Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

Servicios de migración y desarrollos para el Gobierno de Identidades y Control de Accesos

Pliego de condiciones técnicas

Fecha: 02/09/2021

Mediterráneo, 14 • 01010 Vitoria-Gasteiz • Posta-kutxatila / Apartado: 809 • 01080 Vitoria-Gasteiz • Tel. 945 01 73 00* • Fax. 945 01 73 01 • www.ejie.eus

Este documento es propiedad de Eusko Jaurlaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, S.A. (EJIE). Este documento no puede ser reproducido, en su totalidad o parcialmente, ni mostrado a otros, ni utilizado para otros propósitos que los que han originado su entrega, sin el previo permiso escrito de EJIE. En el caso de ser entregado en virtud de un contrato, su utilización estará limitada a lo expresamente autorizado en dicho contrato. EJIE no podrá ser considerada responsable de eventuales errores u omisiones en la edición del documento.

Versión	Fecha	Resumen de cambios	Elaborado por:	Aprobado por:

Indice

1 Introducción 4
2 Objeto del contrato 5
2.1 Objeto del Servicio 5
2.2 Descripción y Alcance del Servicio 6
2.2.1 Implantación del sistema de Gestión de Identidades (Oracle Identity Manager, OIM) 6
2.2.2 Implantación del sistema de Control de Accesos (Oracle Access Manager, OAM) 7
2.2.3 Implantación del sistema de Portal de Peticiones y Workflows 8
2.2.4 Implantación del sistema de Gobierno de Identidades (Oracle Identity Governance, OIG) 9
2.3 Plan de Despliegue de los Sistemas IAM 10
3 Requisitos del producto/servicio 11
3.1 Situación del problema 11
3.1.1 Estado inicial 11
3.1.2 Estado final 11
3.2 Requisitos Identificados 15
3.3 Requisitos Técnicos para la infraestructura de IAM 15
4 Metodología Aplicable y Entorno Tecnológico. 17
4.1 Metodología de desarrollo, normativa y Guía de Estilo 17
4.2 Herramientas del ciclo de vida de las aplicaciones 19
5 Descripción de entregables. 20
5.1 Normativa para la puesta en producción y posterior explotación del sistema 21
6 Planificación y Organización 22
6.1 Plan de Proyecto 22
6.1.1 Plan de Entregas e Hitos de Control 22
6.1.2 Diagrama de Gantt 22
6.2 Organización del Equipo de Trabajo 22
6.3 Transferencia Tecnológica. 22
7 Mecanismos de Seguimiento, Control y Supervisión 23
7.1 Mecanismos de Seguimiento y Control. 23
7.2 Supervisión del proyecto 23

1 Introducción

EJIE, Eusko Jaurlaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, es la Empresa pública de servicios de las tecnologías de la información y las comunicaciones (TIC), cuya razón de existir es contribuir a la consecución de un Sector Público Vasco, moderno y eficiente, en el Marco Legal establecido por el Gobierno, con la seguridad y calidad necesarias y con el debido respeto al medio ambiente.

EJIE tiene como meta final la consecución de la satisfacción de sus clientes, siendo el instrumento común de prestación de servicios TIC en el Sector Público Vasco, y comprometiéndose en:

- Construir y mantener con eficiencia y calidad la infraestructura de los Sistemas de Información, posibilitando su continuidad y seguridad.
- Garantizar la interoperabilidad entre las distintas administraciones.
- Servir de apoyo a las necesidades de planificación y realización de la función informática de los Departamentos y Organismos Autónomos del Gobierno, asegurando la cobertura de sus demandas con el compromiso y profesionalidad adecuados a las relaciones contractuales que se establezcan.

Por tanto, EJIE debe ser un instrumento común de referencia para la prestación de servicios TIC en el Sector Público Vasco:

- Aportando valor añadido.
- Proporcionando soluciones competitivas.
- Transmitiendo confianza a sus clientes.
- Contando con personas cualificadas y comprometidas.

Se puede obtener información más detallada y extensa en nuestra dirección de Internet http://www.ejie.eus

2 Objeto del contrato

2.1 Objeto del Servicio

El objeto del presente pliego es la definición e implementación de la solución Oracle Identity Governance como sistema para el Gobierno de Identidades y Control de Accesos, que permita alcanzar mejor grado de madurez y disponer de una infraestructura transversal a los sistemas de información, de modo que se puedan implementar y automatizar los procesos de concesión de permisos y permitiendo asegurar que sólo accedan a la información las personas que por sus funciones lo requieren conociendo en todo momento quién y cuándo accede a dicha información.

Por lo tanto los servicios a contratar son:

- Servicios de migración del actual sistema de provisión y control de acceso a las soluciones de Oracle Identity Governance
- Servicios de desarrollo de componentes. Modificaciones en los actuales y/o nuevos componentes

La implantación de una solución de Gestión de Identidades y Control de Accesos (en adelante, IAM de sus siglas en inglés: *Identity and Access Management*) ha de proporcionar importantes beneficios en materia de aprovisionamiento de cuentas, gestión de roles, flujos de trabajo para la petición de accesos, generación de informes de auditoría, control de acceso a aplicaciones, autenticación fuerte, gestión del riesgo en seguridad, etc…

Para ello, será necesario la implantación y desarrollo de una nueva solución de IAM para EJIE, apoyándose en la herramienta de Oracle, y que deberá servir para obtener los siguientes beneficios, :

- Contar con una **gestión centralizada** de usuarios, contraseñas y grupos o roles de autorización para el acceso a los sistemas.
- Disponer de un **sistema** para petición de accesos, seguimiento y flujos de aprobación y denegación, todo supeditado a la inclusión de un Portal de Peticiones.
- **Identificación** de usuarios bajo identidad única de acceso al sistema, que identifica quién y qué derechos recibe, y que permita la **gestión del Ciclo de Vida** de las identidades y cuentas.
- **Sincronización con fuentes de confianza** para la actualización fehaciente de la información
- **Proteger los recursos y aplicaciones con un sistema de Control de Accesos** que satisfaga las necesidades en las restricciones de acceso y permitir la utilización a quiénes estén facultados para ello.
- Asignación de derechos de acceso atendiendo a los principios de **mínimo privilegio**, **necesidad de conocer**, y **capacidad de autorizar derechos**.
- Establecer **políticas de acceso** de modo que los accesos se efectúen siempre atendiendo a la **política y normativa de seguridad** definidas.
- Definición de **flujos de autorización y control de accesos avanzado**, lo que permitirá gestionar la autorización con carácter previo un acceso remoto al sistema de información.
- **Registro de actividades** de los usuarios en los sistemas y protección de los registros.
- **Aprovisionamiento automático de perfiles**, al igual que la reconciliación de la información de los distintos sistemas de información.
- Contar con una plataforma que permita a la organización **entender, controlar y tomar las decisiones de negocio** que están relacionadas con la gestión de los accesos de los usuarios y la gestión de los riesgos de accesos.
- Disponer de una solución orientada a las **actividades de negocio** que permitirá asignar los permisos en función de las determinadas actividades, pudiendo establecer roles para tal efecto, y permitiendo identificar mediante procesos analíticos las posibles violaciones de segregación de funciones en los sistemas de EJIE.
- Mejorar la visibilidad y control de los accesos concedidos a los usuarios mediante procesos de **recertificación y consolidación de permisos** a las aplicaciones.
- Capacidad de **asignación de riesgos y actividades de negocio**, con la posibilidad de asignar y controlar la **segregación de funciones**, y disponer de los procesos necesarios para el descubrimiento de las violaciones descubierta y el control de remediaciones.

