DOC 5

PLIEGO DE PRESCRIPCIONES TECNICAS

Contenido

1- Situación actual 3
2.1- Productos de la plataforma y licencias 3
2.2- Arquitectura general 4
2.3- Funcionalidades de GISSO 5
2.3.1- Oracle Access Manager 5
2.3.1.1- Single Sign-On con WebGates 6
2.3.1.2- Federación (SAML 2.0) 6
2.3.1.3- OAuth 7
2.3.1.4- Plugins de Autenticación Customizados 7
2.3.2- Oracle Identity Manager 8
2.3.2.1- Provisión 8
2.3.2.2- Recursos Desconectados 9
2.3.2.3- Políticas de Acceso 9
2.4- Funcionalidades implementadas en la UPV/EHU 9
2.4.1- Control de Accesos 9
2.4.2- Proceso de cambio de contraseña 10
2.4.3- Organizaciones 10
2.4.4- Colectivos 10
2.4.5- Ciclo de vida del usuario 11
2.4.6- Aplicaciones y procesos 11
2.4.7- Código fuente 11
2.5- Inventario de Servidores 12
2- Necesidad e idoneidad de la contratación 14
3- Prestación a contratar 15
3.1- Objeto 15
3.2- Necesidades detectadas 15
3.2.1- Productos de la plataforma 15
4.2.2- Arquitectura general 16
4.2.3- Funcionalidades Oracle Access Manager 16
4.2.4- Funcionalidades Oracle Identity Manager 16

4.2.5- Funcionalidades implementadas en la UPV/EHU 17
4.2.6- Nueva arquitectura de servidores y de productos que contemple 18
4.3- Plan de implantación de la propuesta 19
4.4- Plan de entrega 19
4.4- Plan de formación 19
5- Lugar de ejecución 20
6- Servicio de soporte. 20
7- Garantía y condiciones de las licencias 20
8. Equipo de trabajo 20
9. Confidencialidad. 21

1- Situación actual

1.1- Productos de la plataforma y licencias

Los productos que conforman la plataforma GISSO implantada en la UPV/EHU son los siguientes:

- Oracle Access Manager 11.1.2.3.x
- Oracle Identity Manager 11.1.2.3.x
- Oracle Virtual Directory 11.1.1.2
- Oracle WebLogic 10.3.6.0
- Oracle WebGates 10g (fuera de soporte)
- Oracle Enterprise Single Sign-On 11.1.2.x
- JDK 1.7.0_91 / JDK 1.6.0_14

Oracle Access Manager es una aplicación para el control de accesos, cuya funcionalidad principal es centralizar en un único punto los procesos de autenticación y autorización de las aplicaciones.

Oracle Access Manager realiza el papel de un Proveedor Identidad en el contexto de un entorno de Single Sign-On, permitiendo al usuario autenticarse una sola vez para acceder a sus aplicaciones, y a las aplicaciones delegar los procesos de autenticación y autorización en un único punto.

Oracle Identity Manager es una aplicación de gestión de identidades, y por lo tanto centraliza la administración de las cuentas de usuarios y orquesta los cambios de éstas entre los diferentes repositorios de usuarios de las aplicaciones integradas. Con Oracle Identity Manager se pueden administrar todas las cuentas de un usuario de forma centralizada, de forma que no sea necesario ir aplicación por aplicación para replicar los cambios en un usuario.

Oracle Virtual Directory es un repositorio virtual, que ofrece una vista de tipo LDAP (repositorio jerarquizado de usuarios), es decir, no almacena los datos que muestra, sino que los recoge de otros repositorios, y su protocolo de acceso es de tipo LDAP (Lightweight Directory Access Protocol).

Oracle WebLogic es un servidor de aplicaciones sobre el que despliegan en este contexto Oracle Access Manager y Oracle Identity Manager.

Orace WebGate es un módulo que se instala en los frontales de acceso a las aplicaciones para controlar que el acceso a las aplicaciones se realiza una vez que el usuario se ha autenticado en Oracle Access Manager y que éste le ha autorizado a acceder.

Oracle Enterprise Single Sign-On es un producto que permite delegar la gestión de las contraseñas, tanto para clientes de escritorio como para clientes Web.

JDK es el lenguaje de programación utilizado en este caso por aplicaciones como Oracle Access Manager u Oracle Identity Manager.

La universidad cuenta ya con las siguientes licencias:

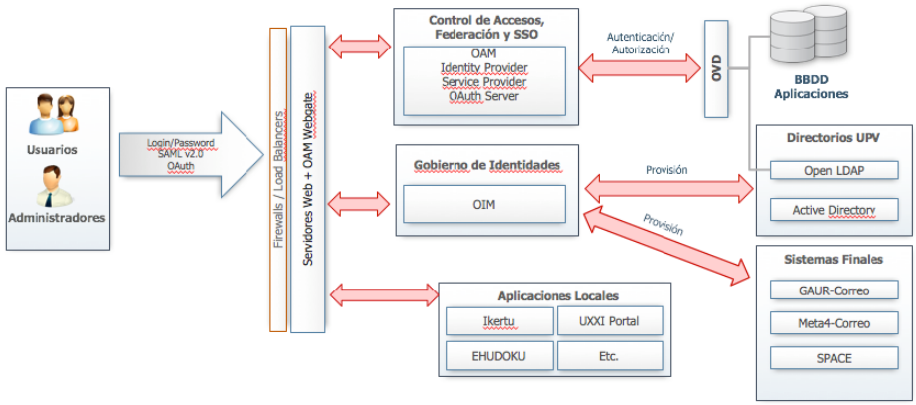
- Oracle Enterprise Single Sign-On Suite Plus - Named User Plus Perpetual (8220 users)
- Oracle Identity and Access Management Suite – Employee User Perpetual (8200 users)

