Contratación del análisis, diseño, construcción e implantación de un Sistema de Información de Contingencia para el Ámbito Asistencial en Osakidetza

Nº EXPTE.: 2020/01154

C/. Alava, 45 – 01006 VITORIA-GASTEIZ
Tfno. 945 006 000
www.osakidetza.euskadi.eus

Índice

Página

1 INTRODUCCIÓN 4
2 SITUACION ACTUAL 5
2.1 Estructura Organizativa de Osakidetza 5
2.2 Sistemas de Información Asistenciales 6
2.3 Antecedentes 8
3 OBJETO DEL CONTRATO 9
4 REQUISITOS FUNCIONALES DE LA SOLUCIÓN 12
4.1 Base de Datos de Contingencia 12
4.1.1 Contenidos: 13
4.1.2 Volcado de Datos a la Base de Datos Intermedia 14
4.1.3 Sincronización Bases de Datos Contingencia 16
4.2 Sistema de Administración del Plan de Contingencias 16
4.3 Aplicación WEB de Contingencia 17
5 REQUISITOS TÉCNICOS DE LA SOLUCIÓN 19
5.1 Alcance técnico de la solución 19
5.2 Entornos 19
5.3 Integración con Sistemas de información Corporativos 20
Osategi 21
e-Osabide. Atención Especializada (HIS hospitalario) 21
Osabide-AP 21
Osabide Global. Estación clínica 21
OsaNaia 22
OsaNaia 22
eOsabide. Farmacia 22
Presbide 22
Onkobide 22
Dietools 22
6 LINEAS DE TRABAJO 23
6.1 Análisis 23
6.2 Definición y diseño de arquitectura 23
6.3 Desarrollo de la solución 23
6.4 Instalación y configuración de la solución 23
6.5 Formación 24
6.6 Finalización del proyecto y Transferencia de Conocimiento 24
7 PRODUCTOS A OBTENER 25
8 PLANIFICACIÓN DEL PROYECTO 26

9 EQUIPO DE TRABAJO 27
10 CONTENIDO DE LAS OFERTAS 28
11 PROPIEDAD DE LOS PRODUCTOS 30
12 CONFIDENCIALIDAD 31
13 PRESUPUESTO, PLAZOS Y FORMA DE PAGO 32
13.1 Presupuesto 32
13.2 Plazos 32
13.3 Forma de pago 32
14 CONSULTAS AL PLIEGO 33
15 ANEXO I: VOLUMETRIA Y SOFTWARE DISPONIBLE 34
15.1 VOLUMETRIA: 34
15.2 Alcance J61 – HODEI 34
16 ANEXO II: ENTORNO TECNOLÓGICO Y METODOLOGÍA APLICABLE 36
16.1 Entorno Tecnológico 36
Arquitectura de la aplicación 36
Albergue de la aplicación 36
16.2 Metodología 36
SecDevOps – Equipo de Producto (Objeto de esta contratación) 36
PlatOps – Equipo de Plataforma (Aportado por Batera, fuera del ámbito de esta contratación) 37
Reparto de responsabilidades entre los dos equipos 37
17 ANEXO III: DOCUMENTO DE ARQUITECTURA Y TECNOLOGÍA (DET) 39
17.1 Arquitectura y tecnología 39
Consideraciones Tecnológicas 39
Dispositivos de entrada/salida 41
Seguridad, acceso, autenticación y autorización 41
Monitorización 43
Backup/Restore 44
17.2 Interoperabilidad 44
Servicios Web 45
Gestor de Eventos 46
17.3 Explotación Información- Business Intelligence 48
17.4 Calidad de uso 49

1 INTRODUCCIÓN

Durante las últimas décadas **Osakidetza** ha promovido e impulsado diferentes iniciativas en el área de las TIC con el objetivo de implantar la **Historia Clínica Electrónica** en Osakidetza, lo que conlleva la implantación progresiva de un complejo ecosistema de Sistemas de Información con un importante nivel de integración entre ellos y, en consecuencia, la **paulatina desaparición de la Historia Clínica en soporte papel**. Por este motivo, las Aplicaciones Asistenciales se han convertido en una herramienta indispensable para los profesionales de **Osakidetza** para la atención a los pacientes.

Toda la información que manejan en sus funciones cotidianas se encuentra en repositorios de informacion en formato digital, soportados por todo un despliegue de infraestructuras de hardware, software y elementos complementarios debidamente protegidos para garantizar la disponibilidad de los servicios críticos las 24 horas del día y los 365 días del año (24x7).

No obstante, siempre existen **amenazas** que pueden comprometer la disponibilidad de los sistemas, en caso de materializarse las consecuencias son críticas en aspectos de seguridad de paciente y calidad asistencial.

Es en este contexto en el que **Osakidetza** se plantea como objetivo el análisis, diseño, construcción e implantación de un **Sistema de Información de Contingencia en el Ámbito Asistencial,** que permita garantizar a los profesionales de **Osakidetza** la continuidad de su actividad asistencial cuando no se dan las condiciones idóneas necesarias para emplear las herramientas informáticas en las que se apoyan.

El proyecto tiene como **objeto** definir herramientas alternativas para continuar la actividad asistencial, que faciliten a los profesionales sanitarios el desempeño de su labor ante:

- Una parada planificada de los Sistemas de Información Asistenciales
- Una contingencia de origen técnico que provoque una pérdida de servicio, total o parcial, de los Sistemas de Información Asistenciales

Por estos motivos, con este documento se pretende establecer las bases técnicas para la contratación del análisis, diseño, construcción e implantación de un **Sistema de Información de Contingencia** que dé respuesta a las necesidades específicas de cada área asistencial, aunque sea prestando un servicio en **modo degradado**.

En definitiva, se plantea un sistema que permita facilitar la información básica de pacientes e historia clínica durante el periodo de tiempo determinado por la duración de la Contingencia, mientras se aplican las medidas necesarias para recuperar el servicio.

.

2 SITUACION ACTUAL

Osakidetza, dispone de una base instalada de **aplicaciones corporativas**, integrada tanto por desarrollos a medida como por productos de mercado, sobre los cuales da soporte a su actividad.

Estas soluciones se albergan en **Centros de Procesamiento de Datos (**CPDs) redundados a nivel de comunicaciones e infraestructuras, conformando plataformas de diversas tecnologías, escalables y tolerantes a fallos, aspectos imprescindibles para asegurar la continuidad de las funciones que proveen.

Dada la criticidad del negocio, todos los elementos que componen el sistema están continuamente sujetos a la aplicación de las medidas preventivas/correctivas que se derivan del **Plan de Continuidad TIC**, tanto de la propia Organización, como de la **Sociedad Informática de Gobierno vasco**(EJIE), como prestador de servicio de infraestructuras y operaciones de **Osakidetza**.

2.1 Estructura Organizativa de Osakidetza

Osakidetza está constituido por **Organizaciones de Servicios** que realizan las funciones de gestión y administración necesarias para la **provisión de servicios sanitarios**.

En el ámbito asistencial se basa en un modelo de **Organizaciones Sanitarias Integradas (OSIs)** que agrupan centros de atención primaria y su hospital de referencia en una demarcación geográfica definida en los tres territorios históricos de la Comunidad Autónoma del País Vasco, de la siguiente manera:

Araba/Álava:

- OSI Araba
  - Hospital Universitario Araba. Consultas Externas
  - Hospital Universitario Araba. Sede Txagorritxu
  - Hospital Universitario Araba. Sede Santiago
  - Ambulatorios y Centros de Salud
- OSI Rioja Alavesa
  - Hospital de Leza
  - Centros de Salud
- Red de Salud Mental Araba

Bizkaia:

- Hospital Gorliz
- Hospital Santa Marina
- OSI Barakaldo-Sestao
  - Hospital San Eloy
  - Centros de Salud
- OSI Barrualde-Galdakao
  - Hospital Galdakao-Usansolo
  - Hospital Gernika-Lumo
  - Centros de Salud
- OSI Bilbao-Basurto
  - Hospital Universitario Basurto
  - Ambulatorios y Centros de Salud

- OSI Ezkerraldea Enkarterri-Cruces
  -
  - Hospital Universitario Cruces
  - Centros de Salud
- OSI Uribe
  - Hospital de Urduliz-Alfredo Espinosa
  - Centros de Salud
- Red de Salud Mental Bizkaia

Gipuzkoa:

- OSI Alto Deba
  - Hospital Alto Deba
  - Centros de Salud
- OSI Bidasoa
  - Hospital Bidasoa
  - Ambulatorios y Centros de Salud
- OSI Debabarrena
  - Hospital Eibar
  - Hospital Mendaro
  - Centros de Salud
- OSI Donostialdea
  - Hospital Universitario Donostia
  - Ambulatorios y Centros de Salud
- OSI Goierri-Alto Urola
  - Hospital Zumarraga
  - Ambulatorios y Centros de Salud
- OSI Tolosaldea
  - Centros de Salud
- Red de Salud Mental Gipuzkoa

En total existen 13 Organizaciones Sanitarias Integradas (6 en Gipuzkoa, 5 en Bizkaia y 2 en Araba) las cuales en total incluyen 13 Hospitales de agudos, 153 centros de salud y 160 consultorios. La red además cuenta con Hospitales de Media y Larga estancia (Santa Marina y Gorliz) y la Red de Salud Mental.

