Universidad de Alcalá
Escuela Politécnica Superior

GRADO EN SISTEMAS DE LA INFORMACIÓN

Trabajo Fin de Grado

“Implementación de un sistema de Gestión de Identidades para una empresa privada”

ESCUELA POLITECNICA
SUPERIOR

Autor: Carlos Fuentes Martínez

Tutor/es: Iván González Diego

2017

UNIVERSIDAD DE ALCALÁ
Escuela Politécnica Superior

GRADO EN SISTEMAS DE INFORMACIÓN

Trabajo Fin de Grado

“Implementación de un sistema de Gestión de Identidades para una empresa privada”

Autor: Carlos Fuentes Martínez

Tutor/es: Iván González Diego

TRIBUNAL:

Presidente: << Nombre y Apellidos >>

Vocal 1º: << Nombre y Apellidos >>

Vocal 2º: << Nombre y Apellidos >>

FECHA: << Fecha de depósito >>

1. ÍNDICE

Contenido

1. ÍNDICE 1
2. RESUMEN EN CASTELLANO 4
3. RESUMEN EN INGLÉS 4
4. PALABRAS CLAVE 4
5. RESUMEN EXTENDIDO 4
6. GLOSARIO DE ACRÓNIMOS Y ABREVIATURAS 5
7. MEMORIA: 6
7.1-RFP HIDRAUAH (SOLICITUD DE OFERTAS) 6
7.2-OFERTA CFM CONSULTING 11
7.2.1-DATOS GENERALES 11
7.2.2-RESUMEN EJECUTIVO 13
7.2.3-RESUMEN DE LA OFERTA 14
7.3-ORGANIZACIÓN DEL TRABAJO 21
7.4-Flujo de Instalación y flujo de Trabajo 23
7.5-CARACTERÍSTICAS TÉCNICAS DESTACABLES 24
7.5.1-SISTEMA OPERATIVO: 24
7.5.2-BASE DE DATOS 26
7.5.3-WEBLOGIC 29
7.5.4-OUD (LDAP) 29
7.5.5-RCU 31
7.5.6-OAM 33
7.5.7-OIM 35
8. PLANOS Y DIAGRAMAS 37
9. MANUAL DE USUARIO 41
9.1-CREACIÓN DE USUARIO EN OIM 41
9.2-CREACIÓN DE USUARIO EN BBDD 44
9.3-CONFIGURACIÓN DE CONECTOR CON BBDD 45
9.4-CONFIGURACIÓN DE CONECTOR CON LDAP 49
9.5-RECONCILIACIÓN BBDD 54
9.6-PROVISIÓN DE CUENTAS 55

9.7-CONFIGURACIÓN OAM 58
9.8-PROTEGER UN RECURSO: 62
9.9-DESPLIEGUE LOGIN 64
10. PRESUPUESTO DEL PROYECTO 65
11. CONCLUSIONES Y TRABAJO FUTURO 66
12. BIBLIOGRAFÍA. Se recomienda el estilo de citación del IEEE. 67

Índice Ilustraciones

Ilustración 1 Precios del S.O Oracle Linux 14
Ilustración 2 Posicionamiento de Oracle Linux en el Ranking de S.O 15
Ilustración 3 Precios del Sistema operativo Windows Server 15
Ilustración 4 Comparación de los distintos Sistemas Operativos 16
Ilustración 5 Esquema de la Gestion de Identidades 17
Ilustración 6 Esquema de la Gestión de Accesos 17
Ilustración 7 Esquema del equipo de CFM Consulting 21
Ilustración 8 Instalación OL5 1 24
Ilustración 9 Instalación OL5 2 24
Ilustración 10 Instalación OL5 3 25
Ilustración 11 Instalación OL5 4 25
Ilustración 12 Instalación OL5 5 26
Ilustración 13 Instalación BBDD 1 26
Ilustración 14 Instalación BBDD 2 27
Ilustración 15 Instalación BBDD 3 27
Ilustración 16 Instalación BBDD 4 28
Ilustración 17 Instalación BBDD 5 28
Ilustración 18 Instalación Weblogic 29
Ilustración 19 Instalación OUD 1 30
Ilustración 20 Instalación OUD 2 30
Ilustración 21 Instalación OUD 3 31
Ilustración 22 Instalaciín RCU 1 31
Ilustración 23 Instalación RCU 2 32
Ilustración 24 Instalación RCU 3 32
Ilustración 25 Instalación OAM 1 33
Ilustración 26 Instalación OAM 2 34
Ilustración 27 Instalación OAM 3 34
Ilustración 28 Instalación OAM 4 35
Ilustración 29 Instalación OIM 1 35
Ilustración 30 Instalación OIM 2 36
Ilustración 31 Diagrama Infraestructura y Funcionamiento 1 37
Ilustración 32 Diagrama Infraestructura y Funcionamiento 2 38
Ilustración 33 Diagrama Infraestructura y Funcionamiento 3 38
Ilustración 34 Diagrama Infraestructura y Funcionamiento 4 40
Ilustración 35 OIM; Creación de usuarios 1 41
Ilustración 36 OIM; Creación de usuarios 1 41
Ilustración 37 OIM; Creación de usuarios 2 42
Ilustración 38 OIM; Creación de usuarios 3 42
Ilustración 39 OIM; Creación de usuarios 4 43
Ilustración 40 OIM; Creación de usuarios 5 43

Ilustración 41 OIM; Creación de usuarios 6 44
Ilustración 42 OIM; Creación de usuarios 7 44
Ilustración 43 Formulario de creación de usuario en la aplicación web 45
Ilustración 44 Conector DBAT OIM 1 45
Ilustración 45 Conector DBAT OIM 2 46
Ilustración 46 Conector DBAT OIM 3 46
Ilustración 47 Conector DBAT OIM 4 47
Ilustración 48 Conector DBAT OIM 5 48
Ilustración 49 Conector DBAT OIM 6 48
Ilustración 50 Conector DBAT OIM 7 49
Ilustración 51 Conector LDAP OUD OIM 1 49
Ilustración 52 Conector LDAP OUD OIM 2 50
Ilustración 53 Conector LDAP OUD OIM 3 50
Ilustración 54 Conector LDAP OUD OIM 4 51
Ilustración 55 Conector LDAP OUD OIM 5 51
Ilustración 56 Conector LDAP OUD OIM 6 52
Ilustración 57 Conector LDAP OUD OIM 7 52
Ilustración 58 Conector LDAP OUD OIM 8 53
Ilustración 59 Conector LDAP OUD OIM 9 53
Ilustración 60 Reconciliación BBDD 1 54
Ilustración 61 Reconciliación BBDD 2 55
Ilustración 62 Provisión LDAP 1 55
Ilustración 63 Provisión LDAP 2 56
Ilustración 64 Provisión LDAP 3 56
Ilustración 65 Provisión LDAP 4 56
Ilustración 66 Provisión LDAP 5 57
Ilustración 67 Provisión LDAP 6 57
Ilustración 68 Provisión LDAP 7 57
Ilustración 69 Configuración OAM 1 58
Ilustración 70 Configuración OAM 2 58
Ilustración 71 Configuración OAM 3 58
Ilustración 72 Configuración OAM 4 59
Ilustración 73 Configuración OAM 5 59
Ilustración 74 Configuración OAM 6 60
Ilustración 75 Configuración OAM 7 60
Ilustración 76 Configuración OAM 8 61
Ilustración 77 Configuración OAM 9 61
Ilustración 78 Protección de recursos 1 62
Ilustración 79 Protección de recursos 2 62
Ilustración 80 Despliegue aplicaciones 1 64
Ilustración 81 Despliegue aplicaciones 2 64
Ilustración 82 Despliegue aplicaciones 3 64
Ilustración 83 Despliegue aplicaciones 4 65
Ilustración 84 Despliegue aplicaciones 5 65
Ilustración 85 Presupuesto por Perfil 66
Ilustración 86 Presupuesto Licencias 66

2. RESUMEN EN CASTELLANO

Este proyecto, va a ser una simulación de un caso de consultoría informática. Una empresa realizará una oferta para implantar un sistema de Gestión de Identidades y actuando como consultora, se entregará un RFP (Request for Proposal) y posteriormente se detallará el proceso de implantación y la fase de pruebas. El objetivo del proyecto consiste en crear una infraestructura capaz de gestionar de manera eficiente las identidades en una empresa para posteriormente poder implantar un sistema de autenticación Single Sign On. Los sistemas a implantar serán Oracle Identity Manager y Oracle Access Manager en un sistema Oracle Linux.

3. RESUMEN EN INGLÉS

This project is going to be a simulation of a consulting case. A company will make an offer to implement an Identity Management system and as a consultant, will be deliver a RFP (Request for Proposal) and then will be detail the implementation process and the testing phase. The target of the project is to create an infrastructure that can efficiently managing identities in a company and then be able to implement a Single Sign On authentication system. The systems to be deployed will be Oracle Identity Manager and Oracle Access Manager on an Oracle Linux system.

4. PALABRAS CLAVE

Gestión / Identidades / Autenticación / Autorización / Login

5. RESUMEN EXTENDIDO

Este proyecto, va a ser una simulación de un caso de consultoría informática. Una empresa lanzará una RFP en la cual solicitará los servicios de distintos proveedores para cambiar su sistema de gestión de empleados y clientes. Esta empresa, llamada HidraUAH, va a solicitar la implantación de una página web en la cual se puedan ver todos sus productos y se puedan realizar pedidos online.

Necesitan un sistema de gestión de identidades para controlar todas las cuentas que tienen de sus empleados, sus clientes y los administradores. Para que el sistema esté protegido, quieren un gestor de accesos, en el cual se darán los derechos de autorización y autenticación a la web, y según los privilegios de cada uno, accederán a una interfaz u otra.

El objetivo en resumen, es tener una web securizada, personalizada y poder controlar las cuentas para posibles temas de auditoría. La consultora a la que se

representará, CFM (Carlos Fuentes Martínez) Consulting, hará una oferta respondiendo al RFP anterior. En esta oferta, se presentará la empresa aportando unos datos generales, también contendrá un resumen ejecutivo en el cual se presenta la propuesta de valor, la ventaja competitiva que ofrece frente a otras empresas, el desarrollo tecnológico que posee y descripción general del equipo.

A continuación se describe el resumen de la oferta en el cual se compararán los diferentes productos que se han valorado para la implantación. Además se incluirá la organización del trabajo.

Los sistemas que se van a implantar van a ser el Oracle Identity Manager y el Oracle Access Manager, todo esto bajo un sistema Linux distribuido por Oracle.

La base teórica para la cual se ha realizado este trabajo, podría englobarse en:

-Base de datos: Como se manejarán bases de datos para el almacenaje primitivo de los usuarios, ha servido para conocer la estructura de una base de datos, hacer consultas, etc.
-Organización de la información y proyectos: Al tratarse de ofrecerle un servicio tecnológico a la empresa HidraUAH, los conocimientos adquiridos en esta asignatura de organización de la información y proyectos sobre Request for proposal (RFP) y ofertas, han resultado muy útiles para plantear dicha situación.
-Ingeniería del Software e Ingeniería del software Avanzada: Han sido muy útiles los conocimientos adquiridos en ambas asignaturas, tanto para la toma de requisitos y especificaciones del proyecto, así como para ver cómo implantar las herramientas en el sistema.
-Programación: Ha sido fundamental para el desarrollo de la web.

6. GLOSARIO DE ACRÓNIMOS Y ABREVIATURAS

OIM: Oracle Identity Manager
OAM: Oracle Access Manager
SSO: Single Sign On
OUD: Oracle Unified Directory
BBDD. Base de Datos
GDI: Gestión de Identidades
SO: Sistema Operativo
RCU: Reporitory Creation Utility
LDAP: Lightweight Directory Access Protocol
TI: Tecnologías de la Información

7. MEMORIA:

7.1-RFP HIDRAUAH (SOLICITUD DE OFERTAS)

La empresa HidraUAH emite un documento (RFP) que contiene las bases y premisas para que los proveedores realicen sus propuestas técnicas, funcionales y de proyecto. A continuación se adjunta dicho documento:

Empresa emisora RFP	HidraUAH	**Fecha**	1 sept, 2016
Título del proyecto: Gestión de identidades			
Contexto y Situación actual			
Somos HidraUAH, una pequeña empresa de hidráulica situada en el campus tecnológico de Alcalá de Henares. Nos dedicamos a la distribución y venta de materiales de hidráulica en nuestra nave. Tenemos un equipo que consiste en: ➢ 22 Empleados cualificados en hidráulica y neumática. ➢ 2 Administradores de los sistemas informáticos. ➢ Una cartera de más de 400 clientes, tanto personas físicas como empresas. Al tratarse de un mercado aislado a un target concreto, nos dedicamos a la venta física y no nos encontramos situados en el mercado digital.			
Necesidades			
Dado que nos encontramos en un mundo en el que predomina la cultura digital, es necesario introducirnos en el mercado online. Para ello queremos solicitar: 1. Una página web con nuestra gama de productos. Queremos una página web con los diferentes productos y diferentes interfaces dependiendo del tipo de empleado que esté haciendo login a la página. 2. Un sistema para gestionar las cuentas de nuestros empleados y clientes, para así poder llevar un seguimiento y almacenaje de datos de ellos. 3. Un sistema seguro de acceso.			
Objetivos			
El objetivo principal es tener una web, securizada y personalizada y mantener un control de nuestros empleados y clientes para facilitar temas de auditoría.			
Requisitos			

Número de requisito	RF001
Nombre de requisito	Validación Usuario.
Tipo	☐ Funcional ☐ Datos ☐ Rendimiento

	☐ Interfaz ☐ Seguridad ☐ Otros
Prioridad del requisito	☐ Alta/Esencial ☐ Media/Deseado ☐ Baja/Opcional
Descripción	Permite o deniega el acceso a las diferentes interfaces disponibles dependiendo de su cargo en la empresa.

Número de requisito	RF002
Nombre de requisito	Propagación de cuentas.
Tipo	☐ Funcional ☐ Datos ☐ Rendimiento ☐ Interfaz ☐ Seguridad ☐ Otros
Prioridad del requisito	☐ Alta/Esencial ☐ Media/Deseado ☐ Baja/Opcional
Descripción	Todas las cuentas deben estar propagadas a todos los sistemas necesarios.

Número de requisito	RF003
Nombre de requisito	Creación de Usuarios.
Tipo	☐ Funcional ☐ Datos ☐ Rendimiento ☐ Interfaz ☐ Seguridad ☐ Otros
Prioridad del requisito	☐ Alta/Esencial ☐ Media/Deseado ☐ Baja/Opcional
Descripción	El sistema debe de poder dar de alta a nuevos usuarios.

Número de requisito	RF004
Nombre de requisito	Modificación de Usuarios.
Tipo	☐ Funcional ☐ Datos ☐ Rendimiento ☐ Interfaz ☐ Seguridad ☐ Otros
Prioridad del requisito	☐ Alta/Esencial ☐ Media/Deseado ☐ Baja/Opcional
Descripción	El sistema debe poder gestionar las modificaciones de los usuarios.

Número de requisito	RF005
Nombre de requisito	Distintas Interfaces.
Tipo	☐ Funcional ☐ Datos ☐ Rendimiento ☐ Interfaz ☐ Seguridad ☐ Otros
Prioridad del requisito	☐ Alta/Esencial ☐ Media/Deseado ☐ Baja/Opcional
Descripción	El sistema debe tener 3 distintas interfaces según el tipo de empleado.

Número de requisito	RNF001
Nombre de requisito	Desarrollos en Java y Javascript.
Tipo	☐ Funcional ☐ Datos ☐ Rendimiento ☐ Interfaz ☐ Seguridad ☐ Otros
Prioridad del requisito	☐ Alta/Esencial ☐ Media/Deseado ☐ Baja/Opcional
Descripción	Todos los desarrollos se realizarán en lenguaje Java.

Número de requisito	RNF002
Nombre de requisito	3 tipos de usuarios.
Tipo	☐ Funcional ☐ Datos ☐ Rendimiento ☐ Interfaz ☐ Seguridad ☐ Otros
Prioridad del requisito	☐ Alta/Esencial ☐ Media/Deseado ☐ Baja/Opcional
Descripción	Se van a considerar 3 tipos de usuarios. Cliente, empleado y Administrador

Número de requisito	RNF003

Nombre de requisito	Alto nivel de Seguridad.
Tipo	☐ Funcional ☐ Datos ☐ Rendimiento ☐ Interfaz ☐ Seguridad ☐ Otros
Prioridad del requisito	☐ Alta/Esencial ☐ Media/Deseado ☐ Baja/Opcional
Descripción	Nuestra Aplicación Web debe de estar protegida

Gestión del cambio

Ya que va a existir un gran cambio en la empresa, se necesita una buena gestión del cambio para que los trabajadores de HidraUAH se integren y participen en este proyecto.

Para ello se seguirán las siguientes pautas:

- Evaluar, priorizar y autorizar los cambios de alcance: HidraUAH deberá evaluar junto con el equipo de proyecto dichas solicitudes para estudiar el impacto en los procesos de negocio. Todos estos cambios deben quedar registrados con la prioridad, clasificación, evaluación, autorización, planificación y programación.

- Gestión de cambios de alcance de emergencia: aquellos cambios que provoquen un impacto mayor deben ser evaluados detenidamente a fin de minimizar futuros riesgos o problemas y asegurar que dichos cambios se realizarán de forma segura y controlada.

- Se realizará un seguimiento de dichos cambios, exigiendo una revisión posterior a la implementación en la que participarán todas las partes afectadas.

- Control del estado de los cambios: se crearán informes para documentar tanto los cambios rechazados como el estado de los aprobados y los que están en proceso y los finalizados.

- Las solicitudes, por lo tanto, deberán incluir el estado en el que se encuentran (rechazada, aprobada, en proceso y finalizada), el registro de los cambios de estado, antigüedad de la solicitud.

- Cierre y documentación: cada vez que se modifique o actualice un cambio deberá quedar reflejado en la documentación del proyecto y la del usuario.

- Será definido un período de retención para la documentación de los cambios, del sistema y del usuario tras el cambio.

Planificación del proyecto y entregables

Para hacer el seguimiento del proyecto, se solicitaran unos entregables en las siguientes fases :

1. Análisis de requisitos
   - ➢ El proveedor deberá realizar un documento de requisitos detallado y aprobado por la dirección de sistemas para continuar con el proyecto.
   - ➢ Durante este proceso se revisará el documento de requisitos en reuniones entre el proveedor y la empresa con el fin de que éste sea totalmente coherente con las necesidades previstas.
   - ➢ Una vez el documento esté completo, deberá entregarse junto con la planificación del resto del proyecto.

2. Diseño del sistema
   El proveedor deberá realizar un diseño completo y funcional del sistema o sistemas requeridos.

3. Desarrollo del sistema
   Deberá informarse el porcentaje de avance en base a la planificación, en los siguientes puntos de control:
   - ➢ Cuando se haya completado un 50% de cada sistema que se esté implantando
   - ➢ Cuando se haya terminado de desarrollar o implantar cada sistema.

4. Pruebas
   - ➢ En la fase de pruebas del sistema se deberá realizar un documento que especifique todas las pruebas previamente acordadas acerca de funcionamiento, compatibilidad, integración y rendimiento.
   - ➢ En dicho documento se deberá especificar como se ha desarrollado cada prueba y los incidentes detectados. Éste se deberá entregar al final de la fase de pruebas.
5. Implantación
   - ➢ La implantación de los sistemas se podrá realizar en paralelo siempre que no esté altamente acoplados entre ellos.
   - ➢ Una vez se haya terminado esta fase, se entrega el informe pertinente sobre la implantación y la formación del personal.

6. Mantenimiento
   El proveedor deberá realizar un mantenimiento del sistema de 1 año para asegurar el correcto funcionamiento del sistema o sistemas implantados.

Plan de contingencia
Las propuestas deben incluir un plan de contingencia que valore, como mínimo, los siguientes aspectos: ➢ Caída del sistema. ➢ Pérdida de datos (total o parcial). ➢ Fallo de alguna de las aplicaciones. ➢ Caída de un servidor o varios. ➢ Que el tiempo de las formaciones de los empleados sea mayor que el estimado. ➢ Que los tiempos de proyecto se excedan de las fechas programadas.

Confidencialidad de la información
La empresa escogida quedará obligada al cumplimiento de la protección de datos de carácter personal de en la Ley Orgánica de Protección de Datos, ciñéndose a los preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, LOPD, y su Reglamento de Desarrollo, RD 1720/2007, de 21 de diciembre. A lo largo del desarrollo del proyecto HidraUAH facilitará toda la documentación e información necesaria. La empresa adjudicataria se comprometerá a: ➢ Tratar de manera confidencial todos los datos, material y documentación facilitada. ➢ No copiar, revelar, duplicar, ceder o vender de manera total o parcial la información a terceros sin una autorización escrita. ➢ No utilizar la información facilitada para otros fines ajenos al proyecto. ➢ Restringir la utilización de la información en función del ámbito de trabajo. ➢ Advertir de las obligaciones respecto a la confidencialidad de la información facilitada a sus empleados, y velar por el cumplimiento de la misma poniendo todos los medios posibles. ➢ Toda la información, documentación y demás datos facilitados deben ser devueltos y/o descargados de los equipos informáticos una vez ha finalizado el período de contratación. ➢ Cualquier infracción de este tipo será calificada como grave y causará la que el contrato sea rescindido, sin perjuicio de las responsabilidades penales o de otro tipo que pudieran incurrir.

7.2-OFERTA CFM CONSULTING

7.2.1-DATOS GENERALES

CFM consulting se fundó en el 1991 y puede describirse como una empresa dedicada principalmente a la consultoría en el sector de las tecnologías de la información.

Trabaja en toda España y cuenta con más de 100 profesionales en plantilla. Ha trabajado para clientes de todos los sectores, ayudándoles a crecer tecnológicamente.

El principal objetivo es cubrir las necesidades de aquellas empresas que no pueden ser satisfechas por una solución estándar, ofreciendo soluciones desarrolladas a medida para la empresa en cuestión. Cuenta con un equipo profesional con experiencia en proyectos:

- Corporativos
- Marketing
- Integración de sistemas
- Diseño
- Consultoría

La empresa tiene capital suficiente para comenzar el proyecto, y realizar el seguimiento contando con un plan de financiación detallado.

La metodología de desarrollo se centra en las necesidades de la empresa a proveer, aplicando tanto controles de gestión de calidad como procedimientos de trabajo, para garantizar los resultados requeridos. Así mismo la calidad de CFM Consulting es conseguida gracias al trabajo de un equipo cualificado así como el trato personalizado con los clientes.

Una vez se formalice el contrato de la empresa a proveer (HidraUAH), será responsable de cubrir todas las necesidades acordadas en la oferta, sometiéndonos a las posibles penalizaciones por incumplimiento.

La principal meta que se quiere alcanzar en HidraUAH al ofrecerles una solución a sus necesidades es la de redirigir la línea de negocio hacia nuevos objetivos y metas empresariales (reestructurando los procesos, consiguiendo cambios en la mentalidad y redireccionando la tecnología).

Para ello, se necesitará trabajar en los siguientes aspectos:

- Implantación de un sistema Gestor de Identidades
- Implantación de un sistema Gestor de Accesos
- Implantación de una Aplicación web

7.2.2-RESUMEN EJECUTIVO

La propuesta de valor que se plantea en la siguiente oferta es la implantación de un Sistema de Gestión de Identidades y de Gestión de Accesos, para ello los sistemas que se van a implantar van a ser el Oracle Identity Manager y el Oracle Access Manager, todo esto bajo un sistema Linux distribuido por Oracle.

En cuanto a la ventaja competitiva que se ofrece con respecto a la competencia, cabe destacar que la candidatura puede aportar a la empresa HidraUAH un mejor funcionamiento interno gracias a los procesos que se implantarán. Además se garantiza seriedad y profesionalidad a la hora de trabajar, es por esto por lo que es una empresa puntera en el sector, habiendo firmado contratos con empresas de un perfil parecido a HidraUAH. La formalización del contrato con la empresa les supondrá un aumento de prestigio que les ayudará a la obtención de nuevos clientes y con ello un notable aumento en los ingresos. Además de esto, se tienen en cuenta puntos importantes como el plan de contingencia, protección de datos, entregables y la formación de los empleados.

- Plan contingencia: Se llevarán a cabo dos medidas para mitigar los posibles riesgos planteados por HidraUAH.

    1. Para evitar que haya caídas en el sistema, fallos en las aplicaciones y pérdidas de datos, se balancearán los servidores y las aplicaciones para tener así alta disponibilidad de datos y, en caso de que falle el nodo primario, quedará el nodo secundario (réplica del primario) activo.

