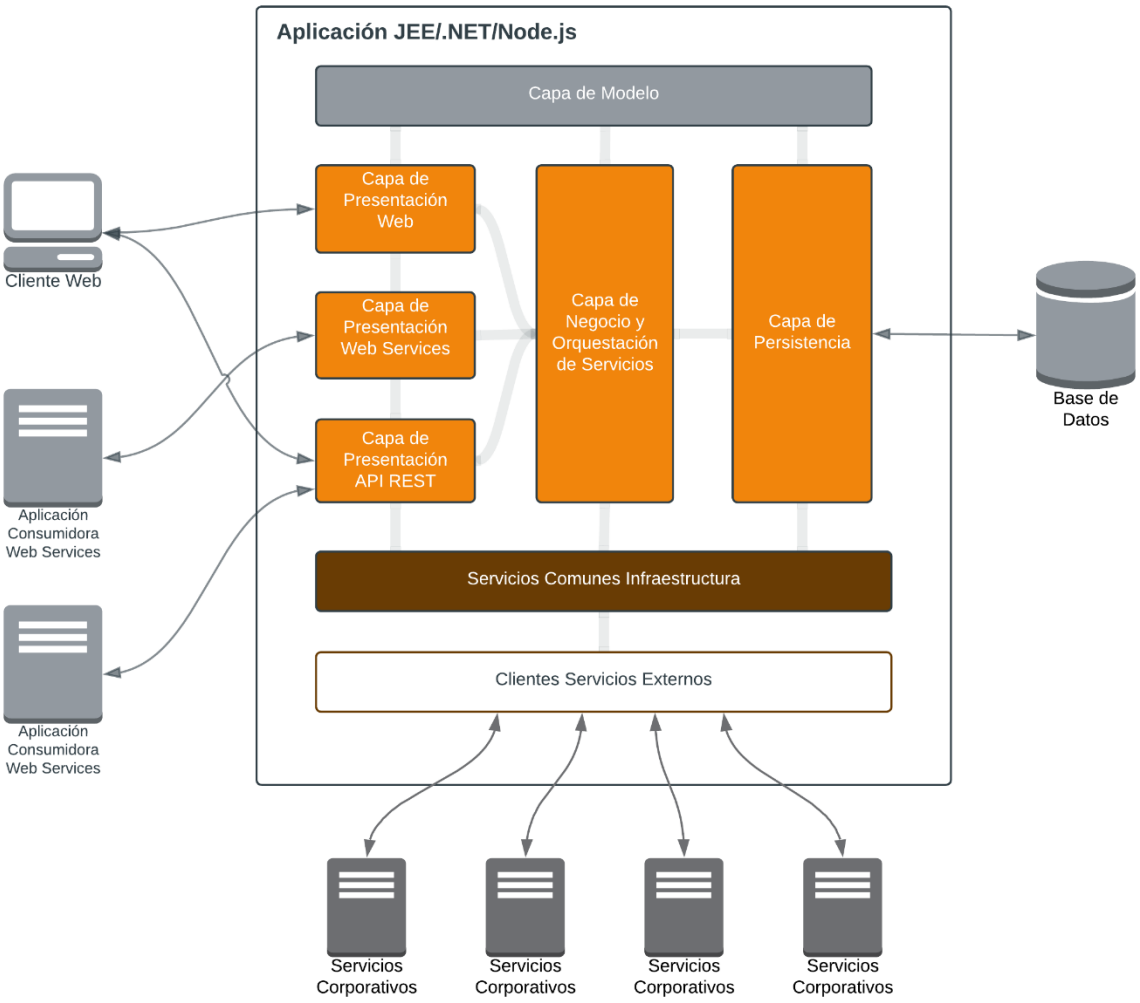


Figura 1. Vista lógica de la arquitectura de referencia

2.2 Directrices de Desarrollo

Se contemplan como directrices de desarrollo, las **normativas**, **estándares** y **recomendaciones** para la elaboración de un **código fuente homogéneo**, **estandarizado** y de **calidad**, con el objeto de **minimizar las tareas de mantenimiento** y la **deuda tecnológica**.

También se incorporan las especificaciones para la obtención de **sistemas de información seguros**, con un **rendimiento óptimo** y adaptado a las necesidades de las tecnologías definidas por las Arquitecturas de Software que se tomarán como referencia en los desarrollos.

A continuación, se enumeran algunas de las **directrices de desarrollo** que deberán cumplir las soluciones desarrolladas para Osakidetza:

2.2.1 Construcción de Aplicaciones por Capas

El principal objetivo de la construcción de aplicaciones por capas, es la **separación de la lógica de negocio, de la lógica de diseño**. Su principal ventaja, es que el desarrollo se puede llevar a cabo en varios niveles y, en caso de que sea necesario llevar a cabo algún cambio, sólo se necesita intervenir al nivel requerido.

El ejemplo clásico de este tipo de práctica y el que se contempla a nivel de directriz, es el consistente en separar las aplicaciones en tres capas: **Presentación**, **Negocio** y **Persistencia**.

Por lo tanto**, las aplicaciones serán desarrolladas en capas**; es decir, se diseñará las aplicaciones **separando entre los modelos de datos, la lógica de aplicación, y la interfaz de usuario**. Si optamos por esta separación de responsabilidades, podremos compartir totalmente el modelo de datos y sólo tendremos que adaptar la interfaz de usuario.

Por cada capa se consideran una serie de **directrices de desarrollo basadas en el modelo de tres capas propuesto por la Arquitectura de Referencia** de Osakidetza.

2.2.2 Capa de Presentación

Mediante la capa de presentación se separa la interacción del usuario respecto a la lógica de negocio.

El uso de la arquitectura en tres capas en el desarrollo de aplicaciones, ha favorecido la aparición de tecnologías que facilitan la implantación de esta capa, además de un conjunto de buenas prácticas que mejoran el proceso de su implementación.

Directrices de Desarrollo para la Capa de Presentación:

Finalidad: *Presentar la información al usuario*.

La capa de presentación, también llamada "capa de usuario", deberá presentar el sistema al usuario, comunicar la información necesaria y capturar la misma en un proceso que realiza un filtrado para validar los datos respecto al formato. **No deberá procesar datos ni tomar decisiones**.

Esta capa se comunica únicamente con la capa de negocio. También es conocida como interfaz gráfica y debe tener la característica de ser "amigable" (comprensible y fácil de usar) para el usuario.

Modularidad: *Controlar la relación entre las vistas.*

En una vista sólo debe hacerse referencia a otras vistas relacionadas con su funcionalidad. En ejecución, se recomienda integrar la vista con un **sistema de plantillas**, para poder aumentar de esta manera la **reusabilidad** y el **encapsulamiento de funcionalidades**.

Internacionalización y localización: *Preparar las aplicaciones para diferentes idiomas y convenciones.*

Las aplicaciones estarán preparadas para que puedan adaptarse a diferentes idiomas y convenciones (formatos de fecha, moneda, etc.), sin necesidad de realizar cambios de relevancia en el código.

Validaciones: *Realizar validaciones sobre los datos introducidos por los usuarios*.

La vista será la responsable de la validación inicial de los datos introducidos por el usuario. La validación debe ser obligatoria sólo para el caso de campos y formato. **Nunca deberá realizarse una validación de negocio desde esta capa**.

Catálogo de controles: *Elaborar un catálogo con la lista de controles.*

Se especificará, si es posible, la función del control, los posibles validadores/conversores que se le puedan asociar, los eventos que pueda lanzar y los atributos que puedan cambiarse para manipular su aspecto externo.

Los controles deberían permitir el tratamiento de componentes y eventos que posibiliten extraer de la vista toda la lógica de interfaz. La consecuencia principal de este enfoque, es que **desde la vista nunca se manipularán los controles**. El objetivo es que **la construcción de la vista sea una tarea totalmente autónoma del resto de componentes de la función de negocio**.

Uso de plantillas: *Facilitar el mantenimiento haciendo uso de plantillas.*

Se debe utilizar un **framework de plantillas (templates) en la capa de presentación**, ya que de esta manera se facilita el mantenimiento del diseño de los sistemas de información. Existen frameworks que posibilitan aislar el diseño de la aplicación en un único fichero de plantilla (o más, si se necesitan). **Esto facilita la tarea de hacer modificaciones en el diseño**.

Controles de interfaz: *Utilizar un identificador único para los controles de interfaz.*

Todos los controles de interfaz, deben mantener **un identificador único** para facilitar su **compresión**, **reutilización** y **batería de pruebas** del mismo.

Independencia entre capas: *Evitar el acoplamiento entre distintas capas.*

Cada capa debe tomar la responsabilidad que le corresponde. En este caso, debe evitarse que la capa de presentación realice atribuciones que le correspondan a otras capas.

2.2.3 Capa de Negocio

La capa de negocio expone la lógica necesaria a la capa de presentación para que el usuario, a través de la interfaz, interactúe con las funcionalidades de la aplicación.

Se utilizarán **componentes de negocio** para abstraer la lógica de negocio de otros problemas generales de las aplicaciones, como la concurrencia, transacciones, persistencia, seguridad, etc…

Directrices de Desarrollo para la Capa de Negocio:

Reglas de negocio: *Implementar las reglas de negocio en esta capa.*

Los módulos que requieran una funcionalidad deberán encontrarla en un solo lugar y única versión. No debe haber réplica de funcionalidades en ninguna de las otras capas (Persistencia y/o Presentación)

Validaciones de datos: Garantizar el valor correcto de los datos.

Esta capa debe garantizar que los datos requeridos para procesarla hayan sido debidamente validados, y sólo se puede iniciar el flujo del proceso de negocio si la validación resultó correcta.

Comunicación entre capas: Definir la estrategia de comunicación entre capas.

La comunicación entre capas se debe establecer mediante objetos del modelo. Se crearán entidades sin métodos, sólo tendrán propiedades, campos y atributos, que nos servirán para almacenar información, como puede ser la asociación de las propiedades a las columnas de la base de datos.

Transacciones: Tratar convenientemente las transacciones de los datos.

La capa de modelo de datos proporciona los datos al sistema, pero **las transacciones** que involucren a dichos datos, **se deben manejar desde la capa de negocio.**

Excepciones: Encapsular en la capa de negocio las excepciones y trasladarlas de forma correcta a la capa de presentación.

El objetivo es **simplificar el manejo de excepciones** de la aplicación. Se recomienda tener bien definida una **política para el tratamiento de excepciones y disponer de una jerarquía propia de excepciones**. Como norma general, **las aplicaciones no deberán nunca extender las excepciones del sistema**, sino las de su propia jerarquía de clases.

Servicios encapsulados: Encapsular la capa de negocio en servicios.

Se debe encapsular la capa de negocio en servicios, para de esta forma **aislar la base de datos respecto de una interacción directa con el usuario**. Estos servicios de negocio conforman un "puente" entre el usuario y los datos. Responden a peticiones de usuarios u otros servicios de negocio aplicando procedimientos formales y reglas de negocio a datos relevantes.

Acceso a servicios: *Controlar el acceso a los servicios en la capa de negocio.*

El control de acceso al servicio de negocio debe hacerse en la capa de negocio, puesto que podemos tener distintas capas de presentación, como, por ejemplo, una capa de presentación web y una capa de presentación Web Services.

El control de acceso puede realizarse tanto a nivel de método, dentro de cada servicio, como a nivel de servicio vertical.