2.2 Sistemas de Información Asistenciales

En el siguiente apartado se describe de manera general los principales sistemas de información en los que se apoyan los profesionales de ámbito sanitario en **Osakidetza**.

Catálogos Corporativos y Actividad Administrativa:

- ✓ **Osategi**: Se basa en un desarrollo a medida en tecnología JAVA (WEB), en la que se gestiona y mantiene la información de **Datos de Pacientes**. Incorpora el CIC (Código de Identificación Corporativo), elemento que identifica a un paciente de forma única en todos los sistemas.
- ✓ **eOsabide:** Se basa en un desarrollo a medida en tecnología JAVA (WEB), en la que se gestiona y mantiene toda la actividad administrativa relacionada con la asistencia sanitaria en las siguientes áreas:
  - Hospitalización

- Urgencias
- Consultas Externas (CCEE)
- Hospital de Día
- Hospital a Domicilio

✓ **OsabideAP:** Se basa en un desarrollo a medida en tecnología .net, en la que se gestiona y mantiene toda la actividad administrativa en:

- Atención Primaria

Estación Clínica (Historia Clínica):

✓ **Osabide Global:** Se basa en un desarrollo a medida en tecnología WPF .net.

Es la Estación Clínica Corporativa de Osakidetza de propósito general para todos los profesionales sanitarios: Médicos, Enfermeras, Matronas, Auxiliares de Enfermería, Farmacéuticos, etc

Se trata de un desarrollo a medida de naturaleza totalmente integradora, que interopera, por tanto, con todos los sistemas de información cuyo propósito es de ámbito sanitario, englobando toda la información que puede contribuir a formar parte de la Historia Clínica de los pacientes y que permite dar continuidad a todos los procesos asistenciales, facilitando la colaboración de los profesionales que intervienen dando una visión transversal de éstos.

Principales Sistemas de Información de Ámbito Sanitario:

✓ **OsaNaia:** Recoge y gestiona toda la actividad de enfermería en metodología basada en taxonomías de NANDA, NOC, NIC. (solución comercial de Bilbomática)

✓ **Farmacia:** Tratamientos de medicamentos y productos sanitarios durante los ingresos en las áreas de Urgencias, Hospitalización y de dispensación ambulatoria en pacientes externos. Desarrollo a medida.

✓ **Presbide:** Tratamientos de medicamentos y productos sanitarios en el circuito de receta electrónica, eRezeta**.** Desarrollo a medida.

✓ **Gestlab (Laborabide):** Gestión del laboratorio, petición y extracción de sangre, en fase de despliegue. (solución comercial de MIPS)

✓ **Onkobide:** Sistema de Gestión del proceso farmacoterapeútico del paciente oncológico (solución comercial de IMF)

✓ **Dietools** Sistema de Información para los servicios de cocina y preparación de menús y dietas. (solución comercial de Dominion)

✓ **Odolbide/e-delphyn:** Banco de sangre (solución comercial de Hemasoft)

✓ **Impax:** Radiología (solución comercial de Agfa)

✓ **Vitropath:** Anatomía Patológica (solución comercial de Vitro)

2.3 Antecedentes

Las Organizaciones de Servicios Integradas, por iniciativa propia, han trabajado en **Soluciones de Contingencia** basadas en **procedimientos internos**, cuyo objetivo fundamental consiste en establecer circuitos y operativas de trabajo coordinadas enfocadas a los procesos más críticos desde el punto de vista asistencial, como elemento de apoyo para orientar a los profesionales. Estos procedimientos se han dirigido a ámbitos locales y **no se están aplicando a nivel corporativo**.

Por otro lado, en la actualidad **Osakidetza** está trabajando en una solución de contingencia más rudimentaria que la que se plantean en este proyecto, **aplicación J61 HODEI.** Fundamentalmente, consisten en producir, en cortes temporales preestablecidos, documentación en archivos formato PDF y XML que recoge la información que se considera crítica en un primer nivel, desde los Sistemas de Información Asistenciales.

Estos documentos son albergados en una **BBDD no relacional**, **MongoDB**, para ser **distribuidos a equipos/servidores en la red**, agrupando los contenidos atendiendo a las características de ámbito de cobertura dentro de la estructura organizativa y áreas asistenciales a las que da servicio de contingencia desde cada ubicación de destino. El objetivo es acercar la información al punto más próximo posible donde se va a necesitar consumir.

Una solución similar se estaba ya aplicando en determinadas áreas de negocio, como la Farmacia Hospitalaria.

Está previsto que, para el momento de la adjudicación de este contrato, este sistema se encuentre plenamente operativo. Servirá de solución temporal durante el periodo de tramitación de este expediente y plazo de ejecución del mismo. Una vez esté implantado y operativo el Sistema de Contingencia objeto de este proyecto pasará a sustituir el sistema J61-HODEI.

3 OBJETO DEL CONTRATO

El objeto del presente expediente es el análisis, diseño, construcción e implantación de un nuevo sistema de información para Osakidetza, **Plan de Contingencia Asistencial** que permita a los profesionales continuar con su actividad clínica en situaciones de:

- Una parada planificada de los Sistemas de Información Asistenciales
- Una contingencia de origen técnico, y que provoque una pérdida de servicio, total o parcial, de los Sistemas de Información Asistenciales

Esta solución se caracterizará por cumplir los criterios funcionales y tecnológicos que a continuación se relacionan.

➢ **Requerimientos Funcionales:**

- Estará capacitado para **obtener y almacenar** en un nuevo repositorio la información mínima necesaria y pertinente para poder dar una atención rápida, ágil, integral y de calidad en escenario de contingencia.

- Incorporará mecanismos para **facilitar la correcta identificación de los pacientes**, incluyendo información de ubicación, actividad programada, así como asignación a Médicos de Familia/Pediatras y cupo de Enfermería para el área de Atención Primaria

- Disponer de la **Información Clínica Mínima** en un nuevo sistema, mediante la incorporación al mismo de la información clínico-asistencial ya existente en otros ámbitos.

- Este Sistema deberá **responder de forma ordenada y práctica**, a las diferentes necesidades asistenciales en cada área de atención.

- El sistema se diseñará desde la perspectiva de **escalabilidad funcional**, facilitando en un futuro, incorporar información de otros sistemas asistenciales/áreas funcionales no contemplados en el alcance inicial.

- Aplicará reglas de tratamiento de la información en función de los parámetros de **tiempo de obsolescencia de los datos** que se determinen el momento en el que se ha de recuperar la información de las fuentes originales.

- Aplicará las mismas **reglas de confidencialidad** en el acceso a la información clínica de los pacientes, en coherencia con los existentes en los sistemas de origen, salvo en las excepciones que en la fase de análisis se considere oportuno.

- **Trazabilidad. Protección de datos**: El sistema deberá generar la traza de los accesos realizados por los distintos usuarios en cumplimiento de la legislación vigente en materia de protección de datos de carácter personal. Para ello se integrará con el sistema de trazabilidad corporativo.

- **Requerimientos Tecnológicos:**

  - El sistema estará diseñado para, en situación de contingencia, **funcionar de forma totalmente autónoma**, por lo que no deberá depender ni compartir ningún elemento TI (Hardware o software) que forme parte del ecosistema productivo

  - La solución propuesta debe ser **accesible** tanto a través de navegadores modernos, como de dispositivos móviles. Tanto el diseño como el contenido tiene que estar adaptado a dispositivos móviles, tablets, smartphone y ser **responsive**.

  - Los **procesos de recolección** de información desde los Sistemas de información productivos se diseñarán de forma que no comprometan la **calidad del servicio** ofrecido a los usuarios

  - El nuevo Sistema de Contingencias cumplirá con los requerimientos tecnológicos necesarios para ser administrado y servidos en las siguientes **modalidades de albergue**:
    - En un **CPD** a determinar por Osakidetza/EJIE
    - Desde plataformas de **Cloud Computing**.

  - Debe de tener en cuenta los principios de **accesibilidad** (Real Decreto 1494/2007, Directiva (UE) 2016/2102)

  - La solución propuesta deberá ser **multi-idioma**, garantizando al menos la implantación en euskera, castellano. La traducción de los textos se realizará por parte de **Osakidetza**.

  - La autenticación de acceso al sistema se realizará a través del Directorio Activo (LDAP) de **Osakidetza**.