    2. Como medida preventiva se entregarán manuales de usuario a la plantilla de la empresa para que en caso de que el tiempo de las formaciones de los empleados sea mayor que el estimado, puedan aprender de manera autodidacta gracias a estos manuales antes de que comience la formación presencial.

    3. En caso de que el tiempo del proyecto se exceda de la fecha programada, se reajustarán las tareas duplicando el personal.

- Protección de datos: CFM consulting se compromete al cumplimiento de la protección de datos de carácter personal de en la Ley Orgánica de Protección de Datos, ciñéndose a los preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, LOPD, y su Reglamento de Desarrollo, RD 1720/2007, de 21 de diciembre. Además se hará cargo de cumplir las pautas requeridas por HidraUAH en lo que a protección de datos se refiere.

- Entregables: Se realizarán entregas en todas las fases marcadas en la RFP, con el objetivo de permitir al cliente tener un seguimiento del proyecto en todo momento.

- Formación: se desarrollará una formación a nivel presencial, en la cual se realizarán los cursos necesarios para que los empleados puedan manejar con soltura los

nuevos sistemas informáticos implementados en la organización. En ella se formará a toda la plantilla de empleados de la empresa HidraUAH. Además se les entregarán unos manuales de usuario en los que se explicarán detalladamente las funcionalidades básicas de la aplicación.

7.2.3-Resumen de la oferta

A continuación se describirán detalladamente las posibles herramientas para llevar a cabo el proyecto, realizándose una comparativa entre ellas, y se finalizará seleccionando una de las opciones redactando el flujo de instalación.

7.2.3.1-Sistemas Operativos

Para comenzar la oferta, el primer asunto a tratar es ver en qué Sistema Operativo se va a desarrollar la implementación. Las dos opciones que se comentatrán van a ser el Oracle Linux y el Windows Server.

Se va a comenzar hablando sobre el SO Oracle Linux. El primer factor que se tendrá en cuenta es que a diferencia de muchas otras distribuciones comerciales de Linux, Oracle Linux es fácil de descargar y de software libre, es decir, cuenta con libertad de distribución y libertad para actualizarlo al gusto.

Está especialmente desarrollado y probado para ofrecer asistencia a las cargas de trabajo más exigentes como las de Oracle Database. Se trata de un sistema compatible con la integridad de datos. Una solución completa para la gestión de la infraestructura de TI de Oracle desde una sola consola. Este SO puede ser una buena opción si elegimos una herramienta de GDI de Oracle, ya que al tratarse de un mismo distribuidor, la compatibilidad y fluidez en los procesos estará optimizada.

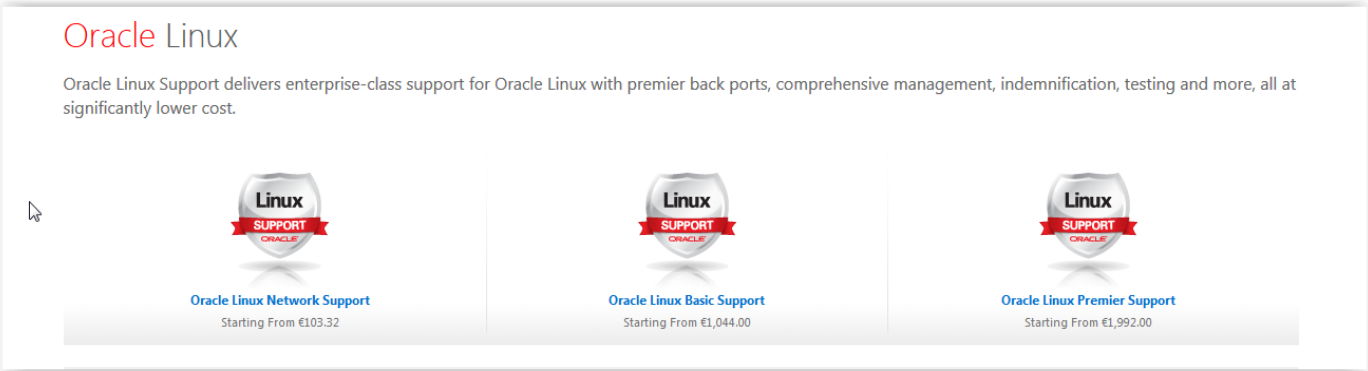

Ilustración 1 Precios del S.O Oracle Linux

RANKING	1st	6th
	In Operating Systems for Business	In Operating Systems for Business
	10,407 Views	101 Views
	3,750 Comparisons	89 Comparisons
	26 Reviews	1 Reviews
	199 Followers	31 Followers
	8.2 Avg. Rating	8.0 Avg. Rating

Ilustración 2 Posicionamiento de Oracle Linux en el Ranking de S.O

Como Desventajas se podría comentar que este sistema requiere de habilidades requeridas especializadas (editor vi, shell scripting, etc). Tiene que tener unos administradores de sistemas altamente cualificados. Al no ser un SO común, no se dispone de tanta información abierta.

Analizando el Windows Server se ve que la principal diferencia respecto a Oracle Linux, es que Windows Server es software propietario. Un dato importante es que se tendrá que comprar las licencias así como el soporte de actualizaciones. Microsoft hace un esfuerzo por superarse cada vez más, mejorar la fiabilidad, escalabilidad, rendimiento y facilidad de uso y administración, factores individualmente relevantes, pero que al producirse juntos dentro del mismo producto, reducen drásticamente el coste total de propiedad (TCO) .Windows Server incorpora innumerables ventajas, mejoras y nuevas tecnologías, orientadas todas ellas a cubrir las necesidades actuales de las organizaciones de cualquier tamaño.

Edición de Windows Server 2016	Ideal para	Modelo de licencia	Requisitos de CAL*	Precios de Open NL ERP (USD)
Datacenter**	Entornos de centros de datos muy virtualizados y definidos por software	Basada en núcleo	CAL de Windows Server	$6,155
Standard**	Entornos de baja densidad o no virtualizados	Basada en núcleo	CAL de Windows Server	$882
Essentials	Pequeñas empresas con un máximo de 25 usuarios y 50 dispositivos	Basada en procesador	No requiere CAL	$501

Ilustración 3 Precios del Sistema operativo Windows Server

Con Windows Server se conseguirá un servidor que puede encargarse de tareas que antes requerían de la intervención de varias máquinas. Windows introduce más procesadores lógicos, más capacidad de disco y más memoria. Proporcionan fiabilidad, disponibilidad y escalabilidad para que se pueda ofrecer la infraestructura de red que los usuarios solicitan. Ayuda a administrar la red al reforzar las políticas, tareas automatizadas y simplificación de actualizaciones. Proporciona un servidor de aplicaciones integrado que le ayude a desarrollar, implementar y administrar servicios web.

Analizando las desventajas, apoyándonos en la siguiente figura, lo primero que se observa en Microsoft es el costo de licencias. Por otra parte, según estudios externos a Microsoft, este es uno de los Servers con más bugs de seguridad conocidos. En tema de manejo e instalación, es un sistema que requiere altísimos conocimiento para poder configurarlo.

Sistema operativo	Windows Server 2012	Ubuntu Server	RHEL	FreeBSD	OpenBSD	OS X Server	AIX	HP-UX
Desarrollador	Microsoft	Canonical Ltd. y Fundación Ubuntu	Red Hat	Proyecto FreeBSD	Proyecto OpenBSD	Apple Inc.	IBM	Hewlett-Packard
Costo	$501 USD (Essentials) $882 USD (Standard) $4809 USD (Datacenter)	Gratuito Soporte técnico $750 USD y $1200 USD	?	Gratuito	Gratuito	$19.99 (paquete adicional a OS X) $499 USD	Incluido con el hardware	$400 USD
Licencia	Propietaria: Microsoft CLUF	Libre: GPL y otras	Libre: GPL y componentes propietarios	Libre: Licencia BSD, Licencia FreeBSD	Libre: Licencia BSD, Licencia ISC	Propietaria: Apple CLUF	Propietaria	Propietaria
Arquitecturas de procesador soportadas	x64	x86, x86-64, ARM	x86, x86-64, Power, ESA/390, z/Architecture	x86, x86-64, DEC Alpha, ARM, SPARC64, IA-64, PowerPC, MIPS	68000, Alpha, x86-64, i386, MIPS, PowerPC, SPARC 32/64, VAX, Zaurus y otras	x86-64	ROMP, IBM POWER, PowerPC, IBM PS/2, System/370, ESA/390	PA-RISC, IA-64
Sistemas de archivos soportados por defecto	ReFS, NTFS, FAT 12/16/32, ExFAT, ISO 9660, UDF	ext2, ext3, ext4, btrfs, FAT 12/16/32, ReiserFS, ISO 9660, UDF, NFS, HFS, HFS+, NTFS, HPFS, FFS, XFS, JFS, y otros	ext2, ext3, ext4, btrfs, FAT 12/16/32, ReiserFS, ISO 9660, UDF, NFS, HFS, HFS+, NTFS, HPFS, FFS, XFS, JFS, y otros	UFS 1/2, FAT 12/16/32, HPFS, FFS, ext2, ext3, ZFS, UDF, ISO 9660	FFS, ext2, FAT, ISO 9660, NFS, otros	HFS+, HFS, MFS, ISO 9660, FAT 12/16/32, UDF, ExFAT, FFS	JFS, JFS2, ISO 9660, UDF, NFS, SMBFS, GPFS	VxFS, HFS, ISO 9660, UDF, NFS, SMBFS
Memoria RAM mínima y máxima soportada	Min. 512 MiB Max. 4 TiB	Min. 128 MiB Max. ?	Min. 1 GiB Máx. 1 TiB (teórico)	Min. 24 MiB Max. ?	Min. 128 MiB Max. ?	Min. 2 GiB Max. ?	?	Min. 1,5 GiB Max. 4 TiB
Almacenamiento mínimo requerido	32 GB	1 GB	4 GB	150 MB	1 GB	10 GB	?	20 GB
Máximo de CPU físicas	64	?	64	?	?	?	?	?
Reloj de CPU mínimo	1.4 GHz	300 MHz	2 GHz	?	100 MHz	?	?	?

Ilustración 4 Comparación de los distintos Sistemas Operativos

7.2.3.2-Sistema de gestión de identidades

El siguiente punto es decidir qué sistema de Gestión de Identidades se va a implantar. Lo primero es definir qué es. Un sistema de gestión de accesos e identidades (IAM, Identity Access Manager) es un sistema que facilita la gestión de las identidades electrónicas. Este Sistema se utiliza para la administración de grupos y usuarios, el autoservicio, la administración delegada, el flujo de las aprobaciones, iniciar, registrar y gestionar identidades de los usuarios y sus permisos de acceso correspondientes de forma automatizada.

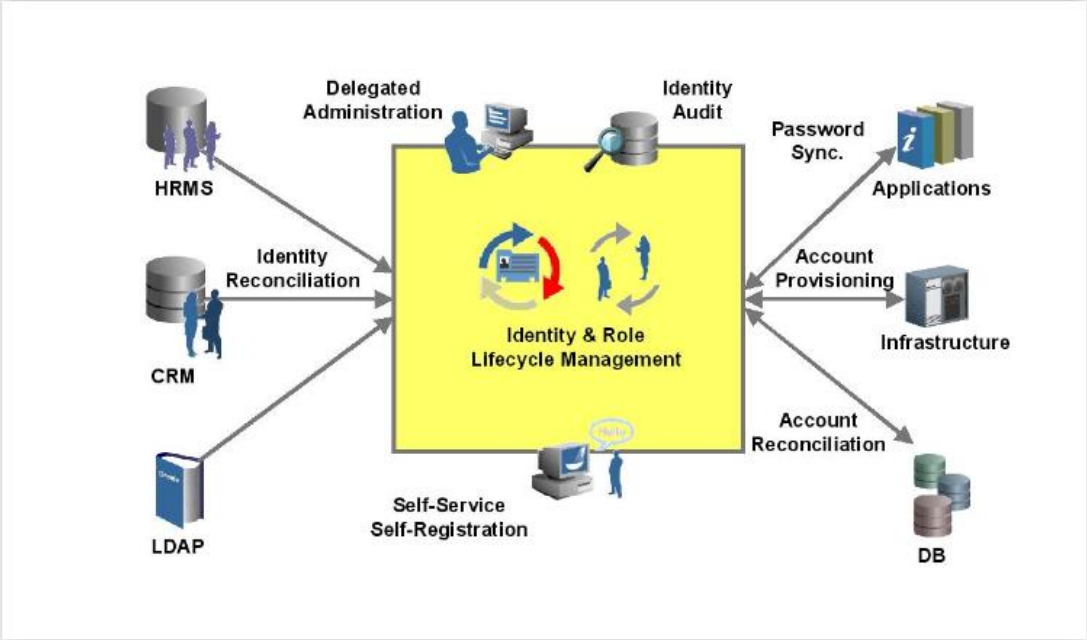

Ilustración 5 Esquema de la Gestion de Identidades

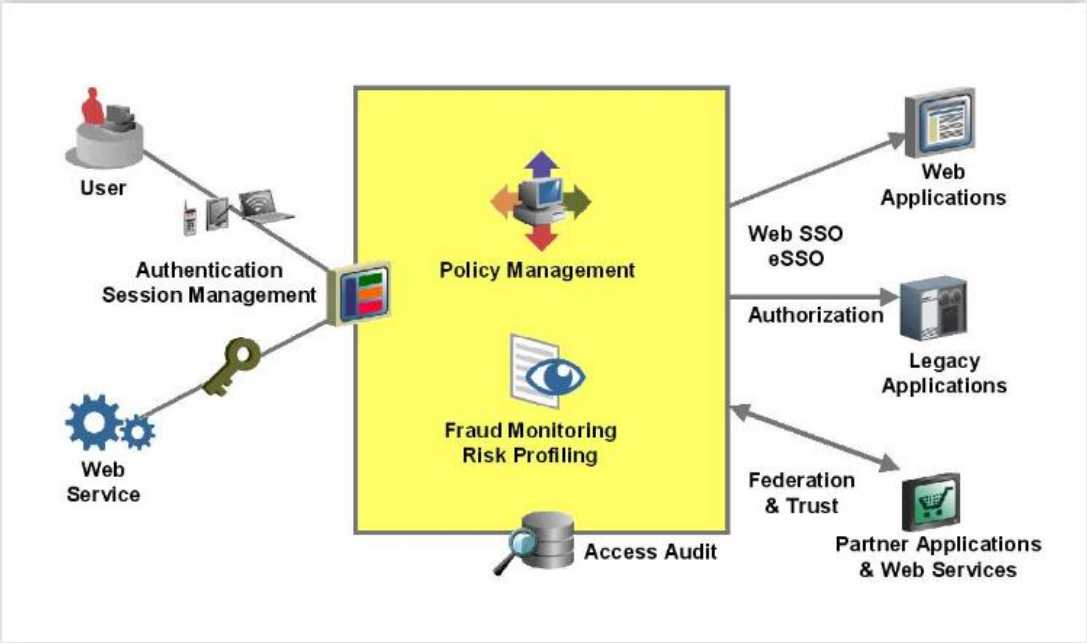

Ilustración 6 Esquema de la Gestión de Accesos

Es necesario realizar correctamente los procesos IAM, ya que en caso de realizarlo erróneamente pueden conducir al no cumplimiento de la normativa. En caso de una auditoria a la empresa, la administración no será capaz de demostrar que los datos de la empresa no están en riesgo de ser utilizados indebidamente.

Es complicado tomar la decisión de implantar un sistema de gestión de identidades, ya que no aumenta directamente la rentabilidad o la funcionalidad. Sin embargo, la falta de gestión de identidades y acceso supone riesgos tanto como para temas de auditoria como para la seguridad general de una organización. Estos problemas de mala gestión aumentan el riesgo tanto de las amenazas externas como las internas.

Se van a comentar las posibles opciones que se tienen en cuanto a Sistemas de GDI:

One Identity Manager, perteneciente a Dell, combina la sencillez en la instalación, configuración y uso. El sistema es compatible con los sistemas de bases de datos más importantes como son Oracle y Microsoft SQL. El producto de auto-servicio es intiutivo y sencillo de usar, de esta maneras los empleados pueden gestionar todas las etapas de la gestión de identidades sin requerir la ayuda del departamento especializado. La gama de productos también incluye el gestor de accesos en la nube, Cloud Access Manager, que habilita las capacidades de inicio de sesión única para una variedad de escenarios de acceso de aplicaciones Web.

El gestor de identidades de IBM, Security **Identity Manager**, está diseñado para ser rápido y fácil de implementar y para que sea compatible con otros productos. El software es compatible con Microsoft Windows Server, SUSE, Linux Enterprise Server, Red Hat Enterprise Linux y AIX de IBM, así como con sistemas de correo electrónico, sistemas ERP y aplicaciones en la nube. La creación y modificación de los privilegios del usuario se llevan a cabo de manera automática a través de un sistema basado en reglas y los derechos de acceso pueden ser añadidos o eliminados para los usuarios individuales.

Oracle Identity Manager es un sistema de gestión de identidades corporativas potente y flexible que gestiona de manera autónoma los privilegios de acceso de los usuarios dentro de los recursos de TI de la empresa. Este producto ofrece integración apta para usar con las tecnologías de infraestructura y aplicaciones empresariales más comúnmente implementadas. Oracle Identity Management, se considera como la mejor suite de soluciones para la gestión de identidad. Permite a las empresas administrar todo el ciclo de vida de identidad de los usuarios tanto dentro como fuera del firewall. Se puede aplicar la protección más minuciosa para recursos empresariales, eliminar automáticamente los privilegios de acceso y abordar las disposiciones reglamentarias y normas de cumplimiento. Oracle Access Manager soporta todos los servidores web, servidores de aplicaciones y servidores de directorios más importantes.

La conclusión que se puede sacar de este pequeño análisis es la siguiente:

Oracle es reconocido como líder en el entorno de gestión de identidad –este reconocimiento es otorgado por analistas del sector, la prensa y sus propios clientes. La gestión de identidad es un área estratégica de foco para Oracle. A medida que el mercado de gestión de identidad sigue desarrollándose, Oracle continúa ofreciendo innovaciones a través de su liderazgo en la comunidad de estándares, así como a través de la estrecha colaboración con sus clientes. Con Oracle Identity Management, los clientes pueden cumplir con todos sus requerimientos de gestión de identidad a partir de un solo proveedor que ofrece capacidades y productos líderes. Esto implica menos tiempo invertido en la integración de componentes, un único punto de contacto para soporte, un solo contrato de licencia y el respaldo de la compañía de software empresarial más grande del mundo.

7.2.3.2-BASE DE DATOS

La siguiente tabla muestra información acerca de Oracle, MySQL y Bases de Datos de Servidores SQL, y como ellas se comparan.

Feature	Oracle	MySQL	SQL Server
Interfaz	GUI, SQL	SQL	GUI, SQL, Various
Lenguaje Soportado	Many, including C, C#, C++, Java, Ruby, and Objective C	Many, including C, C#, C++, D, Java, Ruby, and Objective C	Java, Ruby, Python, VB, .Net, and PHP
Sistema Operativo	Windows, Linux, Solaris, HP-UX, OS X, z/OS, AIX	Windows, Linux, OS X, FreeBSD, Solaris	Windows
Licencia	Propietario	Código Libre	Propietario

El sistema de gestión de bases de datos relacionales de **Oracle DB** ha logrado permanecer en la cima gracias a sus actualizaciones de productos, ya que de esta manera se adaptan al mercado. Se considera a *Oracle Database* como uno de los sistemas de bases de datos más completos, destacando: soporte de transacciones, estabilidad, escalabilidad, y soporte multiplataforma. Su dominio en el mercado de servidores empresariales había sido casi total hasta que recientemente tiene la competencia del Microsoft SQL Server y de la oferta de otros RDBMS con licencia libre como PostgreSQL, MySQL o Firebird.

Las características relacionadas con la capacidad de administración en Oracle Database 11g están diseñadas para ayudar a las empresas a administrar fácilmente y cumplir con éxito las expectativas del nivel de servicio al usuario. Las nuevas características y mejoras en la capacidad de administración de Oracle Database11g ayudan a aumentar la productividad de los DBA y reducir los costos de administración.

- Protege los sistemas de todas las causas comunes relacionadas con el tiempo de baja planificado y no planificado, con inclusión de las fallas en el sitio, en el almacenamiento y en el servidor, así como de una de las causas más importantes, el error humano.
- Proporciona una sola plataforma integrada que ofrece alto desempeño y escalabilidad, y brinda soporte de todas las tecnologías principales actualmente utilizadas por los desarrolladores de aplicaciones.
- Incorpora nuevas capacidades para los entornos de desarrollo de aplicaciones más importantes, permitiendo acortar el tiempo de llegada al mercado y mejorar el desempeño de las aplicaciones.

Microsoft SQL Server es un sistema de gestión de bases de datos del modelo relacional, desarrollado por la empresa Microsoft.

El lenguaje de desarrollo utilizado (por línea de comandos o mediante la interfaz gráfica de Management Studio) es Transact-SQL (TSQL), una implementación del estándar ANSI del

lenguaje SQL, utilizado para manipular y recuperar datos, crear tablas y definir relaciones entre ellas. Algunas de las principales características son:

- Soporte de transacciones.
- Soporta procedimientos almacenados.
- Incluye también un entorno gráfico de administración, que permite el uso de comandos DDL y DML gráficamente.
- Permite trabajar en modo cliente-servidor, donde la información y datos se alojan en el servidor y los terminales o clientes de la red sólo acceden a la información.
- Además permite administrar información de otros servidores de datos.

Otras características notables del producto incluyen la introducción de SQL Server Always On (tecnología de gestión de datos para disminuir el tiempo de inactividad del usuario a raíz de fallos en el sistema), soporte para datos estructurados y semi-estructurados, una mayor compresión, y varios complementos para apoyar a otros productos en el mercado.

La plataforma de **MySQL** al contrario que las otros dos, es de código abierto. La era digital dio lugar a un movimiento de colaboración para el desarrollo de software que se ha convertido en un mercado competitivo para las bases de datos y otros software. De acuerdo con informes de mercado, hay alrededor de 10 millones de instalaciones de MySQL.