- Oracle Identity and Access Management Suite – Non Employee User – External Perpetural (50000 users)
- Oracle Identity Manager Connector – Database Applications Table - Connector Perpetual
- Oracle Identity Manager Connector - IBM Lotus Notes/Domino - Connector Perpetual
- Oracle Identity Manager Connector - Microsoft Active Directory - Connector Perpetual
- Oracle Identity Manager Connector - SAP Enterprise Applications – Connector Perpetual
- Oracle Identity Manager Connector - Sun Java System Directory - Connector Perpetual

1.2- Arquitectura general

La arquitectura de la plataforma se define en el siguiente diagrama:

Diagrama de Arquitectura



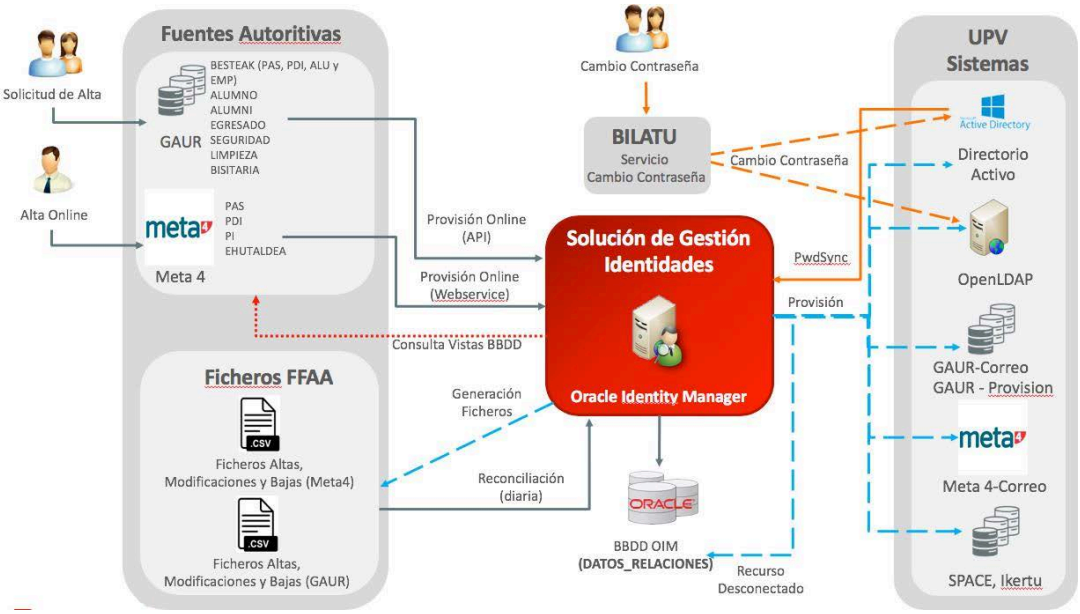
En lo referente al Single Sign-On, Oracle Access Manager permite el Single Sign-On para varias aplicaciones utilizando diferentes mecanismos de propagación de la sesión (WebGates, SAML2.0 y OAuth).

La autenticación la realiza contra Oracle Virtual Directory, que virtualiza usuarios de un OpenLDAP y de una base de datos.

En lo referente a la gestión de identidades, Oracle Identity Manager tiene como fuentes confiables las aplicaciones GAUR y Meta4, Bilatu, Registro y Sarbidea[1] para la gestión de contraseñas. Las tres primeras para personas vinculadas a la universidad y las dos últimas para personas sin vinculación. La información de estas aplicaciones puede llegar desde procesos de reconciliación masivos o desde Web Services si es on-line. Por otro lado, se provisionan una serie de aplicaciones y repositorios (OpenLDAP, Active Directory, GAUR, Meta4, Correos, SPACE, Ikertu, etc.).

Las integraciones de Oracle Identity Manager se recogen en el siguiente diagrama:

[1] Registro y Sarbidea no aparecen en el gráfico siguiente



1.3- Funcionalidades de GISSO

En este capítulo se detallan las funcionalidades de los productos principales de la plataforma GISSO: **Oracle Access Manager** para el control de accesos y **Oracle Identity Manager** para la gestión de identidades.

1.3.1- Oracle Access Manager

Las funcionalidades utilizadas en GISSO de Oracle Access Manager:

- SSO con WebGates
- Federación (SAML2.0)
- OAuth
- Plugins de Autenticación Customizados

El producto ofrece además otras funcionalidades que no han sido implementadas o que actualmente no están en uso:

- Reglas de acceso
- Auditoría de accesos
- Windows Native Authentication (WNA)
- Secure Token Service
- Mobile & Social
- Mobile Security
- Remember Me

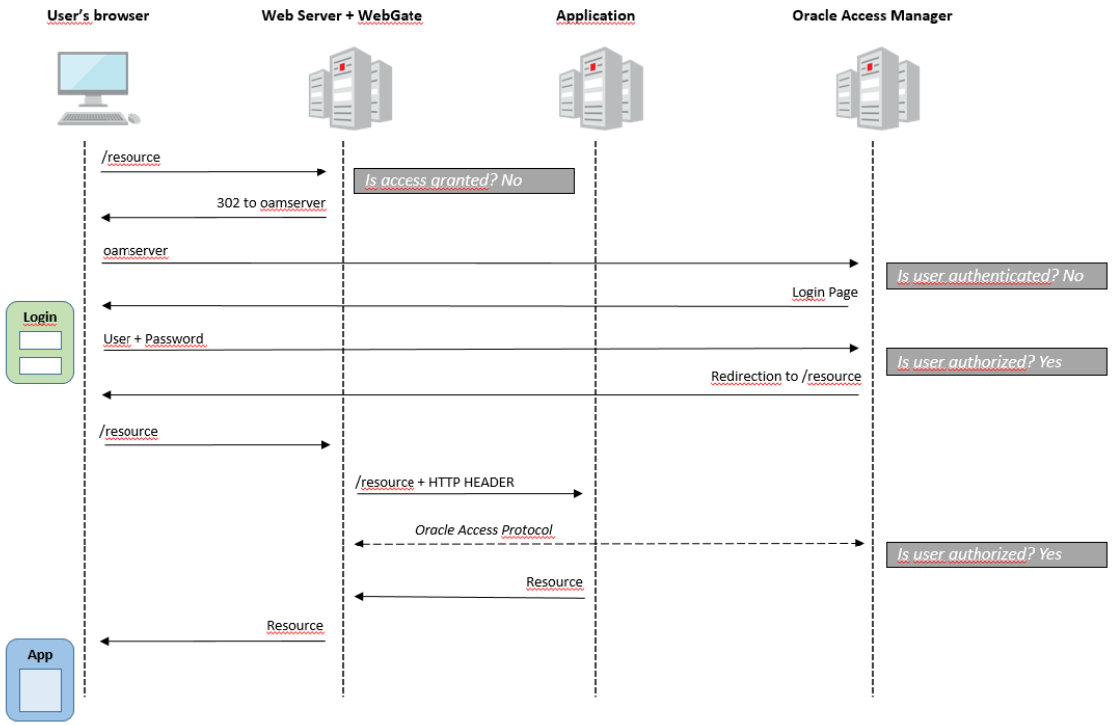
A continuación, se explican los objetivos de las funcionalidades implementadas.

