PLIEGO DE PRESCRIPCIONES TÉCNICAS

SUMINISTRO DE LOS PRODUCTOS Y PUESTA A DISPOSICIÓN DE LOS EQUIPOS NECESARIOS PARA REALIZAR PRUEBAS DE DETECCION MOLECULAR DEL VIRUS SARS-CoV-2 PARA LA RED DE DIAGNÓSTICO BIOLÓGICO DE OSAKIDETZA

NÚMERO DE EXPEDIENTE: **2021/02317**

1. OBJETO DEL CONTRATO

1.1 Justificación de necesidad e idoneidad 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 para la detección molecular del virus SARS-CoV-2 en la Red de laboratorios de Osakidetza. (RDBO)

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.

1.2 Procedimiento de adjudicación

La contratación se realizará mediante procedimiento abierto, sujeto a regulación armonizada de la Ley 9/2017 de 8 de noviembre de Contratos del Sector Público.

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 siguientes:

Laboratorio del Hospital Universitario Cruces
Laboratorio del Hospital Universitario Basurto.
Laboratorio del Hospital Universitario Araba.
Laboratorio del Hospital Universitario Donostia.
Laboratorio del Hospital Galdakao-Usánsolo.

En el caso de los lotes para pruebas urgentes, (lotes 3 y 4), además se suministrarán los equipos y reactivos necesarios para los siguientes laboratorios de respuesta hospitalaria de la Red de Diagnostico Biológico:
Laboratorio del Hospital de Bidasoa.
Laboratorio del Hospital de Mendaro
Laboratorio del Hospital de Zumárraga
Laboratorio del Hospital de Urduliz
Laboratorio del Hospital de San Eloy
Laboratorio del Hospital de Alto Deba

3. LOTES

3.1 Justificación de ausencia de división en lotes

No procede

3.2 Objeto y Descripción. Lotes

Lote	Sublote	Denominación
1	1.1 1.2	Sistema automatizado para la detección molecular del virus SARS-CoV-2 con pool de mutaciones. Sistema automatizado para la detección molecular de los virus SARS-CoV2-Influenza A, Influenza B y virus respiratorio sincitial.
2		Sistema automatizado para la detección molecular del virus SARS-CoV-2 con extracción y amplificación en una única plataforma.
3	3.1 3.2	Sistema automatizado para la detección molecular de los virus SARS-CoV-2, Influenza A, Influenza B, en muestras urgentes. Sistema automatizado para la detección molecular de los virus SARS-CoV-2 en muestras urgentes.
4	4.1 4.2	Sistema automatizado para la detección molecular de los virus SARS-CoV-2, Influenza a, Influenza B y virus respiratorios sincitial en muestras urgentes Sistema automatizado para la detección molecular del virus SARS-CoV-2-en muestras urgentes.
5		Sistema automatizado para la detección molecular del virus SARS-CoV-2, mediante tecnología TMA.
6		Sistema para la detección molecular del virus SARS-CoV-2 y variante HV/69/70

4. REQUISITOS NORMATIVOS GENERALES Y EXCLUYENTES

Los reactivos 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 TECNICOS GENERALES

5.1 Requisitos técnicos informáticos aplicables al lote

Las especificaciones técnicas necesarias, pueden consultarse en el documento adicional Directrices y especificaciones técnicas informáticas (V05).

5.2 Número máximo de adjudicatarios por lote.

Un único adjudicatario por lote.

5.3 Número máximo de lotes a los que licitar

Seis lotes.

6. REQUISITOS TECNICOS EXIGIBLES Y EXCLUYENTES

6.1 Características generales de los laboratorios de la RDBO

Las características generales de los laboratorios son:

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

Automatización: El laboratorio deberá 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 deben garantizar que 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 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 técnicos generales exigibles y excluyentes

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 centros (Laboratorios de nodo principal y laboratorios de respuesta hospitalaria).

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.

Los equipos básicos que cada Unidad de Gestión Clínica de los laboratorios 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 horas y su manejo por personal a turnos.