Inyección de Dependencias: Uso del patrón de diseño 'Inyección de Dependencias' (DI), como forma de 'Inversión de control' (IoC)

La **Inversión de Control (Inversion of Control en inglés, IoC)** es un **método de programación** en el que el flujo de ejecución de un programa se invierte respecto a los métodos de programación tradicionales. En la Inversión de Control se especifican respuestas deseadas a sucesos o solicitudes de datos concretas, dejando que algún tipo de entidad o arquitectura externa lleve a cabo las acciones de control que se requieran en el orden necesario y para el conjunto de sucesos que tengan que ocurrir. Es el principio subyacente a la técnica de Inyección de Dependencias, siendo términos frecuentemente confundidos.

La **Inyección de Dependencias (Dependency Injection en inglés, DI)** es **un patrón de diseño orientado a objetos**, en el que se suministran objetos a una clase en lugar de ser la propia clase quien cree el objeto. La forma habitual de implementar este patrón es mediante un "Contenedor DI" y objetos planos o simples, por ejemplo, los llamados POJO. El contenedor inyecta a cada objeto, los objetos necesarios según las relaciones plasmadas en un fichero de configuración. Típicamente este contenedor es implementado por un framework externo a la aplicación.

La implementación de un patrón de diseño como la 'Inyección de Dependencias' permite gestionar de una manera eficiente las dependencias entre los diferentes componentes de una aplicación, sin tener que recurrir a un acoplamiento no deseable entre estos.

2.2.4 Capa de Persistencia

La necesidad de vincular los datos guardados en una base de datos relacional, con los objetos de una aplicación orientada a objetos, determina la aparición del concepto de **persistencia de objetos**. Siguiendo el paradigma de desarrollo en tres capas, **la persistencia queda recogida en su propia capa, separada de la lógica de negocio y de la interfaz de usuario**.

La persistencia de la información es probablemente la parte más crítica en una aplicación de software y permite ejecutar operaciones en el almacenamiento persistente (base de datos). El modelo de objetos de un sistema, difiere en muchos aspectos del modelo relacional. La interfaz que une esos dos modelos se llama asociación objeto-relacional (ORM en inglés). La capa de persistencia encapsula el comportamiento necesario para mantener los objetos.

Directrices de Desarrollo para la Capa de Persistencia:

Asociación Objeto-Relacional: Usar un mapeador Objeto Relacional para implementar la capa de persistencia.

Se debe utilizar un mapeador Objeto-Relacional para implementar la capa de persistencia, ya que es una técnica que permite convertir los tipos de datos utilizados en un lenguaje de programación orientado a objetos y los utilizados en una base de datos relacional, lo que posibilita el uso de las características propias de la orientación a objetos.

Uso del patrón DAO: Crear una clase DAO por cada objeto de negocio del sistema

El **patrón CRUD**, reconocido como el patrón más importante del acceso a datos, indica que **cada objeto debe ser creado en base de datos para que sea persistente**. Para esto es necesario asegurar que existen operaciones que permiten a la capa inferior (de acceso a datos) leerlo, actualizarlo o borrarlo.

Mediante la implementación de DAO's pueden proporcionarse las operaciones CRUD necesarias para cada aplicación. No es obligatorio que cada DAO implemente todas las operaciones CRUD (puede no ser necesario en la lógica funcional del sistema). Por lo tanto, **se recomienda crear un DAO distinto por cada objeto de negocio en el sistema**.

Manejo de la caché: Usar la caché en las aplicaciones para reducir tiempos de lectura.

Se recomienda **utilizar un sistema de caché** en las aplicaciones, para reducir tiempos de lectura, ya que la mayoría de accesos de lectura acceden a una pequeña parte de los datos de la aplicación. Normalmente, hay un conjunto de datos que son relevantes a todos los usuarios y que, por lo tanto, son accedidos con más frecuencia.

Concurrencia de usuarios: Permitir la concurrencia de usuarios.

Se debe permitir que varios usuarios trabajen en la misma base de datos, **protegiendo los datos de ser escritos erróneamente**. En la mayoría de los casos, se utilizará el bloqueo optimista, soportado por la mayoría de los motores de persistencia como la opción por defecto.

Referencias circulares entre objetos: Evitar las referencias circulares entre objetos de la capa de persistencia.

Se deben evitar las referencias circulares, facilitando la localización de los objetos. De esta manera, se devuelve el objeto solicitado sin necesidad de realizar un recorrido para localizarlo, lo que supone un acceso más efectivo.

Actualización en cascada: Utilizar la actualización en cascada siempre que sea posible.

Utilizar la posibilidad que ofrecen algunos frameworks para la actualización en cascada de objetos. Una actualización en cascada **permite que las modificaciones hechas a un objeto se repliquen en los objetos relacionados**. De esta manera se mejora el mantenimiento de los objetos, se asegura que los cambios introducidos se replican de manera eficiente y se mantiene la **integridad de los datos**.

3 MODELO DE APLICACIONES MODERNAS

Osakidetza se encuentra en un proceso de renovación de la arquitectura tecnológica, con el objeto de adaptarla a las prácticas más actualizadas.

La arquitectura de aplicación tradicional de tres niveles (que comprende un navegador, una aplicación monolítica implementada en un servidor de aplicaciones y una base de datos) es inadecuada para respaldar nuevas demandas comerciales digitales. Las aplicaciones monolíticas inflexibles, la complejidad arquitectónica y la deuda técnica sobrecargan a los equipos de desarrollo e impiden la agilidad llegando a frustrar a los usuarios. La modernización de la cartera de aplicaciones facilitará la transformación del negocio digital, este esfuerzo de modernización comienza con una arquitectura de aplicación moderna.

Las demandas de “negocios digitales” conducen hacia una rápida transformación de aplicaciones, sistemas y procesos, así como la necesidad de aplicaciones innovadoras de múltiples experiencias y obligan a brindar soluciones flexibles que puedan adaptarse rápidamente a los cambios en los requisitos y los avances tecnológicos.

Una arquitectura ágil basada en tecnologías modernas de interfaz de usuario (UI), API y servicios poco acoplados brindan la agilidad y flexibilidad para satisfacer estos requisitos. Este enfoque de arquitectura es lo que el mercado llama MASA (Mesh App and Service Arquitecture), arquitectura de aplicaciones y servicios en malla.

MASA (Mesh App and Service Arquitecture) proporciona tres capacidades arquitectónicas para potenciar el negocio digital:

- multiexperiencia (múltiples experiencias de usuario), este enfoque brinda la oportunidad de crear aplicaciones específicas más pequeñas que son más fáciles de diseñar, desarrollar e implementar. También permite que la aplicación se concentre en cualquier canal que prefiera el usuario al realizar tareas, ya sea una aplicación basada en la web que se ejecuta en una computadora portátil, una aplicación móvil en un teléfono o una interfaz conversacional.
- mediación de API (manejo de las API programáticas), un principio crítico en MASA es garantizar que las partes individuales de la aplicación puedan cambiar según sea necesario sin afectar otras partes de la aplicación. Debido a que las API pueden causar dependencias estrechas entre los componentes de la aplicación, todas las interacciones de la API deben abstraerse para garantizar un acoplamiento flexible.

    Monitorización de interacciones: la mediación de API puede monitorear interacciones desde perspectivas técnicas y comerciales.

    Protección de las interacciones: la mediación de la API puede hacer cumplir las políticas de autenticación y autorización y evitar las intrusiones de malware.

    Gestión del flujo de tráfico: la mediación de API puede admitir el enrutamiento de solicitudes, el equilibrio de carga, la limitación, la redirección y la recuperación automática de interacciones fallidas.

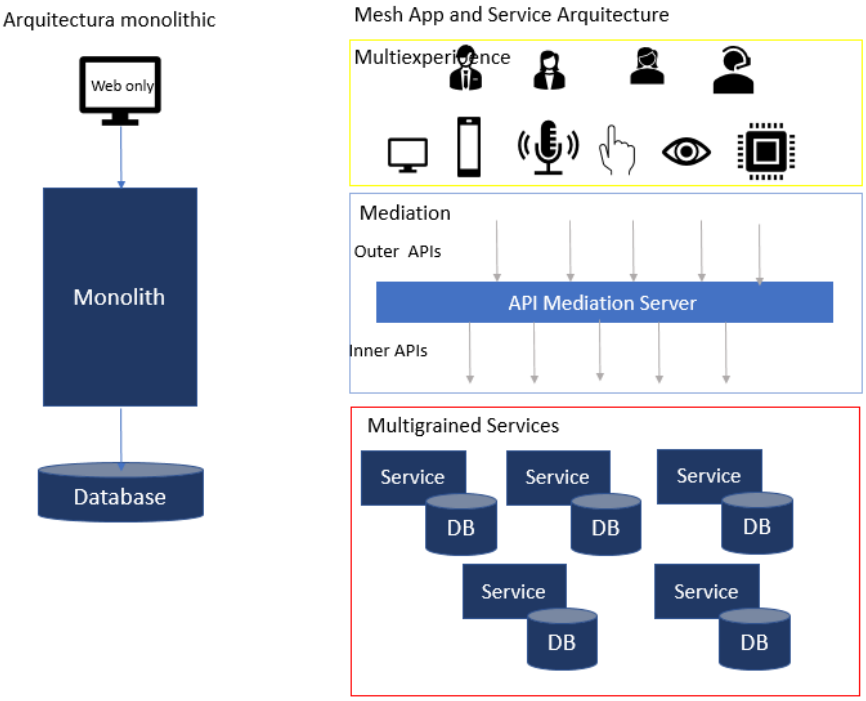
    Gestión de transformaciones: la mediación de API puede traducir entre diferentes protocolos: Puede transformar mensajes, por lo que admite formatos personalizados para diferentes consumidores y asignaciones entre diferentes versiones de API.

- Servicios multigrano (microservicios, mini servicios o web services), cada servicio encapsula una capacidad comercial y expone esa capacidad a los consumidores a través de una API. El tipo de API más común utilizado en MASA es una API REST, pero MASA también admite otros tipos de API de solicitud/respuesta (como SOAP y gRPC), así como API basadas en mensajes y eventos.

  Macroservicios granulares que encapsulan y exponen algunas o todas las capacidades de una aplicación monolítica sin refactorización.

  Miniservicios de implementación independiente y granulares que implementan la funcionalidad a nivel de dominio.

  Microservicios detallados y de implementación independiente que implementan características individuales.



Aplicaciones multiexperiencia

La estrategia de aplicaciones front-end en MASA aplica un enfoque modular y granular para crear aplicaciones de clientes especializadas. Este es un cambio que se aleja del enfoque tradicional donde la intención es poner tanta funcionalidad como sea posible en las aplicaciones de clientes individuales. En lugar de una sola aplicación de cliente compleja, la experiencia del usuario de una aplicación de malla se compone de aplicaciones enfocadas estrechamente alineadas con flujos de trabajo específicos requeridos por diferentes personas que trabajan a través de varias interfaces.

Esto brinda la oportunidad de crear aplicaciones más pequeñas y con un enfoque limitado que pueden usar múltiples servicios desde el back-end. Esto también le permite enfocar las aplicaciones en los canales preferidos del usuario para realizar sus tareas, ya sea una aplicación web en una computadora portátil, una aplicación móvil en un teléfono o una aplicación en una interfaz conversacional.