1.3.1.1- Single Sign-On con WebGates

El Single Sign-On mediante WebGates se basa en la instalación de un módulo denominado WebGate en la capa de frontales de acceso a las aplicaciones (apaches, OHS, IHS, IIS, etc.) que captura el tráfico de acceso a las aplicaciones, y comprueba que el usuario ha sido autenticado y autorizado por Oracle Access Manager.

Una vez autenticado y autorizado el usuario, el WebGate se encarga de transmitir a la aplicación mediante diferentes mecanismos (como la inyección de cabeceras HTTP) quién es el usuario que ha establecido sesión, e incluso algún atributo más de la identidad del usuario si es necesario.

El diagrama de flujos de un proceso de acceso mediante describe a continuación:



Los WebGates deben tener comunicación directa con los servidores de Oracle Access Manager para realizar consultas sobre autenticación y autorización, utilizando el Oracle Access Protocol (OAP).

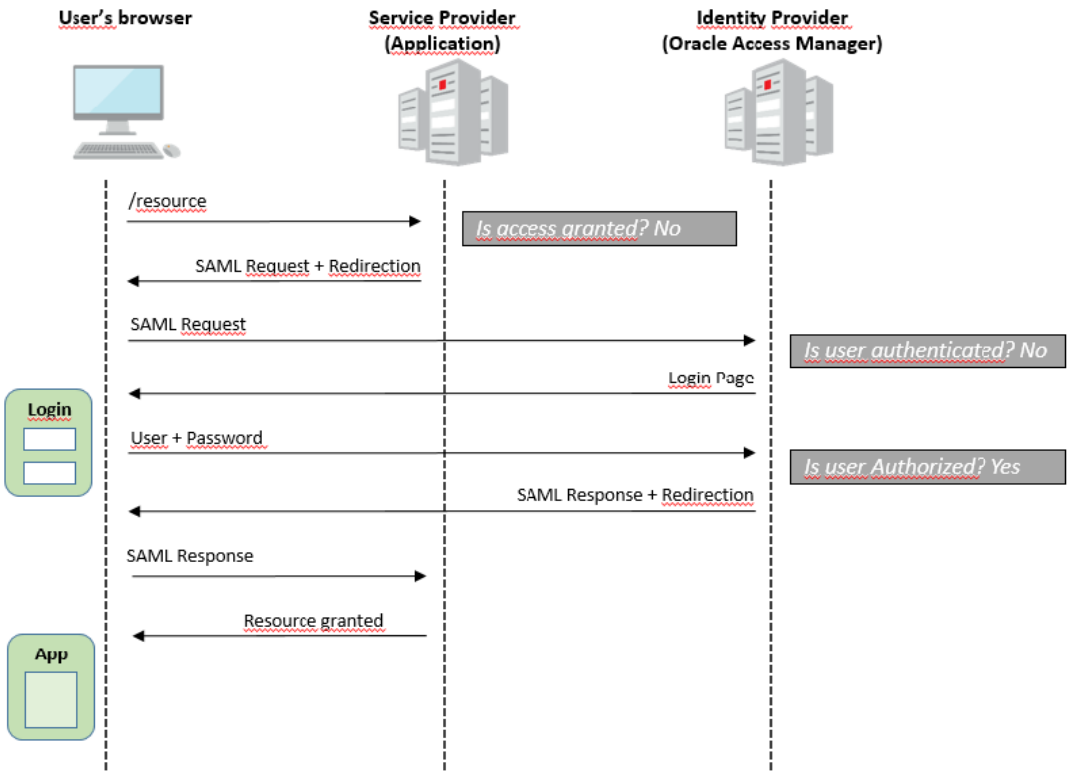
1.3.1.2- Federación (SAML 2.0)

La federación de identidades permite implementar in Single Sign-On entre diferentes dominios de identidad, es decir, entre diferentes aplicaciones en la que cada una tiene su propio repositorio de usuarios.

La federación de identidades en Oracle Access Manager se realiza principalmente con el protocolo SAML 2.0.

Oracle Access Manager puede desempeñar el papel de Identity Provider y/o de Service Provider. Es decir, puede autenticar al usuario y propagar la sesión hacia un Service Provider (otra aplicación), o puede recibir la sesión de un Identity Provider externo.

El siguiente diagrama muestra el flujo de un Single Sign-On:



Actualmente se utiliza federación de identidades para acceder a Alfresco, desempeñando Oracle Access Manager el papel de Identity Provider y Alfresco el de Service Provider.

1.3.1.3- OAuth

OAuth es un mecanismo de Single Sign-On alternativo a SAML 2.0, pensado en ofrecer más escenarios posibles de trabajo que se puede utilizar tanto para aplicaciones Web como para aplicaciones móviles.