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

6.3 Requisitos técnicos exigibles y excluyentes Lote 1

Sublote 1.1. Sistema automatizado para la detección molecular del virus SARS-CoV-2 con pool de mutaciones.

Técnica; Tecnología PCR Real Time multiplex molecular con retrotranscripción y amplificación en un solo paso.

Características; Deberá incluir todos los equipos necesarios para la extracción, amplificación, detección e interpretación de resultados con conexión bidireccional al SIL (sistema de información del laboratorio) así como su mantenimiento.

Dianas; Detección de al menos tres genes para la detección del coronavirus SARS CoV-2, con control interno endógeno y con capacidad de información de cada uno de ellos individualmente, incluyendo pool de mutaciones de las variantes Alfa, Beta, Gamma, Eta y Épsilon, en un mismo tubo de reacción.

Kits; Los kits deberán incluir todos los reactivos necesarios para la realización de las pruebas, incluyendo los reactivos, controles y consumibles de la extracción y amplificación, con control positivo, control negativo y control interno endógeno para monitorizar la calidad de la muestra analizada y para el control de la extracción y PCR.

Trazabilidad; Trazabilidad de muestras completa en todo el proceso mediante código de barras.

Software; Incluirá software con interpretación automática de resultados.

Sublote 1.2. Sistema automatizado para la detección molecular de los virus SARS-CoV-2-Influenza A, Influenza B y virus respiratorio sincitial.

Técnica; Tecnología PCR Real Time multiplex molecular con retrotranscripción y amplificación en un solo paso.

Características; Deberá incluir todos los equipos necesarios para la extracción, amplificación, detección e interpretación de resultados con conexión bidireccional al SIL y su mantenimiento.

Dianas; Detección de al menos tres genes para la detección del coronavirus SARS CoV-2, y las dianas de los virus Influenza A, Influenza B y virus respiratorios sincitial, con control interno endógeno y con capacidad de información de cada uno de ellos individualmente, en un mismo tubo de reacción.

Kits; Los kits deberán incluir todos los reactivos necesarios para la realización de las pruebas, incluyendo los reactivos, controles y consumibles de la extracción y amplificación con control positivo, control negativo y control interno endógeno para monitorizar la calidad de la muestra analizada y para el control de la extracción y PCR.

Trazabilidad; Trazabilidad de muestras completa en todo el proceso mediante código de barras.

Software; Incluirá software con interpretación automática de resultados.

6.4 Requisitos técnicos exigibles y excluyentes Lote 2

Sistema automatizado para la detección molecular del virus SARS-CoV-2 con extracción y amplificación en una única plataforma.

Técnica; Tecnología PCR Real Time multiplex molecular sin intervención del usuario desde la introducción de la muestra hasta la obtención del resultado en una única plataforma.

Tiempo de procesamiento (Incluida la obtención del resultado) Menor o igual a 180 minutos.

Características; Deberá incluir todos los equipos necesarios para la extracción, amplificación, detección e interpretación de resultados con conexión bidireccional al SIL y su mantenimiento.

Dianas; Detección de al menos los genes E y ORF1a/b para la detección del coronavirus-SARS Cov-2.

Kits; Los kits deberán incluir todos los reactivos necesarios para para la realización de las pruebas, listos para su uso, incluyendo todos los reactivos auxiliares, controles y resto de consumibles.

Trazabilidad; Trazabilidad de muestras completa en todo el proceso mediante código de barras.

Software; Incluirá software con interpretación automática de resultados.

Reactivos; Refrigerados.

6.5 Requisitos técnicos exigibles y excluyentes Lote 3

Sublote 3.1. Sistema automatizado para la detección molecular de los virus SARS-CoV-2, Influenza A e Influenza B, en muestras urgentes.

Técnica; PCR Real Time multiplex en muestra urgente.