2.2 Descripción y Alcance del Servicio

El servicio que se solicita en este pliego, es la ejecución de los trabajos para la implantación y desarrollo de una nueva solución de IAM para EJIE con *Oracle Identity Governance*, llevando a cabo las tareas necesarias para abordar la implantación del sistema o sistemas que den respuesta a las problemáticas que origina una gestión de usuarios, con sus identificadores, atributos y permisos, más la autenticación y autorización a los distintos servicios y recursos TIC que EJIE pone a su disposición.

A tal fin, se deberá realizar las tareas de ejecución de trabajos para la adaptación de la infraestructura actual, el diseño técnico detallado de la solución propuesta, instalación e implantación de la plataforma IAM de Oracle y todo lo necesario en relación con el traspaso del conocimiento y gestión del cambio, que garantice una eficiente y efectiva transferencia de gestión dentro de EJIE.

- **Estudio detallado de la situación actual** y antecedentes en EJIE, previos a la implantación de un nuevo sistema de Gestión de Identidades y accesos con Oracle, relacionados con cada uno de los requerimientos funcionales que se definen.
- **Identificación, planificación y revisión** del conjunto de objetivos que conformarán la totalidad de la solución de Gobierno y Gestión de Identidades y Control de Accesos. En este punto EJIE se muestra abierto a asumir cambios que en el desarrollo del estudio se revelen innecesarios o de difícil cumplimiento.
- Adaptación del **enfoque y visión estratégica de la solución de IAM**, aportando las mejores prácticas y estándares de mayor garantía de éxito a la hora de abordar el proyecto de Implantación.
- Proposición del **diseño detallado de Gobierno de Identidades y Control de Accesos** para EJIE, con pleno cumplimiento de los objetivos y requerimientos establecidos teniendo en cuenta la necesidad de dar servicio a tres entornos: desarrollo, pruebas y producción.
- Plan de **implantación, despliegue y migración** de los procesos existentes hacia el nuevo sistema. En este punto es importante ofrecer una convivencia con el actual sistema de control de accesos (XLNETs) para garantizar el funcionamiento de las aplicaciones actuales.
- **Instalación y puesta en marcha** de los procesos sobre la nueva herramienta de Oracle.
- **Formación** y documentación del proyecto.
- **Transferencia** de gestión y explotación.

El servicio que se solicita deberá llevarse a cabo en distintas fases que permitan alcanzar hitos intermedios hasta llegar a la disponer de la solución completa de Gobierno de Identidades y Control de Accesos.

2.2.1 Implantación del sistema de Gestión de Identidades (*Oracle Identity Manager*, OIM)

Se llevarán a cabo las actividades necesarias para la definición, despliegue y configuración del sistema para Gestión de Identidades de Oracle: Oracle Identity Manager (OIM)

Dentro del alcance hay que considerar la realización de los siguientes bloques de tareas:

- Definición de la arquitectura e instalación y configuración de los componentes de la plataforma de Oracle Identity Governance.
- Análisis y diseño de la solución en base a los requisitos de EJIE, los cuales se detallan más adelante
- Integración de fuentes autoritativas para la creación de identidades.
- Integración de los sistemas gestionados, mediante el despliegue y configuración de los conectores provistos por la herramienta y/o conectores a medida cuando esto no sea posible.
- Definición e implementación de Ciclo de Vida de Identidades y políticas de aprovisionamiento automático.
- Implementación del Autoservicio, gestión de contraseñas y administración delegada de identidades.
- Reconciliación de los sistemas gestionados y gestión de cuentas.

- Implementación de la gestión de aprovisionamiento automático, modelo y políticas RBAC para las aplicaciones.
- Reingeniería de la gestión del aprovisionamiento basada en “Puesto” en el OIM actual (ver documento “Análisis de situación actual”). EJIE pretende y está abierta a un posible cambio o desaparición de este concepto en el modo en que se lleva a cabo en la actualidad. Se podría variar por un concepto de grupo, rol funcional o similar para lo que se solicita el estudio y rediseño de los procesos de aprovisionamiento con el nuevo sistema.
- Definición e implementación de informes base de gestión de identidades:
    - Informe de identidades y sus estados
    - Informe detallado de una identidad, incluyendo roles asignados, cuentas aprovisionadas y perfiles asociados en cada una de ellas
    - Informe de roles y sus tipos
    - Informe detalle de un rol, incluyendo identidades asignadas
    - Informe de cuentas existentes por sistemas finales
    - Informe de control para las cuentas huérfanas
    - Informe de acciones realizadas en un periodo de tiempo
    - Informe de historial de cambios en el aprovisionamiento de una cuenta
    - Informe de vinculación/desvinculación a roles de una identidad
    - Informe de aprovisionamiento/revocación de sistemas gestionados de una identidad
- Personalización de imagen corporativa de la interfaz de usuario de la herramienta de gestión de identidades.
- Despliegue y configuración de al menos 2 entornos: Desarrollo y Producción. En este punto hay que tener en cuenta la existencia de cuatro entornos. Esto es debido a que la gestión de identidades y acceso también provisiona cuentas y accesos a aplicaciones que están en desarrollo y preproducción. El sistema debe prever la provisión de estas cuentas, bien desde el propio entorno productivo o mediante sistemas separados.
    - Desarrollo (softbase): Entorno propio de desarrollo y pruebas del proyecto IAM
    - Producción:
        - Entorno de desarrollo para terceras aplicaciones
        - Entorno preproductivo para terceras aplicaciones
        - Entorno productivo.
- Pruebas de validación, elaboración de documentación y formación.