Ya se está utilizando en GISSO, en concreto para el Single Sign-On con las aplicaciones:

- moodleClient
- ehutbClient
- egelaxClient

1.3.1.4- Plugins de Autenticación Customizados

Uno de los mecanismos de extensión de funcionalidades de Oracle Access Manager es el desarrollo de plugins de autenticación. Estos plugins permiten incluir nuevos flujos de autenticación para incorporar nuevas funcionalidades.

Los desarrollos se basan en la implementación de un interfaz Java y de la configuración del plugin en Oracle Access Manager.

Se pueden utilizar para ofrecer un mecanismo alternativo de autenticación para el usuario o incluso un segundo factor de autenticación.

En Oracle Access Manager se utiliza un plugin de autenticación customizado para realizar la autenticación con certificado.

1.3.2- Oracle Identity Manager

Las funcionalidades utilizadas en GISSO de Oracle Identity Manager son las siguientes:

- Provisión
- Recursos Desconectados
- Políticas de Acceso

El producto ofrece además otras funcionalidades:

- Auto-servicio
- Auto-registro
- Flujos de aprobación
- Políticas de Contraseñas
- Políticas de Auditoría
- Certificaciones
- Notificaciones
- Administración delegada
- Auditoría
- Ciclo de vida de roles

1.3.2.1- Provisión

La provisión de usuarios en otros sistemas se realiza en Oracle Identity Manager mediante conectores, cuyo catálogo es extenso y, además, se dispone de la posibilidad de desarrollar conectores propios. Se dividen en tres grupos:

- Conectores 9x
- Conectores 11g
- Conectores 12c

Algunos de los conectores disponibles en 12c:

Box	Concur	Database Application Tables	Database User Management	Google Apps
GoToMeeting	Identity Cloud Service	Microsoft Active Directory User Management	Office365	Oracle e-Business Employee Reconciliation
Oracle e-Business User Management	Oracle Internet Directory	Salesforce	SAP Success Factor	SAP User Management
SAP User Management Engine	ServiceNow	Unix	WebEx	

El desarrollo de conectores se puede realizar directamente en Java, implementando adaptadores, o mediante la implementación de interfaces en Java del estándar ICF (Identity Connector FrameWork). Esta segunda opción permite reutilizar después los conectores en otros ámbitos, ya que implementan un interfaz de un estándar.

1.3.2.2- Recursos Desconectados

Los recursos desconectados permiten simular una aplicación o un servicio, y gestionar éste mediante Tareas Humanas de flujos de SOA y notificaciones.

Se crean al dar de alta una nueva instancia de aplicación, y generan los metadatos de conector necesarios (requieren un sandbox). Se pueden extender para meter atributos adicionales o formularios hijos.

1.3.2.3- Políticas de Acceso

Actualmente se tienda a que el administrador solamente tenga que indicar un rol de alto nivel, y en base a éste se automatice la provisión de las aplicaciones.

Para implementar el modelo de asignación de un rol de alto nivel, Oracle Identity Manager utiliza las Políticas de Acceso que permiten definir las aplicaciones y perfiles de las mismas y los roles que las provisionan de forma automática.

1.4- Funcionalidades implementadas en la UPV/EHU

1.4.1- Control de Accesos

La pantalla de inicio de sesión de GISSO muestra diferentes opciones de autenticación en función de si se quiere acceder con credenciales de Colectivo UPV/EHU, Colectivo externo NOTES o Colectivo no-corporativo GAUR.

En función de estas opciones el proceso de login lo realiza una aplicación diferente. Solamente en el caso de UPV/EHU el proceso de login lo realiza Oracle Access Manager.

Solo se usa por las aplicaciones que pueden integrarse con OAM.

1.4.2- Proceso de cambio de contraseña

La funcionalidad de cambio de contraseña se realiza desde Bilatu, que cambia la contraseña en el OIM y de ahí se distribuye a OpenLDAP y a Active Directory.

1.4.3- Organizaciones

Hoy en día no se está utilizando el modelo organizacional de Oracle Identity Manager y existen aproximadamente 194.832 usuarios repartidos en 4 organizaciones.

1.4.4- Colectivos

Los colectivos existentes actualmente en Oracle Identity Manager son los siguientes:

- Colectivos procedentes de META 4
  - PAS. Personal Administración y Servicios
  - PDI. Personal Docente e Investigador.
  - PI. Personal Investigador.
  - EHUTALDEA (001, 002, 003, 004, 005, 006 y 007). Grupos de personas que con relación no contractual directa con la UPV/EHU.
- Colectivos procedentes de GAUR
  - ALUMNO. Matriculado en UPV/EHU.
  - EGRESADO. Titulado en UPV/EHU.
  - SEGURIDAD. Personal de la contrata de seguridad.
  - LIMPIEZA. Personal de la contrata de limpieza.
  - BISITARIA. Visitas que requieren de tarjeta de acceso.
  - BESTEAK (PAS, PDI, ALU y EMP). Besteak Alumno/PAS/PDI y empleado.
  - BESTEAK 101. Besteak Alumno USAC, programa universitario norteamericano.
  - BESTEAK (102, 103 y 104).
- Colectivos sin vinculación con la Universidad
  - ALUMNI. Servicio al Exalumno.
  - VISITANTES. Auto-Registro-Sarbidea

Algunos usuarios pertenecen a más de un colectivo:

Nº DE COLECTIVOS	USUARIOS
1	70.800
2	9.323
3	800
4	14

1.4.5- Ciclo de vida del usuario

El estado de usuarios por estado es el siguiente:

ESTADO	USUARIOS
ACTIVE	205.575
DELETED	125
DISABLED	31

El ciclo de vida que se aplica es el siguiente:

- Para el PAS/PDI la fecha de caducidad se crea con la fecha fin de contrato. En el caso de contratos indefinidos la fecha es 01/01/4000.
- En el caso de los ALUMNOS la fecha de caducidad se corresponde con el 31/12 del año siguiente al de matrícula. Se va actualizando la fecha cada vez que se matricula. En el caso de anular su matrícula no se actualiza la fecha de caducidad.
- BESTEAK la fecha de caducidad es la fecha de baja del BESTEAK (limitado a un año como máximo). Se actualizará cada vez que se renueve dicho usuario.
- En el caso de los ALUMNI la fecha de caducidad está marcada con la fecha 01/01/3000.