Características; Sistema en cartucho cerrado que deberá incluir todos los componentes necesarios para la extracción, amplificación, detección e interpretación de resultados, con conexión bidireccional al SIL, así como su mantenimiento para el diagnóstico de la infección por los virus SARS-CoV-2, Influenza A e Influenza B en muestra urgente.

Tiempo de procesamiento (Incluida la obtención del resultado). menor o igual a 20 minutos.

Dianas; Detección de al menos los genes N y ORF1ab para la detección del coronavirus SARS-CoV-2, gen matriz del virus Influenza A y gen de la proteína no estructural del virus Influenza B.

Kits; Los kits deberán incluir todos los reactivos necesarios para la realización de las pruebas, listos para su uso, incluyendo todos los reactivos auxiliares, controles y resto de consumibles.

Trazabilidad; Trazabilidad de muestras completa en todo el proceso mediante código de barras.

Software; Incluirá software con interpretación automática de resultados.

Sublote 3.2. Sistema automatizado para la detección molecular del virus SARS-CoV-2 en muestras urgentes.

Técnica; PCR Real Time multiplex en muestra urgente.

Características; Sistema en cartucho cerrado que deberá incluir todos los componentes necesarios para la extracción, amplificación, detección e interpretación de resultados con conexión bidireccional al SIL, así como su mantenimiento para el diagnóstico de la infección por SARS-CoV-2 en un único equipo.

Tiempo de procesamiento (Incluida la obtención del resultado). Menor o igual a 20 minutos.

Dianas; Detección de al menos los genes N y ORF1ab para la detección del coronavirus-SARS- CoV-2.

Kits; Los kits deberán incluir todos los reactivos necesarios para para la realización de las pruebas, listos para su uso, incluyendo todos los reactivos auxiliares, controles y resto de consumibles.

Trazabilidad; Trazabilidad de muestras completa en todo el proceso mediante código de barras.

Software; Incluirá software con interpretación automática de resultados.

6.6 Requisitos técnicos exigibles y excluyentes Lote 4

Sublote 4.1. Sistema automatizado para la detección molecular de los virus SARS-CoV-2 Influenza A, Influenza-B y virus respiratorio sincitial en muestras urgentes.

Técnica; PCR Real Time multiplex en muestra urgente.

Características; Sistema en cartucho cerrado, que deberá incluir todos los componentes necesarios para la extracción, amplificación, detección e interpretación de resultados con conexión bidireccional al SIL, así como su mantenimiento para el diagnóstico de infección por los virus SARS-CoV-2, Influenza A, Influenza B y virus respiratorio sincitial en un único equipo.

Tiempo de procesamiento (Incluida la obtención del resultado). Menor o igual a 45 minutos.

Detección de genes; N2 y E (SARS-CoV-2), M, PB2 y PA (Influenza A), M, NS (Influenza B); Nucleocápside (VRSA/VRSB).

Kits; Los kits deberán incluir todos los reactivos, controles y consumibles necesarios para la realización de la prueba, incluyendo la extracción amplificación y controles internos listos para su utilización inmediata.

Trazabilidad; Trazabilidad de muestras en todo el proceso mediante código de barras

Conservación; Temperatura ambiente.

Sublote 4.2. Sistema automatizado para la detección molecular de los virus SARS-Cov-2-en muestras urgentes.

Técnica; PCR Real Time multiplex en muestra urgente.

Características; Sistema en cartucho cerrado que deberá incluir todos los componentes necesarios para la extracción, amplificación, detección e interpretación de resultados con conexión bidireccional al SIL, así como su mantenimiento para el diagnóstico de la infección por coronavirus SARS-CoV-2 en un único equipo.

Tiempo de procesamiento (incluida la obtención del resultado). Menor o igual a 60 minutos**.**

Detección de genes; N2 y E del coronavirus SARS-CoV-2.

Kits; Los kits deberán incluir todos los reactivos, controles y consumibles necesarios para para la realización de la prueba, incluyendo la extracción, amplificación y controles internos, listos para su utilización inmediata.