Oracle y SQL Server se consideran herramientas que favorecen a los usuarios con los sistemas empresariales de gran tamaño, mientras que MySQL se considera una herramienta destinada más a menudo a las personas interesadas en la gestión de las bases de datos asociadas a sus sitios web. Al igual que con Oracle y SQL Server, MySQL ha liberado actualizaciones para su software casi todos los años

Con su última versión MySQL 5.0 anexa nuevas características importantes que lo hacen más competitivo. Entre sus nuevas características tenemos:

- *Uso de transacciones ACID (Atomic, Consistent Isolated, Durable):* Para construir aplicaciones más seguras mediante commit, rollback, crash recovery y bloqueo por registro.
- *Store Procedures:* Para mejorar la programación.
- *Triggers:* Para mejorar las reglas del negocio.
- *Vistas:* Para que la información sensible sea más segura.
- *Information Schema:* Para un fácil acceso a los metadatos.
- *Transacciones Distribuidas(XA):* Para soportar transacciones entre múltiples ambientes de bases de datos

7.3-ORGANIZACIÓN DEL TRABAJO

En este apartado del documento se va a mostrar de forma clara y detallada la estructura general necesaria para llevar a cabo la realización del proyecto. El organigrama del equipo de trabajo quedaría de la siguiente forma:

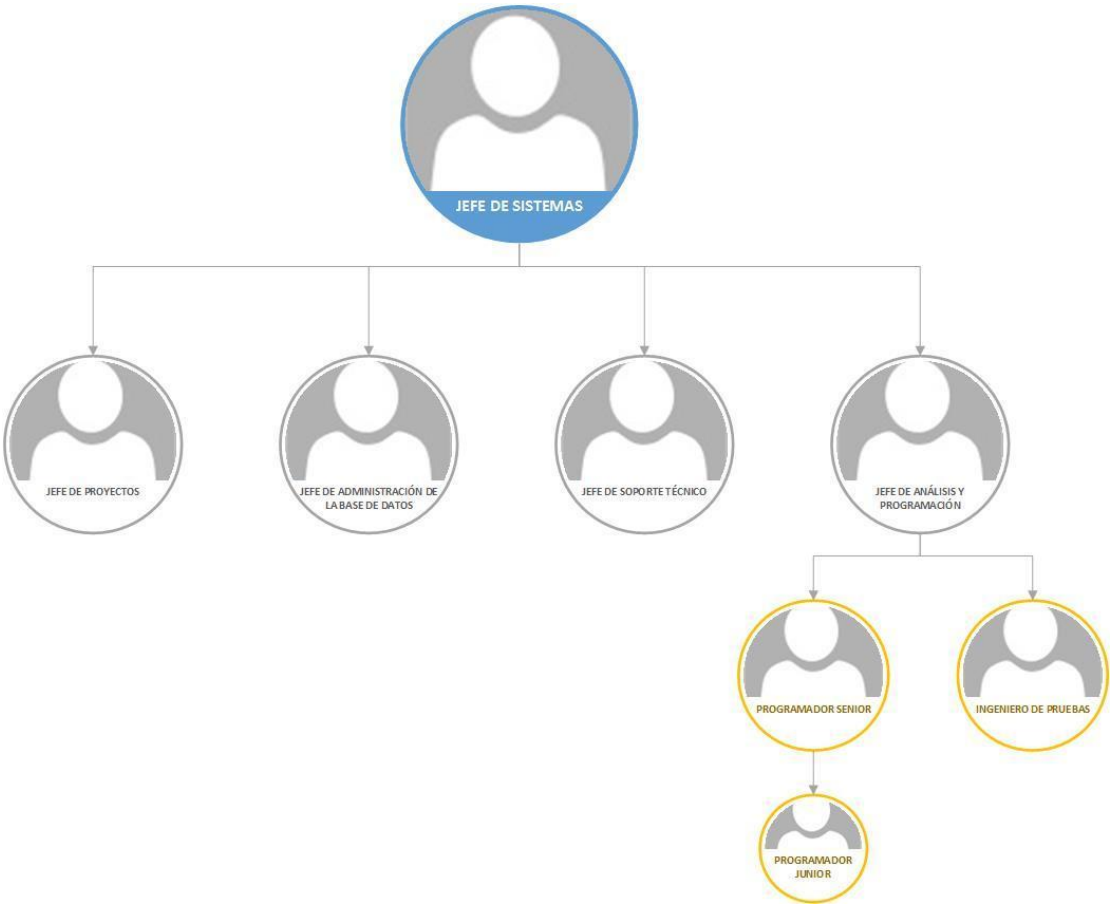

Ilustración 7 Esquema del equipo de CFM Consulting

En la siguiente tabla se representará descrita de forma detallada tanto por función, como por experiencia cada uno de los miembros implicados en el proyecto:

Rol	Función	Experiencia Mínima
Jefe de sistemas	• Dirigir las actividades • Cumplir objetivos de aquellas áreas que interactúan con el departamento de sistemas • Planear y administrar a un grupo de analistas cualificados. • Supervisión de los proyectos de TI.	5 años en el departamento de sistemas.
Jefe de proyectos	• Dirigir un proyecto específico (incluyendo análisis, diseño, implementación y testeo).	3 años en el departamento de proyectos.
Jefe de administración de la base de datos	• Administrar las tecnologías de la información y la comunicación, siendo responsable de los aspectos técnicos, tecnológicos y legales de la base de datos.	6 años en el departamento de base de datos.
Jefe de soporte técnico	• Fijar y hacer cumplir las normas y procedimientos para mantener la disponibilidad del sistema informático, por medio de mantenimiento preventivo y acciones correctivas.	4 años como programador o del departamento de soporte técnico.
Jefe de análisis y programación	• Planificar y dirigir toda la programación y actividades asociadas al departamento de análisis. • Diseñar y probar la lógica y códigos de los programas. • Lograr que los sistemas diseñados cumplan los requerimientos.	8 años como programador senior.
Programador Senior	• Realizar programas con distintos tipos de lenguaje de programación.	5 años como programador.
Programador Junior	• Trabajar en el mantenimiento, diseño y programación del software. • Controlar las mejoras y modificaciones del software.	3 años como programador.
Ingeniero de pruebas	• Realizar un plan de pruebas para todo el proyecto, actualizarlo y corregirlo en caso necesario.	7 años como ingeniero de pruebas

	• Inspecciones de los productos software. • Revisar que se hagan los cambios que indican las pruebas	
Analista de la gestión del cambio	• Alinea la organización y los objetivos de proyecto. • Obtiene información de la situación actual y planea a partir de ella.	8 años como analista de la gestión del cambio
Consultor	• Evalúa el nivel tecnológico de la empresa y transmite mejoras tecnológicas con el fin de optimizar la empresa. • Realizar seguimiento de los desarrollos tecnológicos. • Analizar procesos actuales, planear nuevos con sus objetivos estratégicos y mantener mejoras de rendimiento mediante la optimización de procesos.	7 años como consultor en el ámbito de las tecnologías y negocios.

7.4-Flujo de Instalación y flujo de Trabajo

Primero se comenzará con la instalación del Sistema Operativo, Oracle Linux 5. A continuación se instalará la base de datos, Oracle DB 11g. El siguiente paso será instalar el servidor de aplicaciones, Weblogic y el directorio de usuarios, OUD.

Una vez con esa arquitectura, se ejecutará la utilidad de creación de repositorios de Oracle para ampliar la base de datos con los esquemas necesarios para la instalación de OIM y OAM.

Se instalará y configurará el Gestor de identidades, Oracle Identity Manager y el gestor de Accesos, Oracle Access Manager.

El último paso para dejar el entorno preparado será instalar el servidor web Apache e instalar el Webgate, que es un pluggin del servidor Apache que intercepta las peticiones HTTP y las redirige al Oracle Access Manager.

Como parte independiente a la instalación se van a realizar una serie de despliegues de aplicaciones en el servidor Weblogic. El Oracle Access Maager será el encargado de autorizar o denegar el acceso a estas aplicaciones.

7.5-CARACTERÍSTICAS TÉCNICAS DESTACABLES

Aquí se detallarán algunas características relevantes en la instalación de las herramientas.

7.5.1-SISTEMA OPERATIVO:

Oracle Linux 5 ha sido el sistema operativo seleccionado para la implantación de este sistema GDI.

Ilustración 8 Instalación OL5 1

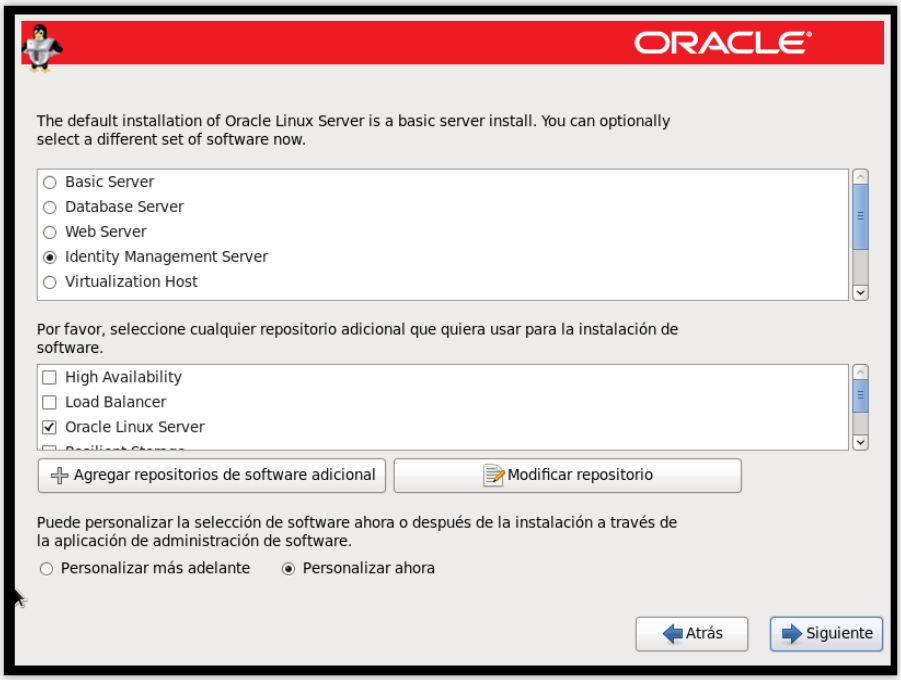

Ilustración 9 Instalación OL5 2

Cabe destacar que se va a instalar el sistema operativo como un servidor de gestión de identidades y se va a seleccionar un par de componentes que se quiere que se incluyan en el SO (un cliente de directorio, servidor web con sus correspondientes módulos, etc.

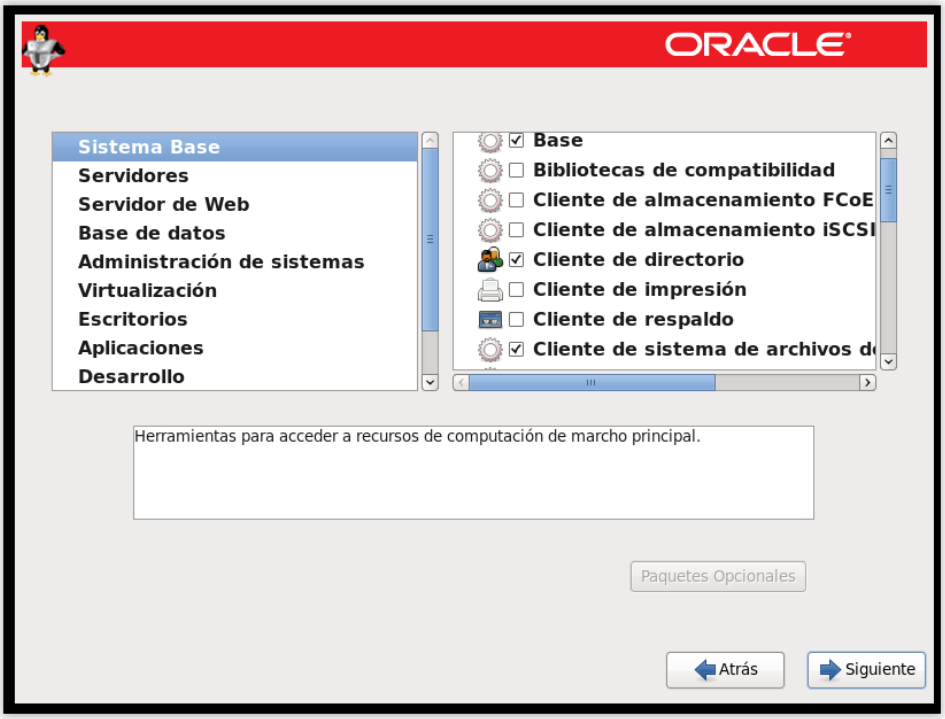

Ilustración 10 Instalación OL5 3

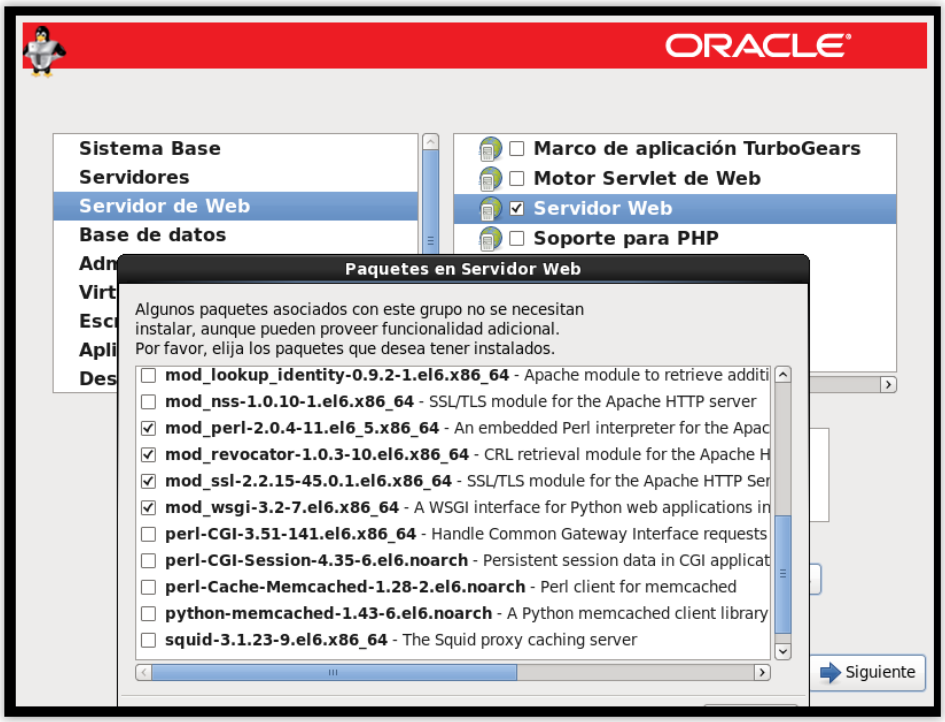

Ilustración 11 Instalación OL5 4

Ilustración 12 Instalación OL5 5

7.5.2-Base de Datos

La base de datos que se va a implantar es la Oracle DB 11g. Se van a tener en cuenta los siguientes apartados de la instalación:

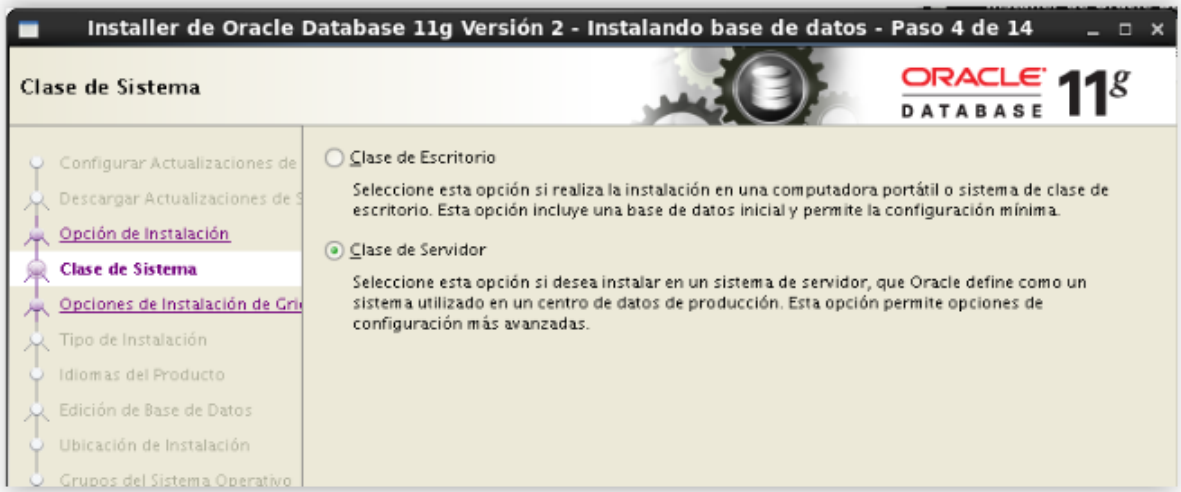

Ilustración 13 Instalación BBDD 1

Se instalará como Base de Datos de instancia única.

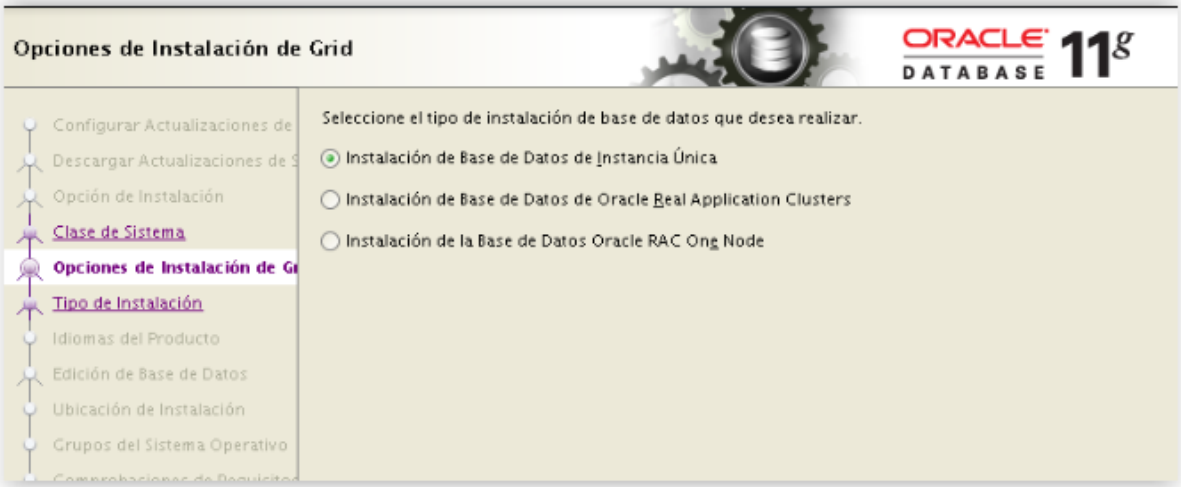

Ilustración 14 Instalación BBDD 2

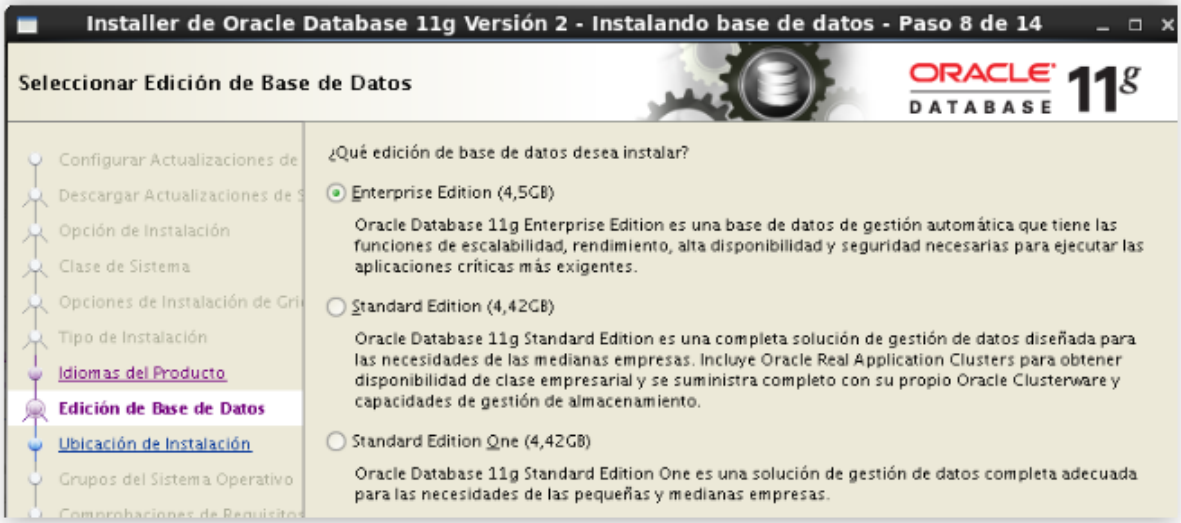

Ilustración 15 Instalación BBDD 3

Se declara el nombre de la Base de Datos global. En este caso: orcl

Ilustración 16 Instalación BBDD 4

Se asigna la misma contraseña a los esquemas principales.

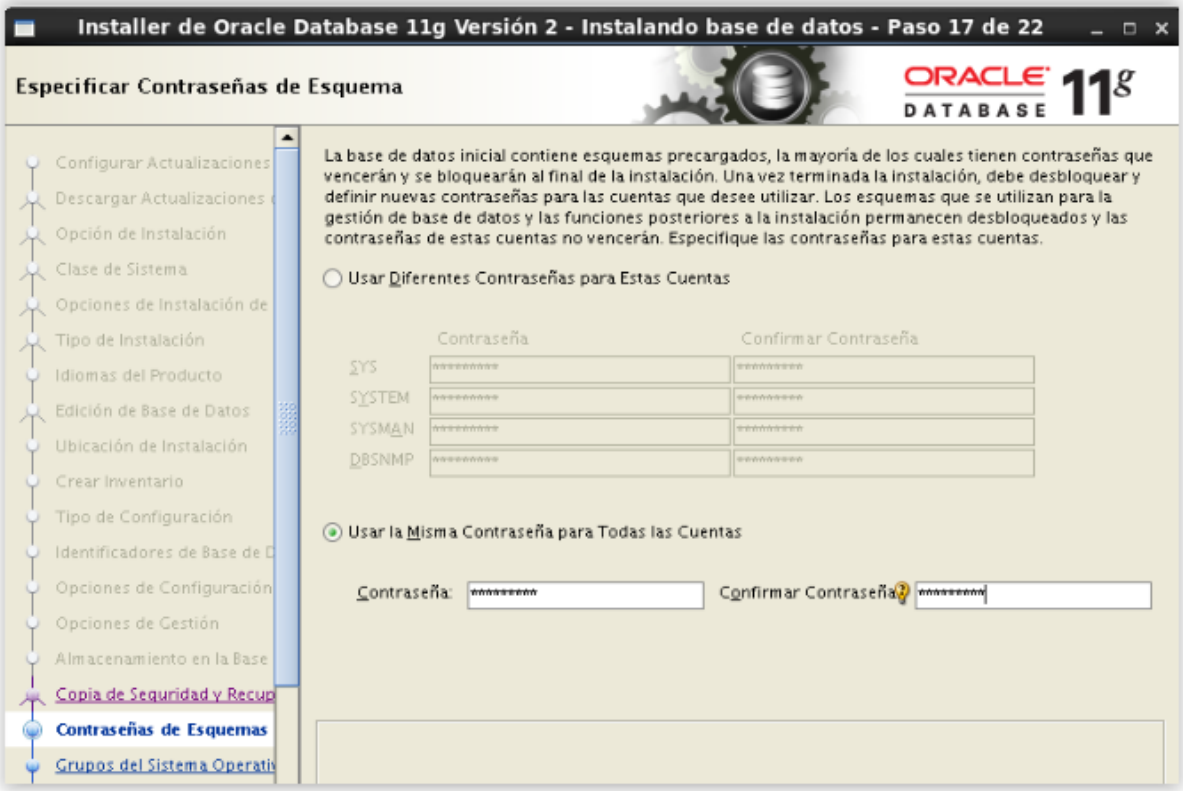

Ilustración 17 Instalación BBDD 5

7.5.3-WEBLOGIC

Tenemos que instalar un servidor Weblogic, que es un servidor de aplicaciones. En este servidor se despliegan el OIM Server y el OAM Server. Se configurará este Weblogic con los siguientes componentes

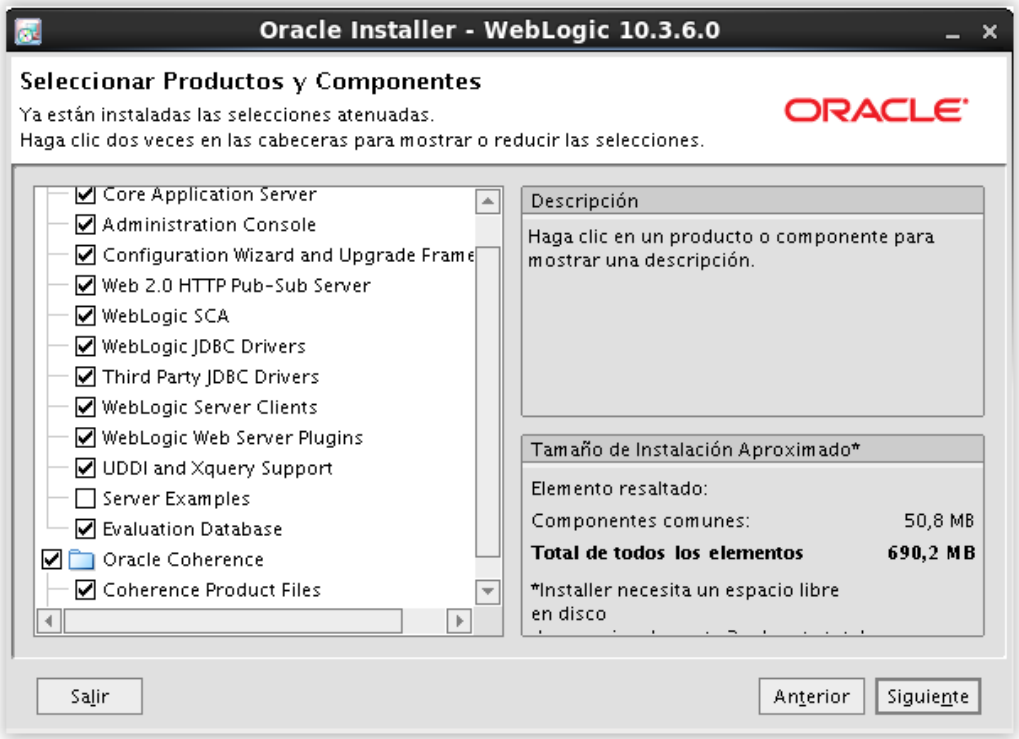

Ilustración 18 Instalación Weblogic

7.5.4-OUD (LDAP)

Para la autenticación con el OAM es necesario instalar el Oracle Unified Directory, que es el almacén de cuentas. Para ello se tiene que desplegar este servicio en un servidor Weblogic.