1.4.6- Aplicaciones y procesos

La lista de aplicaciones y/o procesos en uso es la siguiente:

- Active Directory
- DATOSRELACIONES
- GaurEmail
- GaurEmailBesteak
- GaurEmailExternos
- Ikertu
- Lagun
- Meta4Email
- OpenLDAP
- ProvisionGAURALUMNO
- ProvisionGAURPAS
- ProvisonGAURPROFESOR
- SPACEUser

1.4.7- Código fuente

Se dispone del código fuente en los siguientes proyectos del repositorio de SVN:

- GISSO3CMC_Utils
- GISSOIM_AsignarRolesTask
- GISSOIM_Events

- GISSOIM_Relaciones
- GISSOIM_UPV_PendingRoleGrantsTask
- OIM11gR2_CMC
- OIM11gR2
- OimWsMeta4
- ServidorGaur_11gR2
- UPV_Codigo
- UPV_ConectorGaur_App
- UPV_ConnectorGaur_V2
- UPV_ConectorMeta4_App
- UPV_ReconciliacionTrusted_CMC

Este código arrastra algunas características que no son conformes a las buenas prácticas del fabricante, entre otras:

- Consultas a vistas o tablas de otras bases de datos (DB Link) sin la utilización de pooles de conexión.
- Aperturas de conexiones a base de datos de forma directa, sin la utilización de pooles de conexión.
- Lecturas y escrituras directas en base de datos.
- Gestión de logs no adecuado.
- Uso de clases obsoletas o deprecadas.

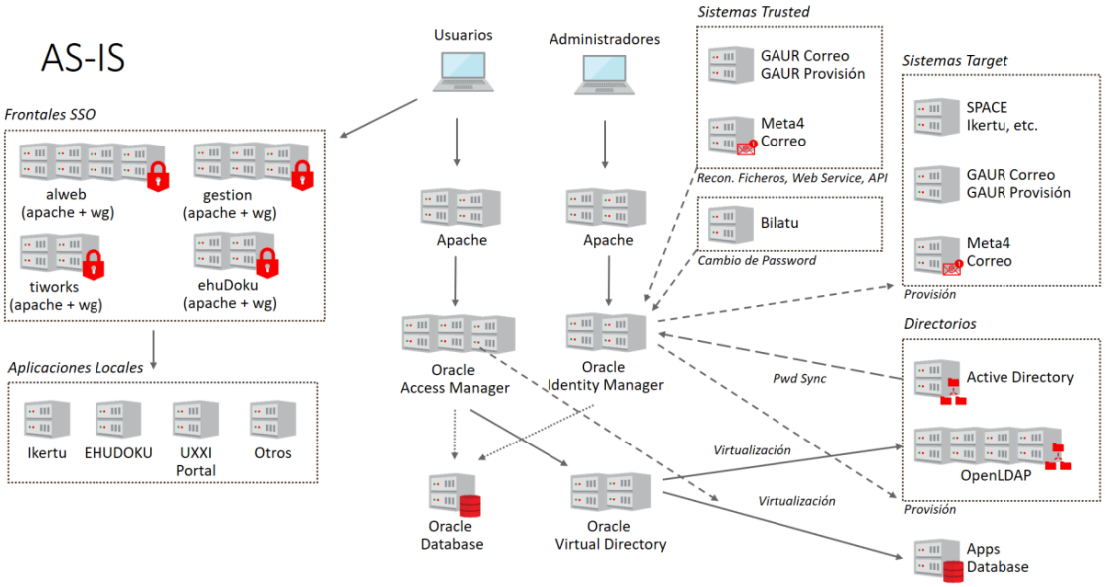
Otras características mejorables:

- Uso de fechas no adecuado en la gestión de los roles (el 86% de las fechas de finalización son después de 2100).
- El esquema del usuario se ha extendido con 96 atributos UDF.
- Procesos de altas/bajas/modificaciones.
- Tareas programadas.
- WebServices.
- Event-handlers.

1.5- Inventario de Servidores

Este capítulo detalla el inventario de servidores realizado en los tres entornos: Desarrollo, Integración y Producción.

El diagrama de arquitectura del entorno de Producción es el siguiente (no se muestran los servidores de Oracle Enterprise Single Sign-On, que son compartidos con los servidores de los Connector Servers):



El número total de servidores es de 68 repartidos en:

- Frontales: 21
- Aplicaciones
    - Oracle Access Manager: 9
    - Oracle Identity Manager: 5
- Base de datos: 3
- Directorios
    - Oracle Virtual Directory: 8
    - OpenLDAP: 7
    - Active Directory: 7
- ESSO/Connector Server: 8

2- Necesidad e idoneidad de la contratación

El objetivo de la presente licitación trata de contratar los servicios necesarios para poner al día los productos de identidad de Oracle que la UPV/EHU tiene contratados, así como la reingeniería necesaria en la arquitectura, funcionalidad, aplicaciones y procesos que permitan contar con una nueva plataforma de gestión de identidad.

El objeto final es que la nueva plataforma permita agilizar tramitaciones y servicios que se dan a día de hoy e implementar nuevas funcionalidades que permitan el desarrollo ágil de proyectos de integración con proyectos locales, nacionales e internacionales.

Se deben contemplar entre otras cuestiones:

- Una nueva propuesta de la gestión de identidades y accesos para la UPV/EHU
- Plan de implantación de la propuesta
- Implementación y puesta en marcha
- Plan de entrega
- Plan de soporte de la arquitectura y sus componentes con una bolsa de horas anual
- Traspaso de conocimiento (Formación).