Trazabilidad; Trazabilidad de muestras en todo el proceso completa mediante código de barras.

Conservación; Temperatura ambiente

6.7 Requisitos técnicos exigibles y excluyentes Lote 5

Sistema automatizado para la detección molecular de los virus SARS-CoV-2, mediante tecnología TMA.

Técnica; Tecnología TMA (Amplificación mediada por transcripción) para la detección molecular de RNA de virus SARS-CoV-2.

Características; Deberá incluir todos los equipos necesarios para la extracción, amplificación, detección e interpretación de resultados con conexión bidireccional al SIL del laboratorio y su mantenimiento.

Tiempo de procesamiento (incluida la obtención del resultado). Menor o igual a cuatro horas.

Detección de genes; Deberá incluir la detección del gen ORF1ab.

Kits; Los kits deberán incluir todos los reactivos, controles y consumibles necesarios para para la realización de la prueba, incluyendo los reactivos y controles de extracción y amplificación.

Trazabilidad; Trazabilidad de muestras completa en todo el proceso mediante código de barras.

Conservación; Temperatura ambiente, refrigerados y/o congelados.

6.8 Requisitos técnicos exigibles y excluyentes Lote 6

Sistema para la detección molecular de los virus SARS-CoV-2 y variante HV/69/70

Técnica; Tecnología PCR Real Time multiplex molecular.

Características; Deberá incluir todos los equipos necesarios para la detección e interpretación de resultados con conexión al SIL y su mantenimiento.

Tiempo de procesamiento (incluida la obtención del resultado). Menor o igual a dos horas.

Dianas; Gen S (delección HV 69/70), OrF1ab, y gen N.

Kits; Los kits deberán incluir todos los reactivos necesarios para para la realización de las pruebas, en formato liofilizado, incluyendo los controles.

Conservación; Temperatura ambiente.

6.9. Middleware

El sistema proporcionará, al menos, las siguientes funcionalidades:

- La trazabilidad total de las muestras dentro del sistema.
- La gestión del control de calidad.
- La gestión remota del equipo y gestión de resultados y alarmas: revisión y validación técnica y facultativa, permitiendo la validación remota de pruebas.
- La gestión de las situaciones contingentes (fallo de un equipo, etc.) ofreciendo alternativas sencillas.
- La explotación de la información para la mejora del proceso.

7. VARIANTES TECNICAS

No se admiten.

8. MUESTRAS

No se admiten.

9. PLAZO Y LUGAR DE ENTREGA DEL SUMINISTRO

9.1 Plazo de entrega:

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

9.2 Lugar de entrega

El contratista estará obligado a entregar los bienes objeto del suministro en el lugar que se designe por cada una de las Organizaciones de Servicios de Osakidetza.

10. EJECUCION

10.1 Condiciones de ejecución.

El adjudicatario deberá:

a) 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.

b) Instalar y mantener el equipamiento y la tecnología, así como el material necesario, para que el laboratorio realice los **procesos**; recepcione, prepare, distribuya, procese y conserve las muestras.

c) 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 se 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 Mips.

d) 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.

e) Ofertar **equipos en redundancia** para asegurar el servicio ante incidencias en los laboratorios.

f) Asegurar la **renovación tecnológica** durante el periodo de vigencia del presente contrato. El licitador se compromete a actualizar el equipamiento durante la vigencia del concurso, así como a adecuarlo ante nuevas actividades no previstas inicialmente.

g) 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.

10.2. Otras condiciones del adjudicatario

10.2.1 Indicadores gestión clínica

Los licitadores deberán 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 UGCs o de personas o entidades en la que deleguen. Los indicadores deberán estar integrados en el sistema de información que la UGC utilice.

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

10.2.2 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.

10.2.3 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 programas de control de calidad internos, a elegir entre uno propio y otro de reconocido prestigio por el laboratorio, así como controles de calidad externos para todas las metódicas y equipos, que correrán a cargo del adjudicatario y serán también elegidos por el laboratorio.