  - La herramienta debe de cumplir con la regulación europea de protección de datos, conocida como **Reglamento General de Protección de Datos**, en cuanto a la metodología para incluir la privacidad desde el diseño. Se incluirá la realización del Análisis de Riesgos para Derechos y Libertades de las personas y si procede, la Evaluación de Impacto sobre la Protección de Datos.

El alcance del proyecto abarca todas las tareas necesarias para llevar a cabo los servicios demandados en el presente Pliego de Bases Técnicas, que se resumen en las líneas de trabajo siguientes:

- Estudio de especificaciones
- Diseño de la solución
- Desarrollo según los requerimientos indicados.
- Implantación y despliegue de la solución en todas las Organizaciones de Servicio de **Osakidetza**, incluyendo las tareas de formación y soporte durante la vigencia del contrato.

No se incluyen en el proyecto los suministros de hardware y elementos de telecomunicaciones necesarios para el adecuado funcionamiento del sistema global.

Para llevar a cabo las tareas detalladas anteriormente, el licitador pondrá a disposición de **Osakidetza** los recursos humanos necesarios en cada momento.

4 REQUISITOS FUNCIONALES DE LA SOLUCIÓN

El objeto del presente expediente es el análisis, diseño, construcción e implantación de un nuevo sistema de información para Osakidetza, **Sistema de Contingencia Asistencial,** que permita a los profesionales continuar con su actividad clínica en situaciones de:

- Una parada planificada de los Sistemas de Información Asistenciales
- Una contingencia de origen técnico, y que provoque una pérdida de servicio, total o parcial, de los Sistemas de Información Asistenciales

Se propone el desarrollo e implantación de una solución informática, Aplicación Web de Contingencia, que facilite la información de pacientes e historia clínica suficiente para que, en caso de activación del Plan de Contingencia, los profesionales del ámbito sanitario puedan identificar y conocer la situación de los pacientes a los que deben asistir durante el tiempo de recuperación de servicio (RTO).

Los dispositivos/herramientas cuyo objetivo sea dar servicio durante el tiempo de contingencia, no deberán compartir activos en los que se desarrolla la actividad en situación de normalidad (Sistemas Productivos). Se plantea albergar dichas herramientas en un entorno aislado, bien en un CPD aparte o en una plataforma de Cloud Computing, cuyos servicios de alberque y administración no son objeto de este contrato.

Además de lo indicado en el apartado objeto del contrato, se deben cubrir al menos los requerimientos recogidos a continuación.

4.1 Base de Datos de Contingencia

La **Base de Datos de Contingencia** albergará toda la información necesaria para garantizar las mínimas condiciones para la práctica asistencial, sin depender de ningún componente hardware y/o software que forme parte del entorno operacional y cuyo servicio pueda verse comprometido ante una incidencia en el servicio.

Es obvio que la captura de información sólo se podrá realizar cuando los sistemas operacionales se encuentren disponibles, es decir, en situación de normalidad del servicio.

Para garantizar la plena autonomía del sistema de contingencia en caso de interrupción del servicio, se plantea una **arquitectura basada en bases de datos sincronizadas entre ellas**, de la siguiente forma:

1.- **Base de datos Intermedia de Contingencia:** para el aprovisionamiento de la información: En este sistema se volcarán y actualizarán los datos recogidos de los Sistemas Operacionales, teniendo en cuenta el tiempo de vigencia que se establece para la validez del dato en caso de activación de contingencia (caducidad del dato).

A la firma de contrato, se realizará la transferencia de los elementos software y BBDD desarrollados en la aplicación J61 – HODEI, con el objeto de facilitar la reutilización de la misma. La empresa adjudicataria recibirá la documentación y

sesiones formativas que aseguren el proceso de transferencia en condiciones adecuadas, que permitan determinar la pertinencia o no de evolucionar el sistema y adaptarlo, en caso afirmativo, para su uso en la solución ofertada.

2.- **Base de datos de Contingencia**: Réplica de la base de datos intermedia. En situación de Activación del Plan de Contingencia, se aislará de forma inmediata para pasar a dar servicio a la Aplicación de Contingencia.
No se consideran objeto del proyecto las tareas que se deriven de la sincronización de estas Bases de Datos, estas tareas serán asumidas por el equipo técnico que EJIE ponga a disposición del proyecto.

4.1.1 Contenidos:

Siguiendo los criterios que un **equipo interdisciplinar de Osakidetza** ha consensuado en diversas sesiones de trabajo, con la participación de profesionales clínicos de la Organización, la información mínima para dar servicio asistencial en modo degradado es la siguiente:

- **Área Catálogos Corporativos:** Contiene la información necesaria para gestionar y distribuir la información de forma adecuada atendiendo a las particularidades de cada área asistencial y centro de conexión del profesional.
    - Estructura Organizativa: [eOsabide]
        - Organización de Servicios Integrada
        - Áreas Asistenciales
        - Servicio
        - Sección
        - Centros
        - Unidad de Enfermería
    - Profesionales: [eOsabide]

- **Área Paciente:** Asegurar la correcta identificación y localización del paciente es la base para dar continuidad a la asistencia clínica, esto implica disponer de los datos demográficos y administrativos de los pacientes, así como la actividad asociada para su localización/ubicación en las distintas áreas asistenciales.
    - **Datos Demográficos y administrativos de pacientes** [Osategi]
    - **Censos**:
        - Urgencias [eOsabide]
        - Ingresos [eOsabide]
        - Pre-admisiones [eOsabide]
        - Hospital de día: Hemodiálisis y paciente Oncológico [eOsabide]
        - Hospitalización a Domicilio [eOsabide]
        - Programación Quirúrgica [eOsabide]

- Programación Actividad Ambulatoria: Consulta externa, Radiodiagnóstico, Rehabilitación, Radioterapia, Pruebas funcionales diagnostico-terapéuticas [eOsabide]
- Programación Actividad de Atención Primaria [OsabideAP]
- Cocina: Censo de Dietas y Menús [Diettools]

- **Área Historia Clínica (Información Clínico-Asistencial):**
  - Informe de Historia Clínica Resumido (HCR): Informe contenido en el proyecto de Historia Clínica Digital del Sistema Nacional de Salud. [Osabide Global]

    Este informe se construye en Osabide Global a través de un servicio que se encarga de recoger la información existente en Osabide Global y la que está distribuida en otros sistemas, para componer el informe completo.

    - Alergias.
    - Vacunaciones.
    - Problemas resueltos, cerrados o inactivos.
    - Problemas y Episodios activos.
    - Tratamiento:
      - Recomendaciones.
      - Fármacos.

    Diagnósticos Enfermeros activos (Código NANDA).
    Resultados de Enfermería (Código NOC).
    Intervenciones de Enfermería (Código NIC).
    Alertas.
  - Unidosis. Prescripción en Ámbito Hospitalario. [eOsabide]
  - Onkobide: Tratamiento de paciente oncológico [Onkobide]
  - Evolutivo: [Osabide Global]
    - Ámbito de la hospitalización convencional y hospitalización a Domicilio: cinco últimas anotaciones.
    - Ámbito de la actividad ambulatoria hospital de día Médico. Dos últimas anotaciones, más la impresión diagnostica, por cada episodio ambulatoria abierto.
    - Actividad área de Urgencias.
    - Actividad área de Atención Primaria. Dos últimas anotaciones.
  - Plan de cuidados de enfermería: [OsaNaia]
    - Ámbito Ambulatorio. Ultimo disponible.
    - Ámbito de Hospitalización: Gradual.

4.1.2 Volcado de Datos a la Base de Datos Intermedia

Será objeto de este contrato el desarrollo de **los procesos de extracción y carga** que permitan disponer de los datos actualizados con la periodicidad y nivel de actualización del dato establecido para cada área asistencial y tipo de información.

Será necesario diferenciar procesos para:

- Las cargas iniciales necesarias previas al arranque del sistema
- Las actualizaciones y/o cargas incrementales
-

A continuación, como referencia, se indican los momentos del día en los que deseablemente se deberá generar y actualizar la información. Estos horarios están sujetos a cambios en función de los requerimientos funcionales y técnicos que se vayan adoptando durante la ejecución del proyecto, por lo que deberán ser administrados desde el propio sistema. Cualquier variación respecto a lo propuesto deberá realizarse bajo la supervisión y previa autorización del Servicio de Informática y Sistemas de Información de Osakidetza.