En una aplicación grande y monolítica, los usuarios deben navegar para encontrar la parte de la funcionalidad que necesitan para realizar las tareas específicas para las que están usando la aplicación. Sin embargo, en una aplicación multiexperiencia adecuada, la aplicación debe ser intuitiva, hacer que las tareas del usuario sean lo más eficientes posible y admitir el canal en el que el usuario desea utilizar la aplicación.

El diseño de la aplicación utilizando personas y escenarios implica un proceso de cuatro pasos:

1. Crear personajes de usuario para establecer una comprensión precisa de sus usuarios. Use las personas para identificar cosas como preferencias de dispositivos, nivel de experiencia, comportamientos y limitaciones de tiempo.
2. Identifique escenarios para comprender mejor las tareas que requieren los usuarios. Los escenarios deben revelar el orden de las tareas requeridas, los pasos para realizar las tareas y las expectativas específicas que los usuarios pueden tener al realizar las tareas en una aplicación.
3. Diseñe flujos de trabajo basados en las personas y los escenarios. Estos flujos de trabajo deben identificar el flujo natural de trabajo, así como las posibles desviaciones que pueden experimentar los usuarios. Tenga en cuenta que la aplicación puede admitir varias personas y flujos de trabajo.
4. Utilice los flujos de trabajo para impulsar el diseño de la aplicación. Implementación de diseño de páginas web/móviles u otras interfaces, así como la navegación entre ellas, para soportar de manera óptima los flujos de trabajo definidos.

Además de diseñar las aplicaciones para que proporcionen una apariencia coherente en varias aplicaciones, la apariencia debe ser coherente en varios canales. Se utilizarán marcos, plataformas y herramientas comunes que garanticen la coherencia entre las aplicaciones y simplificar su implementación:

Frameworks de JavaScript como Angular, React, Vue.js y Polymer para aplicaciones web personalizadas.

Frameworks móviles como Xamarin, React Native e Ionic para aplicaciones móviles personalizadas.

Plataformas de experiencia digital (DXP).

Plataformas de aplicaciones de código bajo (LCAP) y plataformas de desarrollo multiexperiencia (MXDP).

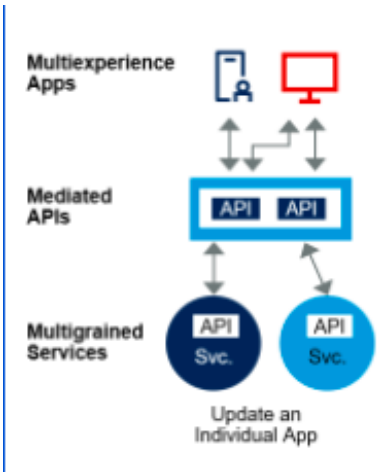
Mediación de servicios, API y eventos

Las API mediadas permiten ofrecer API optimizadas para satisfacer las necesidades de consumidores específicos. El enfoque de API mediado permitirá abstraer las complejidades en la implementación del servicio, así como para implementar un control de acceso, seguridad y administración consistentes.

Un enfoque de API mediada implica la implementación de tres capas distintas:

- API internas habilitan el dominio nativo del servicio y los modelos de interacción.

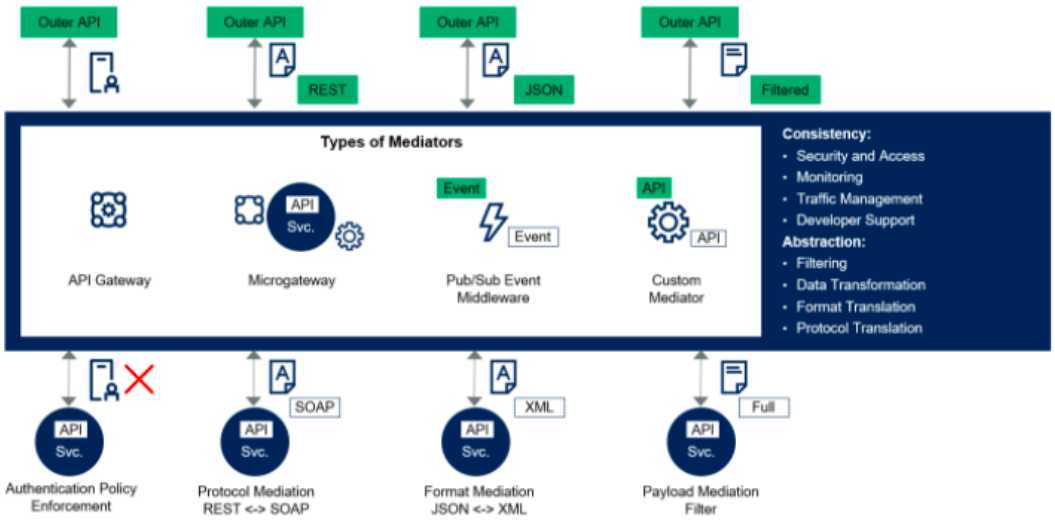
- API externas proporcionan una capa uniforme para que las aplicaciones accedan a la funcionalidad de back-end. Las aplicaciones pueden compartir una API externa o tener una API única. Las aplicaciones usan API externas como parte de su plataforma y, por lo tanto, las tratan como productos de consumo individuales.
- La mediación de API asigna las API externas a las API internas, monitorea y registra las interacciones y aplica políticas de tiempo de ejecución para la seguridad y la gestión del tráfico. Esto incluye actuar como intermediario para traducir protocolos, formatos, estructuras de datos y otras transformaciones a medida que las solicitudes pasan entre las API internas y las API externas.



Implementar una capa de mediación para administrar las API

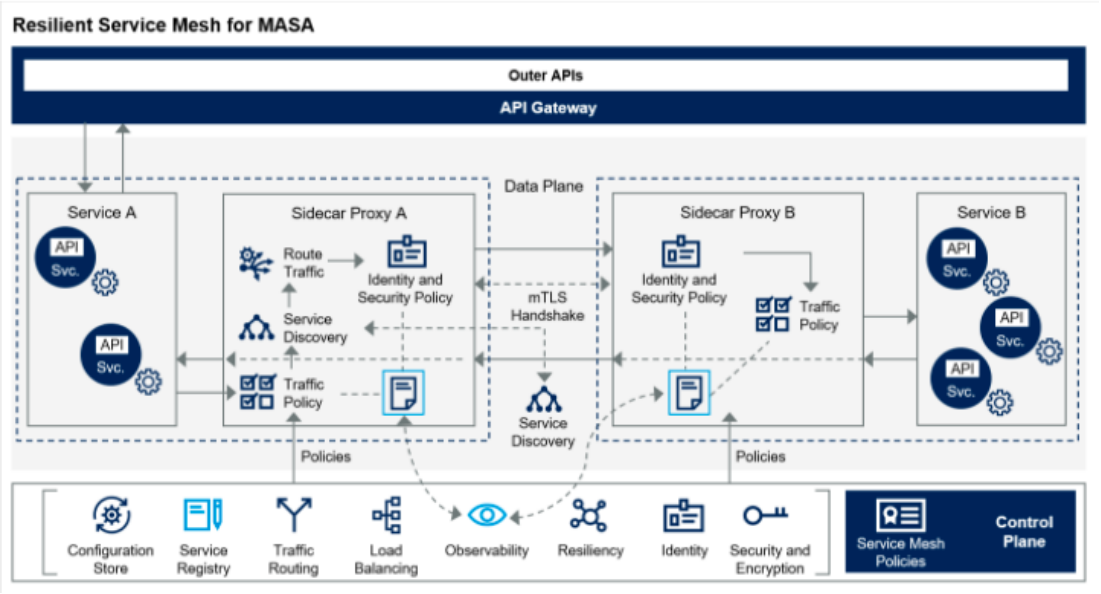
La capa de mediación permite abstraer las complejidades de los servicios de las preocupaciones del cliente de la API externa. La capa de mediación puede usar uno o más mediadores, tecnologías que se ubican entre las API externas que usan las aplicaciones cliente y los servicios. Los contratos técnicos definido en la API externa y el diseño de la API interna ayudan al diseño y la implementación de la capa de mediación. Mapee los requisitos técnicos de la API externa con las capacidades actualmente expuestas por el servicio. Por ejemplo, la API externa puede requerir una interfaz REST mientras que el servicio expone una interfaz SOAP.

Una puerta de enlace API (API gateway) es el lugar óptimo para comenzar con la mediación porque proporciona de manera efectiva una capa consistente para aplicar políticas de administración de seguridad, identidad, monitoreo y tráfico. Además, algunas puertas de enlace API pueden usar políticas para filtrar o transformar datos.



Implementar capacidades de Service Mesh para admitir servicios multigrano

Construir un MASA con servicios multigrano requiere capacidades para habilitar y gobernar las interacciones entre servicios. Una red de servicios (service mesh) es una combinación de componentes de infraestructura, arquitectura y configuración, como puertas de enlace internas o proxies y mediación ligera que proporciona un modelo de comunicación coherente entre servicios débilmente acoplados. Una red de servicios (service mesh) es parte de la capa de mediación de API y es un componente importante de MASA que permite un modelo consistente para definir, implementar y administrar las complejidades de la comunicación entre múltiples servicios desacoplados.

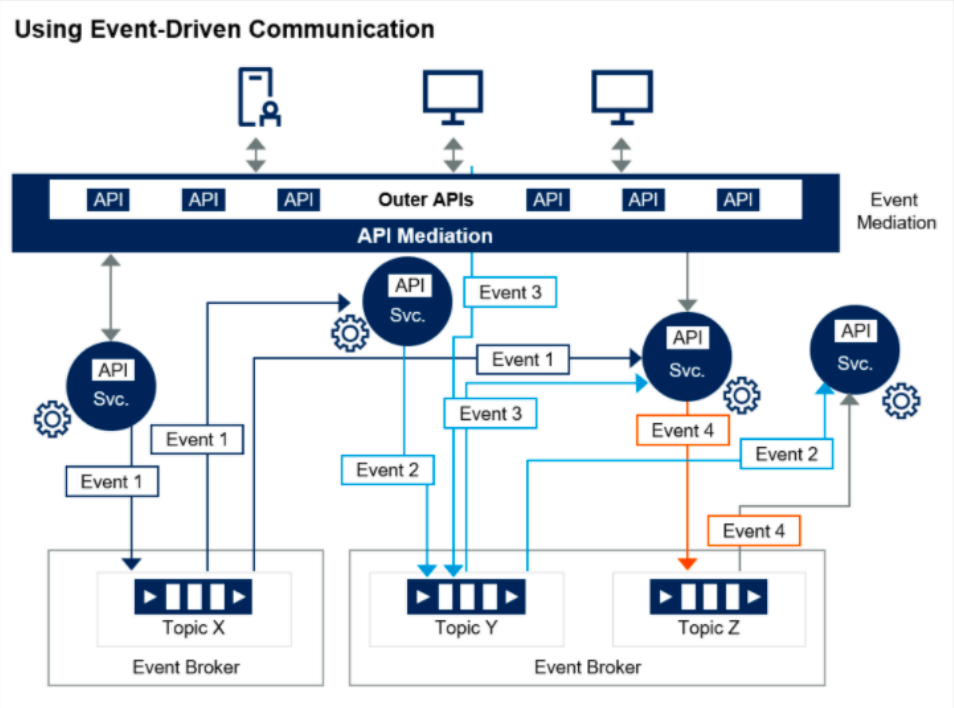


Modelo basado en eventos para la comunicación desacoplada

Un modelo de comunicación basado en eventos proporciona un método altamente desacoplado y eficiente para comunicar cambios de estado y otros eventos entre servicios. En un modelo de comunicación basado