Asimismo, el adjudicatario se compromete a facilitar sin cargo alguno, las adaptaciones necesarias en la documentación, en los procesos o en las conexiones informáticas para garantizar la consecución de la acreditación según la norma ISO-15189 en caso de que la UGC decidiera abordarla.

10.2.4 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).

Contendrá actualizados, al menos, los siguientes procedimientos:

Procedimientos normalizados de los equipos en formato electrónico que detallen los métodos y protocolos que se utilizarán, con su fundamento, la descripción de la preparación de reactivos o medios, la realización de las técnicas, los métodos de medida y los instrumentos necesarios.

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

10.2.5 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.

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

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… y todos los elementos que garanticen el correcto funcionamiento de los equipos.

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

10.2.6 Infraestructura auxiliar

El licitador deberá de proveer de la siguiente infraestructura auxiliar para dar soporte al sistema:

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

Adecuación de las instalaciones de fontanería y conexiones eléctricas e informáticas, si fuera necesario.

Adecuación de las instalaciones necesarias para garantizar un entorno de trabajo confortable, minimizando el ruido generado por los instrumentos, así como la disipación del calor generado por los mismos.

10.2.7 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.

11. 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 adjudicataria deberá facilitar la realización de sus tareas inspectoras, poniendo a su disposición cuanta información y documentos sean necesarios, así como facilitando el acceso a todas las dependencias e instalaciones.

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

12. 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:

iunzaga@osakidetza.eus Tfno. 94 4007368.

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

contrata@osakidetza.eus Tfno. 945006042.

ANEXO I Nº PRUEBAS ESTIMADAS CONTRATO INICIAL (2 AÑOS)

Lote	Sublote	Denominación	TOTAL PRUEBAS (2 AÑOS)
1	1.1	Sistema automatizado para la detección molecular del virus SARS-CoV-2 con pool de mutaciones.	160.029
	1.2	Sistema automatizado para la detección molecular de los virus SARS-CoV2-Influenza A, influenza B y virus respiratorio sincitial.	304.315
2		Sistema automatizado para la detección molecular del virus SARS-CoV-2 con extracción y amplificación en una única plataforma.	326.564
3	3.1	Sistema automatizado para la detección molecular de los virus SARS-CoV-2 Influenza A, influenza B en muestras urgentes.	110.901
	3.2	Sistema automatizado para la detección molecular del virus SARS-CoV-2 en- muestras urgentes.	20.000
4	4.1	Sistema automatizado para la detección molecular de los virus SARS-CoV-2, Influenza A, influenza B y virus respiratorio sincitial en muestras urgentes.	25.976
	4.2	Sistema automatizado para la detección molecular del virus SARS-Cov2-en muestras urgentes.	49.180
5		Sistema automatizado para la detección molecular del virus SARS-CoV-2, mediante tecnología TMA.	155.333
6		Sistema para la detección molecular del virus SARS-CoV-2 y variante HV/69/70.	175.201

Vitoria-Gasteiz, 13 de octubre de 2021

Fdo. Ana Quinteiro Garcia
Red de Diagnóstico Biológico Osakidetza

Osakidetza

DET - Directrices y Especificaciones Técnicas

Versión: v05

HOJA DE CONTROL

Título	DIRECTRICES Y ESPECIFICACIONES TÉCNICAS		
Entregable			
Nombre del Fichero	DET DyM_IOC v05.docx		
Autor	Osakidetza		
Versión/Edición	v05	**Fecha Versión**	01/07/2021
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