2.2.2 Implantación del sistema de Control de Accesos (*Oracle Access Manager*, OAM)

El conjunto de actividades deben cubrir el estudio y entendimiento de la situación actual de EJIE en el ámbito del control de acceso a las aplicaciones y, en base a ese estudio, el establecimiento de un marco de referencia detallado, para la integración de aplicaciones con el sistema Oracle Access Manager, que permita definir cómo dar cumplimento a los requisitos establecidos para los procesos y aplicaciones actuales y establecer el futuro marco de trabajo para el control de acceso e integración de aplicaciones.

Actualmente EJIE dispone de un sistema de control de accesos hecho a medida que se denomina XLNETS, el cual sirve como sistema de *Single Sign-On* (SSO) para la autenticación y autorización de usuarios en aplicaciones desarrollados bajo distintas tecnologías, tanto desarrolladas dentro en EJIE como otras aplicaciones de productos adquiridos, y provee de los componentes necesarios para la seguridad de aplicaciones, estableciendo los mecanismos de autenticación y autorización mediante APIs (Ver documento “Análisis de la situación Actual”)

En este apartado, se pretende disponer de un nuevo sistema de control de accesos sobre Oracle Access Manager que permita a EJIE la migración a medio/largo plazo de las aplicaciones actuales en XLNETs hacia este nuevo sistema.

XLNETs y Oracle Access Manager deberán convivir como sistemas de control de acceso independientes y se deberá facilitar el proceso de migración a futuro con el menor impacto en el uso de las aplicaciones.

Dentro del alcance hay que considerar el desarrollo de los siguientes bloques de actividades:

- Despliegue e instalación del sistema de gestión de accesos Oracle Access Manager (OAM)
- Definición del modelo de integración de nuevas aplicaciones en el sistema de OAM (Libro blanco de integración de aplicaciones en OAM).
- Despliegue y configuración de componentes de OAM para la integración de aplicaciones según lo definido en el modelo de integración.
- Definición del proceso y procedimiento de migración de aplicaciones existentes hacia el nuevo sistema OAM.
- Definición de modelo de autenticación entre procesos (login de aplicación) en el que no existe un usuario que ha realizado autenticación.
- Integración de 3 aplicaciones.
- Realización de plan de pruebas para la validación de la integración de aplicaciones.
- Personalización de imagen corporativa de la interfaz de usuario y frontal de acceso de la herramienta OAM.
- Portal de aplicaciones con enlaces a las que el usuario tenga algún acceso. Puede haber aplicaciones públicas.
- Despliegue y configuración en 4 entornos:
  - Desarrollo OAM: Entorno propio de desarrollo del proyecto OAM (*softbase*); estará dedicado al desarrollo y pruebas de las configuraciones e implementaciones de OAM.
  - Desarrollo Aplicaciones: Este entorno será el sistema para el desarrollo de aplicaciones, y que usaran terceros para desarrollar las aplicaciones. Este entorno contendrá las funcionalidades consolidadas en OAM productivo, y servirá para que el desarrollo de aplicaciones disponga de las funcionalidades OAM para el desarrollo de cara a producción.
  - Pre-producción: Entorno de validación y pruebas previas a producción.
  - Producción

  La disposición de estos entornos para la solución de Access Manager, supone definir los correspondientes flujos de provisión de permisos de aplicaciones siguiendo el proceso de desarrollo de aplicaciones entre entornos.
- Elaboración de documentación. La documentación deberá incluir el procedimiento para gestión de cambio entre entornos, es decir los flujos de configuración y provisión de permisos de aplicaciones siguiendo el flujo de cambios en el desarrollo de aplicaciones
- Formación para la administración de la plataforma

2.2.3 Implantación del sistema de Portal de Peticiones y *Workflows*

Se han de realizar las actividades para disponer del sistema que sirva de portal de peticiones y flujos en OIM para la gestión de solicitud de accesos de los sistemas gestionados y aplicaciones.

En esta fase se tienen que considerar dentro del alcance las tareas a desarrollar para la definición y configuración de OIM como un motor de *Workflow* unido a la gestión de identidades, para la publicación de los

accesos disponibles, como la solicitud de estos accesos y las aprobaciones correspondientes y de la configuración y gestión de los flujos de trabajo relacionados.

Actualmente se dispone de un portal de peticiones en ITSM Remedy en el que los peticionarios adjuntan documentos Word con los requisitos de seguridad para las aplicaciones. Se hace difícil eliminar este portal o modelar completamente las peticiones de seguridad para aplicaciones, por lo que al menos el personal del SASU o los propios grupos de desarrollo en entornos no productivos podrían utilizar el portal de peticiones para incluir las definiciones de seguridad en el sistema.

Los bloques de tareas a considerar en esta fase son:

- Definición e implementación de catálogo de aplicaciones, roles y servicios en OIM. Dentro este catálogo se deberá tener en cuenta la categorización dependiendo de los entornos, considerando la posibilidad de solicitud de accesos para aplicaciones en desarrollo de aplicaciones y/o pre-producción, además de las solicitudes para producción.
- Definición e implementación de flujos:
  - Flujo para Alta/Baja y Modificación de Identidades
  - Flujo para solitud de asignación de roles y recursos (con niveles de aprobación)
  - Flujo de solicitud de asignación de roles y control para la segregación de funciones (SoD) (con niveles de aprobación)
  - Flujo para solicitud de nuevos roles en GID
- Definición e implementación de informes de solicitudes y aprobaciones registradas en el sistema de peticiones.
- Definición e implementación de informes de roles y recursos y aprobadores asignados.
- Personalización de imagen corporativa de la interfaz de usuario de la herramienta de gestión de identidades.
- Despliegue y configuración para dar servicio a los entornos de Desarrollo, Pruebas y Producción.
- Pruebas de validación, elaboración de documentación y formación.

2.2.4 Implantación del sistema de Gobierno de Identidades (*Oracle Identity Governance*, OIG)

En esta fase se pretende ampliar las capacidades funcionales de la herramienta Oracle Identity Manager (OIM) con la incorporación del sistema y componentes de Oracle Identity Governance (OIG) para contar con una plataforma más avanzada que permita a la organización entender, controlar y tomar las decisiones de negocio que están relacionadas con la gestión de los accesos de los usuarios y la gestión de los riesgos de accesos.

Dentro de esta fase se deberán abordar las actividades de definición, despliegue y configuración para mejorar la visibilidad y control de los accesos concedidos a los usuarios mediante procesos de recertificación y consolidación de permisos a las aplicaciones y control de riesgos.

Dentro del alcance de esta fase hay que considerar la realización de los siguientes bloques de tareas:

- Definición de la arquitectura y despliegue e integración de los componentes de la plataforma de OIG junto con OIM para las funciones de Gobierno.
- Definición del modelo de implementación de roles junto con reglas de SoD, para evaluación de riesgos en las aplicaciones y sistemas gestionados en la herramienta de Oracle.
- Definición e implementación de procesos de recertificación de roles y recursos.
- Definición y creación de informes y cuadro de mando base para gobierno de la identidad.
  - Informe de estado de procesos de recertificación
  - Informe de auditoría de cumplimiento o violación de las políticas de SoD
- Integración con el sistema de OIM para el control de roles y remediación.