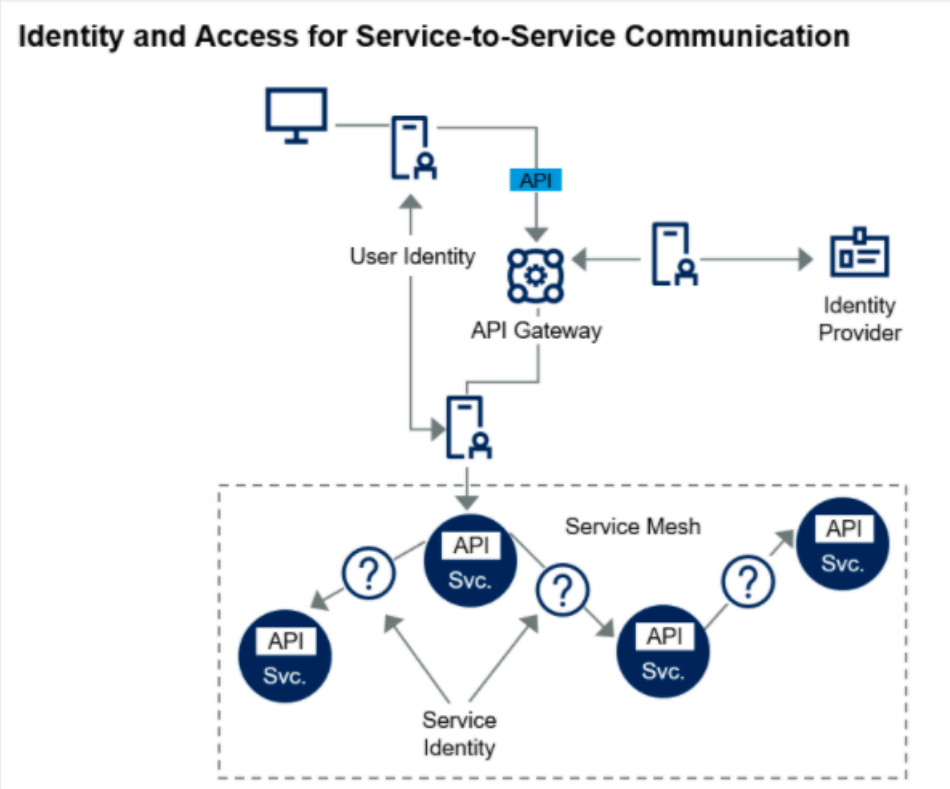
en eventos, los editores de eventos envían eventos a un tema y los consumidores de eventos se suscriben a esos temas y ejecutan la funcionalidad cuando reciben un evento.

Un modelo de comunicación basado en eventos proporciona un mayor grado de desacoplamiento que un modelo de comunicación tradicional de solicitud/respuesta. Los productores de eventos no tienen conocimiento directo de los consumidores intermedios y no dependen del procesamiento de eventos: simplemente notifican al corredor que se ha producido un evento. Los consumidores de eventos tampoco tienen dependencias directas de los productores de eventos: simplemente ejecutan la funcionalidad cuando reciben un evento.



Aplicar una estrategia de identidad y acceso para API y servicios multigrano

Aprovechar la mediación para externalizar la autenticación y la autorización de los componentes de la aplicación. Una aplicación de malla que utiliza la comunicación de servicio a servicio agrega una dimensión adicional a la identidad y el acceso. La protección sólo en la puerta de enlace es un antipatrón. Los servicios necesitan protegerse a sí mismos; no asuma que una red es segura.



La estrategia de identidad y acceso admite la autenticación para las solicitudes de servicio a servicio, además de las solicitudes de las aplicaciones. Usar un servicio de puerta de enlace para convertir los tokens de autenticación de los usuarios (como contraseñas) en tokens de seguridad y páselos entre los servicios. Utilizar la mediación en la red de servicios para administrar la identidad y el acceso de la solicitud en la comunicación de servicio a servicio.

Implementar servicios multigrano

Los servicios son un componente clave para implementar una aplicación utilizando MASA. Los servicios proporcionan la lógica comercial, el acceso a datos y recursos, y otras funciones de back-end requeridas por las aplicaciones. Los servicios exponen esta funcionalidad a través de las API internas que reflejan su modelo de dominio interno y su modelo de interacción nativo, es decir, sus API internas.
El propósito de las API internas es exponer la funcionalidad de los servicios para que la use la capa de mediación. Las API internas desacoplan y abstraen la funcionalidad del servicio para proporcionar flexibilidad, agilidad y escalabilidad en la implementación y despliegue de los servicios. Las API internas deben centrarse en el dominio del servicio para el consumo general de otros servicios y mediadores. Esto es diferente de las API externas, que se enfocan en las necesidades particulares de las aplicaciones de los clientes.
La funcionalidad de aplicaciones empresariales, las aplicaciones heredadas, SaaS y los servicios de integración habilitados a través de API son ejemplos de implementaciones de servicios potencialmente disponibles para las aplicaciones MASA.
Los patrones comunes de integración de servicios personalizados incluyen:

- Orquestación y agregación: las aplicaciones desacopladas en MASA a menudo requieren interacciones con múltiples sistemas de back-end. Los servicios de orquestación personalizados coordinan las solicitudes a múltiples sistemas de back-end para proporcionar un acceso unificado a los datos y el procesamiento de esas aplicaciones. Esto reduce la cantidad de solicitudes que las aplicaciones deben enviar al back-end. Un uso

común de la orquestación son los servicios de agregación, que combinan datos de varios sistemas back-end y pueden aplicar proyecciones, filtros y otras operaciones para optimizar los datos.

- Coreografía: el patrón de coreografía y orquestación le permite realizar una única solicitud a un servicio personalizado que inicia el procesamiento en varios servicios de back-end en un orden específico o a un conjunto específico de sistemas de back-end.

- Backend para frontend: las aplicaciones multiexperiencia a veces requieren una API de back-end especializada que se aplique específicamente a sus necesidades. En lugar de diseñar e implementar un back-end único y completo, un servicio personalizado que abstrae las necesidades específicas de la aplicación de la implementación del back-end le permitirá utilizar las capacidades del back-end existentes.

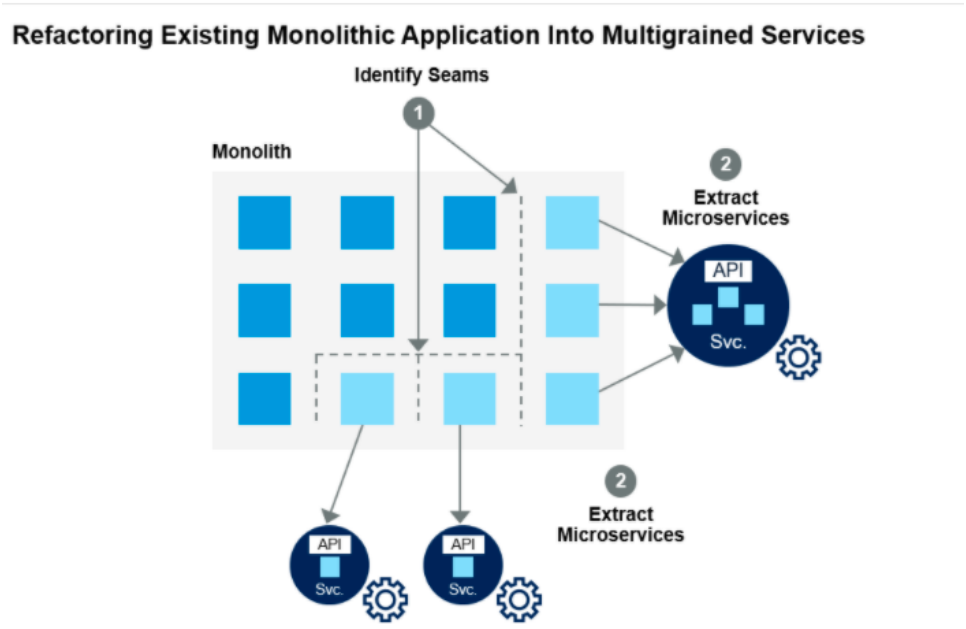
- Procesamiento por lotes: los servicios de integración personalizados proporcionan un método adaptable para implementar el procesamiento por lotes de datos de una variedad de fuentes de datos en un sistema de back-end.

- Integración de servicio a servicio: los servicios de integración personalizados le permiten conectar servicios de back-end de varias maneras, como sincronizar cambios de estado entre dos sistemas de back-end diferentes o ampliar el procesamiento comercial al iniciar procesos comerciales adicionales en otros sistemas.

- Integración basada en eventos: los eventos proporcionan un mecanismo efectivo para integrar los cambios de estado que ocurren en un servicio para procesarlos en un servicio separado con un acoplamiento mínimo.

Refactorizar los sistemas existentes:

Refactorice los sistemas existentes que limitan el rendimiento, la escalabilidad o la cadencia de entrega requerida por la aplicación MASA. Esto evita la fragilidad posterior, las limitaciones de flexibilidad y los problemas de escalabilidad. No necesita refactorizar toda la aplicación, sólo las partes que necesita para la aplicación de malla. La refactorización debe ser un proceso iterativo en el que refactorice el monolito extrayendo piezas.



Implemente nuevos servicios con la granularidad adecuada:

Implemente nuevos servicios para agregar funcionalidades que no existen y que no se pueden refactorizar. Los nuevos servicios también incluyen funciones que pueden orquestar o agregar funciones de otros servicios existentes para admitir nuevas funciones requeridas por la aplicación.
Considere la granularidad de la funcionalidad del servicio MASA como un espectro con macroservicios en un extremo, microservicios en el otro y miniservicios en el medio:

- Macroservicios: servicios detallados que habilitan algunas o todas las funciones de una aplicación monolítica; los cambios requieren reconstruir y volver a implementar todo el monolito.
- Miniservicios: servicios de granularidad gruesa que brindan funcionalidad a nivel de dominio, lo que le permite realizar e implementar cambios en un solo servicio de dominio en la aplicación de malla sin afectar necesariamente a los otros servicios de dominio.
- Microservicios: servicios detallados con capacidades específicas que se implementan de forma independiente y brindan la mayor cantidad de flexibilidad.