Ilustración 19 Instalación OUD 1

Ilustración 20 Instalación OUD 2

Para configurarlo una vez instalado, se declara el puerto de conexión, el host y el usuario propietario.

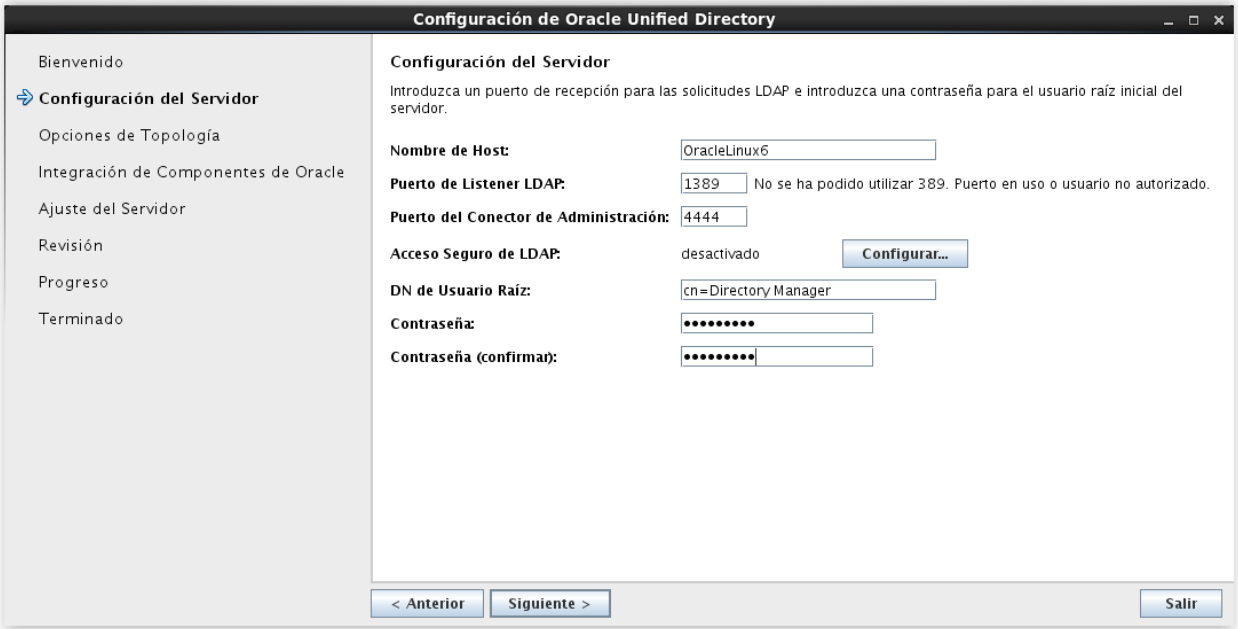

Ilustración 21 Instalación OUD 3

7.5.5-RCU

Antes de instalar el OIM y el OAM, hay que crear una serie de esquemas en la base de datos. Para ello se ejecuta el software de creación de repositorios.

Ilustración 22 Instalación RCU 1

Ilustración 23 Instalación RCU 2

Ilustración 24 Instalación RCU 3

7.5.6-OAM

Una vez instalado el OAM, hay que crear un dominio en Weblogic. Se configura para que soporte Oracle Access Management y Mobile Security y el Oracle Enterprise Manager.

Ilustración 25 Instalación OAM 1

Ilustración 26 Instalación OAM 2

Ilustración 27 Instalación OAM 3

Ilustración 28 Instalación OAM 4

7.5.7-OIM

De la misma manera que con OAM, una vez instalado el OIM, se tiene que crear un dominio en Weblogic

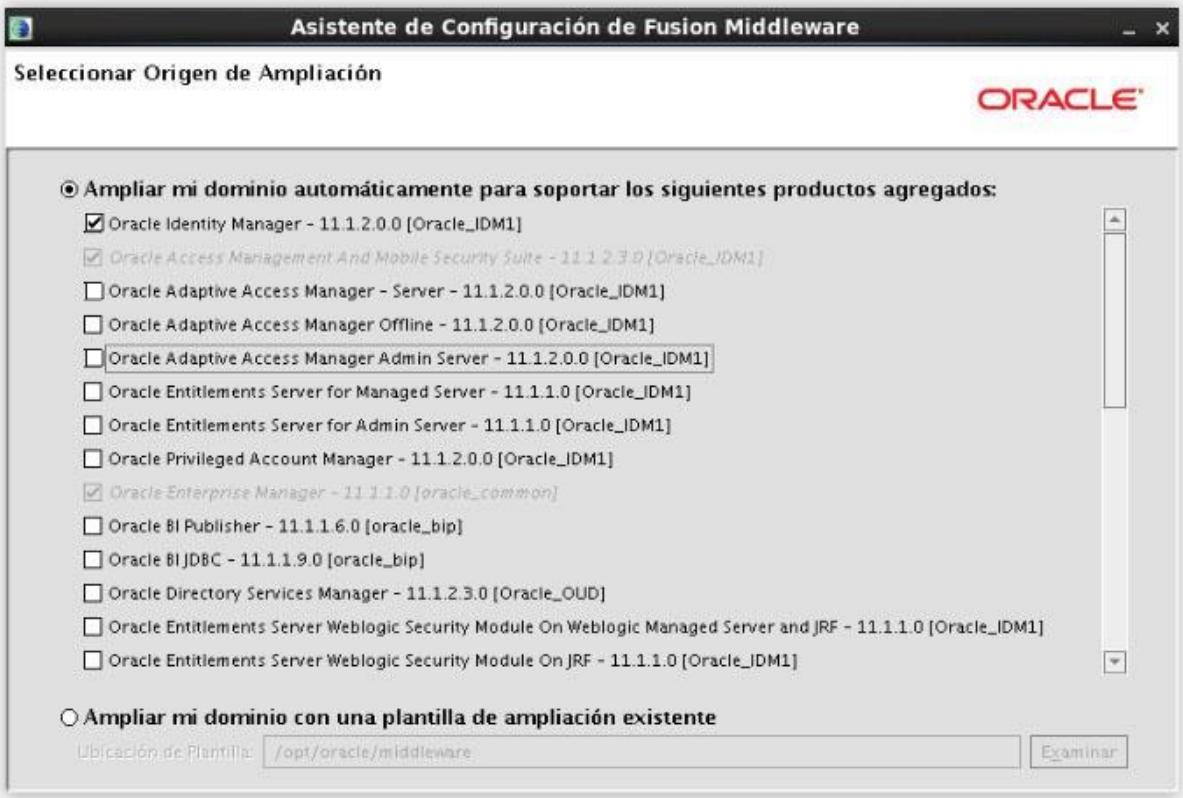

Ilustración 29 Instalación OIM 1

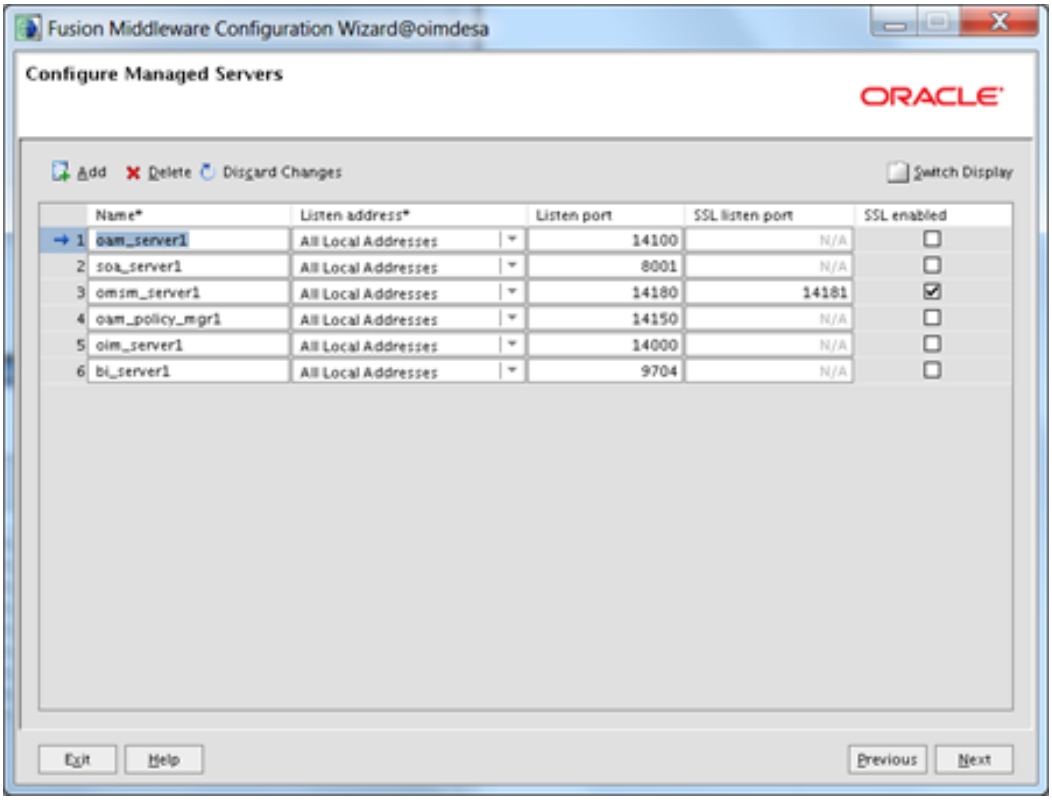

Ilustración 30 Instalación OIM 2

8. PLANOS Y DIAGRAMAS

A continuación se va a analizar unos diagramas para entender el funcionamiento del sistema.

En el primer diagrama se define como el administrador da de alta a los usuarios. El administrador introducirá el nuevo usuario en la BBDD (mediante el formulario que está desplegado en la web o directamente sobre la BBDD). Una tarea programada entre el Sistema de Gestión de Identidades y la BBDD realizará una reconciliación y transformará las diferentes líneas de la BBDD en identidades en el OIM.

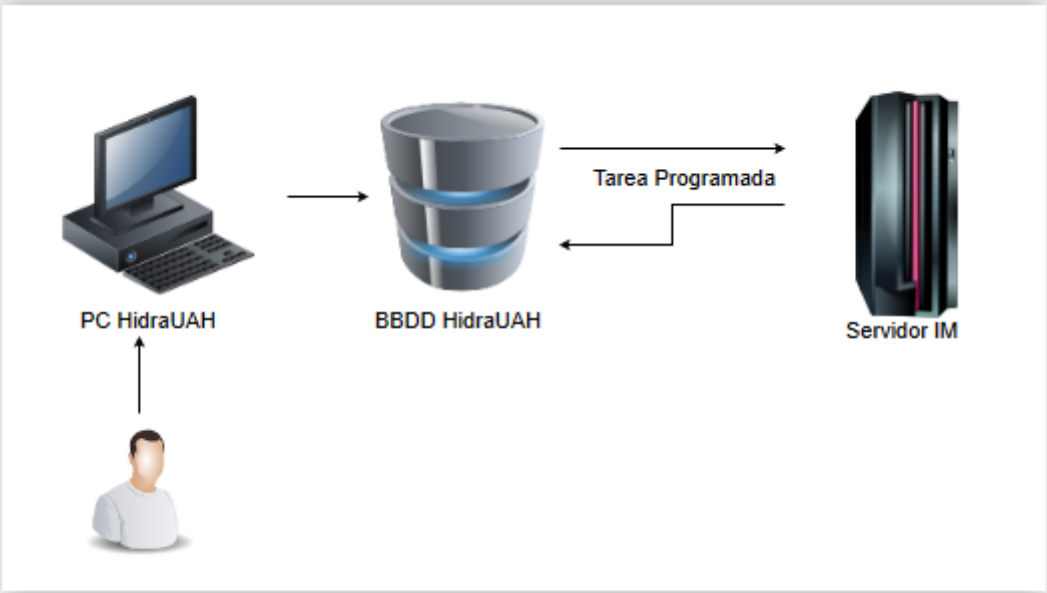

Ilustración 31 Diagrama Infraestructura y Funcionamiento 1

El segundo diagrama muestra la interacción entre el Sistema de Gestión de Identidades y el repositorio de cuentas, el LDAP. Mediante una tarea programada, el Sistema Gestor de Identidades (OIM) envía a los usuarios al LDAP, almacenándose allí como cuentas para su posterior uso para la autenticación

Ilustración 32 Diagrama Infraestructura y Funcionamiento 2

En este diagrama se define cómo se gestionan los accesos. El primer paso es acceder a nuestra web. Al introducir nuestro dominio, con unos credenciales (usuario y contraseña) , el gestor de accesos comprobará esos credenciales en el LDAP. En caso de que el usuario tenga los credenciales correctos, se le dará acceso a la parte de la aplicación web para la cual tenga permisos. En caso de no tener acceso se lanzará una ventana de error.

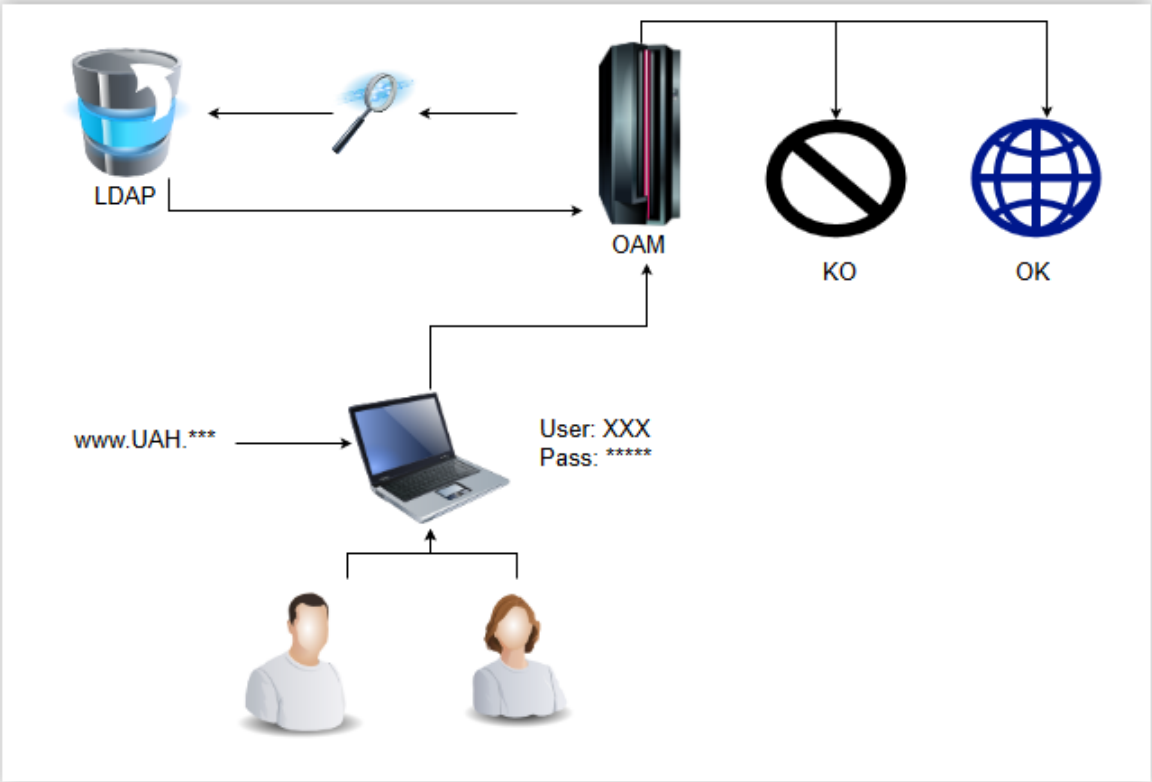

Ilustración 33 Diagrama Infraestructura y Funcionamiento 3

En el último diagrama se expone la infraestructura al completo de tal manera que se ve reflejado en una imagen como está estructurado el sistema y sus relaciones.

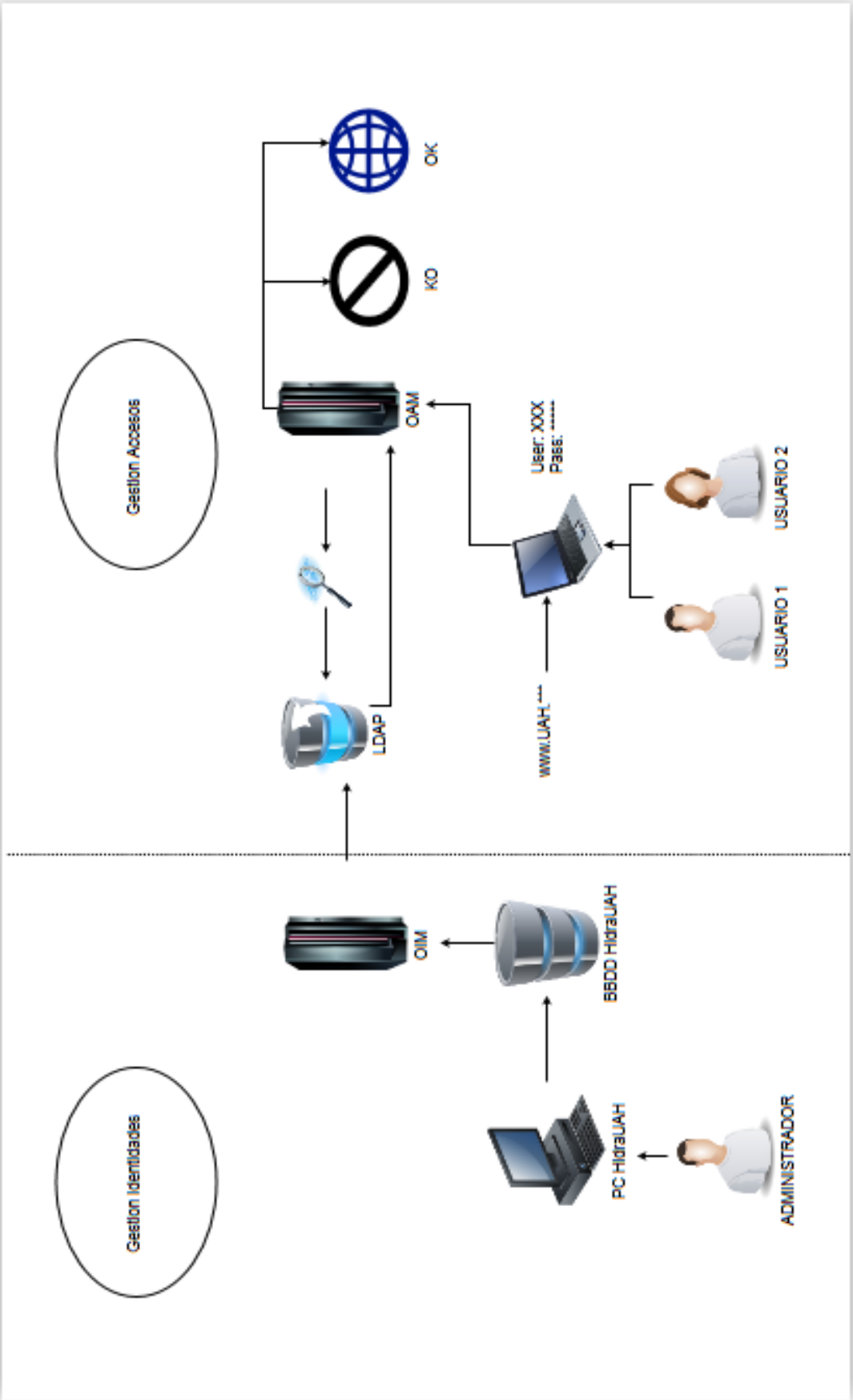

Ilustración 34 Diagrama Infraestructura y Funcionamiento 4

9. MANUAL DE USUARIO

9.1-CREACIÓN DE USUARIO EN OIM

Para crear un usuario en el sistema OIM serán necesarios seguir los siguientes pasos:

- Crear los atributos de la identidad.

.Para ello se accede a la consola de administración de OIM

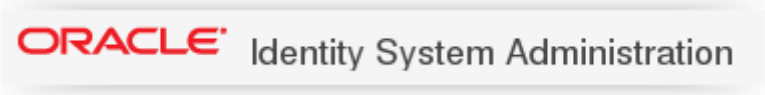

Ilustración 35 OIM; Creación de usuarios 1

El primer paso para realizar cualquier modificación es:
Crear Sandbox->Realizar las modificaciones->Publicar Sandbox

Una vez creada la sandbox para crear los atributos, se accede en System Entities al apartado Users. Se pulsa en Crear y lo primero que se debe hacer es seleccionar el tipo de atributo.

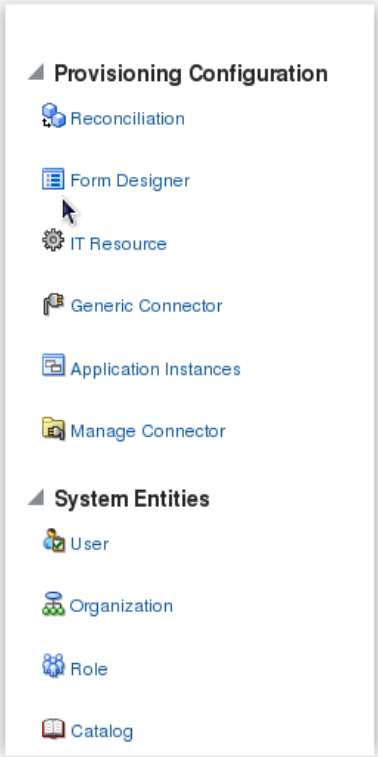

Ilustración 36 OIM; Creación de usuarios 1

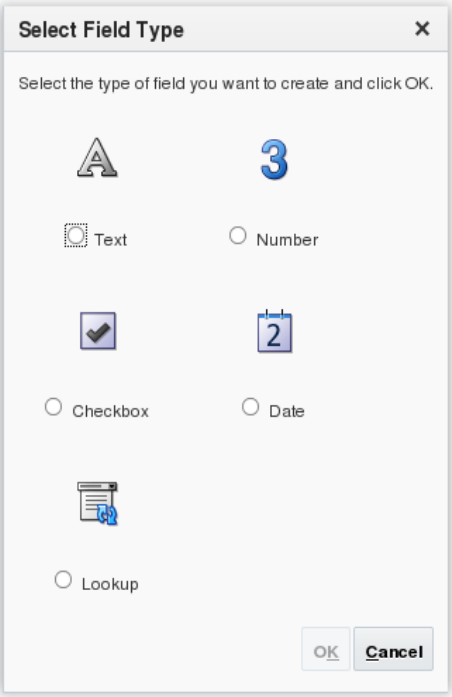

Ilustración 37 OIM; Creación de usuarios 2

Una vez seleccionado el tipo de atributo se tendrá que dar un Display Label (nombre que tendrá en el frontal del sistema), Nombre (nombre que llevará en el back-end del sistema) y Descripción.