- Integración con el sistema de Portal de Peticiones para el control de SoD y flujos de niveles de aprobación.
- Personalización de imagen corporativa de la interfaz de usuario de la herramienta de gestión de identidades.
- Despliegue y configuración para dar servicio a los entornos de desarrollo, pruebas y producción.
- Pruebas de validación, elaboración de documentación y formación.

2.3 Plan de Despliegue de los Sistemas IAM

Como se ha mencionado en el punto anterior 2.2, como parte del alcance se deberá elaborar un plan de implantación, despliegue y migración de los procesos existentes hacia el nuevo sistema. Este plan deberá considerar la existencia de los sistemas y procesos actuales en los diferentes entornos, proponiendo un plan de implantación que asegure la migración con el menor impacto posible; así como un plan de arquitectura con alta disponibilidad que permita garantizar la disponibilidad de la solución.

Este plan de despliegue deberá incluir, al menos, los siguientes aspectos:

- Plan de despliegue de sistemas y componentes, y plan de arquitectura para alta disponibilidad del servicio en producción.
- Plan de migración e implantación de procesos y servicios actuales hacia los nuevos sistemas, y requisitos o restricciones que se hayan de considerar para causar el menor impacto y el mayor éxito en la migración.
- Plan de contingencias y procesos operativos para recuperación y/o marcha atrás y operación de la plataforma en caso de incidencia grave.

Desde la primera puesta en producción hasta la finalización del proyecto el adjudicatario deberá ofrecer disponibilidad telefónica 24x7 para la intervención en situaciones eventuales en el proceso de implantación de los nuevos procesos relacionadas con el sistema desplegado. En caso de incidencia urgente en la plataforma, se podrá requerir, por parte de los servicios de operación de EJIE, el soporte fuera del horario presencial habitual, ya sea de forma remota o presencial, en casos de incidencia e indisponibilidad de los sistemas IAM.

3 Requisitos del producto/servicio

3.1 Situación del problema

3.1.1 Estado inicial

El estado actual del sistema se encuentra detallado en el documento “Análisis de situación actual v2.0.docx”

3.1.2 Estado final

Como resultado de la realización de un proyecto para la implantación de una solución de Gobierno de Identidades y Control de Accesos, se quiere llegar a la situación final de disponer del conjunto de sistemas y herramientas que capaciten a EJIE para la gestión, administración y gobierno de identidades, y el control de accesos a las aplicaciones.

Actualmente EJIE dispone de la herramienta Oracle Identity Manager en la versión 9.0.1, la cual está en un estado inicial que ha tenido pocos avances evolutivos, y se encuentra fuera de soporte por parte del fabricante Oracle.

Este conjunto de sistemas al que se pretende llegar, será la nueva plataforma y solución en gestión de identidades y control de accesos, que sustituirá la herramienta actual y sobre la cual se implementará y mejorarán los procesos actuales, incorporando nuevas funcionalidades y requisitos.

Una breve aproximación sobre los sistemas que han de formar el estado final de la plataforma de gestión de identidades y control de acceso, se puede delimitar con los siguientes elementos:

- **Identity Manager & Governance**. Bloque funcional que engloba tanto los elementos de un gestor de identidades como de gobierno y cumplimiento normativo. El presentarse conjuntamente responde a que los elementos o componentes tienen un fuerte acoplamiento y una alta interacción.
- **WorkFlow.** Bloque funcional con los componentes y elementos necesarios para dotar a la solución de un portal de peticiones y de un motor de flujos de trabajo (BPM), donde se puedan establecer los requisitos necesarios para validar las peticiones. Es importante destacar a los actores principales que estarían compuestos por los peticionarios y por los aprobadores.
- **Identity Manager Synchronization.** Es un sistema o bloque funcional que, aunque por su importancia se ha establecido como elemento, lo cierto es que debe estar integrado en el sistema de Identity Manager. Está compuesto por los componentes que permiten la lectura, transformación y validación de la información de las fuentes de confianza para introducirla formalmente en el sistema de gestión de identidades.
- **Access Manager.** Este sistema o bloque funcional se encargará de gestionar los permisos y el control de accesos a los sistemas de información que se establezcan en la solución. Es sistema recibirá peticiones de acceso y éste establecerá las necesidades que se han de satisfacer para permitir el acceso. Contendrá las políticas de acceso a los sistemas, los derechos y los permisos, las cuentas de usuario y las credenciales, los métodos de autenticación y autorización.
- **Sistemas Gestionados.** Es el bloque engloba todos los sistemas finales que serán gestionados desde el punto de vista de la gestión de identidades.
- **Actores.** Son el conjunto de administradores, usuarios de aplicación y usuarios finales que interaccionan con la solución propuesta.
- **Sistemas autoritativos.** Son el conjunto de fuentes de confianza que se establecen como fuentes autoritativas que sirve como punto de entrada de la información válida al sistema de gestión de identidades.

En el diagrama a continuación, se representa el mapa de sistemas para el estado final:

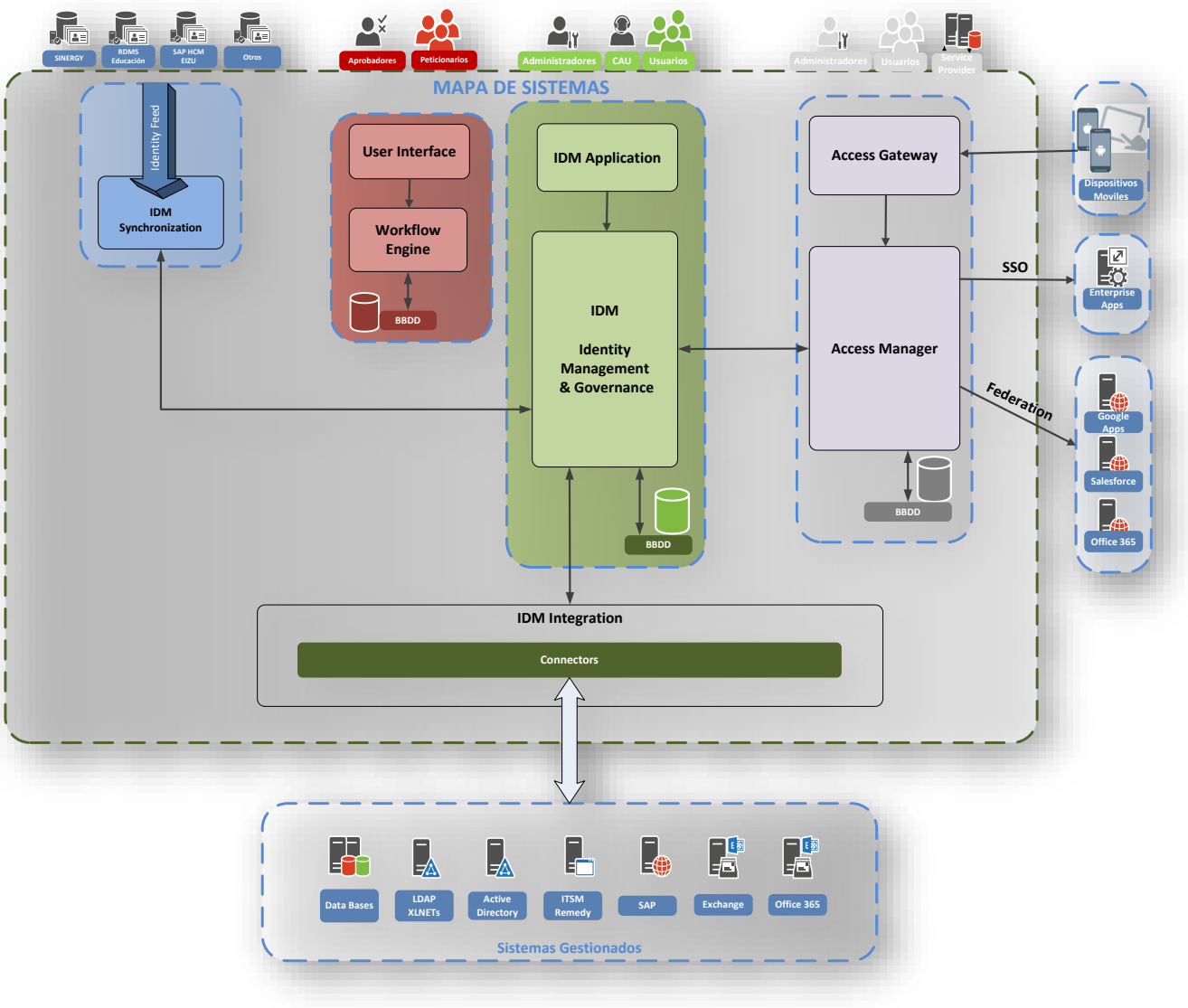


Ilustración 1. Mapa de Sistemas

En el diagrama se pueden identifican los siguientes sistemas que formaran parte en una solución integral de Gobierno de Identidades y Control de Accesos:

- **IDM**. Sistema para la gestión de identidades (*Identity Management*, IDM de sus siglas en inglés) que contiene y debe servir para satisfacer los siguientes funcionalidades y necesidades:

    - Identidad Corporativa
    - Ciclo de vida de las Identidades
    - Propagación de la Identidad
    - Sincronización Información de las Identidades
    - Sincronización de Contraseñas
    - Políticas de Contraseñas
    - Gestión de Cuentas huérfanas
    - Integración con Fuentes Autoritativas
    - Integración con sistemas gestionados
    - Modelo RBAC
    - Caducidad de Accesos
    - Administración Delegada

- Auditoría

Adicionalmente el sistema IDM tendrá que desempeñar además con los siguientes procesos y capacidades:

- Aprovisionamiento automático de Accesos
- Reconciliación de los sistemas
- Establecimiento de Reglas de Mapeo
- Registro y relación de cuentas y personal
- Centralización procesos de aprovisionamiento
- Sincronización con Sistemas Finales
- Uso de estándares de integración
- Escalabilidad
- Remediación
- Bloqueo de cuentas

- **Fuentes Autoritativas (FF.AA)**. Define los procesos necesarios para la sincronización de información con las fuentes de datos autoritativas.

  Esta parte funcional contiene los elementos necesarios para establecer los procesos de incorporación de las Identidades hacia el sistema IDM, y va a dar cobertura a las siguientes funcionalidades:

  - Definición de atributos para la Identidad Corporativa
  - Definición de estándares de integración para la sincronización de la información
  - Integración con RRHH
  - Integración de fuente autoritativa para Personal Externo

- **Portal de Peticiones**. Describe el conjunto de interface de usuario para permitir a los usuarios finales realizar peticiones de acceso a los sistemas y de autoservicio de contraseñas.

  Este bloque funcional contendrá los elementos necesarios para dotar a la solución de una interfaz de autoservicio que facilitará la disposición de un catálogo de recursos y la interacción de los actores técnicos y organizativos en la gestión automática de los recursos. El portal de peticiones dará cobertura a las siguientes funcionalidades y necesidades:

  - Consola de Administración y Autoservicio
  - Autoservicio de Contraseña
  - Interfaz Web de gestión
  - Workflow de petición de Roles y Accesos
  - Solicitud de nuevos Roles
  - Registro de peticiones de acceso
  - Compatibilidad con dispositivos móviles
  - Flexibilidad en cuanto a los mecanismos de autenticación y autorización

- **Access Manager**. Es el sistema que debe gestionar las necesidades inherentes a los accesos a los sistemas de información.

  Este bloque funcional contendrá los elementos necesarios para establecer la integración de las aplicaciones y el control de accesos a las mismas, debiendo satisfacer las siguientes necesidades:

  - Control de Accesos Centralizados
  - Compatibilidad con Federación de Identidades
  - Gestión de *Token* para Federación de Identidades
  - Federación con soluciones *SaaS*

- Portal de aplicaciones a las que el usuario tenga acceso.
- Sesiones programáticas e intercambio de sesiones entre procesos automatizados
- Interface Web de Gestión
- Interface de gestión Automatizada
- Integración con diferentes sistemas de Autenticación
- Niveles de Autenticación y Autorización
- Autenticación Adaptativa
- Control basado en origen
- Agregación de datos a las aplicaciones
- Compatibilidad con fuentes de datos
- Control y gestión de sesiones
- Auditoría e Informes
- Sistema de Notificaciones
- Gestión de eventos y *logs* remotos

- **Gobierno y Cumplimiento Normativo**. Es el sistema que describe todo lo relacionado con las Reglas de Negocio de los accesos a los sistemas, los procesos de recertificación, y las asignaciones de los permisos acordados.

  Este bloque funcional contiene los elementos necesarios para establecer los procesos de control y trazabilidad en el cumplimiento de los accesos según los criterios establecidos y validados, para garantizar los siguientes principios y necesidades:

  - Creación de Roles para la Organización.
  - Implementación de un modelo RBAC.
  - Automatización de Roles.
  - Asignación de Roles bajo demanda.
  - Recertificación de accesos.
  - Separación de tareas (SoD)
  - Evaluación de riesgo de accesos asignados

3.2 Requisitos Identificados

Los requisitos identificados se recogen el documento “GID-Requisitos.docx”

En este punto EJIE se muestra receptivo a flexibilizar algunos requisitos o incluir algunos no contemplados.