ÍNDICE

1 Objeto 4

2 Especificaciones para Desarrollo 5

2.1 Arquitectura de Referencia 6

2.1.1 Vista lógica 7

2.2 Directrices de Desarrollo 9

2.2.1 Construcción de Aplicaciones por Capas 9

2.2.2 Capa de Presentación 9

2.2.3 Capa de Negocio 11

2.2.4 Capa de Persistencia 13

3 Directrices tecnológicas de IOC 16

3.1 Entorno tecnológico 16

3.2 ESPECIFICACIONES DEL CLIENTE (MAQUETA) 20

3.3 Dispositivos de entrada/salida 22

3.4 Seguridad, acceso, autenticación y autorización 23

3.5 Monitorización 26

3.6 Backup/Restore 27

4 Interoperabilidad 28

4.1 Servicios Web 29

4.2 Gestor de Eventos 30

4.2.1 Estándares de comunicación 30

4.2.2 Mensajería. Definición de Evento 31

5 Explotación Información- Business Intelligence 33

6 Soluciones Móviles 34

6.1 Tecnologías Cliente 35

6.1.1 Apache Cordova 35

6.1.2 AngularJS 35

6.1.3 Ionic Framework 35

6.2 Tecnologías Servidor 36

6.2.1 Nginx 36

6.2.2 Node.js 36

6.2.3 MongoDB 36

7 Calidad de uso 37

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 competencia de la Subdirección de 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 diseño 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.

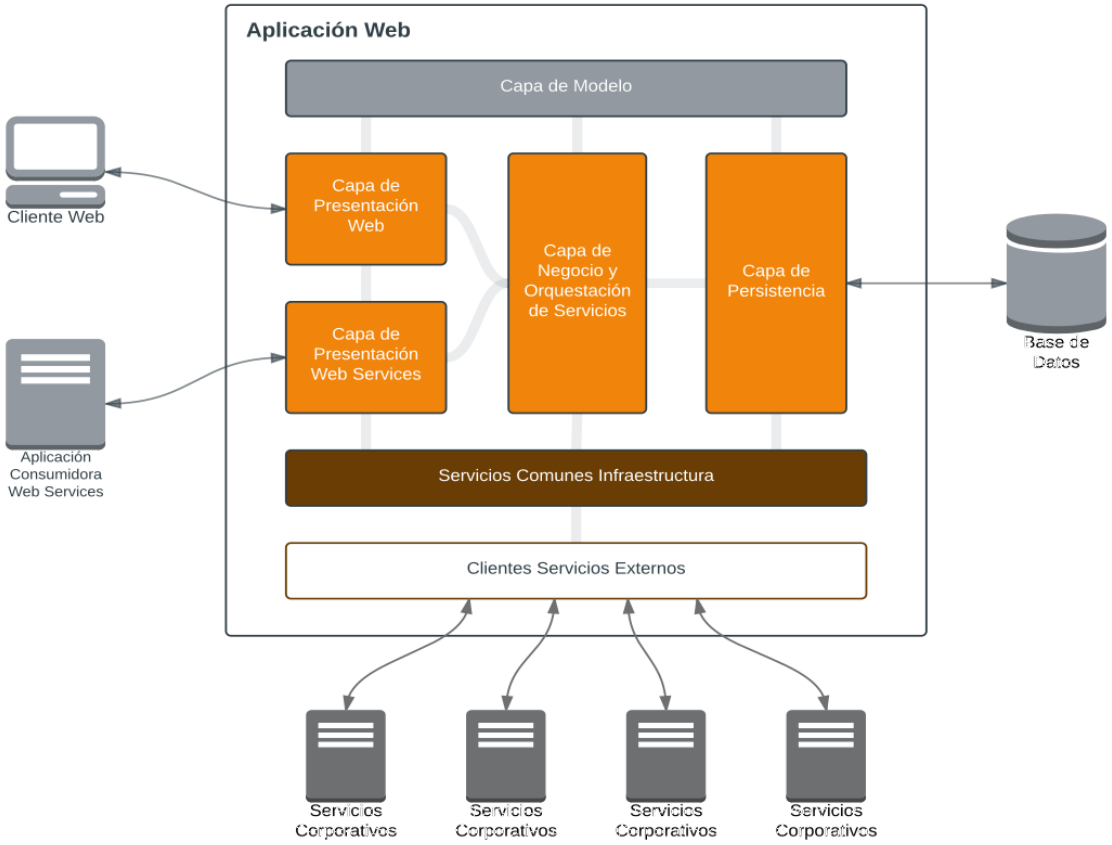


Figura 1. Vista lógica de la arquitectura de referencia

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 Directrices 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).