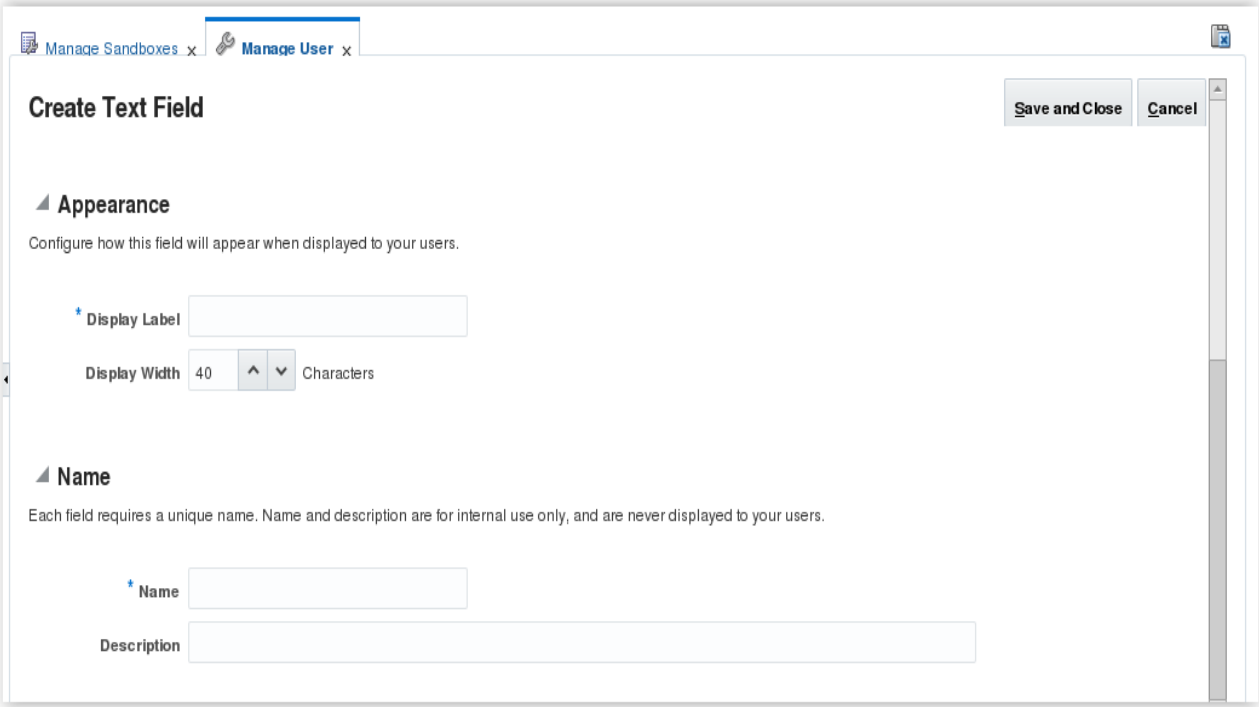

Ilustración 38 OIM; Creación de usuarios 3

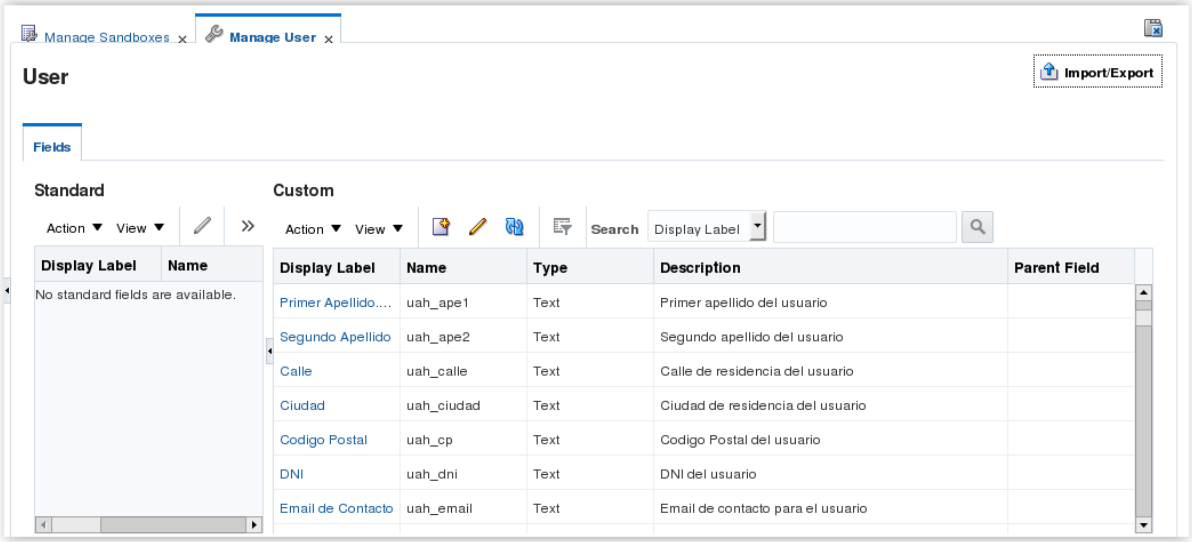

Ilustración 39 OIM; Creación de usuarios 4

- Creación del formulario

Para ello se va a acceder a la consola de Servicio de Identidades

En esta consola se accede al apartado Usuarios.

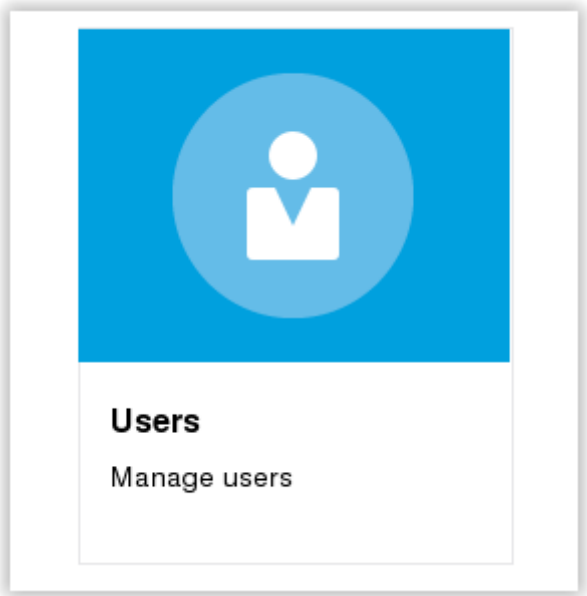

Ilustración 40 OIM; Creación de usuarios 5

Y con la sandbox correspondiente creada, se abre el apartado Crear,Modificar y Ver se pulsa en Customizar

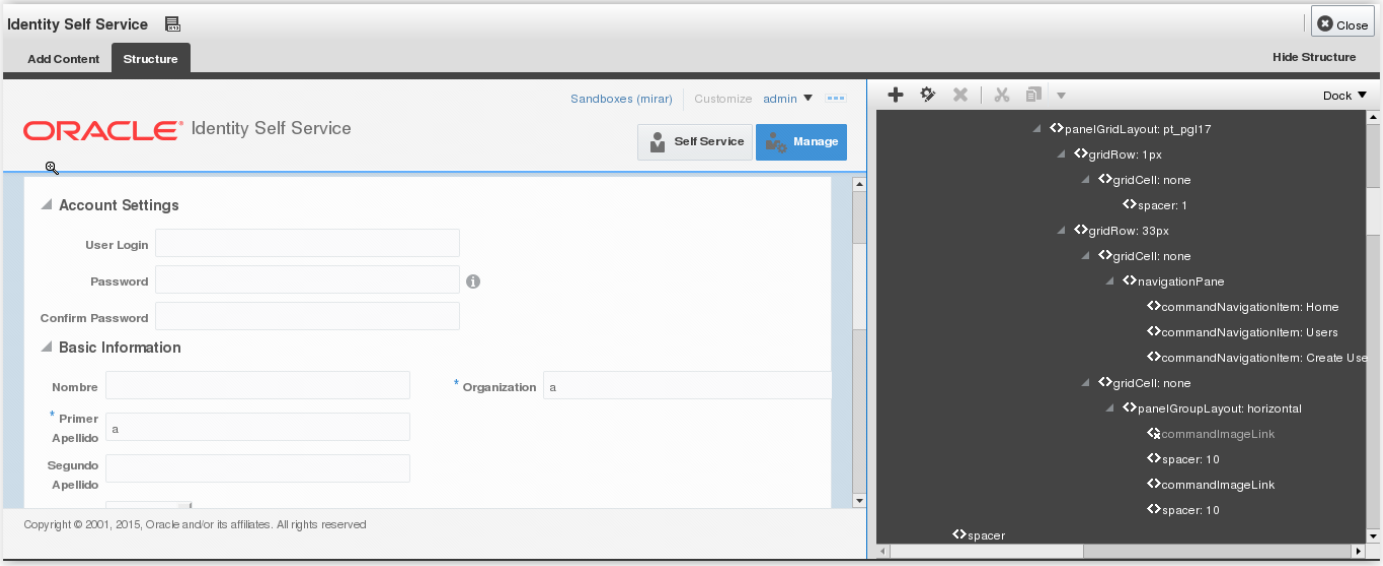

Ilustración 41 OIM; Creación de usuarios 6

En esta pantalla se podrá añadir campos de texto con los atributos que se necesiten. Una vez publiquemos esta sandbox, podremos crear usuarios, ver su información y modificarlos.

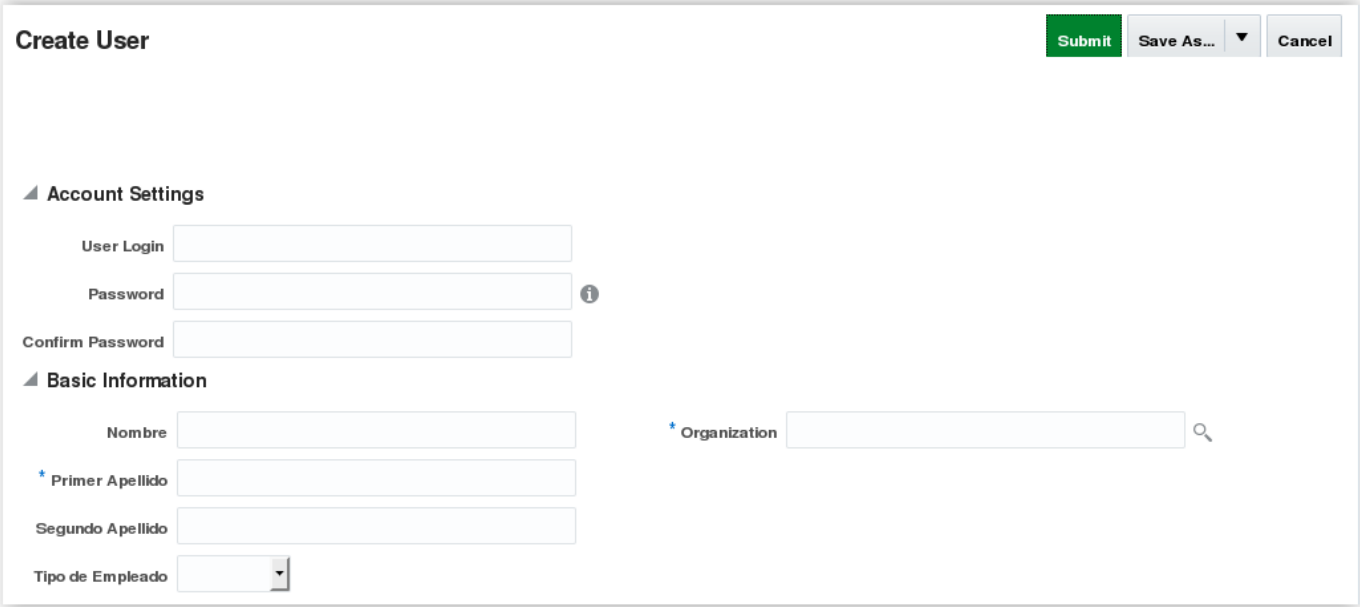

Ilustración 42 OIM; Creación de usuarios 7

9.2-Creación de Usuario en BBDD

Para la creación de un usuario en la base de datos se ha desplegado un formulario en la parte de la aplicación web que solo tendrá acceso el administrador. Una vez se rellene este formulario, se dará de alta al usuario en la tabla Users, la cual está conectada mediante el conector dbat al sistema de gestión de identidades. Posteriormente se programará la tarea que ejecutara la reconciliación entre bbdd y OIM.

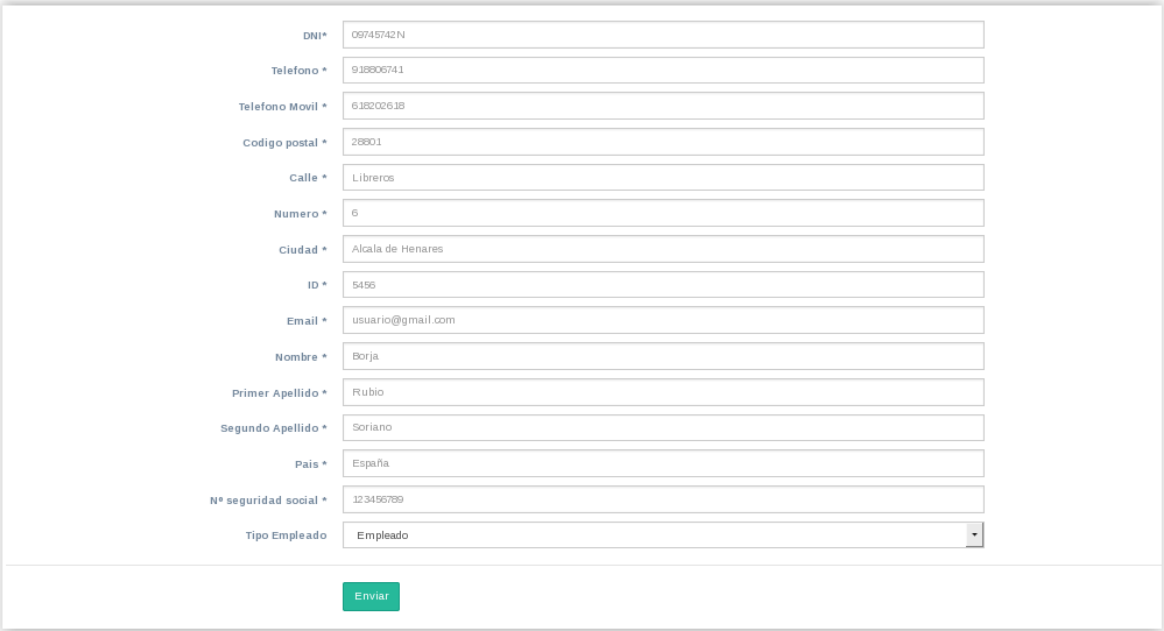

Ilustración 43 Formulario de creación de usuario en la aplicación web

9.3-CONFIGURACIÓN DE CONECTOR CON BBDD

Para configurar el conector de BBDD, que hará la reconciliación con OIM, y traerá los usuarios al sistema, habrá que realizar los siguientes pasos:

Instalar el conector DBAT Trusted. Para ello se accede a la consola de Administracion y en el apartado Provisioning Configuration se accede a Manage Connectors.

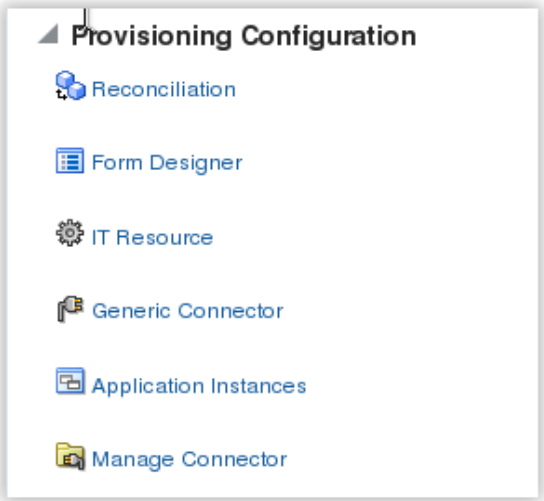

Ilustración 44 Conector DBAT OIM 1

En esta ventana se selecciona el conector DBAT Trusted.

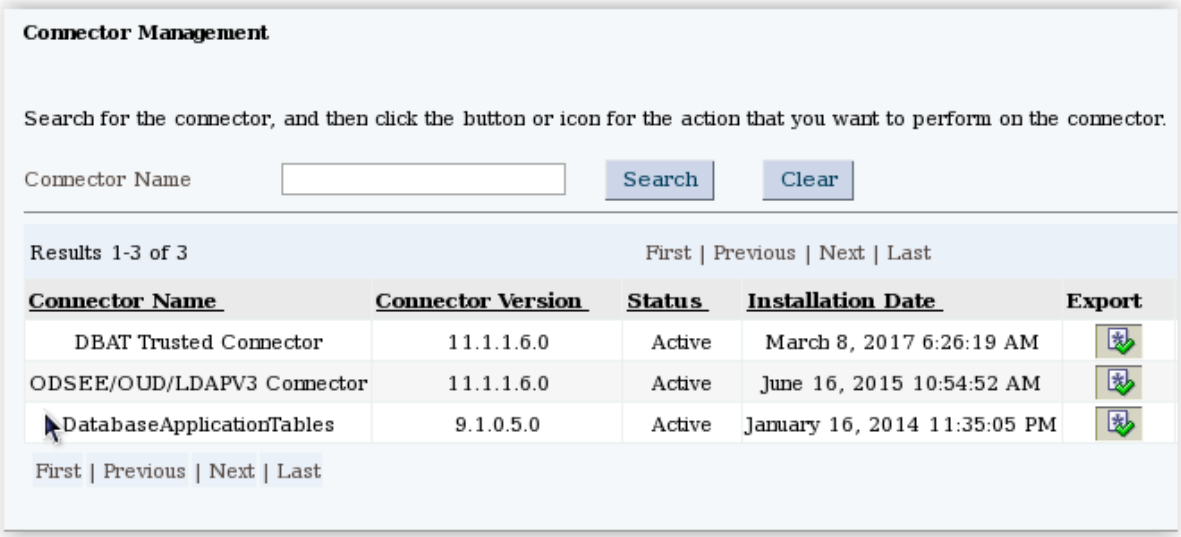

Ilustración 45 Conector DBAT OIM 2

En la misma consola de Administración, ahora accedemos a IT Resouces. Crearemos DBAT Trusted y aquí introduciremos los datos de conexión con la BBDD

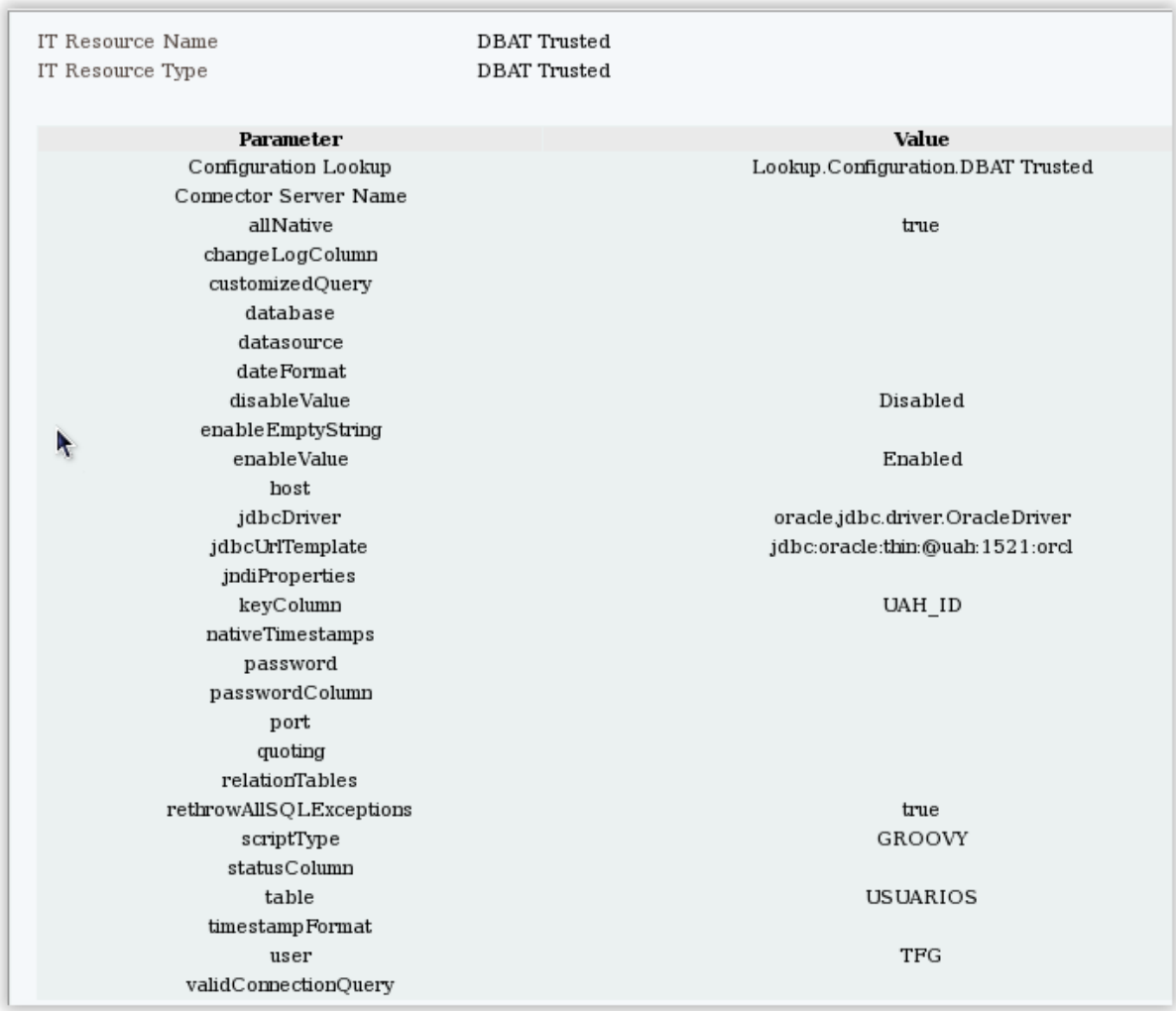

Ilustración 46 Conector DBAT OIM 3

Una vez configurado el IT Resource, se tendrá que crear el Resource Object, Process Definition y configurar la Lookup de Reconciliación.
Para esta tarea, se abrirá la Consola de Diseño.

Ilustración 47 Conector DBAT OIM 4

El primer paso es crear el Resource Objet DBAT User. Aquí se añadiran todos los atributos que se quiere que tenga el objeto, y se pulsa en crear perfil de reconciliación.

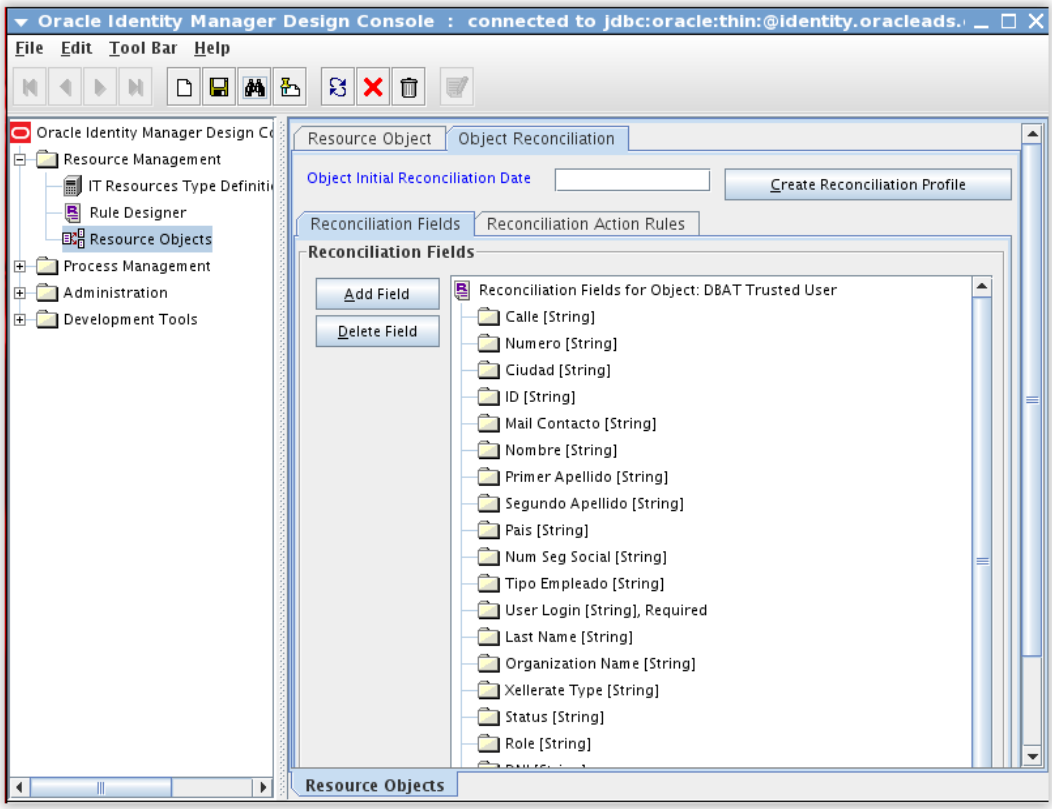

Ilustración 48 Conector DBAT OIM 5

Posteriormente se creará el Process Definition DBAT. Aquí se relacionan los atributos del objeto DBAT creado anteriormente, con los atributos creados en la consola de administración.