- **Catálogos Corporativos:** Carga inicial y volcado nocturno
- **Pacientes-Datos demográficos y administrativos:** Carga inicial y actualización de todas las modificaciones que se produzcan
- **Pacientes-Censos:**
  Hospitalización: 8:00/17:00/22:00 Horas.
  Urgencias: cada dos Horas.
  Pre-Admisión: 23:59 Horas.
  Bloque Quirúrgico: 23:59 Horas.
  Hospital de Día Médico: 23:59 Horas.
  Hospital a Domicilio: 23:59 Horas.
  Consulta Externa: 23:59 Horas.
  Atención Primaria: 14:00/23:59 Horas.
  Dietas: 12:00/20:00/23:59 Horas.
- **Historia Clínica (Información Clínico-Asistencial) - Informe de Historia Clínica Resumido** (HCR): Carga inicial y actualización cada vez que se realiza un contacto (Apunte en la Historia clínica) ** Se valorará pertinencia de disminuir la frecuencia de carga en Hospitalización y realizarlo en los horarios establecidos para los censos
- **Farmacia: Unidosis hospitalaria. Farmacia Ambulatoria.**
  Hospitalización: 8:00/14:00/20:00/23:59 Horas.
  Bloque Quirúrgico: 12:00/15:00/22:00 Horas.
  Hospital de Día Médico: 12:00/15:00/22:00 Horas.
  Hospital a Domicilio: 12:00/15:00/22:00 Horas.
  Urgencias: 8:00/12:00/15:00/22:00 Horas.
- **Onkobide:** Carga inicial y actualización cada vez que se realiza un contacto (Apunte en la Historia clínica)
- **Evolutivos:** Carga Inicial y cada vez que se realiza un contacto (Apunte en la Historia clínica) ** Se valorará pertinencia de disminuir la frecuencia de carga en Hospitalización y realizarlo en los horarios establecidos para los censos
- **Plan de Cuidados de Enfermería:** Carga Inicial y cada vez que se realiza un contacto (Apunte en la Historia clínica de OsaNaia) ** Excepto Hospitalización *14:00/20:00/23:59 Horas.*

Para la obtención de esta información, será necesario desarrollar o adaptar el software de los Sistemas de Información Asistenciales de la siguiente forma:

1. Desarrollo de nuevos servicios de integración en los sistemas de información corporativos

2. Optimización y adecuación de servicios ya existentes en los sistemas de información corporativos

3. Procesos planificados para la extracción de la información

El desarrollo y/o adaptación de software relacionados con los sistemas de información corporativos derivados de este proyecto, se incluyen dentro del alcance del mismo. Es por ello que deberá existir una coordinación permanente con el adjudicatario del mantenimiento de esos sistemas de información, que proveerá la documentación necesaria para los desarrollos a realizar.

La implantación y despliegue de los nuevos servicios o sus adaptaciones, será supervisada y coordinada por Osakidetza.

4.1.3 Sincronización Bases de Datos Contingencia

Como ya se ha indicado anteriormente, las necesidades relacionadas con el sistema de sincronización de las bases de datos intermedia y de contingencia correrán a cargo de EJIE, no obstante, la solución ofertada deberá ser técnicamente compatible con este objetivo.

4.2 Sistema de Administración del Plan de Contingencias

El sistema deberá incluir un **módulo que permita al usuario con perfil de administrador**, gestionar información relativa a los parámetros de configuración, así como administrar y monitorizar todo el sistema.

- Permitirá definir **roles y usuarios** que podrán realizar las funciones que se asignen:
  - Activación/Desactivación por ámbito organizativo
  - Envío comunicaciones (avisos) por ámbito organizativo
  - Simulacros
  - Trazabilidad LOPD
  - Consultas
- Permitirá **monitorizar** y administrar todo lo relativo a la ejecución de los procesos de carga:
  - Horarios establecidos para cada área
  - Periodo temporal establecido para la actividad programada (espacio temporal a futuro)
- Desde este módulo se podrán realizar las tareas propias de la **activación/desactivación del sistema** de forma total o parcial dentro de la Estructura Organizativa
- Se podrá **activar/desactivar el sistema en "Modo Simulacro"**, que podrá ser sometido a chequeo para verificar el correcto funcionamiento del sistema
- El sistema dispondrá de un **sistema de publicación de avisos** para comunicar a los usuarios de la situación durante el periodo de contingencia

- Se podrá consultar la información de **accesos a HC** (trazabilidad LOPD)

- Se podrá acceder a **consultas** de situación:
  - Volumen de información almacenada en el repositorio en cada momento
  - Fecha de última actualización de la información
  - Información histórica de activaciones reales y simulacros realizados: Ámbito de activación, duración, usuario de activación, nº de usuarios que han accedido durante la contingencia…

Los usuarios con acceso a solución descrita, se validarán contra la plataforma corporativa LDAP de **Osakidetza.** Dado que el sistema debe garantizar plena autonomía respecto a los elementos comunes del entorno operacional, EJIE será el encargado de ofrecer una alternativa que cubra los requerimientos de autenticación en condiciones de contingencia, desde la nube o en un CPD aparte.

4.3 Aplicación WEB de Contingencia

Se propone el desarrollo de una **aplicación web** que, en caso de activación del plan de contingencia, permitirá acceder y navegar en la información de pacientes, censos, actividad programada e información básica de Historia Clínica a los profesionales sanitarios en **Osakidetza**.

La aplicación autorizará el **acceso** únicamente a los profesionales asignados a los centros afectados por la contingencia (ámbito de activación) y siempre a los profesionales autorizados en caso de simulacro.

El acceso a la información de pacientes se realizará teniendo en cuenta los **criterios de confidencialidad** que rigen los Sistemas de Información Asistenciales, de la siguiente forma:

- Atención Primaria:
  - Búsqueda de pacientes: Acceso abierto a todos los pacientes de la Unidad de Atención Primaria, mediante búsquedas por los criterios de Nombre, Apellidos, DNI, TIS, CIC, etc…
  - Acceso a los pacientes citados en las agendas de los centros pertenecientes a la Unidad de Atención Primaria

- Puntos de Atención Continuada (PACs):
  - Búsqueda de pacientes: Acceso abierto a todos los pacientes de las Unidades de Atención Primaria pertenecientes a la Organización de Servicios Integrada, mediante búsquedas por los criterios de Nombre, Apellidos, DNI, TIS, CIC, etc…

- Urgencias Hospitalarias:
  - Búsqueda de pacientes: Acceso abierto a todos los pacientes de las Unidades de Atención Primaria pertenecientes a la Organización de

Servicios Integrada, mediante búsquedas por los criterios de Nombre, Apellidos, DNI, TIS, CIC, etc…
  - Censo de Urgencias

- Resto de Áreas Asistenciales: acceso exclusivo a pacientes incluidos en los censos correspondientes
  - Hospitalización
  - Pre-Admisión
  - Bloque Quirúrgico
  - Hospital de Día Médico
  - Hospital a Domicilio
  - Consulta Externa
  - Información de Dietética y Menús

El **acceso a los datos clínicos** se realizará a partir de la búsqueda de un paciente o de la selección de un paciente en el censo en que se esté trabajando.

La visualización de datos de Historia Clínica será completa, salvo en el caso de los profesionales de **Cocina**, que únicamente podrán consultar la información asociada a los menús

El sistema deberá garantizar la **trazabilidad** de todos los accesos realizados durante el tiempo en el que el sistema se encuentra operativo. El registro de trazabilidad podrá ser consultado desde el Módulo de Administración y será sincronizado en la BBDD de Contingencia Intermedia una vez se haya recuperado el servicio. Se dará la posibilidad de volcar la información de trazas a alguno de los sistemas de información operacionales.

Desde todas las pantallas del sistema se dará **acceso a utilidades del sistema**, al menos las siguientes:

- Lectura de avisos que se publiquen desde el módulo de administración del sistema.
- Documentación de interés como: Manual de usuario, Procedimiento de Contingencia, etc…

5 REQUISITOS TÉCNICOS DE LA SOLUCIÓN

5.1 Alcance técnico de la solución

El Sistema propuesto debe cumplir los siguientes requisitos:

- El licitador quien deberá proponer el modelo de Desarrollo que considere óptimo, para la correcta operativa del sistema y para garantizar la operatividad del servicio en situación de contingencia, independientemente de cual haya sido la causa que provoca la pérdida de servicio. El modelo propuesto deberá ser aprobado por **Osakidetza**, valorándose aquellas soluciones que se adecúen a los estándares de **Osakidetza** (Anexos II y III), facultándose a ésta el derecho de modificarlo.

- El licitador deberá detallar en su oferta las **necesidades de infraestructura** de soporte al sistema. **Osakidetza** una vez aprobado el dimensionamiento propuesto, será responsable del suministro de la misma.

- La solución ofertada debe estar preparada para su **monitorización, soporte y mantenimiento en remoto.**

- La solución propuesta deberá ser **accesible** a través de navegadores modernos, tablets y smartphones. El sitio WEB debe de estar optimizado para todos los dispositivos desde los que se vaya a acceder. El **diseño** tiene que estar adaptado a dispositivos móviles y ser **responsive**.

- La elección, adquisición y administración de los dispositivos portátiles o tablets no forman parte del alcance de este contrato.

- La solución a desarrollar debe integrarse con el **Directorio Activo** de Osakidetza, o en su defecto, el que ponga a disposición del proyecto.

- El licitador deberá **proponer el modelo de arquitectura** que considere óptimo para poder ser alojado en un CPD o en plataformas de Cloud Computing. El modelo propuesto deberá ser aprobado por **Osakidetza**.