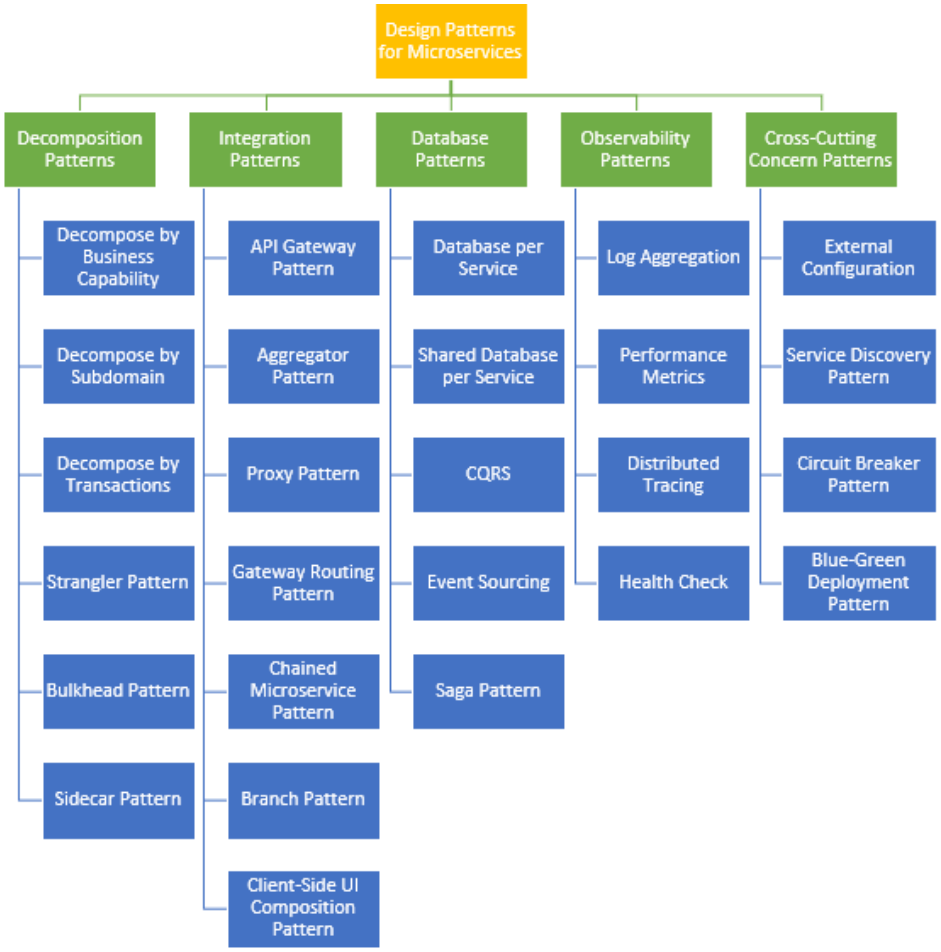
Con esta renovación se persiguen los siguientes objetivos:

- Contar con una base tecnológica plenamente actualizada.
- Profundizar en la modularización del sistema, donde cada módulo mantenga una total independencia, tanto en su versionado, como en cuanto al equipo responsable de desarrollo y mantenimiento.
- Mejorar el Time to Market de los nuevos desarrollos.
- Posibilitar una correcta gobernanza del sistema en Producción, optimizando la relación infraestructuras / rendimiento.
- Maximizar la reutilización de código.
- Automatizar al máximo las tareas de integración, pruebas, despliegue y control de calidad.

3.1 Especificaciones de desarrollo

Microservicios se refiere a servicios independientes e implementables adjuntos a un dominio particular. Los microservicios se comunican a través de redes. La arquitectura de microservicio consta de múltiples microservicios que colaboran y es una forma de arquitectura orientada a servicios (SOA).

https://learncsdesign.medium.com/microservices-design-patterns-91fe56a33a47



Patrones de descomposición:

- Descomponer por capacidad empresarial

Los microservicios tienen que ver con hacer que los servicios estén poco acoplados, aplicando el principio de responsabilidad única. Se descompone por capacidad empresarial. Definir los servicios correspondientes a

las capacidades del negocio. Una capacidad empresarial es un concepto del modelado de arquitectura empresarial, es algo que hace una empresa para generar valor.

- Descomponer por subdominio

Descomponer una aplicación usando capacidades comerciales puede ser un buen comienzo, pero hay algunas clases que no serán fáciles de descomponer. Estas clases serán comunes entre múltiples servicios. Defina los servicios correspondientes a los subdominios de diseño controlado por dominio (DDD). DDD dominio consta de varios subdominios. Cada subdominio corresponde a una parte diferente del negocio.

- Patrón de descomposición por transacciones

Puede descomponer los servicios sobre las transacciones. Entonces habrá múltiples transacciones en el sistema.

- Patrón de estrangulador

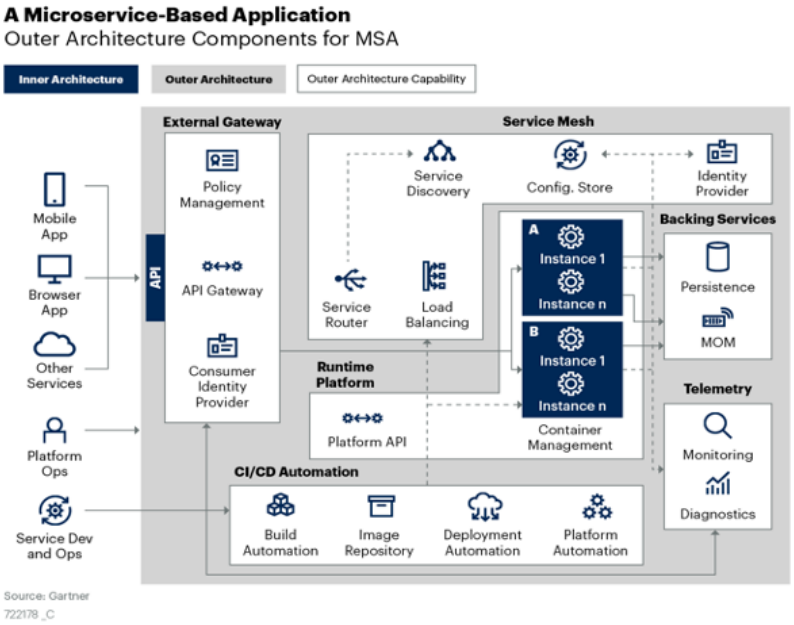
Los patrones de diseño por los que pasa descomponen aplicaciones para Greenfield, pero el 80 % del trabajo que realiza es con aplicaciones brownfield, que son aplicaciones grandes y monolíticas (base de código heredada). El patrón Strangler viene al rescate o solución. Esto crea dos aplicaciones separadas que viven una al lado de la otra en el mismo espacio URI. Con el tiempo, la aplicación recién refactorizada "estrangula" o reemplaza la aplicación original hasta que finalmente puede cerrar la aplicación monolítica.

- La malla de servicio (Service Mesh)

patrón informático distribuido, implementado como middleware, que optimiza las comunicaciones entre servicios de aplicaciones.
Proporciona mediación de proxy y/o liviana para comunicaciones de servicio a servicio y admite funciones como autenticación, autorización, encriptación, descubrimiento de servicios, enrutamiento de solicitudes, equilibrio de carga e instrumentación de servicios.

  - ➢ Sidecar proxies

- API gateways
- OAuth 2.0
- Microservices orchestration



3.2 Entorno tecnológico

Existen 2 estrategias a nivel de utilización de imágenes base:

3.2.1 Contenedores

3.2.1.1 Modo no gestionado

En este modo todo el peso del contenedor recae en el desarrollo. Se proveen flujos de CI/CD para el despliegue de la imagen, pero ésta no es gestionada desde Osakidetza.

A pesar de eso puede ser exigible el cumplimiento de ciertos requisitos de seguridad durante el despliegue.

3.2.1.2 Modo gestionado

En este modo desde Osakidetza se proveen imágenes base de plataformas, asegurando el ciclo de vida de las mismas, y los parcheos, tanto evolutivos, como de seguridad.

Desde la aplicación a su vez existen 2 opciones para adaptarse al ciclo de vida de estas imágenes base.

- Utilizar la versión "latest" de la misma, de forma que en cada despliegue siempre se utilice la última versión publicada de la imagen base.

- Utilizar una versión concreta de la misma, de forma que el control de la versión a utilizar en cada despliegue, dependa de desarrollo.

A nivel tecnológico existen imágenes base de las siguientes plataformas:

- Tomcat
- Nginx (basada en la imagen oficial)
- NodeJS (basada en la imagen oficial)
- Spring boot
- MongoDB
- Redis (en construcción)

3.2.2 Orquestación de contenedores

La aplicación funcionará sobre una plataforma para aplicaciones modernas (*cloud-native application platform*) basada en contenedores orquestados por Kubernetes.

Esta plataforma se apoya en el portfolio de soluciones de VMware Tanzu y aporta:

- El entorno de ejecución nativo e integrado en el cloud privado sobre el que está desplegada el resto de la infraestructura de Osakidetza.
- Capacidades de gestión, operación y obervabilidad para los contenedores.
- Prestaciones de seguridad de la información, pudiéndose establecer además políticas transversales con las partes basadas en máquinas virtuales
- Gestión del ciclo de vida del software
- Soluciones de continuidad como backup y recuperación y posibilidad de despliegue en CPDs de respaldo.
- Capacidad para que la aplicación pueda funcionar en diferentes proveedores de cloud pública del mercado sin precisar de adaptaciones e hibridada también con el entorno on-premise estando federados entre sí.

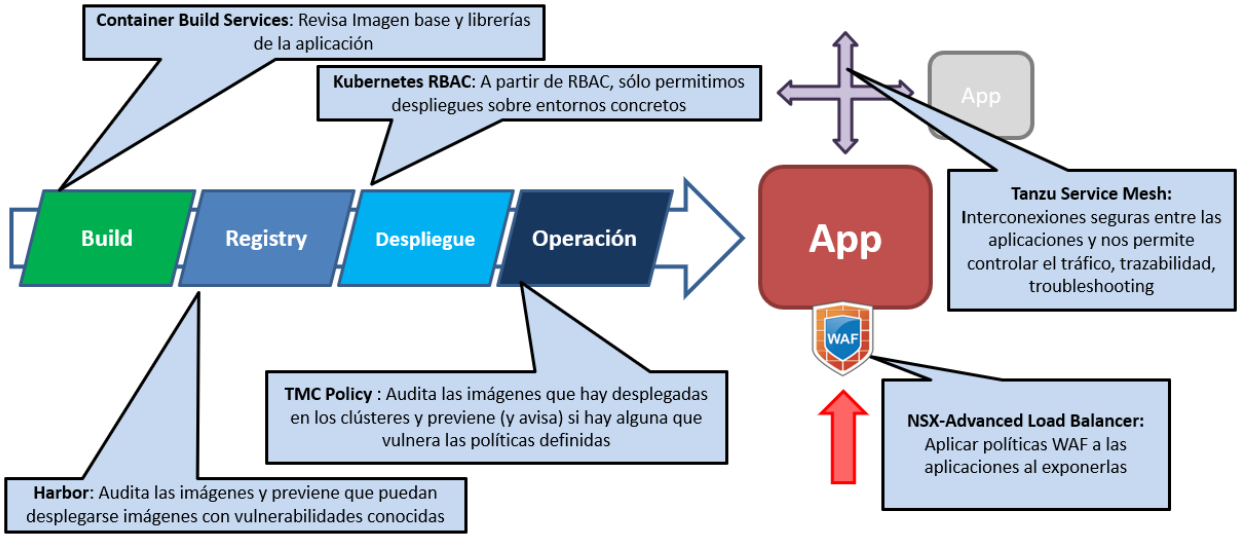
En cada una de esas ubicaciones se podrá disponer a su vez de entornos de no-producción y producción según se precise por criterios de calidad del software, testing, conveniencia o agilidad.

La plataforma en general estará operada a distintos niveles según responsabilidades por el equipo que da servicio a Osakidetza de Plataforma (PlatOps), Infraestructura (CloudOps) y Seguridad (SecOps) siendo el equipo de desarrollo de la aplicación un usuario consumidor de la misma. El equipo de PlatOps será su principal punto de interacción primándose la automatización y las capacidades de autoservicio.

3.2.3 Plataforma operativa y seguridad

Apoyándose en componentes de la plataforma descrita en el apartado anterior, el alineamiento con buenas prácticas de seguridad de la información en todas las etapas del ciclo del software se articula en cada etapa de un pipeline CI/CD concebido específicamente para aplicaciones modernas.