3.3 Requisitos Técnicos para la infraestructura de IAM

Bajo la iniciativa «BATERA» se está llevando a cabo un proceso de convergencia en materia TIC, circunscrita a las instalaciones y otros elementos relacionados (como son las Infraestructuras, Comunicaciones, Puesto de trabajo y Servicios corporativos unificados). BATERA establecerá las nuevas líneas que regirán el modelo de gestión TIC para los próximos años del Sector Publico de la Comunidad Autónoma de Euskadi. El nuevo modelo tiene como principal objetivo aprovechar sinergias y evitar posibles duplicidades.

El ámbito del proyecto BATERA comprende la Red Corporativa Administrativa del Gobierno Vasco y las Redes Sectoriales, así como cualquier infraestructura informática y de comunicaciones utilizada por las entidades del sector público de la CAE. Se abordan los siguientes aspectos:

- Consolidación de los CPDs y Salas Técnicas
- Convergencia de las comunicaciones
- Gestión unificada de servicios corporativos
- Racionalización de los CAU
- Virtualización del puesto de trabajo
- Consolidación y unificación de los servicios de impresión
- Seguridad y cumplimiento de la Ley Orgánica de Protección de Datos
- Obsolescencia

Áreas afectadas

- **Infraestructuras CPD.**
  El objetivo principal que se persigue en este ámbito es transformar y modernizar las infraestructuras de los CPDs. Consolidar tanto las instalaciones (CPD y Salas Técnicas), como la infraestructura de servidores, almacenamiento y *backups* (así como servicios compartidos), soportando todos los procesos de negocio de cada uno de los organismos involucrados.

- **Comunicaciones.**
  El objetivo en esta área es desarrollar un sistema de múltiples proveedores para cada servicio con un contrato único, así como incrementar la flexibilidad de los servicios para adaptarse a las necesidades puntuales de las Redes Sectoriales y Organismos.

- **Puesto de Trabajo.**
  El objetivo es buscar sinergias en la prestación de servicios alrededor de los equipos PC para los puestos de trabajo, que ofrece grandes posibilidades para homogeneizar su configuración, adquisición de licencias, etc... y, de esta forma, aumentar la flexibilidad y la movilidad.

- **Servicios Corporativos Unificados.**
  Dentro de este epígrafe están incluidos servicios como:
  - Correo Electrónico
  - Herramientas de Colaboración (ofimática, almacenamiento de información y soluciones para trabajo compartido)
  - Mensajería unificada (videoconferencia, voz, reuniones web)
  - Identidad y Gestión de Accesos (infraestructura para la gestión de las personas usuarias y perfiles de cualquier aplicación informática)

La infraestructura hardware de la solución IAM deberá alojarse, por tanto, en BATERA. Para ello EJIE, a través de BATERA, dispondrá del hardware, licencias y comunicaciones para el despliegue de todos los componentes

necesarios en la arquitectura que se proponga. El adjudicatario deberá realizar un análisis y diseño de arquitectura, comunicaciones y dimensionamiento hardware de la solución IAM con Oracle, así como de los requisitos software base que se requieran, a fin de solicitar a BATERA la disposición de los recursos TI.

Sera responsabilidad de adjudicatario la instalación de pre-requisitos software y software de los productos y componentes para la solución *Oracle Identity Governance,* conjuntamente con el área de soporte en EJIE.

4 Metodología Aplicable y Entorno Tecnológico.

Como norma de modo habitual, la organización del trabajo y la prestación de los servicios están basados en ARINbide, No obstante, tal y como se ha mencionado con anterioridad, el nivel de cumplimiento de los mismos dentro de los servicios a prestar deberá concretarse en las fases iniciales del proyecto. Aun así, las ofertas presentadas deberán tomar como referencia dichos modelos y metodologías, que se explican brevemente a continuación.

4.1 Metodología de desarrollo, normativa y Guía de Estilo

ARINbide-Predictivo se concibe como una metodología práctica para el ciclo de vida completo del software, basada en Métrica 3, y adaptada a las necesidades y directrices de EJIE Además consta de un apartado para el establecimiento de una metodología de Gestión de Proyectos. Como Plan de Calidad la propia metodología, en sus apartados de trabajo habitual, genera los registros de calidad necesarios para el sistema de calidad de EJIE.

Para todo el ciclo de vida del proyecto, ARINbide-Predictivo define los siguientes procesos:

- Ingeniería del Software (ISW)
- Gestión del Proyecto (GPR)
- Gestión de Riesgos del Proyecto (GRP)
- Gestión de la configuración (GCO)
- Mantenimiento del Sistema de Información (MSI)

El proceso principal de ingeniería del software (ISW) describe y normaliza la secuencia de fases y actividades a realizar en el proyecto de desarrollo de un sistema de información, así como los entregables a obtener en cada una de ellas. En este ámbito, ARINbide-Predictivo contempla el desarrollo de las siguientes fases metodológicas:

- Catálogo de Requisitos de Usuario (CRU) (proceso diferenciado dentro del Análisis del Sistema de Información, ASI)
- Análisis del sistema (ASI)
- Diseño del sistema (DSI)
- Construcción del sistema (CSI)
- Implantación y aceptación del sistema (IAS)

El ciclo de vida descrito en la metodología de desarrollo ARINbide-Predictivo se alinea y complementa a lo largo del tiempo con la metodología de pruebas corporativa PROBAMET, centrándose ésta última en la especificación de todas las actividades relacionadas con la planificación, definición y ejecución de los diferentes tipos de pruebas. Existe una correspondencia entre las fases de ejecución de ARINbide-Predictivo y las fases de ejecución de PROBAMET.

En la sección "Perfil de contratante>Información técnica>Metodología de desarrollo" de la página web de EJIE se puede obtener información detallada sobre ARINbide-Predictivo.

En las distintas fases del proyecto y, teniendo en cuenta las mencionadas metodologías la empresa adjudicataria deberá basarse, entre otros, en los siguientes elementos:

- Diseño del sistema. Lo realizará en su totalidad la empresa adjudicataria y en sus dependencias. Debe incluir:
    - Diseño de las aplicaciones, DSI. (EDS)
    - Especificar el detalle del Plan de Pruebas del sistema por cada uno de los niveles de prueba: unitarias, de integración, de sistema, de implantación y de aceptación.

- Construcción del sistema.