3- Prestación a contratar

3.1- Objeto

Como se ha anticipado ya, se necesita poner al día de manera integral la plataforma GISSO implementada desde hace ya más de 10 años en la UPV/EHU. Para ello se requiere abordar un proyecto integral con una empresa especializada en servicios de ingeniería en los productos y las tecnologías de identidad de Oracle. Estos servicios pueden ser proporcionados por parte de la propia Oracle o de algún partner con las máximas capacitaciones del fabricante del software en dichas tecnologías.

El proyecto debe abordar todas las fases del mismo, desde la identificación de objetivos, prioridades y tareas en base a las necesidades de la UPV/EHU, pasando por el plan de implantación, la ejecución del mismo, la entrega y el posterior soporte.

A continuación, se van a concretar las necesidades en los distintos ámbitos de todo lo relacionado con GISSO siguiendo el orden en el que se ha planteado la situación actual de todo lo relacionado con la gestión de identidades en la universidad.

3.2- Necesidades detectadas

3.2.1- Productos de la plataforma

Se requiere que los componentes que se vayan a utilizar en GISSO estén actualizados a la última versión recomendada por el fabricante:

- Oracle Access Manager
- Oracle Identity Manager
- Oracle WebLogic
- Oracle WebGates
- JDK
- Otros

En caso de que algún componente no sea necesario no se tendrá en cuenta para la nueva arquitectura. En el caso de componentes nuevos habrá que contemplar además si se dispone de licenciamiento o si se necesitan licencias adicionales.

De momento se ha detectado que la funcionalidad de Oracle Enterprise Single Sign-on puede ser reemplazado por WNA (Windows Native Authentication) y Oracle Virtual Directory puede ser reemplazado por OID (Oracle Internet Directory)[2] y por OpenLDAP.

[2] Siempre que se eliminen las necesidades que requieren la necesidad de usar OVD: Cruces entre entornos, uso de cuentas locales de aplicaciones en el SSO y matriz de certificación con openldap

3.2.2- Arquitectura general

Se requiere una revisión de la arquitectura de cara a identificar mejoras en la misma, componentes que puedan estar obsoletos o nuevos componentes que puedan ser necesarios. También hay que analizar si las fuentes y destinos de los datos siguen siendo correctos o si se necesitan hacer cambios.

3.2.3- Funcionalidades Oracle Access Manager

- Revisión y puesta al día de SSO con Webgates
- Revisión y puesta al día de los protocolos y servicios de federación con aplicaciones y entidades externas, tanto para actuar como Identity provider, como de Service provider
- Revisión y puesta al día del protocolo OAuth como protocolo complementario a SAML cuando sea necesario
- Revisión y puesta al día de los plugins de autenticación customizados
- Revisión y puesta en marcha del mecanismo de reglas de acceso para cuando se requieran aplicar filtros o validaciones
- Revisión y puesta en marcha de la auditoría de accesos, así como la obtención de informes previstos de manera nativa por la solución con OBI (Oracle BI Publisher)
- Puesta en marcha de WNA para reemplazar a Oracle Enterprise Single Sign-on
- Puesta en marcha de Secure Token Service para mejorar la seguridad de las aplicaciones en su interconexión vía Tokens SAML
- Revisar e incorporar OpenID connect (soportado en la nueva versión)
- Valorar la activación de la funcionalidad Mobile & Social para integración con redes sociales
- Valorar la activación de la funcionalidad Mobile Security
- Valorar la activación de la función Remember Me
- Revisar el control de acceso y asignación granular de permisos en las aplicaciones (hasta donde se pueda llegar)
- Puesta en marcha de un segundo factor de autenticación en el OAM para las aplicaciones que lo necesiten.

3.2.4- Funcionalidades Oracle Identity Manager

- Revisión de los conectores necesarios para las funcionalidades actuales y futuras (Zoom, M365, etc…), así como de los conectores desarrollados hasta ahora.
- Revisión y puesta al día del Connector Server
- Revisión y puesta al día de los servicios desconectados de cara a que la información fluya de las fuentes autoritativas a la gestión de identidades mediante colas de mensajería (Rabbit MQ o Apache Kafka).
- Revisión de las políticas de acceso, roles necesarios, aplicaciones y perfiles para poder activar otros servicios dependientes de esta funcionalidad
- Revisión y puesta al día del Access Policy Harvesting
- Revisión y puesta al día del auto-servicio, por el que los propios usuarios pueden solicitar servicios y las autorizaciones se escalan según las políticas de acceso establecidas

- Revisión y activación de la consola de usuario y administración que debe ser multi idioma (al menos inglés, castellano y euskera), accesible (WCAG 2.1 nivel AA) y adaptada a la identidad de marca de la UPV/EHU
- Revisión y activación de la funcionalidad de auto-registro para poder registrar usuarios externos. Debe habilitarse el formulario de registro en las mismas condiciones que la consola en cuanto a idiomas, marca y accesibilidad, así como el flujo de aprobación necesario para gestionar el ciclo de vida de esta funcionalidad: Pantalla login – Registro – Obtener número de petición – Flujo de aprobación – Revisión de peticiones – Creación de usuario
- Revisar e implementar las políticas de contraseñas en cuanto a complejidad, ciclo de vida, protección contra ataques de fuerza bruta, etc. y su despliegue a los directorios y OAM. Implementar mecanismos de recuperación de contraseñas olvidadas y de mecanismos de seguridad adicional, como credenciales de doble factor u otros
- Revisar e implementar el sistema de notificaciones por distintos canales (email, SMS, etc…). Se deben revisar también las plantillas para que cumplan la normativa universitaria en cuanto a imagen, lenguaje no sexista y multi idioma. Se deben activar al menos las notificaciones para aplicar el ciclo de vida de las contraseñas
- Implementar la funcionalidad de administración delegada. Para ello hay que definir los roles necesarios, sus tareas y servicios a asignar a cada uno de ellos
- Implementar el sistema de auditoría en la gestión de identidades. Definir los niveles de eventos a registrar y su explotación por parte de los gestores
- Definir e implementar las políticas de auditoría. Definir segregación de funciones y establecer incompatibilidades entre roles, aplicaciones, valores en la identidad de usuario, etc.
- Definir e implementar las certificaciones dentro del módulo de cumplimiento, de cara a distribuir el trabajo de validación de usuarios
- Definir e implementar el ciclo de vida de los roles para poder hacer una gestión de los mismos
- Revisar e implementar funcionalidades nativas de OIM que puedan estar implementadas en otras aplicaciones, como reseteos de contraseña, auto-registros, gestión de grupos, etc.
- Implementación y puesta en marcha de la consola de administración de la gestión de la identidad de las personas accesible, adaptada a la identidad de marca de la UPV/EHU y plurilingüe (al menos en inglés, castellano y euskera).
- Implementar el servicio de “altas masivas” para facilitar a los responsables funcionales la posibilidad de añadir conjuntos de personas previamente autorizadas.