3.1 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.

3.2 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

3.3 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.

3.4 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.

3.5 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 la 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.

3.6 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.

4 Interoperabilidad

Los requisitos de integración de diversos sistemas de información de Osakidetza se realizaran 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

4.1 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 cubrirán 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

4.2 Gestor de Eventos

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

4.2.1 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.

4.2.2 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 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.

<u>Versiones utilizadas:</u>

- 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)

6 Soluciones Móviles

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

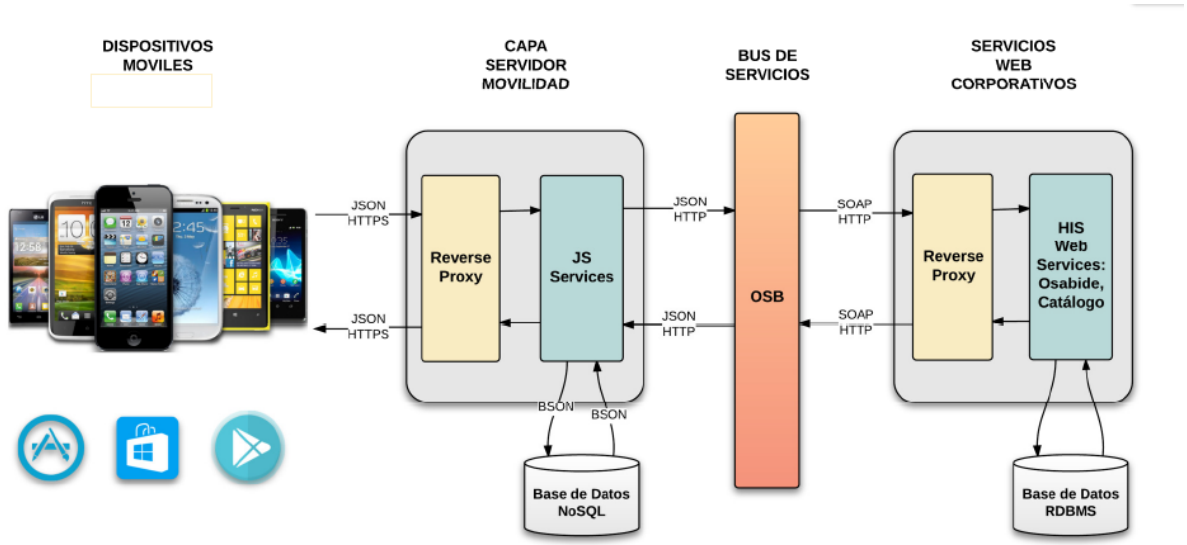
Comprende dos capas:

- 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.



6.1 Tecnologías Cliente

6.1.1 Apache Cordova

Apache Cordova es un framework para el desarrollo de aplicaciones.
Permite a los programadores desarrollar aplicaciones para dispositivos móviles utilizando herramientas genéricas tales como JavaScript, HTML5 y CSS3.
Las aplicaciones resultantes son híbridas, es decir que no son realmente aplicaciones nativas al dispositivo (ya que el renderizado se realiza mediante vistas web y no con interfaces gráficas específicas de cada sistema), pero tampoco se trata de aplicaciones web dado que son aplicaciones empaquetadas.

6.1.2 AngularJS

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.

6.1.3 Ionic Framework

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 Cordova.

6.2 Tecnologías Servidor

6.2.1 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.

6.2.2 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.

6.2.3 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 las base de datos relacionales, MongoDB guarda estructuras de datos en documentos tipo JSON con un esquema dinámico.

7 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.

Documento firmado por: ANA ISABEL
QUINTEIRO GARCIA
En la fecha 12.01.2022 11:10:28 CET