- La solución propuesta, deberá proponer las **soluciones tecnológicas adecuadas para la captura y actualización de la información**, teniendo en cuenta el volumen de información a generar y actividad diaria desarrollada (Anexo I), sin que supongan un riesgo en la **calidad del servicio** de los Sistemas Operacionales**.**

5.2 Entornos

Los entornos a utilizar en el proyecto y para los cuales deberán ser suministradas las licencias suficientes, serán los siguientes:

- **Entorno de Pre-producción/certificación (integración):**
  - **Osakidetza** se hará cargo de la gestión de este entorno.
  - Su finalidad es la de las pruebas de carga y certificación de arranques o nuevas versiones de productos

- **Entorno de Producción:**
  - **Osakidetza** se hará cargo de la gestión de este entorno.
  - En caso de que se conceda acceso al entorno de producción a usuarios técnicos, el acceso se realizará bajo las condiciones previstas en este contrato con respecto al registro de accesos y las circunstancias que puedan justificar ese acceso.

Los entornos de trabajo se ubicarán en el CPD / Plataforma Cloud que **Osakidetza** ponga a disposición del proyecto.

5.3 Integración con Sistemas de información Corporativos

Para cubrir las necesidades de captura de datos enunciadas anteriormente, se podrán utilizar las siguientes tecnologías:

- **Generación/consumo de eventos** con mensajes: Cuando alguna información que se debe compartir se registre en el sistema ofertado se generarán eventos para propagar dicha información a los sistemas que se encuentren suscritos a dichos eventos. Igualmente, cuando algún sistema externo genere información que deba recibir la aplicación ofertada generará eventos para que ésta pueda consumirlos.

- **Publicación/acceso a servicios web**: El sistema ofertado publicará información mediante servicios web que puedan ser consumidos en cualquier momento por las aplicaciones que lo necesitaran. Igualmente podrá invocar a los servicios web del resto de aplicaciones cuando fuera necesario.

- Dada la naturaleza del proyecto, se podrán plantear **soluciones alternativas de volcado de datos desde los Sistemas propietarios** del dato hacia el nuevo sistema, siempre y cuando la propuesta sea valorada y aceptada por **Osakidetza**.

El licitador deberá definir de forma detallada en su oferta el modelo de integración propuesto, que deberá cumplir los estándares detallados en los **Anexos II y III**.

La solución propuesta deberá, además, tener en consideración las siguientes necesidades:

- **Osakidetza** dispone de una arquitectura SOA (Service Oriented Architecture) para gobernar y orquestar los servicios disponibles en la organización. El sistema de información ofertado deberá inventariar y hacer públicos los contratos de los servicios que pondrá a disposición de otros sistemas de información.
- Los requisitos de integración on line del sistema ofertado deberán de ser resueltos mediante uno de estos dos métodos:
  - ✓ Escenario 1 - Propagación y consumo de eventos: Event Manager (desarrollo propio)
  - ✓ Escenario 2 - Consumo de servicios: Oracle SOA Suite (Oracle BPEL Process Manager, Oracle Service Bus, Oracle Business Rules, ...)
- Utilización de mensajería HL7, debiendo aceptar las versiones HL7 2.x (no XML) y 3, y debiendo adaptarse a las evoluciones que se realicen desde **Osakidetza** en la adopción de nuevas versiones.
- Utilización del estándar CDA como arquitectura de documentos clínicos electrónicos.

- El modelo definido deberá permitir la implementación de integraciones fuera de estándar en aquellas que **Osakidetza** considere, y únicamente en aquellas que dicha entidad permita.
- Todas las integraciones entre los aplicativos deben registrar la traza en el registro de accesos exigido por la LOPD e identificar unívocamente a cada usuario que accede.

Los sistemas de información a considerar son:

Osategi
Sistema de Información de Gestión de datos de Pacientes Corporativo.

Este sistema tiene como característica principal su integración online y bidireccional con la base de datos poblacional del Departamento de Salud: SIABP.

Tecnología: J2EE y Oracle

e-Osabide. Atención Especializada (HIS hospitalario)
HIS corporativo de **Osakidetza** en el que se registra toda la actividad realizada en el ámbito de la Hospitalaria.

Este sistema gestiona todos los Catálogos Corporativos de uso en el ámbito Asistencial. Entre ellos, Estructura Organizativa y Profesionales.

Tecnología: J2EE y Oracle

Osabide-AP
Estación clínico-administrativa de Atención Primaria.

Tecnología: VB .net y Oracle

Osabide Global. Estación clínica
Estación Clínica de Osakidetza. Desde este sistema el clínico puede realizar cualquier acto médico interactuando con cualquiera de los sistemas departamentales, consolidando la verdadera Estación Clínica.

Se compone de diferentes módulos que constituyen Sistemas de Información diferenciados en sí mismos, pero que comparten la misma base de información de la HC:

- Urgencias: Orientado al Área Asistencial de Urgencias
- Hospitalización: Orientado al Área Asistencial de Hospitalización tradicional
- CCEE: Orientado al Área Asistencial de Consultas Externas
- Hospitalización a Domiciliación a Domicilio
- Hospital de Día
- Atención Primaria: Orientado al Área Asistencial de Atención Primaria, es el último módulo que se ha desarrollado en Osabide global y que sustituye a OsabideAP en su funcionalidad clínica.

Tecnología: .NET WPF y Oracle

OsaNaia

Solución propietaria de la empresa Bilbomática para la gestión de los cuidados de enfermería. Se basa en las taxonomías NANDA, NIC, NOC

Tecnología: .NET WPF y Oracle

OsaNaia

Solución para la gestión de los cuidados de enfermería. Se basa en las taxonomías NANDA, NIC, NOC
Producto Comercial, propiedad de la empresa Bilbomática

eOsabide. Farmacia

El HIS corporativo de **Osakidetza** incluye un módulo de Farmacia para la prescripción, dispensación y administración de la medicación en el ámbito de la Hospitalaria.

Tecnología: J2EE y Oracle

Presbide

Sistema de Prescripción de Medicamentos y Productos Sanitarios para todos los profesionales sanitarios, integrado con el sistema de Receta Electrónica de la CAPV (eRezeta)
Incorpora el Historial Farmacoterapeutico del paciente.

Tecnología: J2EE y Oracle

Onkobide

Solución software que cubre el circuito completo de prescripción en el paciente oncológico (prescripción, validación, preparación y administración).
Instalación del Producto Comercial Farmis_Oncofarm, propiedad de la empresa IMF

Dietools

Solución para la gestión de la cocina y la dietética en los centros.
Producto Comercial Dietools, propiedad de la empresa Dominion

6 LINEAS DE TRABAJO

6.1 Análisis

Será necesario definir en las primeras fases de este proyecto, un análisis para contrastar las ideas propuestas por el licitador.

En esta fase se planificarán las sesiones de transferencia de la aplicación J61-HODEI.

Es por ello, que el licitador deberá incluir en su propuesta el equipo de consultores que en colaboración con los interlocutores que **Osakidetza** designe, **definirán un "modelo tipo del diseño y contenidos de la solución"**, que una vez aprobado, se desarrollará según plan establecido.

En esta fase también se deberá realizar el Análisis de Riesgos para Derechos y Libertades de las personas y si procede la Evaluación de Impacto sobre la Protección de Datos, esta documentación, servirá para describir el sistema desde el punto de vista de cómo afecta a la protección de datos y a la seguridad de la información, de modo que, si se detectan riesgos de seguridad, se establecerá el plan de tratamiento de riesgos.

6.2 Definición y diseño de arquitectura

Definición y diseño de la arquitectura, y de las necesidades de sistemas, componentes y elementos de software que garanticen la escalabilidad y continuidad del servicio.

En el apartado se deberá incluir una descripción detallada de la infraestructura requerida para los diferentes entornos de trabajo

El diseño de arquitectura planteado deberá tener el visto bueno de **Osakidetza**.

6.3 Desarrollo de la solución

En esta línea de trabajo se diseñará y construirá la solución (tanto la **aplicación web** como el **repositorio de datos de contingencia**) según los requerimientos indicados en la fase de análisis.

En esta línea de trabajo se realizarán al menos las siguientes actividades:

- Construcción/parametrización de la solución.
- Procesos de captura de datos (migración) y almacenamiento en las BBDD de Contingencia
- Construcción de aplicación web de contingencia.
- Diseño de pruebas: integradas (casos de uso).
- Pruebas de rendimiento y carga.

6.4 Instalación y configuración de la solución

En esta línea de trabajo se llevarán a cabo las actividades de implantación de la solución ofertada, en base al diseño de arquitectura definido, entregándose la documentación técnica de la solución que se mantendrá actualizada durante la vigencia del contrato.