3.2.5- Funcionalidades implementadas en la UPV/EHU

A día de hoy se disponen de diversas soluciones implementadas que deben evolucionar para ser asumidas por las funcionalidades nativas de OAM y de OIM. Para ello se requiere:

- Incorporar los colectivos externos a OIM para simplificar la pantalla de autenticación. En caso de aplicaciones que no se puedan integrar con OAM se usará una pantalla diferente.
- El cambio y reseteo de contraseña se realiza en Bilatu, por lo que se requiere que esta funcionalidad sea asumida por el ciclo de vida de contraseñas nativo de OAM y OIM.
- Aunque ya se ha indicado en los puntos anteriores, se requiere implementar el modelo organizacional de OIM para poner en marcha las funcionalidades de reparto de carga administrativo (administración delegada), aplicar distintas políticas (ciclo de vida, contraseña, etc.) a distintos grupos de usuarios y dar visibilidad de aplicaciones y roles a grupos de usuarios.

- Replanteamiento de la identidad actual (organizaciones y colectivos) para adecuarlo a al modelo por organizaciones de GISSO.
- Dar solución a la necesidad de que una persona pueda pertenecer a varias organizaciones y que en algunos casos se necesite una priorización entre ellas.
- Definir y poner en marcha el ciclo de vida del usuario teniendo en cuenta que un usuario dado de baja podría reincorporarse en el futuro.
- Revisar los procesos actuales por los que se decide si una persona ya estaba o no en la casa e implementar o mejorar los mecanismos de detección de duplicidades de usuarios para evitar el que una persona obtenga dos identidades diferentes.
- Revisar y puesta al día de las herramientas y procesos de unificación de identidades para corregir los errores esporádicos que generan las fuentes autoritativas
- Dado que las diferentes aplicaciones disponen de distintos mecanismos y políticas con las cuentas, hay que revisar dichas aplicaciones, el estado de las cuentas, incorporarlas al ciclo de vida establecido y hacer el ajuste correspondiente cuando corresponda (p.e. purgar cuentas obsoletas).
- Revisar aplicaciones del punto 2.4.7 y ver si siguen siendo válidas y si el código se ajusta a las buenas prácticas del producto. En caso de que no sea así, se requiere ajustar el código de cada una de las aplicaciones que sigan siendo válidas adaptándolo a las recomendaciones del fabricante.
- Revisar el uso de fechas de los roles para adecuar su uso a las recomendaciones del fabricante.
- Revisar el uso de los atributos UDF y su posible eliminación o sustitución por atributos nativos del OIM.
- Eliminación o adaptación de procesos o aplicaciones que queden obsoletos.
- Integración nativa de la nueva arquitectura con Office365 tanto a nivel de gestión de identidades como desde la gestión de accesos.

3.2.6- Nueva arquitectura de servidores y de productos que contemple

Diseño de una arquitectura simplificada y resiliente de servidores en tres entornos (Producción, Integración y Desarrollo). Se dimensionará el número de servidores y la capacidad de cada uno de ellos a las necesidades de cada uno de los entornos.

Los servidores se implementarán en el entorno de virtualización que ya dispone la UPV/EHU, para lo que habrá que asegurar que hay capacidad suficiente para dotar de los recursos necesarios para la nueva solución o proponer los cambios necesarios para que dicha capacidad pueda dotarse. Habrá que tener en cuenta que durante un tiempo deben convivir la solución actual y la nueva.

Los productos que se implementarán deben ser la versión más actual posible, tanto el sistema operativo, como los componentes intermedios necesarios, cuyo ciclo de vida esté vigente en la duración del contrato. En caso de que no sea posible asegurar esta circunstancia para algún producto o componente, debe quedar acreditado.

Activación de protocolos de seguridad que faciliten la interconexión con aplicaciones o plataformas de manera estándar y federación con otras entidades o proveedores de servicios.

Todos los sistemas y productos deben estar ausentes de vulnerabilidades conocidas en el momento de la puesta en producción y optimizados (tunning) para la carga esperada disponiendo de un margen de seguridad suficiente para que los distintos elementos de la solución funcionen con un tiempo de respuesta aceptable con distintas cargas de trabajo.

3.3- Plan de implantación de la propuesta

De cara a poder llevar a cabo este proyecto se requiere contemplar una serie de fases que deben concluir con la puesta en producción de la nueva solución. Dichas fases, independientemente de que se puedan proponer otras, son:

- Estudio de la solución actual implementada en la UPV/EHU
- Propuesta de una nueva solución que contemple lo reflejado en las necesidades del punto 4.2.
- Propuesta de mejoras a lo expuesto si las hubiera.
- Propuesta de un plan de ejecución que contemple al menos:
    - Tareas de alto nivel o fases con los objetivos esperados.
    - Tareas de detalle en cada fase con plazos y recursos necesarios por parte de la UPV/EHU.
    - Calendario de hitos teniendo en cuenta las fechas de distintos procesos de la UPV/EHU.
    - Análisis de impacto en otros servicios, infraestructuras o aplicaciones.
    - Análisis de riesgos.
    - Plan de pruebas funcionales, de carga y auditoría de seguridad.
- Plan de puesta en producción “Out-of-Place“ con afección mínima imprescindible a otros servicios en producción.