- Lo realizará en su totalidad la empresa adjudicataria en sus dependencias, teniendo en cuenta las directrices de EJIE en lo que se refiere a los módulos estándar, las normas de funcionamiento y albergue de las aplicaciones en Internet/Intranet, el Manual de Identidad Corporativa del Gobierno Vasco y las directrices de la Dirección de Atención a la Ciudadanía en lo que respecta a estética, diseño y funcionalidades de las páginas Web.
- Incluirá la ejecución del Plan de Pruebas, para verificar el cumplimiento de los requisitos establecidos en el mismo, abarcando pruebas unitarias, de integración y del sistema.
- Los entregables de esta fase incluyen la Especificación de Construcción del Sistema (ECS) y el sistema construido.
- Asimismo, deberán respetarse las convenciones adoptadas para un desarrollo de aplicaciones homogéneas.
- El diseño del sistema tendrá en cuenta el nivel de accesibilidad AA (WAI-AA), para aquellos módulos que sean accesibles desde Internet.
- Todos los sistemas desarrollados deberán soportar al menos los siguientes idiomas: euskera, castellano.
- La aplicación, las páginas, los textos, los mensajes de error/aviso y/o cualquier otro componente (tool-tip, textos en imagen…) dirigidos al/a la usuario/a final deberán estar al menos en ambos idiomas: euskera y castellano.

- Implantación en desarrollo. La empresa adjudicataria realizará los siguientes puntos
  - La entrega de la aplicación en el sistema corporativo de control de versiones, tanto de la entrega inicial como de las sucesivas
  - Llevará a cabo la instalación de la aplicación en el entorno de desarrollo de EJIE, habiendo realizado previamente las pruebas necesarias durante la fase de construcción
  - Ejecución de las Pruebas del sistema, acorde con lo establecido.
- Implantación en entornos de test o preproducción y producción. La empresa adjudicataria efectuará los siguientes puntos
  - Preparará los paquetes y llevará a cabo la realización de la correspondiente implantación en los entornos de preproducción y producción junto con el personal de soporte de EJIE.
  - Ejecución de las Pruebas del sistema, y en el caso de que se requiera, estas pruebas se realizarán en las dependencias de EJIE en sus distintos niveles de prueba, incluidas las Pruebas de Aceptación.
- Pruebas de prestaciones:
  - Realización de pruebas de rendimiento y carga, que incluyen la verificación de los niveles de respuesta de la aplicación ante las previsiones de carga del sistema, así mismo se verificará el comportamiento global del sistema en cuanto a consumo de memoria y CPU de sus componentes, así como según se considere de capacidad, stress, escalabilidad
- Implantación en producción y puesta en marcha del sistema. Incluirá:
  - Fuentes de la aplicación.
  - BBDD: scripts y carga inicial de datos.
  - Sistema implantado en los entornos de EJIE
  - Informe de los resultados de los distintos niveles de pruebas.
  - Manuales requeridos para la prestación del servicio en producción y definidos por los procesos ITIL de EJIE.
  - Manuales de Usuario y la Ayuda On-line deberán estar en ambos idiomas: euskera y castellano.
  - Formación a los/las usuarios/as y administradores/as del sistema.
  - Sistema implantado en entorno de producción.

En todas las fases del proyecto, así mismo será de referencia el documento de Estándares de desarrollo de sistemas software, que establece requisitos obligatorios y recomendaciones a seguir en todo el proceso de ejecución del proyecto, en cuanto a la elaboración de los productos y la entrega de los mismos a EJIE Cabe destacar que para el caso de desarrollo de aplicativos con interfaz web basado en navegador que será desplegado en el contexto de internet, las pruebas del sistema deberán contemplar los ensayos necesarios

para garantizar que el sistema se comporta correctamente en los navegadores más utilizados (Internet Explorer, Firefox, Chrome, Opera, y Safari). Mientras que si el contexto de despliegue es intranet (con PCs gestionados), el sistema deberá soportar los navegadores homologados por los estándares tecnológicos publicados por la Dirección de informática y telecomunicaciones del GV para dicho contexto. Para el caso de extranet, la lista de navegadores a soportar se deberá decidir en función de los colectivos usuarios de la aplicación y del uso o no de PCs gestionados.

Igualmente será de referencia el **Documento de Estándares Tecnológicos** de Gobierno Vasco, publicado en: www.euskadi.eus/informatika

4.2 Herramientas del ciclo de vida de las aplicaciones

Como soporte e instrumento necesario en la ejecución de todas las fases del proyecto, existe un conjunto de Herramientas homologadas por EJIE, que abarcan todo el ciclo de vida de las aplicaciones, y que facilitan la realización de distintas tareas y normalizan la obtención de entregables.

Estas herramientas homologadas son las que se utilizan en el entorno de trabajo de EJIE, no pudiendo utilizarse en el mismo otras herramientas similares o equivalentes.

Para los trabajos a realizar en las dependencias de la empresa proveedora, su uso es recomendado frente a otros productos o herramientas del mercado, para dar cobertura a los cometidos para los que están destinadas. No obstante, en los casos en los que el resultado de uso de las herramientas sea un entregable con un formato específico y normado, su uso será obligatorio frente a otras herramientas de mercado, o bien en cualquier caso deberá proporcionarse un formato compatible.

En el documento PCT-Anexo Herramientas se detallan las herramientas homologadas.

5 Descripción de entregables.

Los productos a entregar, tanto productos software como la documentación, serán aquellos que define la metodología de desarrollo ARINbide-Predictivo en referencia a las fases definidas dentro del alcance del proyecto.

Con independencia de lo descrito y requerido a nivel metodológico (metodología de desarrollo ARINbide-Predictivo, y Metodología de Pruebas), a continuación, se detallan las tareas y entregables a realizar/suministrar por la empresa adjudicataria:

Presentación del Proyecto

Plan de Gestión del Proyecto que incluya la planificación de todas las fases establecidas.

Diseño de la arquitectura de la solución.

Diseño funcional detallado de la solución.

Documento de albergue de la solución en cada entorno.

Plan de instalación y despliegue.

Libro Blanco de integración de aplicaciones en el sistema de Control de Accesos y procedimientos para la migración de aplicaciones XLNETs

Definición, ejecución y gestión del Plan de Pruebas de integración y aceptación requeridas en cada uno de los sistemas y fases establecidas.

Informe detallado de las pruebas realizadas y resultados

Manuales de usuario y operación. Confección y entrega de la documentación (funcional, técnica, de explotación y de usuario/a) correspondiente a cada una de las fases del proyecto tanto en formato papel, como en formato electrónico.

La documentación destinada a usuario/a deberán estar en ambos idiomas: euskera y castellano

Instalación de software e implantación en los entornos de Softbase, Desarrollo Pruebas y Producción de EJIE así como documentación final con el detalle de la implementación.