6.5 Formación

La planificación, gestión y ejecución de la formación, correrá a cargo del proveedor, que formará directamente a los siguientes tipos de usuarios:

- **Formación a Referentes de la Organización:** el adjudicatario formará a los referentes de la organización que indique la dirección del proyecto., que previsiblemente puedan tener papel activo en situaciones de contingencia. La formación deberá ser la suficiente para que los referentes puedan realizar la formación en cascada. Esta formación se realizará antes de la puesta en marcha de la solución.

- **Formación técnica**: orientada al departamento de informática y enfocada a la administración de la aplicación y a las herramientas de desarrollo y programación inherentes, si es que las hubiera. Esta formación se realizará antes de la puesta en marcha de la solución.

La documentación de los cursos de formación, así como la documentación y guías de uso de las diferentes funcionalidades que ofrezca la solución ofertada, es tarea del proveedor, que deberá proporcionar puntualmente antes de que cualquier formación tenga lugar o cualquier funcionalidad entre en producción.

El licitador entregará en la oferta una planificación detallada que explique el alcance de los contenidos de formación y en el que se deberá indicar el número de horas previstas de formación para los usuarios y para el personal de informática. Este número de horas es orientativo y en ningún caso será el límite de horas a impartir si la formación no ha llegado al nivel adecuado para la adopción de sistema.

6.6 Finalización del proyecto y Transferencia de Conocimiento

Antes del cese o finalización de este contrato, el adjudicatario deberá garantizar el proceso de transferencia de conocimiento, mediante la entrega de la documentación que se estime oportuna e impartiendo unas sesiones de capacitación/formación sobre la solución ofertada, incluyendo al personal operativo que designe Osakidetza.

7 PRODUCTOS A OBTENER

El resultado final consistirá en la implantación del Sistema Informático de Contingencia en Osakidetza, junto con la documentación del Sistema.

Los productos a obtener serán, como mínimo, los siguientes:

- Planificación del proyecto.
- Especificaciones hardware y software necesarias para la implantación de la solución.
- Documentación técnica de la solución.
- Informes de seguimiento del proyecto.
- Aplicación implantada en producción.
- Manual de Usuario.
- Manual de Explotación.
- Manual de Instalación.

8 PLANIFICACIÓN DEL PROYECTO

Es necesario que los licitadores presenten los cronogramas en los que se deben especificar los contenidos o tareas y su distribución en el tiempo.

Estos cronogramas incluirán, asimismo, los diferentes hitos a cubrir y los entregables.

9 EQUIPO DE TRABAJO

Las empresas interesadas en la adjudicación del contrato presentarán en su propuesta la descripción de su equipo de trabajo, especificando los recursos humanos que destinarán al proyecto, sus perfiles profesionales, y las dedicaciones por cada una de sus categorías.

Asimismo, se indicarán los precios unitarios/jornada por cada categoría profesional ofertada.

Existirá un Director del Proyecto por parte de la empresa adjudicataria, representante de la misma e interlocutor y responsable de los trabajos ante la Dirección del Proyecto de **Osakidetza**.

Osakidetza aportará también la figura de un Director de Proyecto, con la función de coordinar la participación de los recursos humanos del mismo que sean necesarios en cada momento.

Osakidetza controlará, mediante la figura de su Director de Proyecto, el cumplimiento de los términos acordados, así como la calidad y adecuación del servicio objeto de este contrato, quedando ambos sujetos a lo que marca la Ley de Contratos de las Administraciones Públicas (texto refundido), en cuanto hace referencia a completar los términos y calidad de los productos desarrollados.

Asimismo, deberán identificarse los responsables únicos en cuantas actividades que, por su importancia, se considere oportuno: análisis, desarrollo, control de calidad y sus funciones y relaciones con el resto del equipo y **Osakidetza**.

Osakidetza, por su parte, deberá asegurar la colaboración de Técnicos, responsables de la aplicación en las distintas fases del proyecto y designará un responsable, que coordine las necesidades de éstas y a través del cual se canalicen cuantas consultas sean necesarias para el conocimiento detallado del entorno de la unidad y sus disciplinas.

10 CONTENIDO DE LAS OFERTAS

Con carácter obligatorio, las propuestas deberán presentarse en soporte digital, compatible con las herramientas instaladas en **Osakidetza** (MSWord 2010, Adobe Acrobat Reader 10).

Las ofertas se presentarán en dos modalidades:

- **Oferta resumen ejecutivo**, donde se recogerán los aspectos fundamentales de la oferta y sus elementos de valor añadido esenciales, conteniendo la información más relevante para la evaluación de la oferta por **Osakidetza** según los criterios de adjudicación publicados.

  Este resumen ejecutivo no podrá superar el número de 25 páginas (25 páginas A4).

- **Oferta completa,** donde se podrá explicar y detallar los diferentes aspectos de la oferta, siempre que supongan una información directamente relacionada con los servicios propuestos en el pliego.

  La oferta completa no podrá superar el número de 300 páginas (300 páginas A4).

Ambas modalidades de ofertas se deberán ajustar al siguiente contenido y formato:

1. Introducción

Se detalla el contexto en el que se realiza la oferta y las capacidades globales del licitador para entender y satisfacer los requerimientos del contrato.

En este apartado se expondrá la estrategia que la empresa ofertante considera apropiada para alcanzar los objetivos del proyecto.

2. Descripción de la solución propuesta

Descripción detallada de la solución ofertada que a priori se consideran apropiados para la realización del proyecto (diseño, usabilidad…), justificando su adecuación a los objetivos del mismo

Se explicará con detalle el alcance funcional y de diseño del software propuesto y como se cumplen las especificaciones demandadas en este pliego.

Se indicarán las utilidades y acciones que cada licitador proponga y justifique como mejora al objeto del pliego. Utilidades relacionadas con el diseño, calidad y usabilidad del funcionamiento de la solución.

3. Arquitectura tecnológica y modelo de integración

Descripción detallada de la arquitectura propuesta, modelo y elementos que la componen, con garantías de escalabilidad y continuidad del servicio.

Se valorarán aquellas soluciones alineadas con los estándares de **Osakidetza**, detallados en **Anexos II y III**.

Se deberá detallar de forma exhaustiva la infraestructura requerida para la arquitectura propuesta, describiendo de forma detallada las características de dicha infraestructura para los diferentes entornos.

4. Organización y Equipo de Trabajo

Modelo organizativo
Modelo global del proyecto y del equipo humano, distribución de funciones y responsabilidades, tareas, coordinación, dedicación al proyecto, flujos de comunicación, etc.

Equipo de Trabajo
Dimensión, configuración, perfiles y volumen de horas/perfil, del equipo de trabajo propuesto.

Detalles sobre el personal propuesto para las funciones principales demandas en este pliego.

5. Descripción del proyecto y Plan de Trabajo

En este apartado se hará una descripción detallada de cada una de las líneas de trabajo y servicios a prestar para el buen fin del proyecto, propuestas por cada licitador.

Se incluirá la planificación en el tiempo de cada línea de trabajo o actividad, los hitos que se producirán y los productos resultantes, que permitirán la certificación del proyecto, a través de la certificación de sus actividades.

Se realizará una descripción del contenido de cada actividad o fase, estrategia y operativa de trabajo en cada actividad, recursos y procedimientos de trabajo utilizados, relación entre las actividades, etc. y lo que cada licitador estime oportuno incluir.

11 PROPIEDAD DE LOS PRODUCTOS

Todos los productos descritos en el punto 6 de este documento que entregue el adjudicatario quedarán en propiedad exclusiva de **Osakidetza**, así como su propiedad intelectual, quedando el adjudicatario obligado a renunciar a cualquier derecho sobre estos conceptos.

12 CONFIDENCIALIDAD

En consideración al tipo de información procesada, el adjudicatario está obligado a mantener la más absoluta confidencialidad sobre todos aquellos datos y documentos a que tengan acceso con motivo de esta adjudicación. A ellos accederán, exclusivamente, las personas estrictamente imprescindibles para el desarrollo de las tareas inherentes a la misma. Todas ellas serán advertidas del carácter confidencial y reservado de la información a la que tendrán acceso.

Todos los ficheros que se pongan a disposición del adjudicatario para la ejecución del contrato son propiedad de **Osakidetza** y están registrados y sometidos a la salvaguarda que establece la legislación vigente, en especial la relativa a la protección de datos personales. Toda cesión a terceros será perseguida en los tribunales.

Osakidetza se reserva el derecho de establecer cualquier tipo de marcaje de los ficheros que se dejarán al adjudicatario, de manera que sus características puedan constituirse como prueba que posibilite localizar el origen y los responsables de las eventuales cesiones.

Bajo ningún caso ni circunstancia, el adjudicatario podrá suministrar a terceros, ni utilizar para sí ni para otros, datos facilitados por **Osakidetza**, para fines distintos a los contemplados en el objeto del presente contrato.

El adjudicatario estará obligado a poner en conocimiento de **Osakidetza**, inmediatamente después de ser detectada, cualquier sospecha de eventuales errores que se puedan producir en el sistema de seguridad de la información.