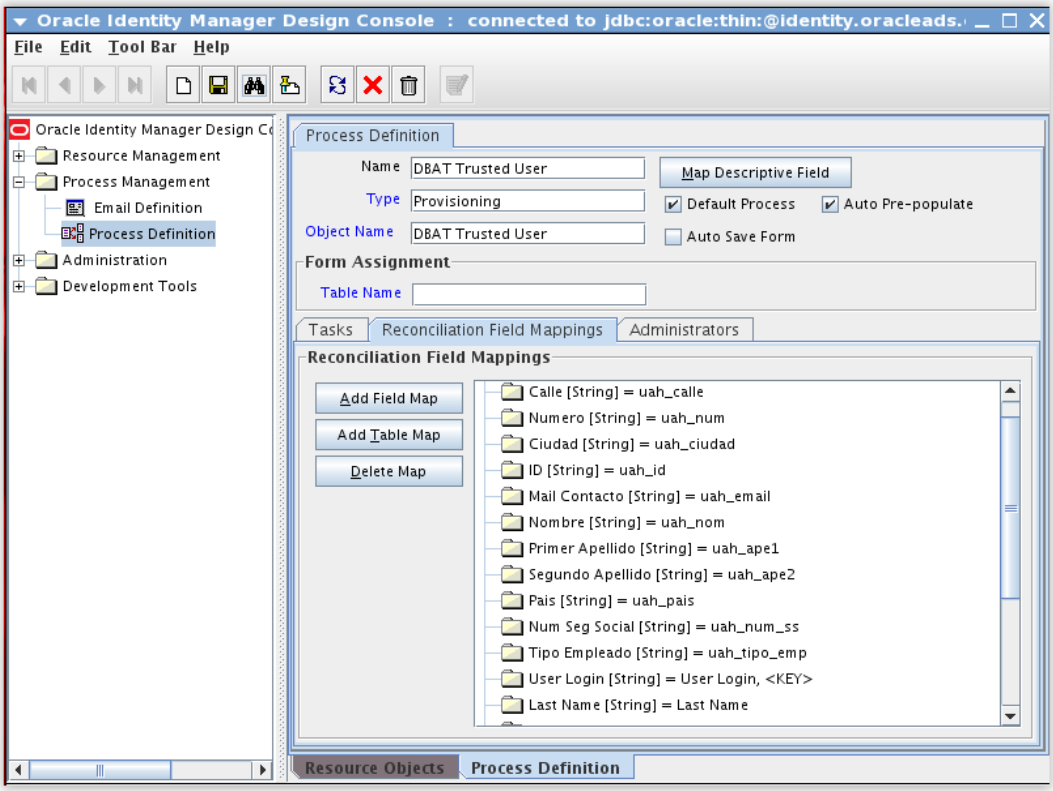

Ilustración 49 Conector DBAT OIM 6

Para finalizar, se editará la Lookup de Reconciliación, en la cual se mapean los atributos del objeto DBAT con los atributos de la BBDD

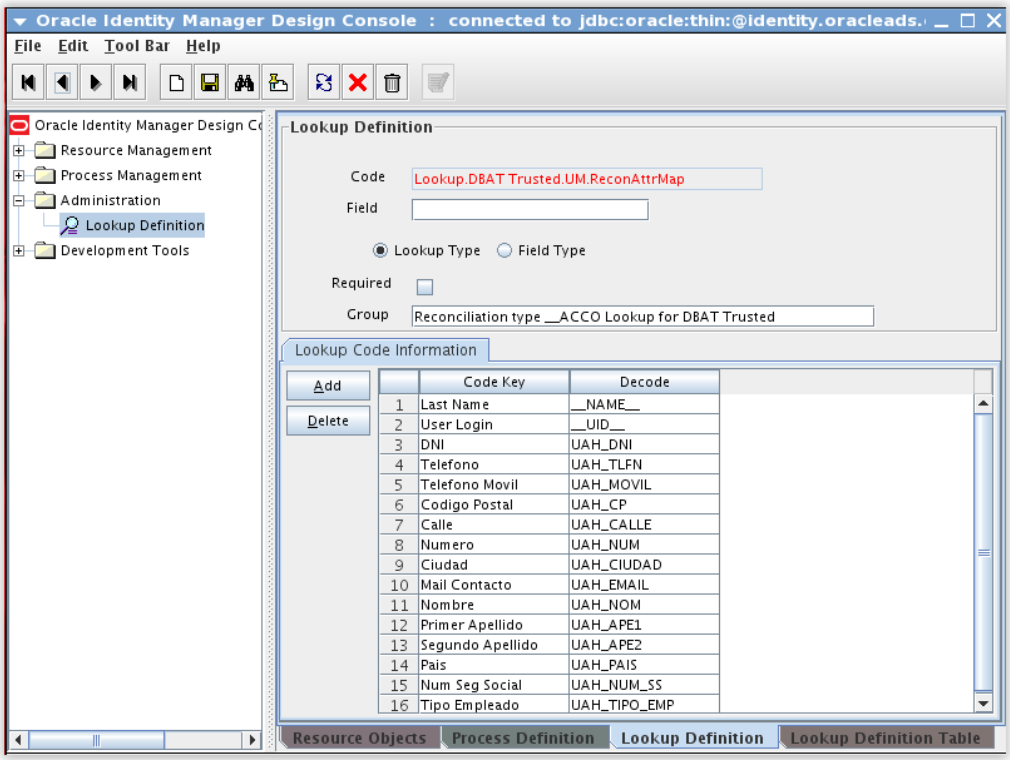

Ilustración 50 Conector DBAT OIM 7

9.4-CONFIGURACIÓN DE CONECTOR CON LDAP

Para configurar el conector de LDAP, que se provisionará con las identidades de OIM, habrá que realizar los siguientes pasos:

Instalar el conector ODSEE. Para ello se accede a la consola de Administración y en el apartado Provisioning Configuration se accede a Manage Connectors.

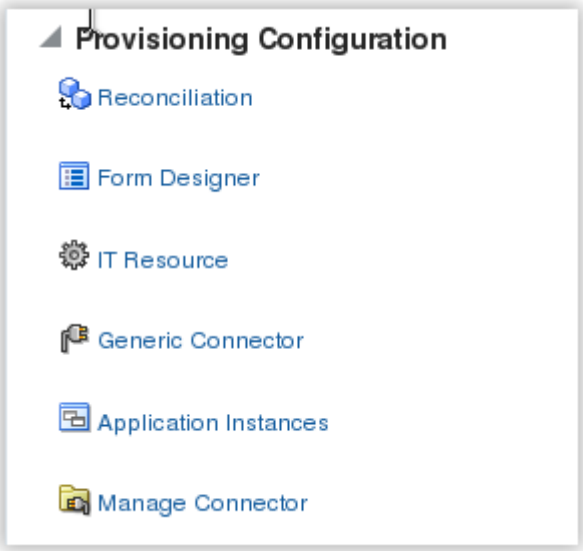

Ilustración 51 Conector LDAP OUD OIM 1

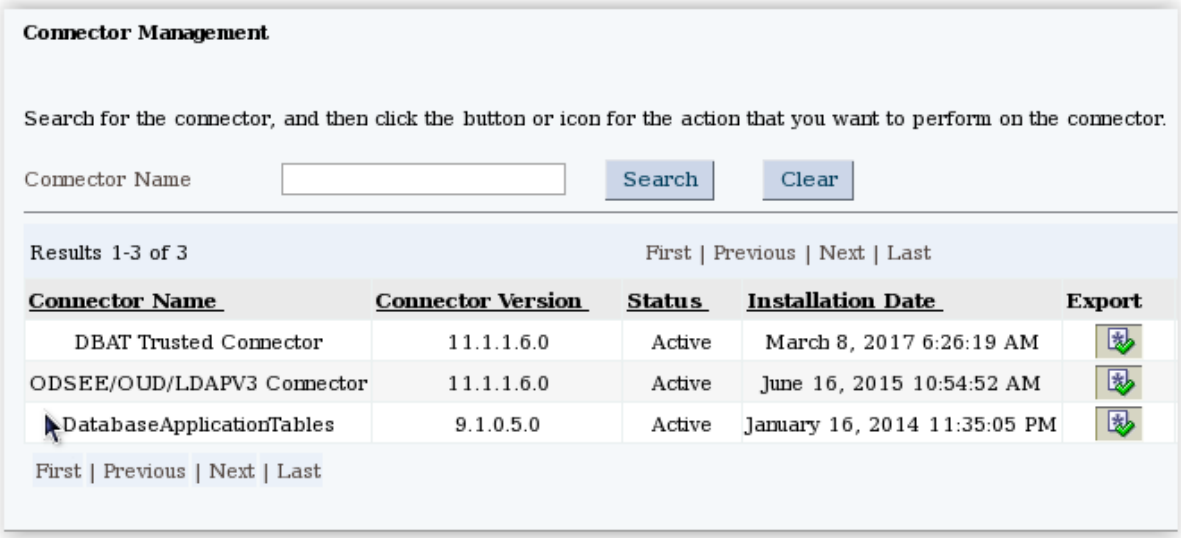

Ilustración 52 Conector LDAP OUD OIM 2

Se tiene que crear el IT Resource OUD, configurando la cadena de conexión con el LDAP.

Ilustración 53 Conector LDAP OUD OIM 3

Como se hizo anteriormente con el conector DBAT, se tendrá que crear los siguientes componentes en la consola de diseño.

Resource Object; en el cual se crean los atributos que tiene que tener el objeto LDAP

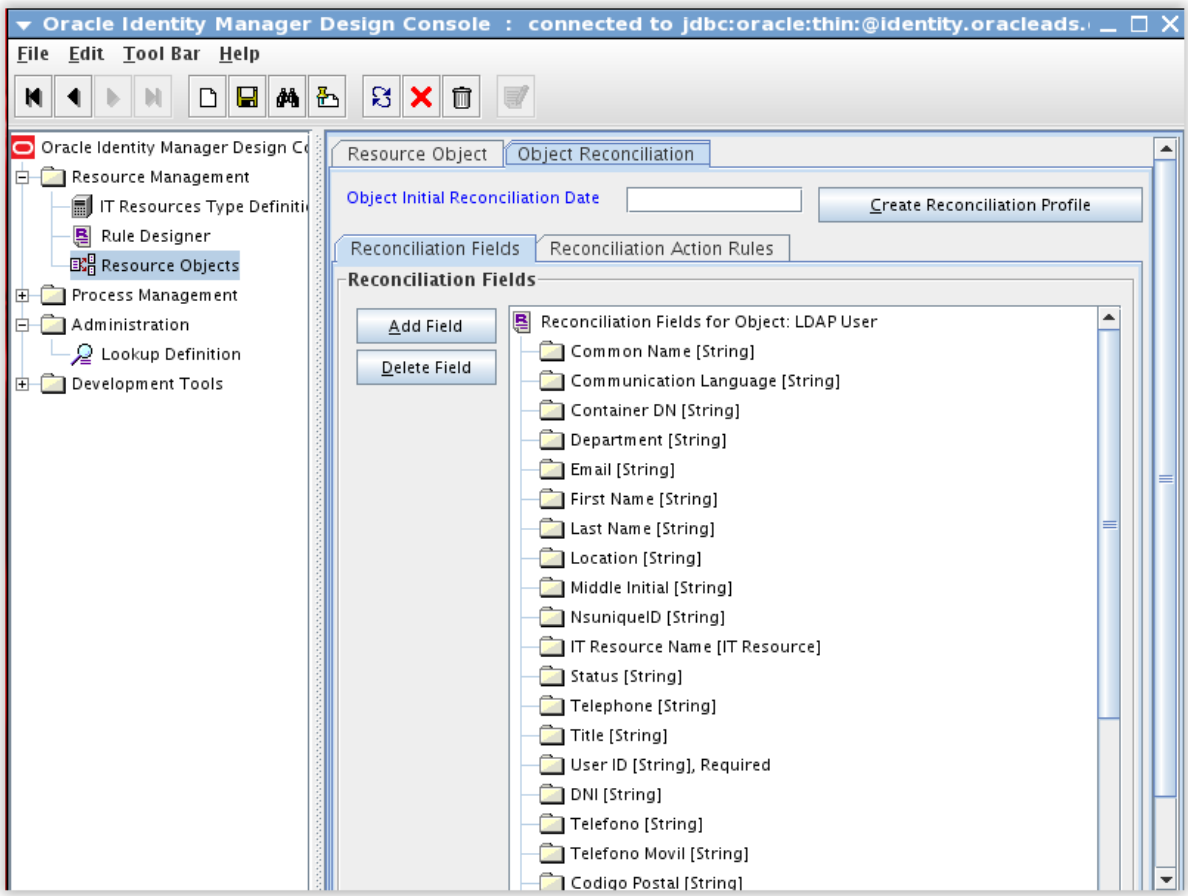

Ilustración 54 Conector LDAP OUD OIM 4

En el Process Definition se mapean los atributos del objeto LDAP con los campos del formulario.

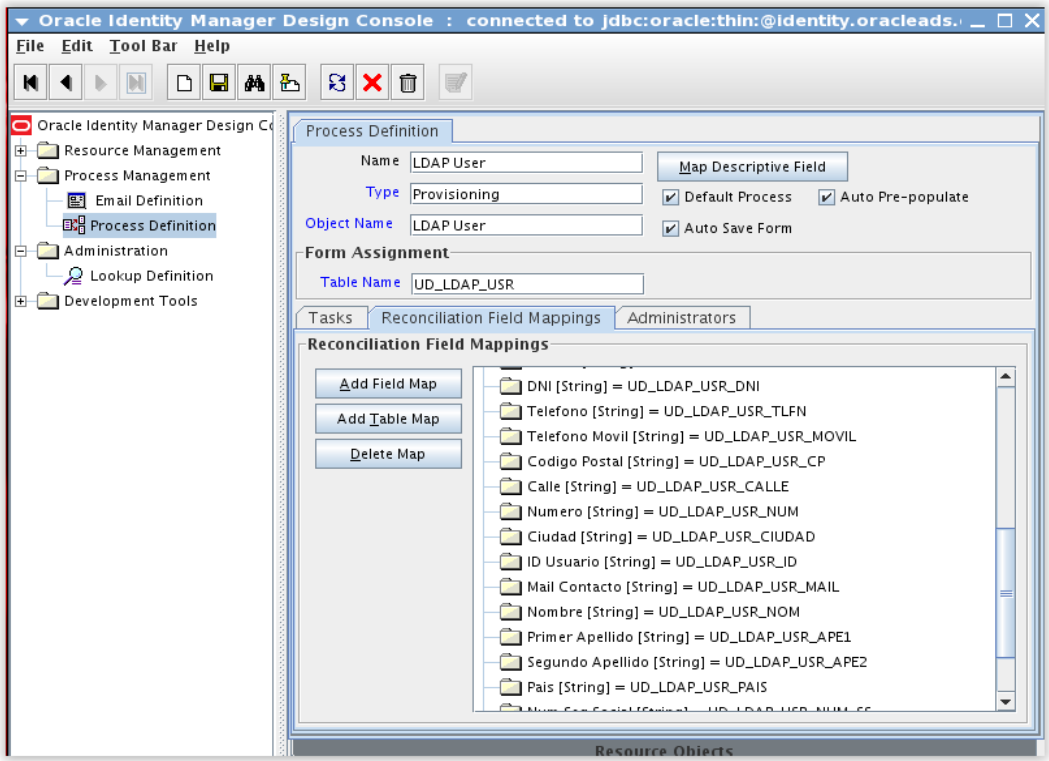

Ilustración 55 Conector LDAP OUD OIM 5

En la Lookup de Reconciliación se mapean los atributos de la identidad con los atributos del LDAP.

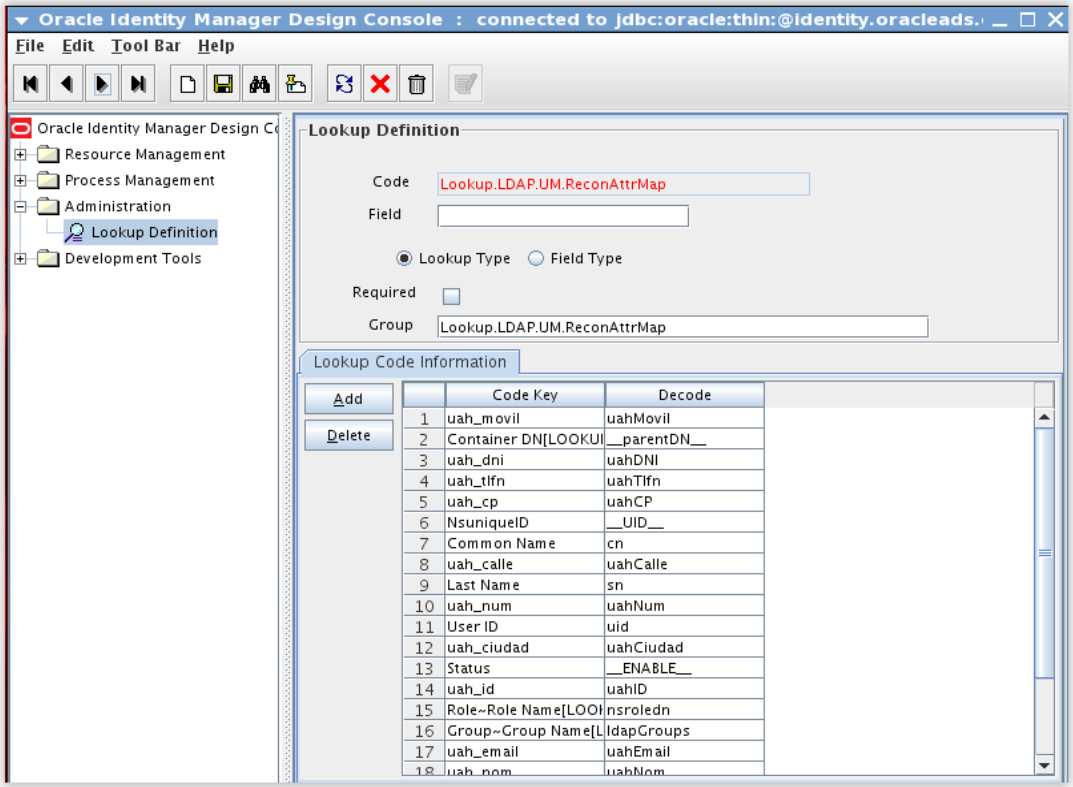

Ilustración 56 Conector LDAP OUD OIM 6

En el apartado formulario se añaden las columnas con los atributos que se quiere que tenga el LDAP.

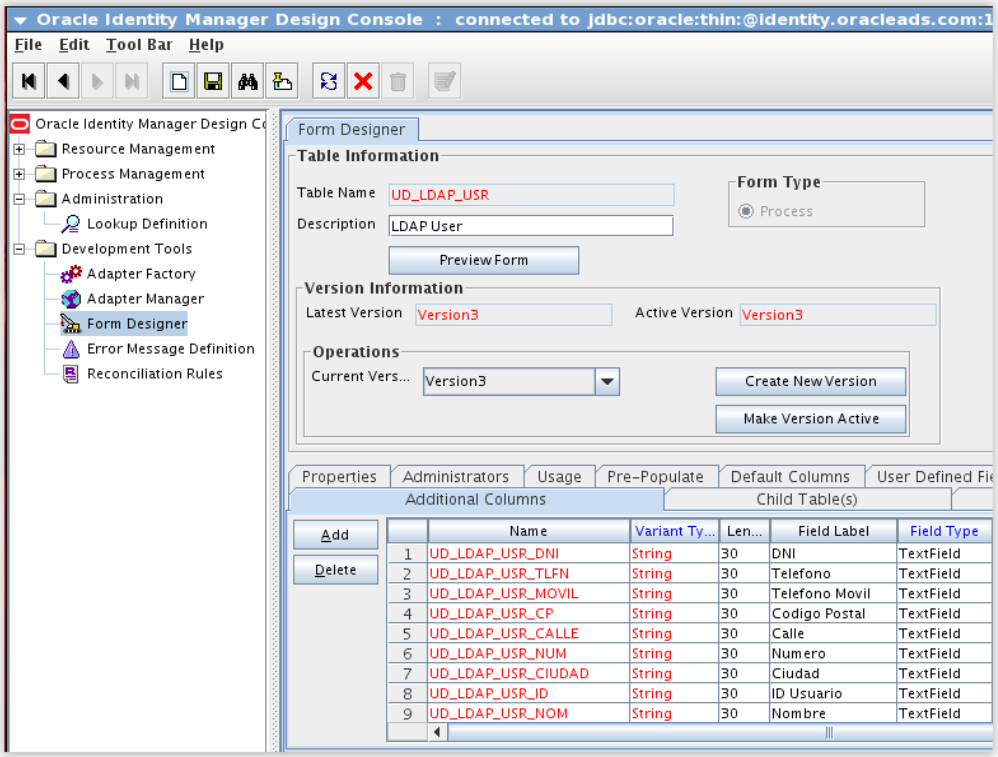

Ilustración 57 Conector LDAP OUD OIM 7

Posteriormente en el apartado Pre-Populate se mapea el atributo del objeto LDAP con los atributos de la identidad.

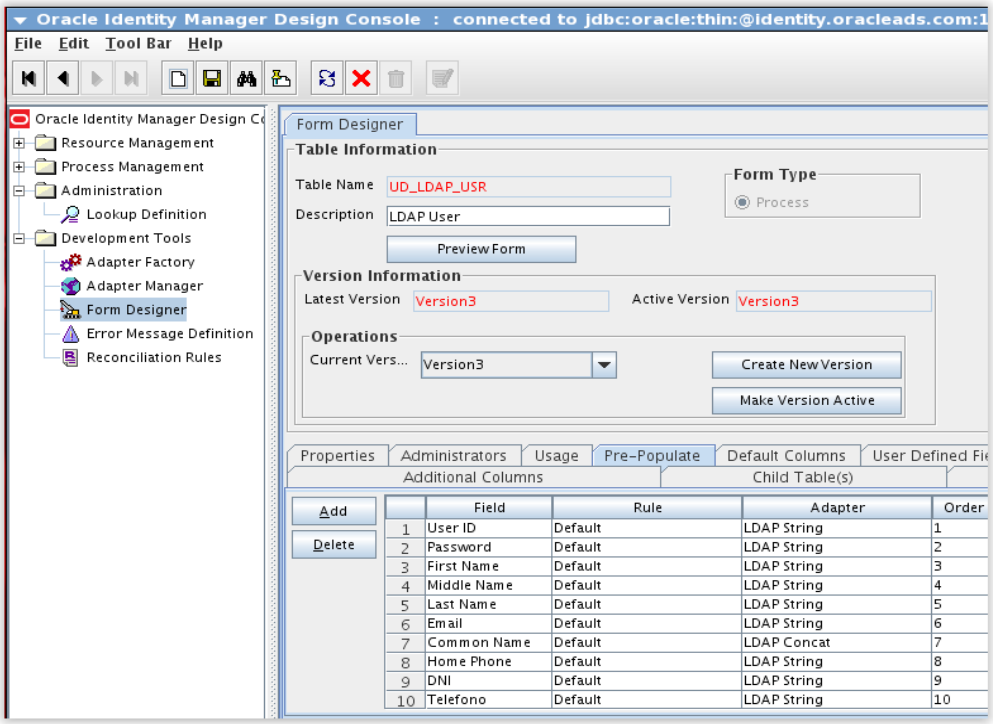

Ilustración 58 Conector LDAP OUD OIM 8

Se selecciona el atributo del objeto, con un adaptador String, y mapeado con la definición de usuario (atributo de la identidad)

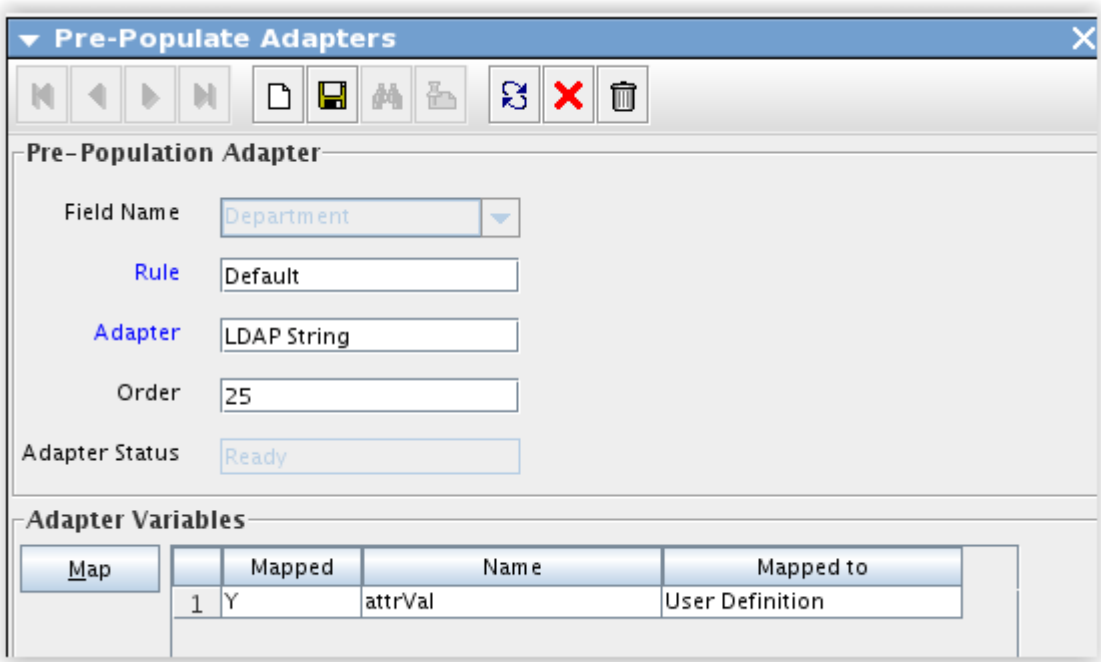

Ilustración 59 Conector LDAP OUD OIM 9

Para crear un Objeto uahPerson en el OUD, será necesario cargar el dichero 99UserLdif en el sistema. Este fichero consta de la declaración de los atributos, y finalmente la declaración del objeto con todos los atributos.