La aplicación, las páginas, los textos, tablas de códigos, los mensajes de error/aviso y/o cualquier otro componente (tool-tip, textos en imagen…) dirigidos al/a la usuario/a final deberán estar en ambos idiomas: euskera y castellano.

Entrega de fuentes de todos los componentes, ficheros de configuración, elementos gráficos utilizados y cualquier otro elemento que se considere necesario para el normal y adecuado mantenimiento/evolución del sistema, en soporte magnético y/o electrónico.

Todos los entregables que procedan deberán proporcionarse utilizando las herramientas homologadas en EJIE para el ciclo de vida de las aplicaciones, o en su caso proporcionando formatos compatibles.

5.1 Normativa para la puesta en producción y posterior explotación del sistema

EJIE cuenta con actividades formalizadas para la gestión e implantación de los sistemas de información generados en los distintos entornos, establecidas en base a los procesos de Gestión de Cambios y Gestión de Despliegues.

A partir de estos procesos se garantiza que los sistemas que serán instalados en la infraestructura de EJIE cumplen con los estándares y normativas técnicas de la organización, que no impactarán en el correcto funcionamiento del resto de productos y que se conocen los procedimientos y particularidades relacionadas con su operación y soporte.

Para ello, es necesario que, durante el ciclo de vida del proyecto, el equipo de trabajo genere una serie de entregables, que serán validados a través del proceso de Gestión de Cambios:

Ficha de proyecto y Plan de Implantación: primera aproximación a Gestión de Cambios donde se informa qué se va a hacer y calendario aproximado.

Documento de albergue: recoge el diseño lógico e información de cualquier elemento no estándar o que pueda impactar tanto en necesidades de infraestructura como de usuario/a final.

Manual de implantación: recoge los aspectos técnicos y configuraciones necesarias que deben ser realizadas para implantar la aplicación en un entorno tecnológico de EJIE.

Manual de producción: contiene toda información que necesita tanto operación como los procesos para poder dar correctamente el servicio de explotación a partir del día de Puesta en Producción del proyecto.

Plantilla de monitorización: recoge los elementos no estándar cuya monitorización permite conocer el estado de los sistemas.

Para cada uno de estos documentos EJIE dispone de plantillas estándar que el proveedor deberá utilizar y entregar según los procedimientos establecidos.

Asimismo, en la cumplimentación de las plantillas se podrá solicitar el asesoramiento de los/las distintos/as Responsables de Proceso y Coordinadores/as de Infraestructura, para asegurar que la solución construida e implantada cumple con la normativa de EJIE y es posible operarla y soportarla con garantías.

6 Planificación y Organización

6.1 Plan de Proyecto

6.1.1 Plan de Entregas e Hitos de Control

La empresa licitadora deberá incluir en su Documento de Propuesta Técnica una descripción de las principales:

- Fases y tareas del proyecto,
- Entregas resultantes de cada fase,
- Hitos de control y/o verificación,

Junto con sus correspondientes fechas orientativas de finalización.

Así mismo, la empresa licitadora podrá establecer propuestas de entregas y/o certificaciones parciales acordes con el planteamiento del proyecto establecido, siempre que:

- Lo considere más adecuado para facilitar la implantación y puesta en marcha del objeto del contrato.
- No se establezca nada en sentido contrario en los apartados de: *Objeto, Alcance y Descripción del Proyecto*.

6.1.2 Diagrama de Gantt

La empresa licitadora deberá presentar un Diagrama de Gantt o Cronograma de las Fases y Tareas propuestas para la ejecución de las realizaciones objeto del presente pliego.

6.2 Organización del Equipo de Trabajo

La empresa licitadora deberá describir en su Documento de Propuesta Técnica:

- La organización (perfiles) del equipo de proyecto asignado a la realización de las actividades resultantes del presente pliego
- Las funciones de los mismos.

6.3 Transferencia Tecnológica.

Durante la ejecución de los trabajos objeto del contrato la empresa adjudicataria se compromete, en todo momento, a facilitar a las personas designadas por la Dirección del proyecto de EJIE, y a tales efectos, la información y documentación que ésta solicite para disponer de un pleno conocimiento de los trabajos desarrollados, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos, y herramientas utilizados para resolverlos.

7 Mecanismos de Seguimiento, Control y Supervisión

La gestión del proyecto se realizará según las normas procedimentales y de calidad de la Gestión de Proyectos de EJIE

El control y seguimiento de la calidad de servicio, será realizado por la Dirección del Proyecto de EJIE

Durante el desarrollo y ejecución del proyecto, EJIE podrá establecer controles de calidad sobre la actividad desarrollada.

7.1 Mecanismos de Seguimiento y Control.

El equipo de trabajo estará dirigido por un/una Responsable del Proyecto con dedicación estable y suficiente, quien coordinará las tareas implicadas en el proyecto y será el/la interlocutor/a principal con la Dirección del Proyecto de EJIE

Deberán establecerse todos los mecanismos de control que permitan verificar de forma continuada el cumplimiento de los objetivos especificados, tanto en plazos como en términos de calidad final. Para ello se contempla:

- Reuniones de seguimiento: a partir del plan de entregas requerido se celebrarán reuniones periódicas o coincidiendo con los puntos de decisión, destinadas a revisar el grado de cumplimiento de las tareas planificadas, le entrega de productos, las reasignaciones de personal, la validación de las programaciones de actividades a realizar, etc.
- Reuniones de control económico: de control económico del proyecto para llevar a cabo el plan de pagos establecido.
- Informes de situación y progreso: con los que la empresa adjudicataria comunicará a la Dirección del Proyecto de EJIE, del estado puntual de los trabajos, de los objetivos alcanzados, de las incidencias ocurridas, etc.
- Certificaciones parciales: si procede.
- Hojas de control de tareas: si procede.
- Documentos de gestión de proyectos: a solicitud del/de la responsable de EJIE, la empresa adjudicataria cumplimentará los documentos de gestión de proyectos, según un modelo definido: actas de reuniones, registro de inspección y ensayo, informes de progreso, control de configuración (módulos-componentes instalados), etc.

7.2 Supervisión del proyecto

Tanto la dirección como la supervisión del Proyecto serán llevadas a cabo por el personal de EJIE, S.A. asignado al proyecto.

Los productos del trabajo deberán ser aprobados tanto por el/la Responsable del Proyecto por parte de la empresa adjudicataria, como por la Dirección del Proyecto de EJIE, si los encuentran conformes, emitirán su informe favorable, empezándose a computar desde ese momento el período de garantía que todo trabajo de realización externa debe aportar en previsión de defectos no detectados en las pruebas realizadas.

El incumplimiento de los plazos pactados sin causa que lo justifique dará lugar a las penalizaciones que se acuerden en el presente pliego (si existieran).