El adjudicatario faculta a **Osakidetza** para que, al terminar el proyecto, pueda responsabilizarlo y/o repercutirle los costes derivados de posibles reclamaciones ocasionadas por negligencia y/o falta de confidencialidad del mismo.

Adicionalmente y como condición general, todos los servicios prestados deberán contar con las medidas de seguridad y de confidencialidad adecuadas al grado de sensibilidad de la información suministrada, de acuerdo con lo descrito en la LOPD.

13 PRESUPUESTO, PLAZOS Y FORMA DE PAGO

13.1 Presupuesto

El presupuesto base de licitación y los plazos máximos de ejecución para este proyecto son los siguientes:

- **Presupuesto base de licitación** :**200.000 €**(SIN IVA)

  La valoración económica esta expresada en Euros, es máxima e incluye la totalidad de los conceptos devengables.

  Además se prevé una posible ampliación de **40.000€ (sin IVA),** para dar cobertura a adaptaciones derivadas de migraciones tecnológicas por obsolescencia de productos, implantación no contemplada de infraestructuras y tecnologías y evolutivos urgentes de carácter estratégico en los sistemas de información corporativos, no existentes en el momento de la elaboración de este expediente, por lo que el valor estimado del contrato asciende a **240.000€ (sin IVA).**

  La suma total de los conceptos anteriormente señalados no podrá exceder del precio de licitación total.

  La valoración económica deberá **ir obligatoriamente en el sobre B**: "Oferta económica y criterios evaluables de forma automática mediante la aplicación de fórmulas".

13.2 Plazos

El plazo máximo de ejecución será de **1 año** contado desde la fecha de formalización del contrato.

Además, se contempla la posibilidad de ampliar el plazo de ejecución inicial en **4 meses** para dar cobertura a posibles retrasos derivados de la complejidad de la Gestión del Cambio, de la coordinación con otros proveedores en la integración de los sistemas corporativos, así como los imprevistos que puedan surgir de una primera instalación en plataforma CNAP (Cloud-Native Application Platform).

13.3 Forma de pago

El pago se realizará de la siguiente forma:

- ✓ Se presentará una factura a la finalización de cada una de las líneas de trabajo detalladas en el capítulo 6 de este Pliego. Para la facturación de estos conceptos se requerirá el VºBº del responsable de **Osakidetza**.

14 CONSULTAS AL PLIEGO

Durante el período de licitación y ante cualquier necesidad de aclaración sobre cuestiones referidas a las especificaciones recogidas en el presente Pliego de Bases Técnicas, los licitadores deberán remitir por correo electrónico las preguntas e información que consideren necesarias para elaborar la Propuesta Técnica.

Los licitadores podrán dirigir sus consultas o aclaraciones a la dirección de correo electrónico de la Subdirección de Informática y Sistemas de Información:

SISI.SIAEXP@Osakidetza.eus

Los licitadores deberán identificar, a un único responsable de la oferta, que será durante al período de licitación, el interlocutor único con **Osakidetza** para cualquier tipo de consulta o aclaración sobre los términos expuestos en el presente Pliego, no admitiéndose ninguna consulta o aclaración de persona distinta a la señalada.

Así mismo los licitadores para formular sus consultas o aclaraciones deberán cumplimentar la siguiente información:

- Nº. Pregunta
- Capítulo/Apartado
- Página
- Párrafo
- Descripción de la Consulta

15 ANEXO I: VOLUMETRIA Y SOFTWARE DISPONIBLE

15.1 VOLUMETRIA:

A continuación, facilitamos información de **volumetría** por tipo de dato y actividad registrada:

Tipo de Información	Volumetría
Profesionales / Usuarios potenciales	15.000
Pacientes	3.300.000
HCR	3.300.000
Consultas Atención Primaria	100.000 día
Consultas Atencion Hospitalaria (CCEE) + Hospital de Día	56.000 día
Censo Hospitalización	5.000 camas
Censo Urgencias	3.000 puntos de atención
Bloque Quirúrgico	1.100 intervenciones día
Cocina. Menús y dietética	8.000 pacientes

Osakidetza dispone de soluciones de Interoperabilidad y Software ya construido que describe la situación de partida para la ejecución de este expediente.

15.2 Alcance J61 – HODEI

Dado que la situación de partida de este expediente parte de la disponibilidad del software ya construido en la solución J61 – Hodei, exponemos el alcance de dicho sistema.

La solución se concentra en la obtención de los Informes de Historia Clínica Resumidos (HCRs), Datos de Farmacia Hospitalaria y Censos.

Los documentos generados se almacenan en la BBDD MongoDB, mediante procesos de carga iniciales y procesos planificados para su actualización.

Documento	Sistema Productor	Formato	Actualización
HCR	SW Osabide Global (*)	JSON (metadatos) PDF XML	Planificador / SIO Proceso planificado que recorre pacientes a partir de un índice de actividad realizada: • Ingresos en cualquier área asistencial • Altas en cualquier área asistencial • Contactos en primaria o CCEE • Nacimientos • Altas de pacientes (no nacimientos) • Fusiones de Pacientes
Farmacia Hospitalaria	eOsabide (**)	JSON (metadatos) PDF	Planificador / SIO
Censos • Hospitalización • Urgencias • Pre-Admisión • Bloque Quirúrgico • Hospital de Día Médico • Hospital a	eOsabide	JSON (metadatos) PDF	Planificador / SIO

Domicilio • Consulta Externa			
Censos • Atención Primaria	OsabideAP (**)	JSON (metadatos) PDF	Planificador / SIO

Los archivos JSON incorporan únicamente la información de referencia necesaria para la generación de las colecciones (Estructura Orgánica y CIC de pacientes), para su posterior distribución en la red

(*) El Servicio Web de Osabide Global que compone el informe de Historia Clínica Resumido, devuelve el informe completo en formato XML (CDA Nivel1), PDF y el JSON.
(**) El Servicio Web de eOsabide devuelve el informe en formato PDF y el JSON.
(***) El Servicio Web de OsabideAP que compone el censo de atención primaria, devuelve el informe en formato PDF y el JSON.

16 ANEXO II: ENTORNO TECNOLÓGICO Y METODOLOGÍA APLICABLE

16.1 Entorno Tecnológico

Arquitectura de la aplicación

La aplicación objeto de contratación se debe desarrollar utilizando los componentes software open source del stack MEAN:

- MongoDB como base de datos NoSQL.
- Express como framework para la aplicación en la parte servidor (back-end)
- AngularJS como framework para la parte de cliente (front-end).
- NodeJS como runtime del backend.

El backend de la aplicación estará repartido entre dos escenarios diferentes:

- El entorno *on-premise* de Osakidetza, que contendrá el repositorio origen de la información resumida de los pacientes que irá siendo actualizado por otras aplicaciones corporativas que precisen reflejar un cambio en la información
- El entorno *cloud*, que contendrá la propia aplicación que funcionará sobre una réplica del repositorio mencionado en el punto anterior. Por la propia naturaleza de la aplicación que pretende cubrir escenarios de contingencia este entorno tiene que funcionar de forma totalmente autónoma, desacoplada y sin ninguna dependencia del entorno *on-premise* (salvo la propia sincronización de datos).

Albergue de la aplicación

La aplicación funcionará sobre una plataforma CNAP (Cloud-Native Application Platform) basada en contenedores orquestados por Kubernetes y que incorpora también una solución para gestión del ciclo de vida del software, así como 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 desarrollo, pre-producción y producción según se precise por criterios de calidad del software, testing, conveniencia o agilidad.

16.2 Metodología

La contratación objeto de esta licitación se engarzará en la siguiente estructura:

SecDevOps – Equipo de Producto (Objeto de esta contratación)

El licitador debe presentar una propuesta que indique claramente cómo da respuesta a los siguientes requisitos:

- Unificación de responsabilidades no sólo del propio desarrollo de la aplicación y su mantenimiento correctivo y evolutivo, sino de todo su ciclo de vida (incluyendo la puesta en producción) siguiendo prácticas SecDevOps y Agile.
- Modelo de equipo de trabajo orientado a producto (en contraposición a orientado a proyecto).
- Enfoque de entrega continua (Continuous Delivery).
- Compromiso de calidad continua, automatización, estabilidad, resiliencia y buenas prácticas de Seguridad de la Información que va más allá de ceñirse a requisitos funcionales.
- Interacción con el equipo PlatOps que se detalla en el siguiente apartado

PlatOps – Equipo de Plataforma (Aportado por Batera, fuera del ámbito de esta contratación)

Equipo multidisciplinar formado por perfiles de desarrollador y de técnicos de sistemas que mantienen, operan y evolucionan la plataforma que se menciona en el apartado anterior como un producto. Sus clientes/consumidores son diferentes equipos de desarrolladores que utilizan la plataforma para construir y ejecutar sobre ella aplicaciones de sus respectivos negocios dando continuidad a sus procesos SecDevOps y Agile de trabajo.