99UserLdif:

```
dn: cn=schema
objectClass: top
objectClass: ldapSubentry
objectClass: subschema
objectClass: uahPerson
cn: schema
modifiersName: cn=Directory Manager
attributeTypes: ( 1.2.3.4.5.6.15 NAME 'uahNom' DESC 'Nombre' EQUALITY caseIgnoreMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 X-ORIGIN 'user defined' )

ObjectClasses: ( 1.2.3.4.56789.1.0.200 NAME 'uahPerson' DESC 'Persona TFG' SUP inetOrgPerson STRUCTURAL MAY ( uahTlfn $ uahDNI $ uahMovil $ uahCP $ uahCalle $ uahNum $ uahCiudad $ uahID $ uahEmail $ uahNom $ uahApe1 $ uahApe2 $ uahPais $ uahNumSS $ uahTipoEmp ) X-ORIGIN 'user defined' )
```

9.5-RECONCILIACIÓN BBDD

Para lanzar la tarea de reconciliación entre la base de datos y el OIM se accede a la consola de Administración, y se accede a Scheduler (Programador)

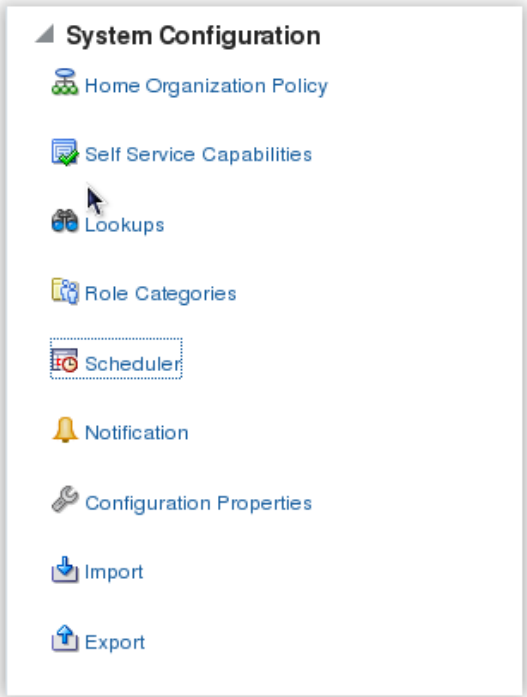

Ilustración 60 Reconciliación BBDD 1

Se busca la tarea DBAT Trusted Resource User Reconciliation.

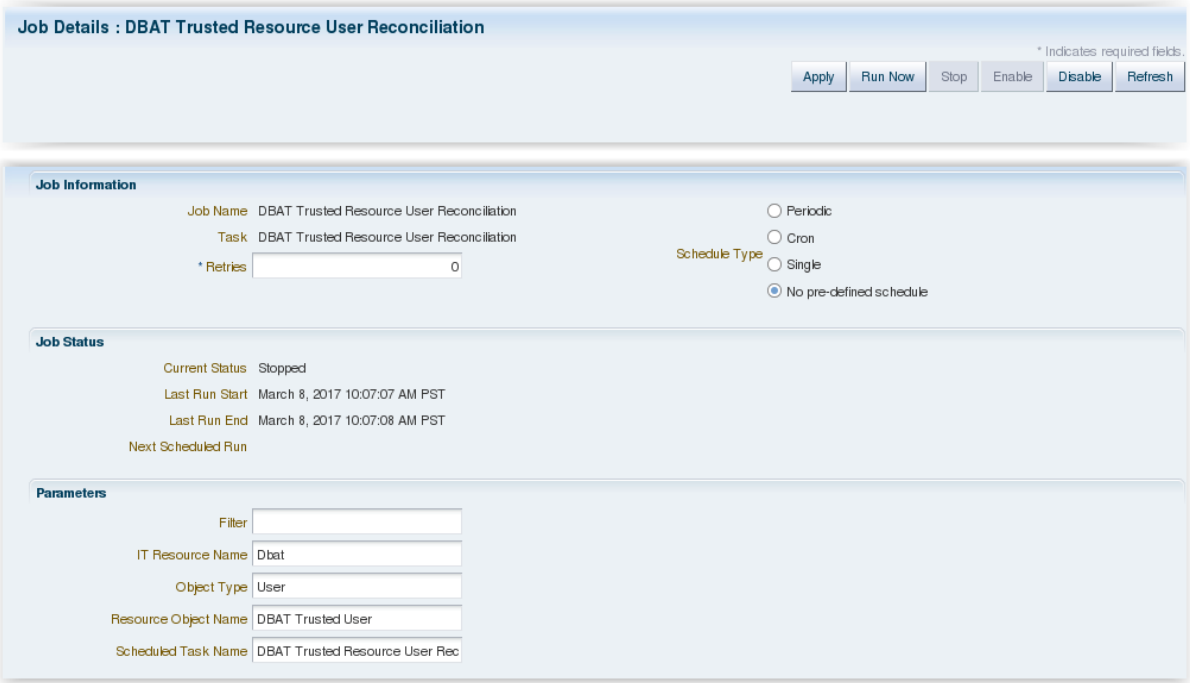

Ilustración 61 Reconciliación BBDD 2

Al ejecutar la tarea (Run Now) se ejecutará la tarea y la base de datos enviará los usuarios al OIM

9.6-Provisión de Cuentas

Para mandar los usuarios del OIM al LDAP (para su posterior intervención en el proceso de login con OAM) se accede a la consola de Servicios. Se pulsa en usuarios.

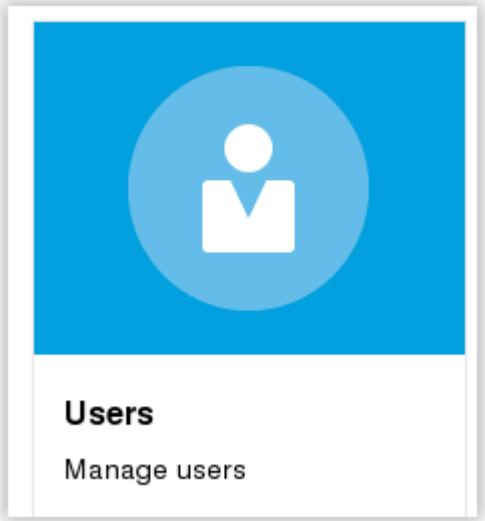

Ilustración 62 Provisión LDAP 1

Se busca un usuario al que se quiera solicitar una cuenta LDAP.

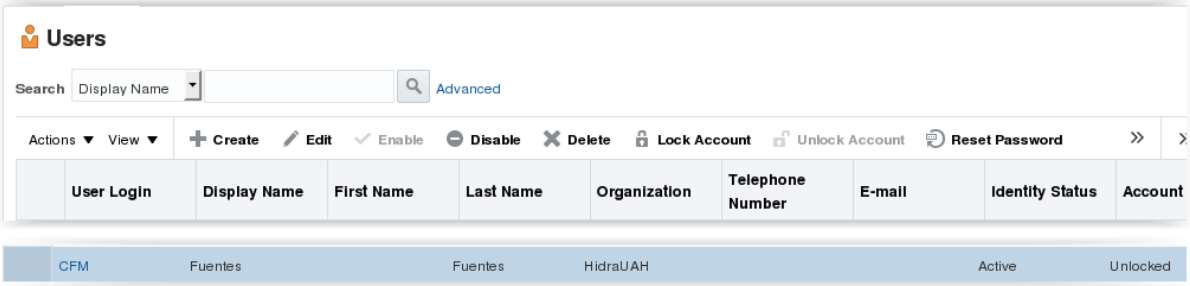

Ilustración 63 Provisión LDAP 2

Se accede al apartado Accounts.

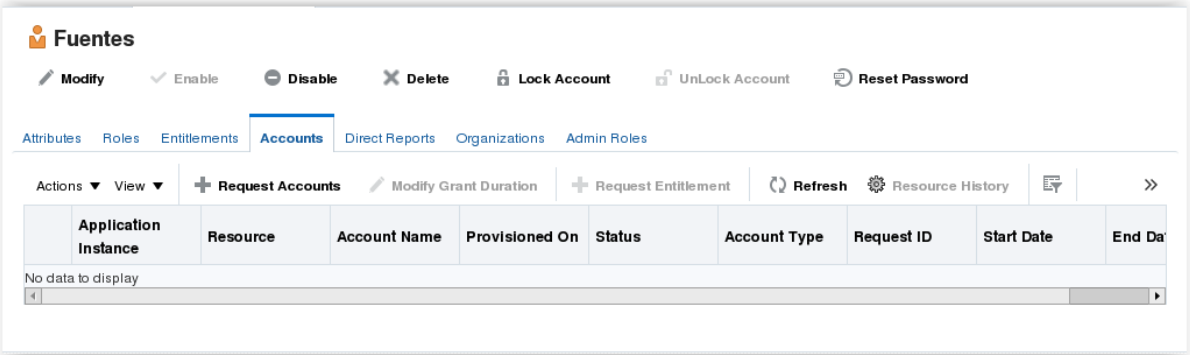

Ilustración 64 Provisión LDAP 3

Se pulsa en Add to Cart la cuenta Enterprise Directory OUD.

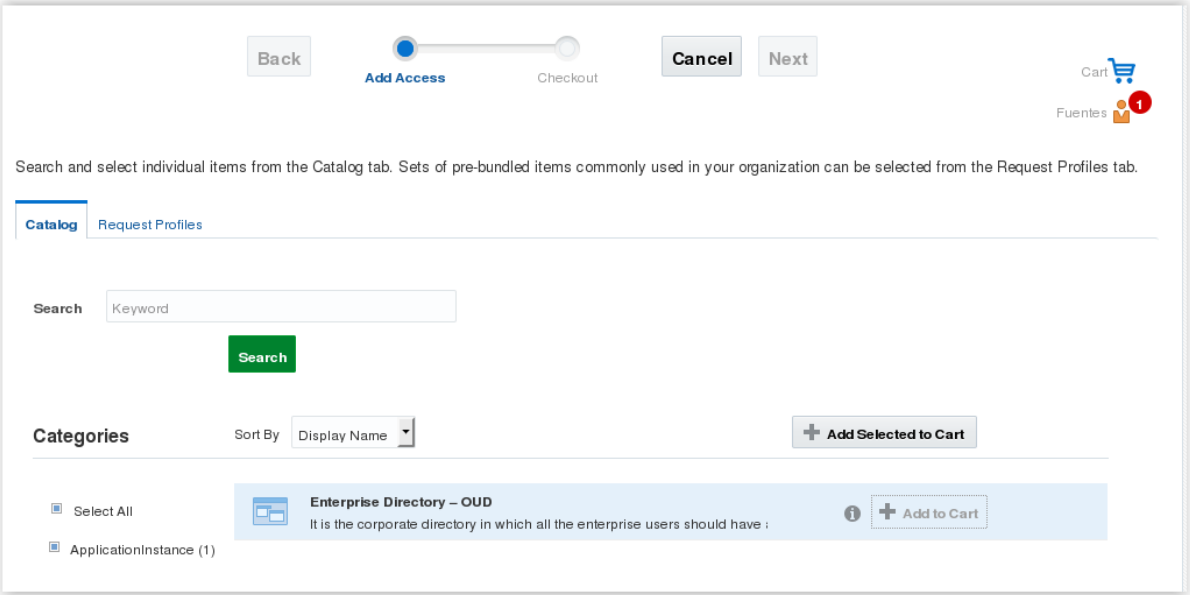

Ilustración 65 Provisión LDAP 4

En la siguiente ventana se pulsa en Update

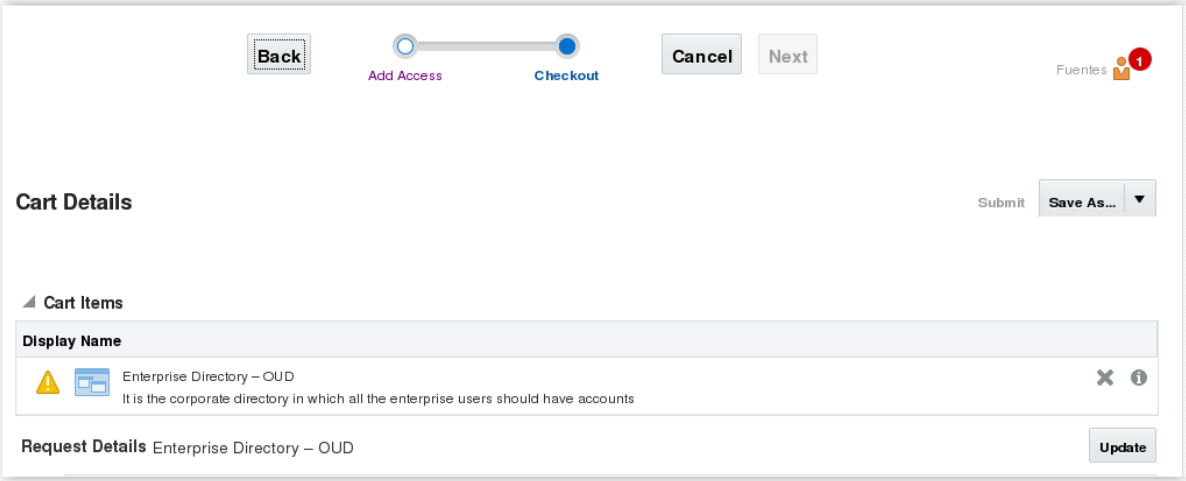

Ilustración 66 Provisión LDAP 5

Y para concluir se pulsa en Submit.

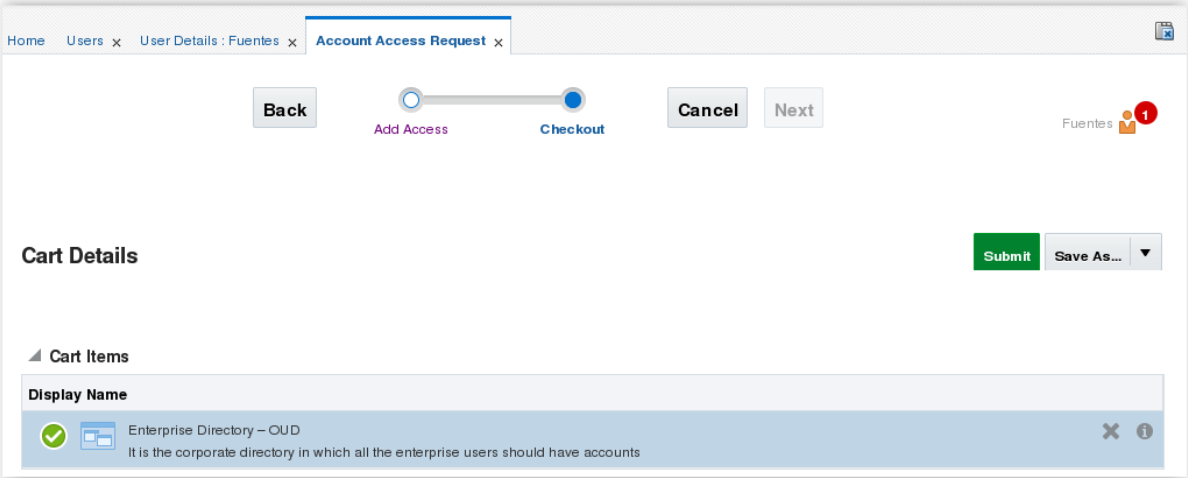

Ilustración 67 Provisión LDAP 6

Cuando el proceso termine de cargar, aparecerá el estado de la cuenta como provisionado y ya se tendrá ese usuario cargado el LDAP.

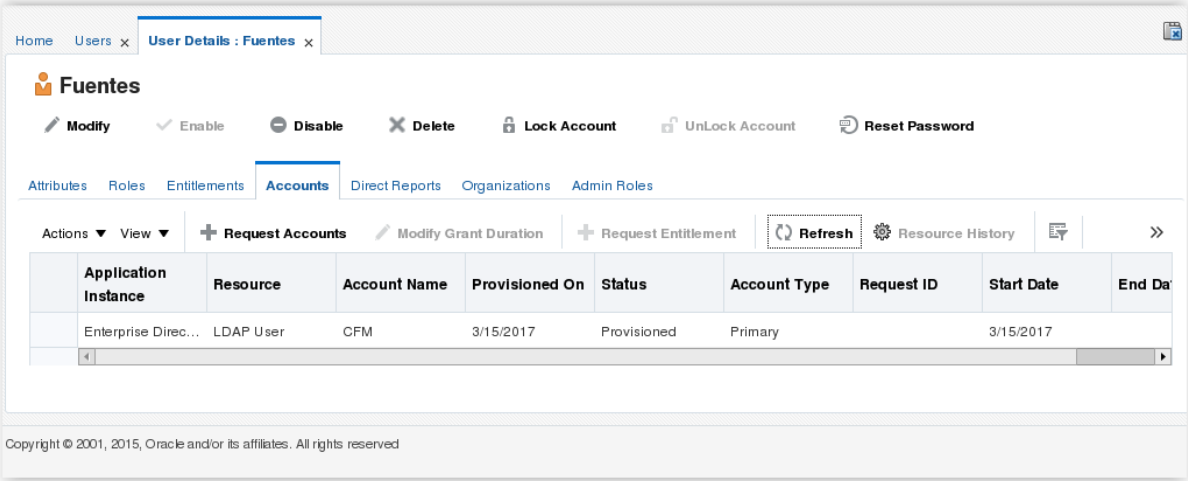

Ilustración 68 Provisión LDAP 7

9.7-CONFIGURACIÓN OAM

Se tiene que crear un almacén de identidades, para ello se pulsa en configuración, y en Almacenes de Identidades de Usuario. Aquí se creará un almacén de identidades con los datos de conexión del LDAP.

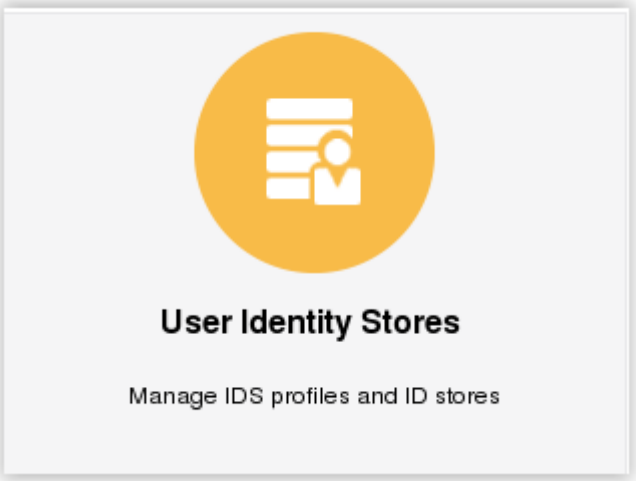

Ilustración 69 Configuración OAM 1

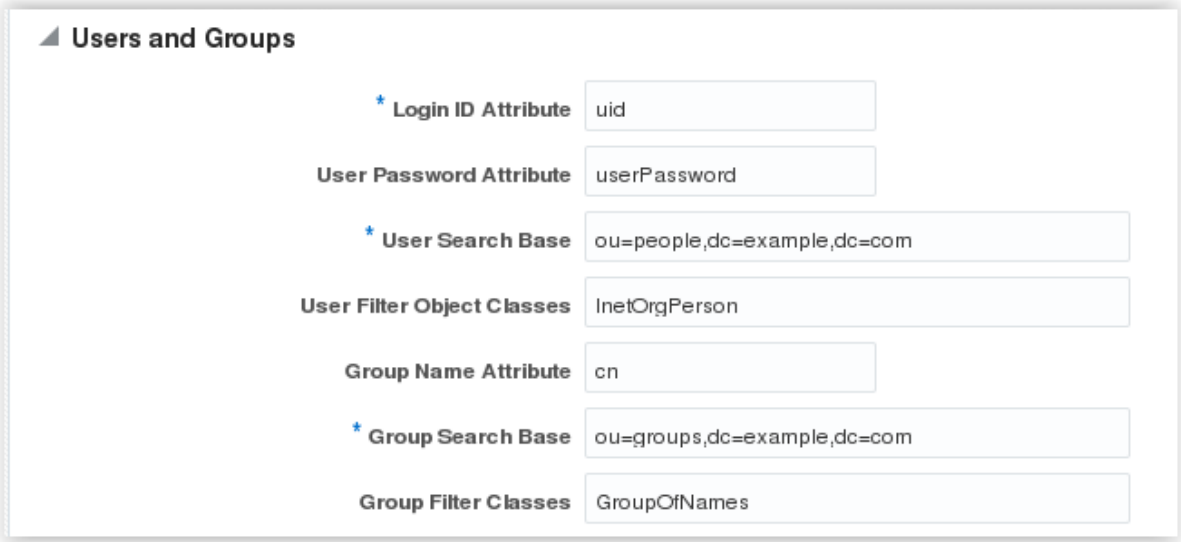

Ilustración 70 Configuración OAM 2

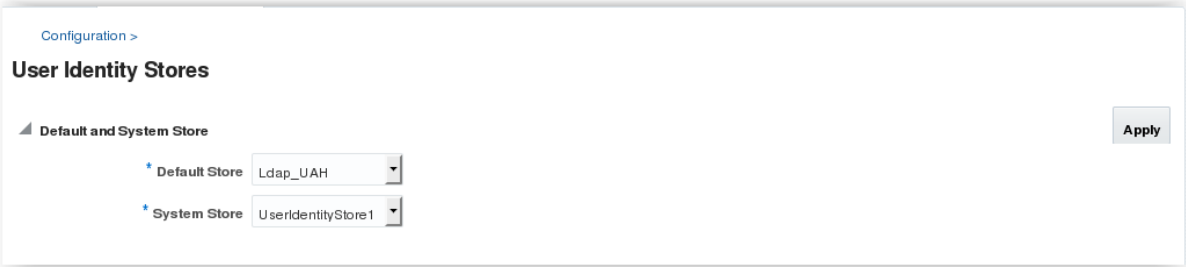

Ilustración 71 Configuración OAM 3

Crear un Módulo de autenticación LDAP, en el cual se selecciona como almacén de identidades el LDAP que se ha creado previamente.

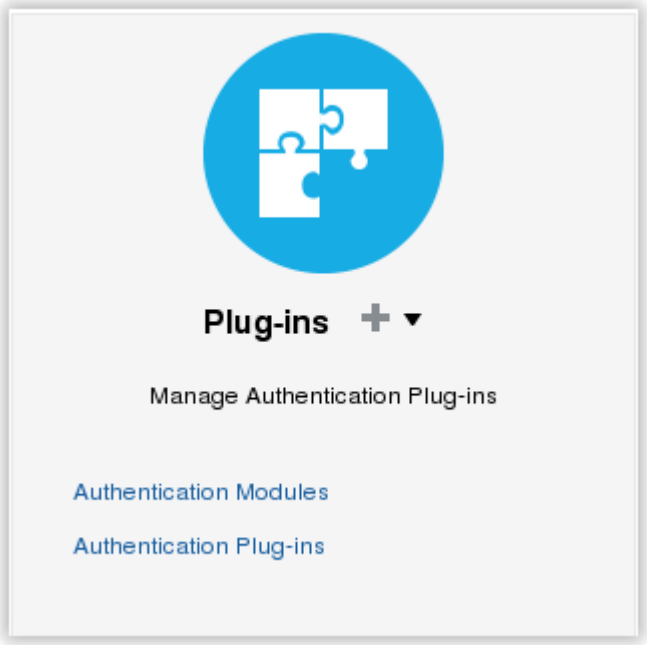

Ilustración 72 Configuración OAM 4

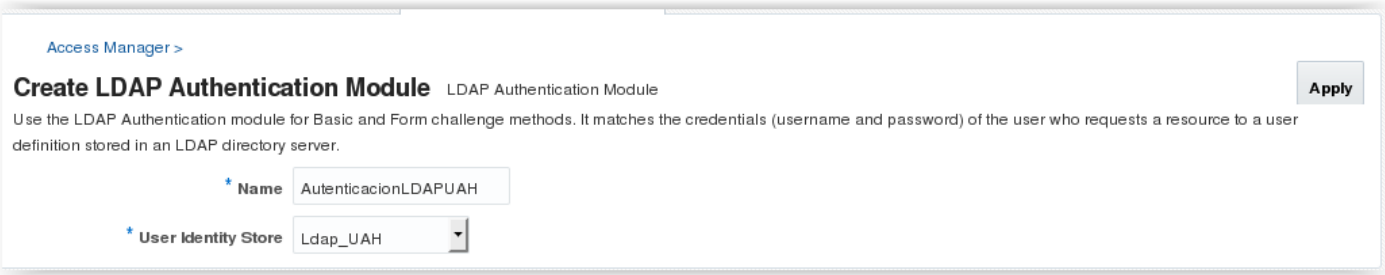

Ilustración 73 Configuración OAM 5

Se crea un esquema de autenticación, donde se selecciona con qué frontal se va a realizar el login.