3.4- Plan de entrega

Para la entrega del proyecto se tendrán en cuenta al menos los siguientes puntos:

- Documentación de la arquitectura, productos y funcionalidades implementadas.
- Documentación de administración, explotación y soporte de la solución.
- Documentación de uso de la consola para el usuario final.
- Documentación de integración con aplicaciones de terceros mediante protocolos estándar, APIs u otras tecnologías.
- Plan de contingencia ante eventuales fallos o problemas que puedan surgir.
- Código fuente de todos los desarrollos realizados.
- Documentación de todas los componentes y sus conexiones para facilitar la resolución de incidencias.

3.4- Plan de formación

El plan de formación deberá ser suficiente, junto con la documentación, para que la UPV/EHU sea capaz de gestionar todos los componentes que dispondrá la plataforma:

En el plan de formación se tendrán en cuenta al menos los siguientes puntos:

- Formación al equipo de sistemas que administrará la plataforma, tanto a nivel de sistema operativo, como de consola de administración.
- Formación de operación que incluirá, entre otros puntos, la formación en añadir nuevos colectivos, nuevos roles, nuevas aplicaciones a proteger, nuevos derechos de acceso.

- Formación para administradores funcionales para poder realizar la administración delegada, tanto de OIM como de OAM.
- Formación de las capacidades nativas de la plataforma instalada para conocer todo lo que es capaz de realizar la nueva plataforma.

Opcionalmente puede incluirse formación reglada del producto o productos instalados.

4- Lugar de ejecución

Campus de Leioa de la UPV/EHU de manera presencial o remota según sea necesario, aunque se evitarán las intervenciones presenciales siempre que se pueda acometerse el trabajo de manera remota sin merma de calidad y eficiencia.

5- Servicio de soporte.

Se deberá ofrecer un servicio de soporte 24x7 directo del fabricante Oracle, sin intermediarios ni terceros, ante incidencias y problemas para todos los productos contemplados durante la vigencia del contrato de, al menos, 150 horas.

El SLA no puede ser superior a 4 horas durante el horario laboral (lunes a viernes de 8:00 a 17:00).

El servicio de soporte incluirá las horas adicionales (hasta 200 horas) que la contratista haya ofertado, en su caso, para la realización de labores de apoyo en la explotación de sistemas o funcional y para consultoría, en el caso de que se requiera implementar nuevas funcionalidades o formación.

6- Garantía y condiciones de las licencias

El resultado final debe tener una garantía mínima de 6 meses en los que se atenderán las incidencias o problemas que se detecten y que se constate que son propias de la implantación o migración de datos.

Quedan excluidos cualquier tipo de licenciamiento OEM o similares, es decir, las licencias deberán adquirirse a través de Oracle.

En las licencias se incluyen los derechos de actualización de los productos, aunque estos cambien de denominación siempre que la funcionalidad de los mismos sea la misma o mejorada sobre las actuales.

El contratista expedirá a la UPV/EHU el documento acreditativo de cesión o entrega de las licencias en los términos del presente pliego, en cuanto a producto, número y tipo de licencia. Igualmente, se hará cargo ante la universidad de todos los productos y servicios objeto de este contrato.

7. Equipo de trabajo

La empresa adjudicataria deberá aportar un equipo de trabajo que cumpla con las competencias profesionales y la experiencia mínimos especificados en el documento de adscripción de medios, así como

con las posibles mejoras sobre dichos perfiles que se incluyan en la oferta y que hayan sido objeto de valoración.

En el hipotético caso de que a lo largo del proyecto algún miembro del proyecto deba sustituido por otra persona, esa sustitución solo podrá realizarse por una persona con la misma capacitación profesional y experiencia para el perfil ofertado en el contexto de este pliego, y previa aprobación por parte de la UPV/EHU.

8. Confidencialidad.

Ambas partes se comprometen a guardar la máxima reserva y confidencialidad en relación con todos aquellos documentos, datos e informaciones a los que cada parte tenga acceso, como consecuencia de los servicios objeto del contrato.

Se considerará información confidencial, cualquier información marcada como tal o que por su naturaleza lo sea, relacionada con cada una de las informaciones transmitidas entre las partes.

Se considera información confidencial toda aquella relativa al contrato y acuerdo de intenciones, listas de clientes, sistema informático, procedimiento de trabajo y organizativo, productos, personal y, en general, toda documentación marcada como reservada.

En ningún caso tendrá carácter de confidencial la información referente a:

- cualquier asunto que aparezca en bibliografía pública o que pase a ser de dominio público, a no ser que haya llegado a ser de dominio público a causa del incumplimiento de una de las partes,
- cualquier información o conocimiento adquirido de terceros, divulgación requerida por ley o por alguna normativa, información referente a datos económicos o de otra índole que deban ser aportados ante la Administración estatal, local o autonómica, por requerimientos fiscales o de contratación administrativa.

El personal de la Universidad, la contratista o cualquier persona dependiente de la misma, que desempeñe las funciones objeto de este pliego deberá mantener plena confidencialidad sobre la información caracterizada como confidencial relativa a los servicios objeto de este contrato.

Esta obligación de confidencialidad se entenderá plenamente vigente, incluso con posterioridad a la extinción del servicio prestado.



Firmado digitalmente por LIBORIO REVILLA ALONSO - 15986567A
Fecha: 2022.02.08 08:23:17 +01'00'

Fecha y firma