Reparto de responsabilidades entre los dos equipos

Aunque los dos equipos colaboran en una modalidad cliente/proveedor, a modo de ejemplo sin ánimo de ser exhaustivos, y para ilustrar la organización que se pretende se enumeran ejemplos de responsabilidades que tendría cada uno de los equipos que sí que están diferenciadas:

Responsabilidades del equipo Platform Ops:

- Definición del runtime de contenedores.
- Establecer normativa base para el desarrollo de aplicaciones contenerizadas.
- Ciclo de vida del clúster Kubernetes e imágenes base de contenedores en base al soporte de fabricante.
- Mantenimiento de Operadores Kubernetes
- Autenticación y autorización de usuarios, acceso de aplicaciones y servicios a la plataforma. Gestión de políticas de red y de routing del tráfico de aplicaciones.
- Gestion de la configuración, asignación de cuotas, gestión manifiestos y recursos.
- Monitorización, logging, métricas y seguimiento del comportamiento de aplicaciones.
- Mecanismos de alta disponibilidad y PCN de la propia plataforma, backup y recuperación de la misma.
- …

Responsabilidades del equipo SecDevOps:

- Asegurar que la aplicación cumple los SLA.
- Seguir buenas prácticas de Seguridad de la Información.

- Realizar controles de desarrollo seguro durante todas las fases desde el inicio
- Planificar e implementar la alta disponibilidad de la aplicación.
- Crear las imágenes de los contenedores aplicando la normativa base, y conforme a buenas prácticas para mantenerlos ligeros, de reducido tamaño y alineados con un único servicio lógico.
- Desacoplar la configuración de la aplicación de la imagen del contenedor.
- Despliegue y validación del contenedor.
- Colabora con PlatOps en establecer cuotas y niveles de calidad de servicio.
- …

17 ANEXO III: DOCUMENTO DE ARQUITECTURA Y TECNOLOGÍA (DET)

La solución ofertada deberá estar alineada tecnológicamente con las directrices que se indican a continuación.

17.1 Arquitectura y tecnología

El proveedor definirá la arquitectura de la solución y especificará los componentes lógicos y físicos de la misma, así como el diagrama de capas lógicas y su distribución en la infraestructura, los productos software y/o hardware requeridos, protocolos utilizados, necesidades de comunicación (apertura de puertos, balanceadores, …), siguiendo las directrices de **Osakidetza** que se indican a continuación; será validada por las áreas de Arquitectura e Infraestructuras, Operación y Comunicaciones de **Osakidetza**.

El diseño de la arquitectura será escalable y garantizará el cumplimiento de la normativa de seguridad y de planes de contingencia de **Osakidetza**, garantizando el óptimo rendimiento de la solución ofertada sobre dicha arquitectura.

El diseño de arquitectura se realizará para los entornos de:

- Preproducción (debe ser igual que el entorno de producción)
- Producción

La dotación de la infraestructura necesaria para la implantación de la solución correrá a cargo de **Osakidetza**.

Consideraciones Tecnológicas

La solución (producto/aplicación/desarrollo) será una solución Web (sin plug-ins), con arquitectura de n-capas preferentemente 3 capas: presentación, negocio y persistencia, compatible con tecnología de virtualización y almacenamiento SAN y NAS.

El albergue de las capas de negocio y persistencia será centralizado y la capa de presentación distribuida.

Plataforma de virtualización

- VMWare
- Sphere 5.5

Almacenamiento

- SAN: EMC VPLEX
- NAS. Hitachi HUS

Plataformas de desarrollo de la solución:

- .NET sobre Windows 2012R2
- Java sobre Red Hat Enterprise Linux 7
- Aplicaciones móviles:
    - Node.js, Express, AngularJS, MongoDB sobre Red Hat Enterprise Linux 7
    - Ionic, Cordova sobre Android, iOS o WindowsPhone

Sistemas Operativos:

- Servidores:
  - Windows 2012 R2
  - Red Hat Enterprise Linux 7
- Puesto de trabajo fijo: Windows 7 Enterprise N SP1 32 bits
- Puesto de trabajo móvil: Android, iOS, WindowsPhone

Servidores Web:

- Apache Webserver 2.4
- MS IIS 8.5 (S.O. Windows 2012 R2)
- Oracle Web Server 11.1.1.7
- Web Dispatcher de SAP Netweaver 7.20
- Nginx 1.8.0

Servidores de Aplicación:

- Apache Tomcat 7 + JDK 7 / JDK 8
- Oracle Weblogic Server 12c + JDK 8
- MS IIS 8.5 + .NET Framework 4.5
- Application Server de SAP Netweaver 7.X
- Node.js 4.1.0

Sistemas de Gestión de Bases de Datos (*)

- Oracle 12c (RAC)
- Microsoft SQL Server 2012 (Always on)
- MongoDB 2.6

(*) Continuidad de negocio y Alta disponibilidad: Oracle RAC, SQL Server Always ON

Gestión de contenidos:

- MS SharePoint 2010 Enterprise
- EMC Documentum 7.2

Infraestructura SOA:

- Oracle Service Bus 12c (12.2.1) + JDK 8.0

Plataforma de firma (PKI):

- Izenpe

Autenticación:

- Directorio Activo de MS (AD)
- Directorio Ligero de MS (LDS)

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 **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.

La solución (producto/aplicación/desarrollo) deberá ser compatible con la relación de versiones indicadas en el párrafo anterior (las que apliquen).

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.

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.

Además, para los sistemas de información 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 serán:

- **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 (DA). Por cada perfil que tenga la aplicación (médico, enfermera, administrativo, administrador de la aplicación,…) se creará un grupo de autorización en el DA. Se mapeará el perfil al grupo.

Monitorización

La solución incluirá un apartado de monitorización en la que se detallen los elementos a monitorizar para asegurar un correcto funcionamiento del sistema, proporcionando los scripts necesarios para que la operativa del sistema pueda ser realizada por un operador, así como los scripts de arranque y parada.

La monitorización se puede realizar a través de:

- SCOM mediante Management Pack para sistemas Microsoft
- Instalación de agente de CA Wily Introscope para tecnología Web
- Instalación de agente de Pandora FMS para sistemas Linux, Unix
- Enterprise Manager Cloud Control para SGBD Oracle
- Mensajes SNMP
- Activación de logs que se enviarán a un servidor virtual dedicado

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.

Backup/Restore

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

Nota: el hardware y herramientas de backup son provistas por **Osakidetza**

17.2 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, enrutar 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

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

Gestor de Eventos

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

- **Estándares de comunicación**
  La mensajería del Servicio **Osakidetza** se implementará de acuerdo con las especificaciones del estándar HL7 versión 2.XX o con cualquier otro formato propio de **Osakidetza**; de esta manera se asegura la interoperabilidad entre los sistemas de información.
- **Relación de tecnologías soportadas para la publicación y subscripción a eventos.**
  Tecnologías que soporta el gestor de eventos para la publicación y subscripción a eventos, así como si la modalidad soporta transaccionalidad y las opciones de seguridad disponibles:

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

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

- **Mensajería. Definición de Evento**

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

- ✓ **id:** Es el identificador del tipo de evento. Se genera durante el proceso de alta del evento en el sistema de administración de Event Manager. Durante el procesamiento de un evento se verifica que el id sea válido.
- ✓ **correlation:** Es un campo libre en el que el publicador del evento indica un número correlativo relativo a su sistema.
- ✓ **source:** Es el identificador del publicador. Se genera durante el proceso de alta de un publicador en el sistema de administración de Event Manager.

Durante el procesamiento de un evento se verifica que el source sea válido.

- ✓
- ✓ **timestamp:** Lo establece el publicador del evento en el momento del envío.
- ✓ **metadata**: Puede contener un xml que ayude a describir el contenido del evento. Event Manager puede utilizar esta información para tomar decisiones de enrutado.
- ✓ **payload:** Es el contenido del evento. Puede ser cualquier cadena de texto o XML.

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

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

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

17.3 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>

- Motor Business Intelligence

- Oracle Business Intelligence 11.1.1.6.2

- Servidor Web
  - WebLogic Server: 10.3.5.0

- BBDD (Exadata)
  - Exadata: Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production

- ETL
  - ODI -> Oracle Data Integrator 11g Build ODI_11.1.1.7.0 GENERIC_130302.2156

17.4 Calidad de uso

Rendimiento

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.
- Flexibilizar las posibilidades con las que el usuario y el sistema pueden intercambiar información, permitiendo la multiplicidad de vías para realizar la tarea, similitud con tareas anteriores y la optimización entre el usuario y el sistema.
- 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.

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).

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 período de mantenimiento.

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

Documento firmado por: MARIA TERESA CUADRADO ZUBIZARRETA
En la fecha 2020.06.09 15:24:02 CEST