Este pipeline que tiene el acento en la parte "CD" del despliegue continuo y sirve como base para formar una cadena de suministro segura extremo a extremo, con diferentes momentos de actuación (build vs runtime).



Los controles básicos de segmentación, autenticación y autorización de microservicios se basarán en un service mesh mesh en la mayoría de los casos, para que su aplicación sea realista y abordable. Esta service mesh se debe conciliar y/o con la capa de mediación de API en los casos que esta última sea de aplicación.

Aunque se prioricen los controles que estén incorporados en la plataforma de orquestación, se podrán usar herramientas externas por excepción cuando la singularidad, criticidad o particularidad del escenario lo requiera.

El desarrollador de la aplicación debe seguir las políticas, reglas y estandarizaciones establecidas meticulosamente y ser partícipe dentro de su diligencia debida y ámbito de responsabilidad del alineamiento con las buenas prácticas.

3.2.4 Plataformas horizontales

Plataformas distribuidas de transmisión de datos, como Kafka, almacenamiento de objetos, etc.

En múltiples ocasiones existen escenarios mixtos en los que la aplicación se evoluciona a un modelo sobre contenedores, pero el dato sigue persistiendo en BBDD's "tradicionales".

En estos casos las versiones estándarizadas son:

- Oracle Database Single Instance 19c
- Oracle RAC Database 19c

4 MySQLDirectrices tecnológicas de IOC

Osakidetza dispone de múltiples aplicaciones desarrolladas en diversas tecnologías (principalmente Java y .Net), y albergadas en diferentes plataformas (principalmente Apache HTTP Server, Microsoft IIS y VMware Horizon como soluciones de presentación, Oracle WebLogic, Apache Tomcat y Microsoft IIS como servidores de aplicación y Oracle RDBMS, Microsoft SQL Server, MongoDB como servidores de BBDD).

El modelo de referencia de las aplicaciones es una solución Web (sin plug-in's), con **arquitectura** de n-capas preferentemente **3 capas**: presentación, negocio y persistencia, compatible con tecnología de virtualización y almacenamiento SAN y NAS.
Dicha arquitectura es **escalable horizontalmente** en cuanto a las capas de negocio y persistencia (reparte la carga equitativamente entre los diversos servidores que ejecutan la lógica de negocio y estos a su vez, mediante un pool de conexiones acceden a la capa de persistencia), y es **tolerante a fallos** garantizando la continuidad de negocio.
Los servidores que atienden a las capas de negocio y persistencia están ubicados en los dos CPDs de la Dirección General de Osakidetza siendo el reparto de los mismos proporcional en un CPD u otro; la capa de presentación está distribuida en los puestos de trabajo fijos, portátiles, móviles y tabletas en los diversos centros de Osakidetza (Hospitales, Centros de salud, etc..).
De modo que la solución (producto/aplicación/desarrollo) a suministrar deberá ser compatible con el modelo de arquitectura indicado en el párrafo anterior y con la relación de productos y tecnologías que se indican a continuación (las que apliquen).

4.1 Entorno tecnológico

En conjunto, el entorno tecnológico de las soluciones actualmente en producción es:

- Plataformas de desarrollo:
  - .NET sobre Windows 2016*
  - Java sobre Red Hat Enterprise Linux 8
  - Aplicaciones móviles:
    - Node.js, Express, AngularJS, MongoDB sobre Red Hat Enterprise Linux 8
    - Ionic, Cordova sobre Android, iOS

    - (*) En la actualidad 2019 en construcción
    -
    -
    - Plataforma de virtualización:
    - VMWare vSphere 7.0 U2
    -
    - Almacenamiento:
    - SAN: EMC VMax
    - NAS: EMC Isilon

    - Sistemas Operativos:
    - Servidores:
    - Windows 2016 (en la actualidad en construcción 2019)
    - Red Hat Enterprise Linux 8
    - Puesto de trabajo fijo: Windows 10, Enterprise x64

- Puesto de trabajo móvil: Android, iOS
-
- Servidores Web:
- Apache Webserver 2.4.X (en la actualidad 2.4.6)
- MS IIS 10 (S.O. Windows Server 2016)
- SAP Web Dispatcher 7.73 (actual 7.20 obsoleta)
- Nginx 1.18.0
-
- Servidores de Aplicación:
- Apache Tomcat 9.0.32 + JDK 8
- Oracle Weblogic Server 12c + JDK 8
- MS IIS 10 + .NET Framework 4.6.2
- Application Server de SAP Netweaver 7.5
- Node.js 12.17.0
-
- Sistemas de Gestión de Bases de Datos (*)
- Oracle RAC 19c (para réplicas se usa Active Data Guard)
- Oracle 19c Single instance
- Microsoft SQL Server 2016 (En la actualidad 2019 en construcción)
- MongoDB 4.4.1
-
- (*) Continuidad de negocio y Alta disponibilidad: Oracle RAC, SQL Server Always ON solo para aplicaciones críticas
-
- Gestión de contenidos:
- MS SharePoint Online (O365)
- Documentum 20.4
-
- Infraestructura SOA:
- Oracle Service Bus 12c (12.2.1.4) + JDK 8.0
-
- Plataforma de firma (PKI):
- Izenpe
-
- Autenticación:
- Directorio Activo de MS (AD)
-
-
- Modo de ejecución/escritorio:
- local: puesto fijo o móvil
- Cliente de Horizon 5.3
-
- 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
- Señal:
- Ganancia de la antena: Mínimo 3 dBi
- Sensibilidad <= -70 dBm a 11Mbps

Consideraciones en relación a los de productos y tecnologías indicados anteriormente:

- En cuanto al navegador, se debe **evitar** el uso de Applets (Java), componentes ActiveX (.NET), Flash u otras tecnologías que impliquen la **descarga y ejecución de software embebido en el navegador**.
- Al respecto de Office 2010, **no está permitido** el uso, dependencia o interrelación con Access.
- Al respecto de los dispositivos inalámbricos se han especificado los **requisitos mínimos** que deben cumplir.

4.2 ESPECIFICACIONES DEL CLIENTE (MAQUETA)

Actualmente, la versión de maqueta que se instala en los equipos de **Osakidetza** es la *2.1,* aunque convive con versiones anteriores instaladas.

- Hardware (mínimo existente):
  - PC arquitectura Intel o equivalente
  - Procesador con un mínimo de Tecnología de 45 nm, Caché L2 de 3 Mb. y FSB de 1.066 MHz.
  - Memoria RAM 2 Gb (4 GB en W10)
  - Disco duro 250 Gb (500 Gb en W10)
  - Monitor 19 pulgadas con resolución 1440x900 mayoritaria o 1280x1024. (21-22" 1920x1080 en W10)

- Restricciones de escritura en disco C: para usuarios standard, excepto en su perfil de usuario (C:|users\)
  - En cuanto al navegador, se debe evitar el uso de Applets (Java), componentes ActiveX (.NET), Flash u otras tecnologías que impliquen la descarga y ejecución de software embebido en el navegador.
  - Al respecto de Office 2016, no está permitido el uso, dependencia o interrelación con Access.
  -
  - Mismas restricciones (navegador y Office) que W7.

Sistema Operativo que instala esta imagen				
X	Actual - Windows 10, Enterprise x64 1709 Actualizando - Windows 10, Professional x64 1909			
Idiomas Disponibles:	Castellano (es-ES); Euskera (eu-ES)			
Hotfixes:				
Descripción		Clasificación		
Compatible desde 1703 hasta el update y actualizaciones de seguridad de W10 en vigor en todo momento		Updates Críticas y de seguridad		
Parámetros de Configuración de Software				
Fabricante	Producto	Versión	Idioma	Plataforma
Microsoft	Silverlight	5.5.1	Castellano	x64
Microsoft	Visual C++ 2008	9.0.30729.4148	Castellano	X64,x86

Microsoft	Visual C++ 2010	10.0.30319	Castellano	x64;x86
Microsoft	Visual C++ 2012	11.0.60610	Castellano	x64;x86
Microsoft	Visual C++ 2013	12.0.30501	Castellano	x64;x86
Microsoft	Visual C++ 2017	14.11.25325	Castellano	x64;x86
Oracle	Java	8.1510.12	Castellano	X64;x86
Adobe	Acrobat Reader	15.020.20039	Castellano	x64
Adobe	Shockware	12.2.4.194	Castellano	x64
7zip Org	7zip	16.04	Castellano	x64
FNMT	DNIe	14.0	Castellano	x64
FNMT	Certificados Raiz			
FNMT	TC-FNMT	6.1.3	Castellano	x64
Xuxen	Corrector Xuxen	5.2	Euskera	X86
LibreOffice	LibreOffice	5.4.5.1	Multiligual	X64
Firefox	Firefox	58.0.2	Castellano	X64
Microsoft	RSTA Cliente	1709	Castellano	X64
Microsoft	Cliente One Drive	17.3.6816.0313	Castellano	x64
IZENPE	Middleware_Izenpe	4.0.2.436	Castellano	X64
IZENPE	Idazki-desktop-win	3.3.1	Castellano	X64
Vmware	Horizon Client	4.7	Multilingual	x64
Parámetros de Configuración de Software Personalización de Osakidetza				
Oracle	Cliente Oracle	12.1.0.2	Castellano	x64
VMWare	Cliente Horizon	5.0.0		
Microsoft	Office Standard	2016	Castellano	x86
Microsoft	Office ProPlus	2016	Castellano	x86
Microsoft	Access Runtime (Con versión Standard 2016)	2016	Castellano	X86
Business Objects	Crystal Reports	10.5.0.0.sp16	Ingles	X86
Business Objects	Crystal Reports runtime engine	13.0.22	Ingles	X86
NDDigital	nddDigital DCS Server (Pago por impresion)	2.0.0.6	Ingles	X64
NDDigital	nddDigital nddPrint Agent	5.20.5	Ingles	X64
BitDefender	Bitdefender Endpoint Security Tools	6.6.11	Castellano	X86

Microsoft (integrado con el SO)	NET Framework	3.5 (incluye .NET 2.0 y 3.0)		X64
Microsoft (integrado con el SO)	Servicios avanzados de .NET Framework	4.7(ASP.NET 4.7)		X64
Unify	Team Developer 5.2 Deployment	5.2.0000		x86

4.3 Dispositivos de entrada/salida

La solución deberá ser capaz de interactuar con diversos dispositivos de entrada y salida de diversos fabricantes; siendo dichos dispositivos: pantallas táctiles, impresoras térmicas, monitores, por tanto, el interface con los mismos será en base a estándares del mercado.

Así mismo la solución deberá adaptarse a la resolución de las diversas pantallas.

En relación a dispositivos móviles se deben tener en cuenta ciertas particularidades en relación a las características de movilidad, tamaño, comunicación inalámbrica e interacción con las personas:

- Son aparatos pequeños.
- La mayoría de estos aparatos se pueden transportar en el bolsillo del propietario o en un pequeño bolso.
- Tienen capacidad de procesamiento.
- Tienen conexión permanente o intermitente a una red.
- Tienen memoria (RAM, tarjetas MicroSD, flash, etc.).
- Normalmente se asocian al uso individual de una persona, tanto en posesión como en operación, de modo que puede adaptarlos a su gusto.
- Tienen una alta capacidad de interacción mediante la pantalla o el teclado.

En lo que se refiere a dispositivos sobre los que tienen que ejecutar soluciones de movilidad hay dos ámbitos que son las soluciones orientadas a profesionales de Osakidetza y soluciones orientadas al ciudadano.

Las aplicaciones orientadas al ciudadano se ejecutarán en dispositivos de consumo ya sean móviles, tabletas o cualquier otro dispositivo al que vaya destinada la solución. En este caso el desarrollo deberá ejecutarse en dispositivos con los diferentes sistemas operativos que haya en el mercado.

En las aplicaciones orientadas a los profesionales de Osakidetza las aplicaciones deberán de ejecutarse en el dispositivo elegido y homologado para soportar la solución. Habrá que tener en cuenta los siguientes aspectos:

- Ergonomía, tamaño y usabilidad del dispositivo, se refiere a que cumpla las expectativas del usuario en ámbito en el que se va a desarrollar el proyecto.
- Especificaciones de limpieza y resistencia a los golpes.
- Características de comunicaciones como pueden ser conectividad Wifi y 4G.

4.4 Seguridad, acceso, autenticación y autorización

El tratamiento de los datos cumplirá lo establecido por la legislación vigente en materia de **seguridad** y protección de datos.

En el ámbito intranet se permitirá el acceso mediante los **transportes** RMI, JMS, HTTP y HTTPS.

El proveedor de **servicios de certificación** de Osakidetza es Izenpe.

Osakidetza ha dotado a todos sus profesionales de certificados corporativos reconocidos, en soporte tarjeta criptográfica, con capacidad de firma de documentos y mails, cifrado y autenticación en el AD.

Además, para los nuevos SI que necesitan firma electrónica ágil, Osakidetza ha implantado una solución horizontal de firma, basada en certificados alojados en HSMs, llamada "firma centralizada". Son certificados con las mismas características y garantías que los alojados en tarjeta criptográfica. Estos HSM son de última generación y cumplen con las más exigentes normas internacionales (FIPS 140-2 Level 2 and Level 3, Common Criteria at EAL 4+ y RoHS compliant). Permiten la firma a través de CSP propio (applets) y la firma directa basada en una Pasarela de firma propietaria.

Izenpe es también el proveedor de la infraestructura de autenticación, validación y firma basada en certificados electrónicos. Osakidetza dispone de 2 Zain en HA (equipos TrustedX de Safelayer) en propiedad y su backup, en modo servicio, en los Zain de Izenpe. La integración con estos equipos se puede realizar mediante su librería Smartwrapper. Provee diferentes servicios web (validación, evolución de firmas, firma en servidor, etc.) alojados en los OSB de Osakidetza.

Así mismo, Osakidetza dispone de su propia infraestructura de Custodia de documentos firmados, para asegurar la validación de cualquier firma realizada en sus sistemas de información con certificados electrónicos. Está constituida por 2 equipos Siaval en HA, de la empresa SIA, y HSM Ncipher propios.

Para la firma electrónica de documentos in-situ por parte de sus pacientes, Osakidetza dispone de una solución denominada "firma biométrica", que asegura la validez de todas las firmas implicadas. Se apoya en la solución SmartAccess de Telefónica.

Osakidetza está inmerso en la adecuación de toda su infraestructura y sistemas de información al reglamento europeo eIDAS. Tanto en cuestión de certificados como de niveles de aseguramiento (autenticación).

Los sistemas de **autenticación** validos son:

- **Autenticación** basada en **Directorio Activo (Microsoft Active Directory) corporativo,** que permite identificar un empleado de Osakidetza mediante usuario/contraseña o la tarjeta profesional.
- **Token de Kerberos**, que habrá sido emitido por el Directorio Activo corporativo.
- **Autenticación** basada en **infraestructura de certificación digital (PKI)**. Esta autenticación permite la identificación de personas (certificados personales) o de sistemas de información (certificados de servidor)
- **Certificados X.509 de servidor**, que permitirán identificar sistemas (máquinas) y establecer confianza entre ellas.
- **Certificados X.509 de cliente**, que permitirán identificar individuos (personas)
- Para los servicios web, el estándar **WS-Security** permitirá aplicar políticas de autenticación.
- El bus de servicios sólo se utilizará para la autenticación basada en **certificados X.509** de servidor.

El sistema de **autorización** se implementará por medio de la definición de roles de usuario en base a los cuales se gestionarán los permisos y acciones sobre los distintos procesos por los que estará compuesta la solución. De modo que cada usuario en función del rol que tenga asignado podrá acceder a una serie de funcionalidades, así como a los datos relativos a su organización de servicio, centro de trabajo, servicio/área de atención.

Se crearán grupos de autorización del Directorio Activo. Por cada perfil que tenga la aplicación (medico, enfermera, administrativo, administrador de la aplicación, …) se creará un grupo de autorización en el DA. Se mapeará el perfil al grupo.

4.5 Monitorización

Osakidetza dispone de una **plataforma de monitorización** a través de la cual ya tiene establecida una línea de monitorización base de su infraestructura y SI.

En este sentido la solución deberá incluir un apartado en el que se describan los elementos a monitorizar para asegurar un correcto funcionamiento del sistema, servicio o producto suministrado de forma integral dentro de la mencionada plataforma de monitorización.

La monitorización se podrá llevar a cabo a través de alguna combinación de los siguientes productos o métodos que Osakidetza integra dentro de su plataforma de monitorización:

- SCOM mediante Management Pack para sistemas Microsoft.
- Nagios XI para sistemas Linux.
- Enterprise Manager Cloud Control para SGBD Oracle / EM 13 y servidor de aplicaciones Weblogic para rendimiento.
- Instalación de agente Dynatrace (1.219.131) para aplicaciones web/Horizon

Las herramientas de monitorización se integran con Evanios/ITOM (gestión de eventos) para las plataformas Batera.

Con el objetivo de monitorizar la solución que vaya a ser suministrada, deberán detallarse los objetos concretos a monitorizar para garantizar su correcto funcionamiento más allá de los aspectos generales de la infraestructura de sistemas que los alberguen; dicha relación de objetos podrá incluir, aunque no exclusivamente, algunos como:

- Procesos en ejecución
- Puertos de comunicaciones a la escucha
- Eventos concretos en registros del sistema
- Unidades de disco o File Systems

Para cada uno de ellos deberán incluirse los umbrales de consumo que se consideren anormales, especificándose 2 valores a partir de los cuales establecer el correspondiente nivel de alerta preventiva o alerta crítica según proceda.

Adicionalmente podrán suministrarse scripts o procesos para llevar a cabo:

- Pruebas sintéticas de los sistemas cuyo resultado determine el correcto funcionamiento del sistema o el correspondiente nivel de alerta preventiva
- Operativas sobre el sistema que puedan ayudar a determinar o especificar las condiciones concretas de los errores o alertas producidos.
- Operativas sobre el sistema para intentar remediar automáticamente la condición de la alerta o error, como reinicio de procesos o servicios, etc.

Todos estos procesos deberán entregarse con su correspondiente documentación, y su operativa deberá resultar sencilla de modo que pueda ser realizada por un operador.

4.6 Backup/Restore

Osakidetza dispone de una infraestructura para la realización de copias de seguridad y restauración a través de red basada en CommVault.

De modo que la solución deberá especificar los procedimientos necesarios a llevar a cabo para la recuperación del servicio ante la pérdida del mismo, corrupción de sus datos o alguno de sus componentes. En este sentido se plantearán escenarios de recuperación independientes para cada uno de los posibles componentes impactados y el orden de ejecución en caso de que deban ejecutarse secuencialmente para la recuperación de varios componentes o del sistema completo en su conjunto.

A partir de los procedimientos anteriormente descritos y en cada uno de ellos, se inferirá **los elementos concretos** sobre los **que se requiere hacer Backup**, en qué **orden**, con qué **frecuencia** y **política de persistencia** deben llevarse a cabo **para poder satisfacer** los distintos **escenarios de recuperación** del servicio contemplados. Así mismo deberán indicarse las restricciones que pudieran existir para la realización del Backup: posible impacto en el servicio, restricciones horarias, etc.

Los distintos procedimientos de recuperación suministrados con la solución deberán ser validados por Osakidetza para garantizar su compatibilidad con la infraestructura de copia de seguridad y restauración existente.

5 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, enrrutar 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
  - JSON – REST (para aplicaciones móviles)
- 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
  - WSSecurity: JWT Token (aplicaciones móviles en internet)
- 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
  - HTTPS

5.1 Servicios Web

Los Servicios Web se implementarán de acuerdo con las especificaciones WSDL v1.1, SOAP v1.1, v1.2, JSON-REST (en el caso de aplicaciones móviles), 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
- oracle_http_jwt_token_server_policy

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.
- Entre el OSB de intranet y el OSB de intranet, se realiza una federación de servicios con las condiciones de seguridad habituales.

Nota: OSB -> Oracle Service Bus 11.1.1.7 -> Paso a OSB 12c

5.2 Gestor de Eventos

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

5.2.1 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 transaccionabilidad 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.

5.2.2 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, aqui se informa el código del error.

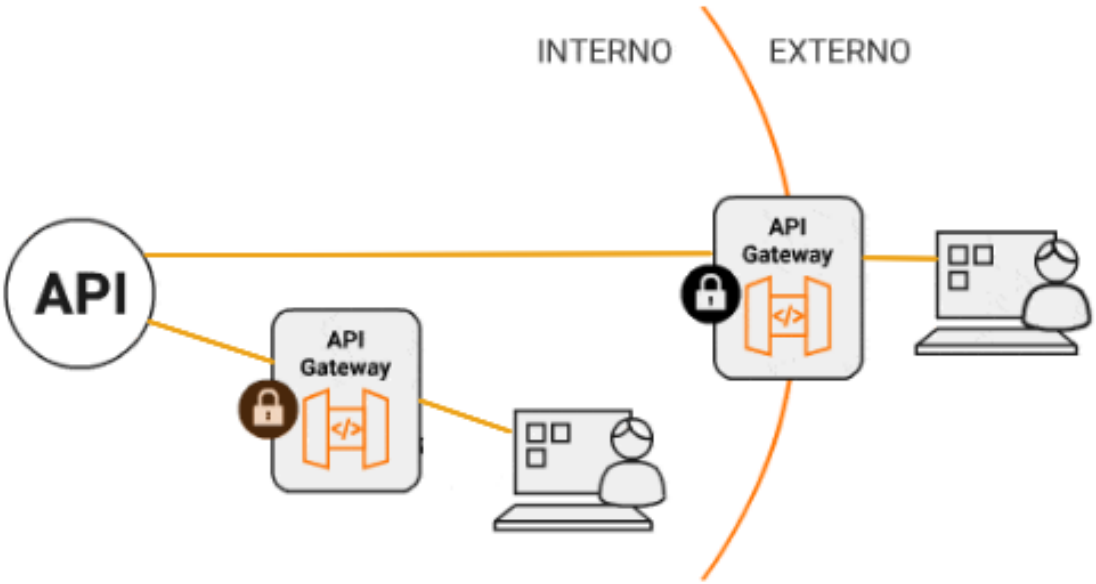
- ✓ **errorDescription**: Si se ha producido un error contiene la descripción de éste.

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

5.3 Arquitectura API REST

De forma adicional a la Arquitectura SOA, Osakidetza permita la interoperabilidad mediante API REST.

El componente centrar de la la arquitectura API REST de Osakidetza el API Manager.



Las funciones del API Manager son:

- Exponer las APIs de manera fácil y segura a consumidores internos y externos.
- Implementar flujos de autorización estándara, como OAuth, OpenID Connect y JWT.
- Gestionar el correcto diseño y el tiempo de ejecución para todo el ciclo de vida de las APIs
- Monitorización y estadísticas de uso.

Osakidetza requiere que las API sigan las buenas de desarrollo tal y como se indica en el documento distribuido a tal fin.

Las API deben tener documentación elaborada mediante Swagger/Open API 3.0.

6 EXPLOTACIÓN INFORMACIÓN- BUSINESS INTELLIGENCE

La herramienta usada para desarrollo de tecnología Business Intelligence es Oracle Business Intelligence Enterprise Edition (OBIEE).

Esta herramienta es una herramienta web, que está soportada por una cada de presentación en Apache, y un servidor Web (Weblogic). En esta capa web de Weblogic se definen los ROLES de usuario (grupos y perfiles de usuario) que luego se usan para la Seguridad de Acceso a Datos y a partes de la aplicación

En este servidor también se alberga el RPD, que es donde se desarrolla toda la metadata y las distintas Áreas accesibles por usuarios.

Todos los datos accesibles desde OBI están almacenados en una única BBDD de Producción.

Para realizar la carga de datos (Incremental), utilizamos la herramienta de extracción (ETL) en ODI.

Para poder realizar las cargas incrementales necesitamos que los orígenes de datos tengan alguna fecha o característica que indique que el dato se ha modificado el día anterior, y así poder hacer cargas de sólo aquello que no existe en destino o se ha modificado. (Un LAST_MODIFIED por ejemplo). Las cargas son normalmente diarias, aunque existen cargas anuales o trimestrales.

Versiones utilizadas:

- OAS (Oracle Analytics Server) 5.5
- OBIEE 12.2.15
- ETL
    - ODI -> Oracle Data Integrator 11g Build ODI_11.1.1.7.0
    - Oracle WarehouseBuilder (DWH) (11.2.0.4)

7 SOLUCIONES MÓVILES

Este apartado refleja las tecnologías para el desarrollo de aplicaciones móviles, definida por Osakidetza.

Comprende dos capas:

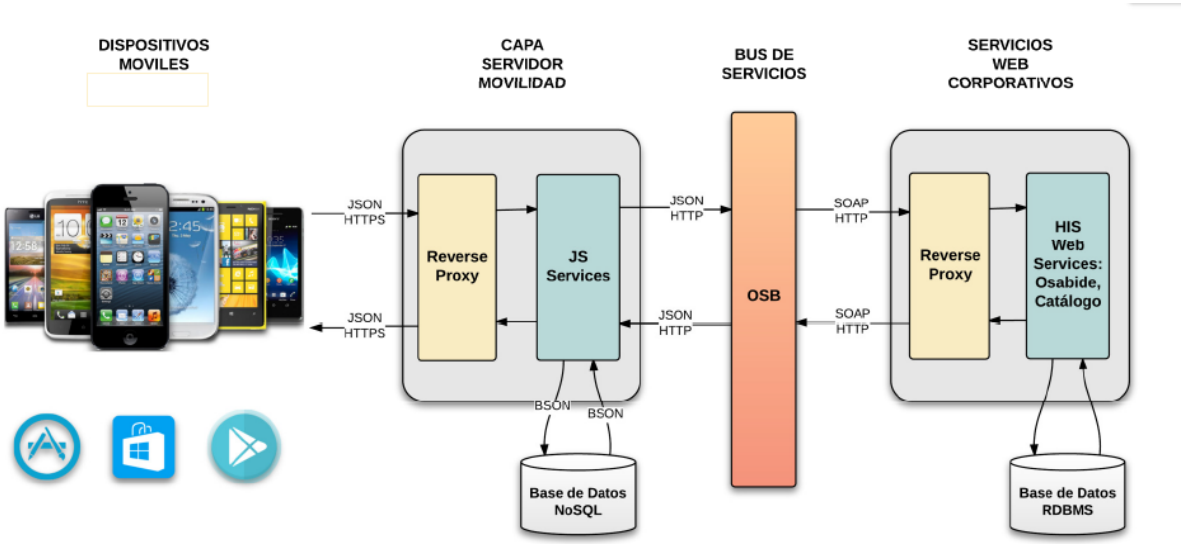
- Tecnologías para el desarrollo en cliente: aplicaciones para dispositivos móviles tales como tablets, smartphones (iOS, Android)

- Tecnologías para el desarrollo en servidor: servicios para la integración con servicios backend, seguridad y lógica de negocio movilidad.

Las características comunes a todas las tecnologías de movilidad son:

- Licencia de código abierto (open source)
- Permiten el desarrollo de aplicaciones multiplataforma
- Lenguajes de programación JavaScript, HTML5, CSS3

En la siguiente figura se muestra la **vista lógica** de la arquitectura de referencia para aplicaciones en movilidad.



7.1 Tecnologías Cliente

7.1.1 Angular

AngularJS es un framework de JavaScript de código abierto, mantenido por Google, que ayuda con la gestión de lo que se conoce como aplicaciones de una sola página. Su objetivo es aumentar las aplicaciones basadas en navegador con capacidad de Modelo Vista Controlador (MVC), en un esfuerzo para hacer que el desarrollo y las pruebas sean más fáciles.

La biblioteca lee el HTML que contiene atributos de las etiquetas personalizadas adicionales, entonces obedece a las directivas de los atributos personalizados, y une las piezas de entrada o salida de la página a un modelo representado por las variables estándar de JavaScript. Los valores de las variables de JavaScript se pueden configurar manualmente, o recuperados de los recursos JSON estáticas o dinámicas.

7.1.2 Ionic Framework 5 o superior

Ionic es un SDK completo de código abierto para el desarrollo de aplicaciones móviles híbridas. Construido sobre AngularJS y Apache Cordova, Ionic ofrece herramientas y servicios para el desarrollo de aplicaciones móviles híbridos utilizando tecnologías web como CSS, HTML5, y Sass.

Las aplicaciones pueden ser construidas con estas tecnologías Web y luego distribuidas a través de las tiendas de aplicaciones nativas para ser instalado en los dispositivos mediante el aprovechamiento de Capacitor.

7.2 Tecnologías Servidor

7.2.1 Nginx

Nginx es un servidor web/proxy inverso ligero de alto rendimiento.

Actualmente Nginx se usa en más de 100 millones de sitios web.

Es un software moderno y su adopción ha sido muy rápida debido a su implementación ligera, que proporciona unos tiempos de respuesta muy bajos con un consumo de recursos hardware mínimo.

7.2.2 Node.js

Node.js es un entorno de programación en la capa del servidor basado en el lenguaje de programación ECMAScript (JavaScript), asíncrono, con I/O de datos en una arquitectura orientada a eventos y basado en el motor V8 de Google.

Node.js es ligero y eficiente ejecutando aplicaciones que hacen uso intensivo de grandes cantidades de datos en tiempo real y corren en dispositivos distribuidos.

7.2.3 MongoDB

Mongodb es una base de datos No SQL open source. Mongodb está orientada a documentos, en vez de guardar los datos en tablas como se hace en la base de datos relacionales, MongoDB guarda estructuras de datos en documentos tipo JSON con un esquema dinámico.

8 CALIDAD DE USO

Rendimiento

Se exigirá que el rendimiento de la aplicación en uso (producción) cumpla y se ajuste a los requisitos no funcionales y al plan de pruebas diseñado en etapas tempranas. En cualquier caso, el comportamiento de la aplicación deberá cumplir de forma obligatoria los siguientes criterios en la ejecución de las pruebas técnicas.

INDICADOR	DESCRIPCIÓN	DESVIACIÓN
Prueba de escalabilidad	El tiempo de respuesta de la aplicación deberá mantenerse invariable con el incremento de usuarios concurrentes(a menos que exista alguna saturación de recursos del sistema), al menos hasta alcanzar la carga pico estimado.	+/- 10%
Prueba de estrés	Tras someter al sistema al doble de carga nominal, tras la disminución de dicha carga a la carga normal de trabajo (80%), la aplicación deberá garantizar su estabilidad y recuperación sin necesidad de reinicio.	+/- 10%
Prueba de estabilidad	La aplicación deberá garantizar un tiempo de respuesta estable manteniendo una carga nominal normal (80 %) durante al menos 12 h	+/- 10%

Usabilidad

Se exigirá que la aplicación mantenga unos criterios de usabilidad que permitan:

- Facilitar el aprendizaje de la aplicación sin requerir conocimientos técnicos en su uso. El sistema deberá ser fácil de usar, asegurando unos bajos costes de aprendizaje y de asistencia o ayuda al usuario.
- Asegurar la velocidad de uso de la aplicación permitiendo el acceso a la información en el menor número posible de clics de ratón.
- El interfaz de usuario deberá ser amigable de forma que se incremente la satisfacción y la productividad de los usuarios.
- Optimizar los costes de diseño, rediseño y mantenimiento.

La ISO 9241-11:1998 “Guidance on usability”, define la usabilidad como: " *La medida con la que un producto se puede usar por usuarios determinados para conseguir objetivos específicos con efectividad, eficiencia y satisfacción en un contexto de uso concreto*"

Osakidetza exigirá el cumplimiento de las directrices de la ISO 9241-151 en cuanto al cumplimiento del grado de usabilidad a exigir en el desarrollo de la aplicación

Accesibilidad

El cumplimiento de la accesibilidad de la aplicación incorporará posibilidades de navegación que garanticen el acceso a la información y a los servicios proporcionados minimizando al máximo las limitaciones y/o restricciones por razón de discapacidad de cualquier carácter o condicionantes técnicos, atendiendo así a la normativa existente.

Se deberán aplicar todas las pautas correspondientes al nivel de accesibilidad AA, llegando a un nivel AAA en las secciones que la configuración de los contenidos y diseño lo permita (Sede electrónica). La accesibilidad se regirá por las pautas WAI indicadas por el Word Wide Web Consortium (W3C).

La accesibilidad no se refiere únicamente a personas discapacitadas. Un sitio web accesible y que se adapte a diferentes tipos de usuario podrá ser visitado por más personas; esta flexibilidad también da beneficios a personas con discapacidades temporales (una convalecencia o enfermedad, problemas de visión), personas de edad avanzada, con una conexión lenta a Internet, que utilizan un dispositivo móvil, etc.

Compatibilidad y portabilidad

Osakidetza exigirá la compatibilidad de la aplicación con los siguientes navegadores web al menos en su última versión estable del fabricante y al menos dos anteriores: Internet Explorer, Firefox, Google Crome, Safari y Mozilla.

La empresa adjudicataria garantizará el funcionamiento de la aplicación con estos navegadores y se responsabilizará de la actualización de la aplicación en caso de necesidad para garantizar la compatibilidad de la misma con estos navegadores durante toda la ejecución del contrato y su periodo de mantenimiento.

El interfaz debe visualizarse independientemente del sistema operativo utilizado por el cliente.

Si procede el diseño deberá ser multi-dispositivo, es decir, accesible y visible desde cualquier dispositivo tipo teléfono móvil, tablet, etc.

Vitoria-Gasteiz, 2025eko apirilaren 7a Vitoria-Gasteiz, a 7 de abril de 2025

IZ./FDO.:

Red Diagnóstico Biológico Osakidetza
Osakidetzako Diagnostiko Biologikoko Sarea

Documento firmado por: MERCEDES SOTA BUSSELO
En la fecha 18.06.2025 09:07:00 CEST