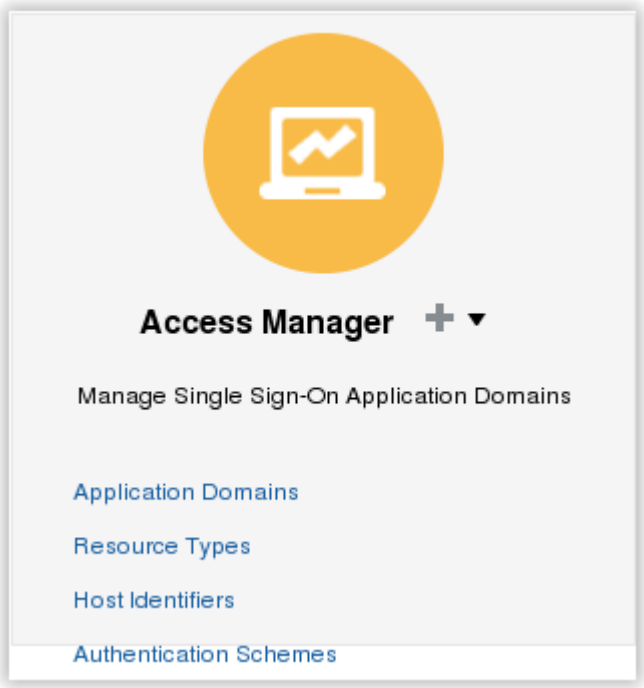

Ilustración 74 Configuración OAM 6

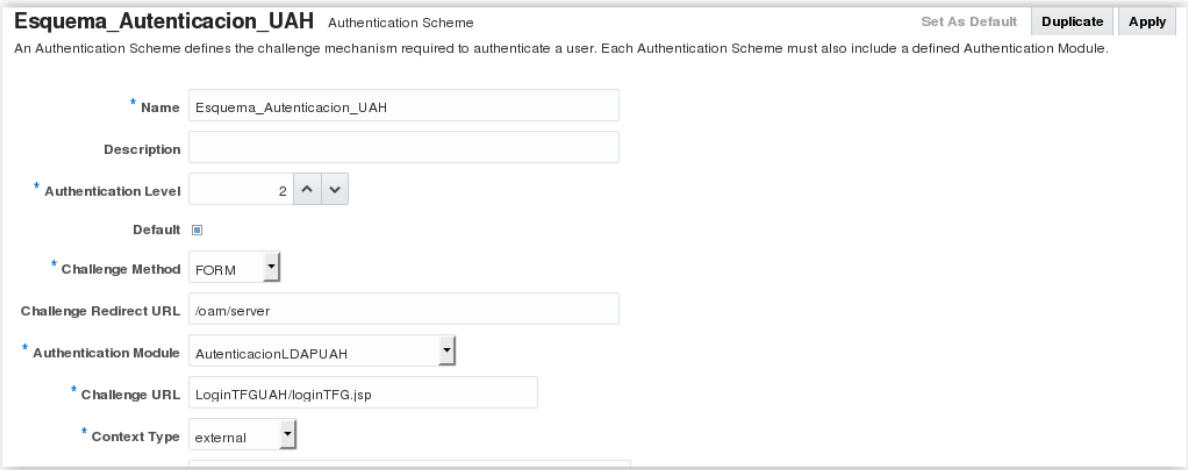

Ilustración 75 Configuración OAM 7

Se crea un dominio donde se configurarán los recursos a proteger y las políticas de autorización y autenticación

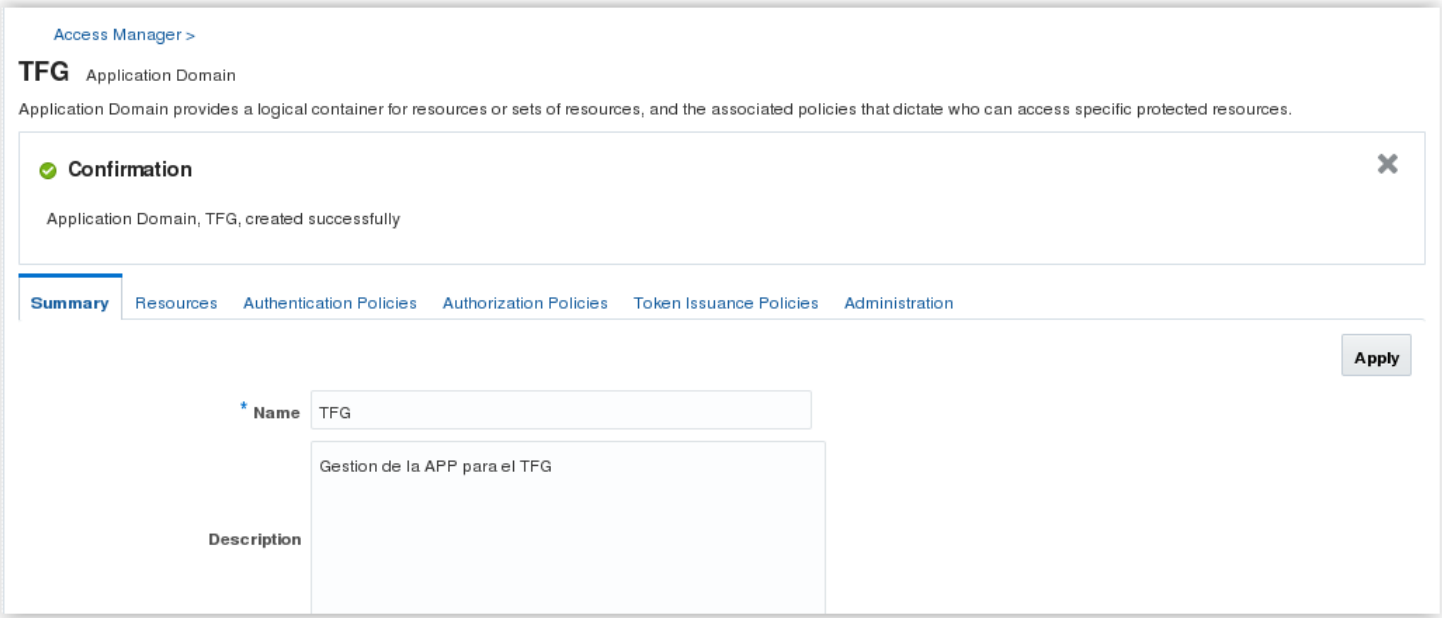

Ilustración 76 Configuración OAM 8

Crear Identificador de Host

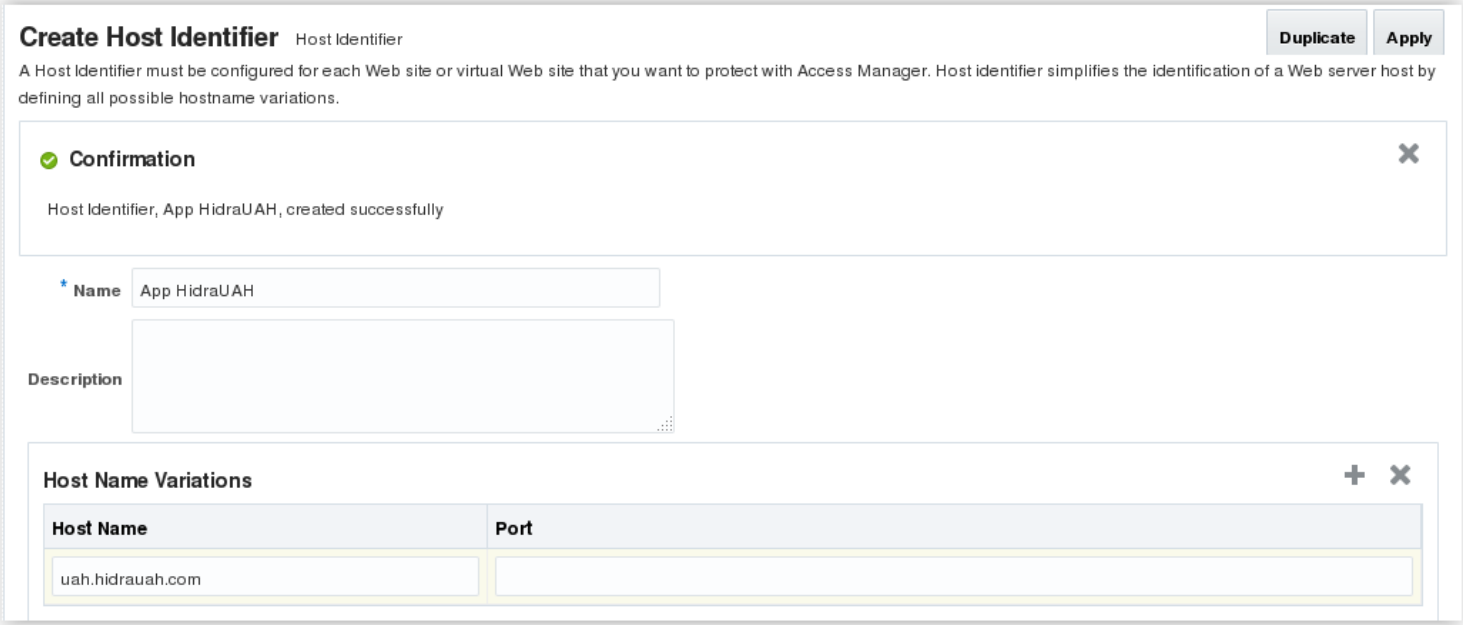

Ilustración 77 Configuración OAM 9

9.8-PROTEGER UN RECURSO:

Para proteger un recurso, lo primero que se debe hacer es crear una política de autenticación y una política de autorización. Para ello se accede al dominio de aplicación deseado, y se crea la política rellenando los siguientes campos:

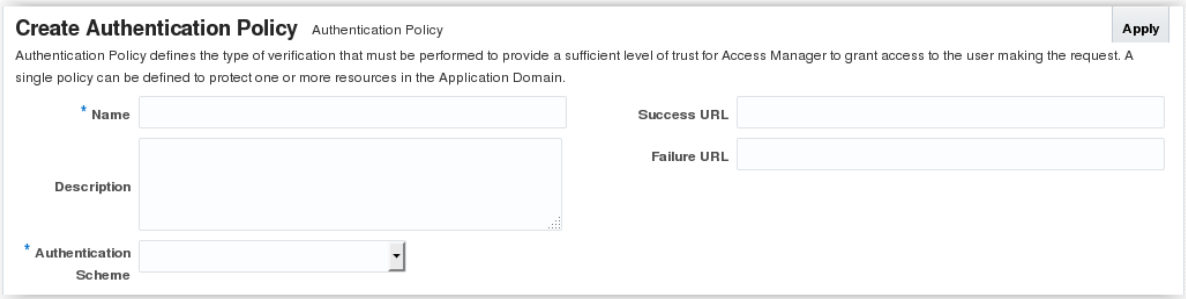

Ilustración 78 Protección de recursos 1

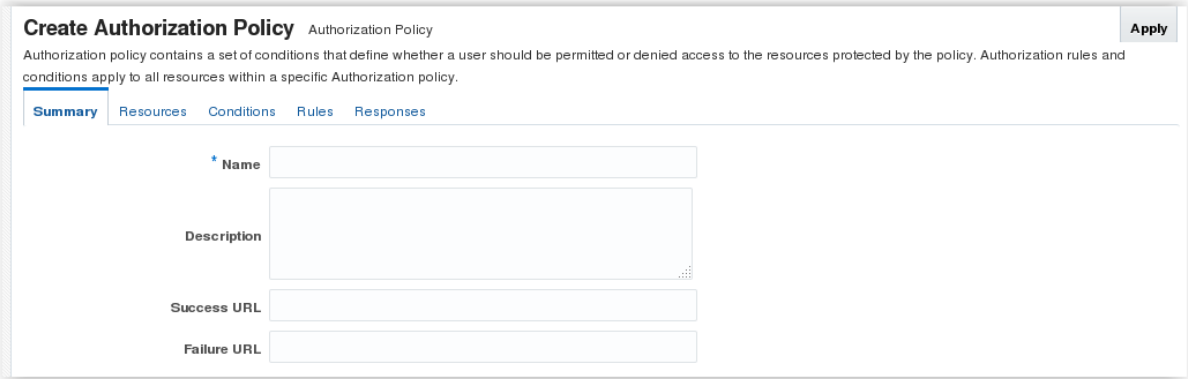

Ilustración 79 Protección de recursos 2

Para crear un recurso protegido se pulsa en recursos. Y cuando se vaya a crear aparecerán las siguientes opciones:

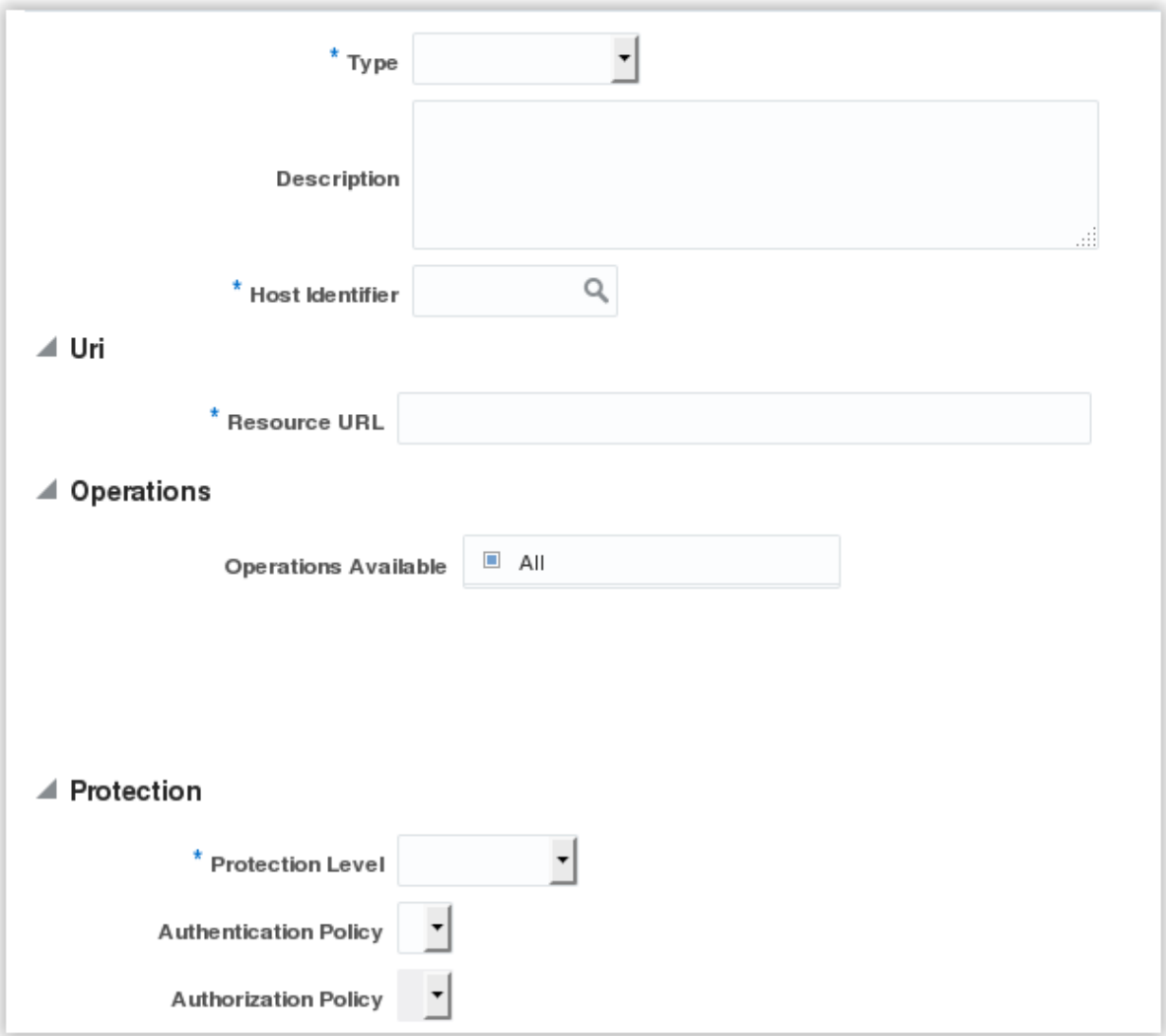

Ilustración Protección de recursos 3

9.9-DESPLIEGUE LOGIN

Para desplegar el login (y cualquier aplicación) se accede a la consola del Weblogic. Al apartado Deployments. Se pulsa en Install

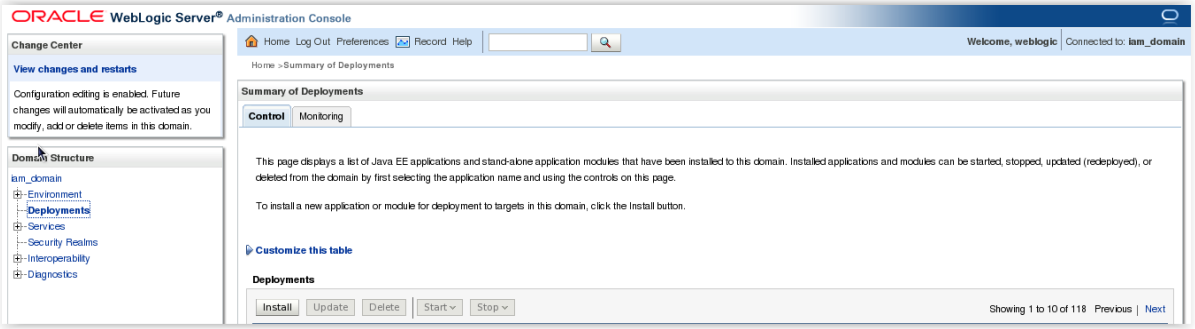

Ilustración 80 Despliegue aplicaciones 1

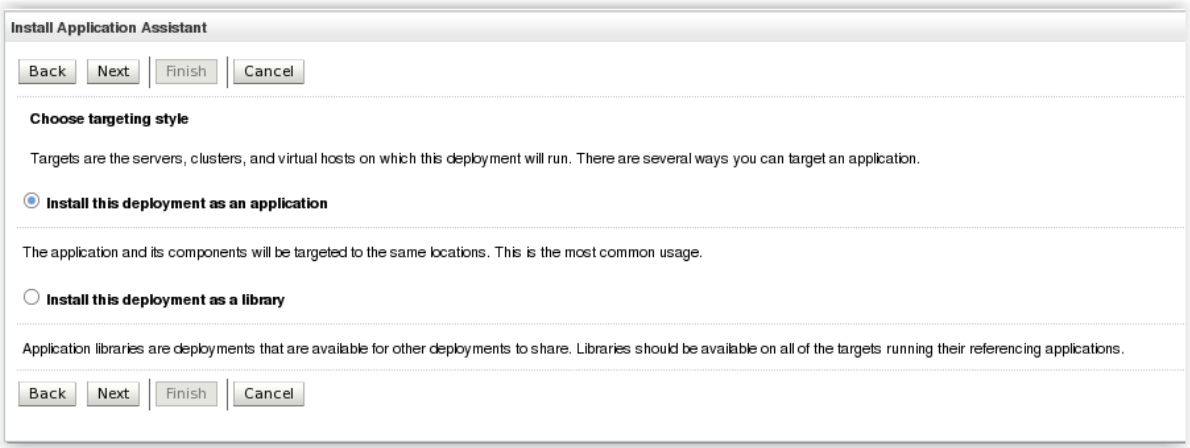

Ilustración 81 Despliegue aplicaciones 2

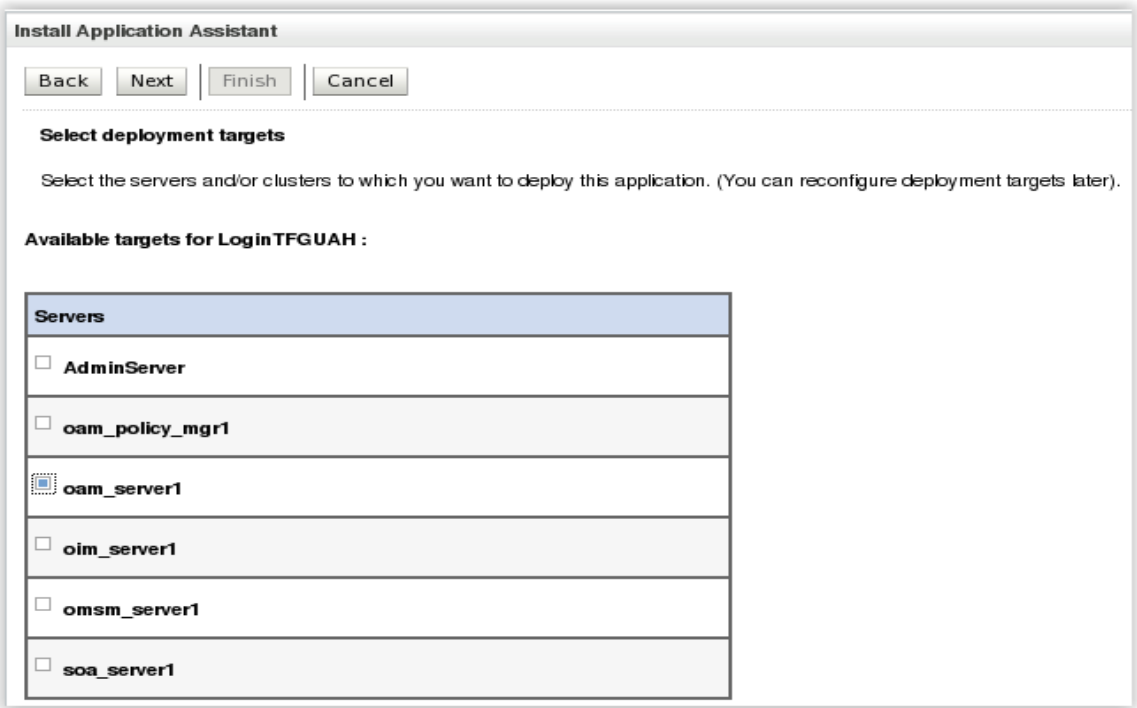

Ilustración 82 Despliegue aplicaciones 3

Ilustración 83 Despliegue aplicaciones 4

Ilustración 84 Despliegue aplicaciones 5

10. PRESUPUESTO DEL PROYECTO

La consultora CFMConsulting propone la tabla de perfiles con la tarifa de cada uno de ellos. Las horas estimadas para un mes de 21 días laborables supone un total de 69.510 €. Teniendo en cuenta que el proyecto tiene una duración de 6 meses, el coste total de los recursos asciende a 417.060€ (IVA incluido). La composición del equipo es una propuesta que puede ajustarse a las necesidades de HidraUAH en todo momento sobre la base de los perfiles tipo ofertados.

La facturación para el servicio se realizará de forma mensual. El periodo de pago se establece en 30 días desde la fecha de emisión de la factura.

Recursos	Experiencia requerida	Tarifa/Hora	Horas/dia	MES	Total
Jefe de Sistemas	5	68 €	4	5.712,00 €	34.272,00 €
Jefe de Proyecto	3	65 €	6	8.190,00 €	49.140,00 €
Jefe BBDD	6	58 €	8	9.744,00 €	58.464,00 €
Jefe Soporte Técnico	4	58 €	8	9.744,00 €	58.464,00 €
Jefe de Analisis y Programación	8	65 €	8	10.920,00 €	65.520,00 €
Programador Senior	5	50 €	8	8.400,00 €	50.400,00 €
Ingeniero de Pruebas	7	52 €	8	8.736,00 €	52.416,00 €
Programador Junior	3	48 €	8	8.064,00 €	48.384,00 €
				69.510,00 €	417.060,00 €

Ilustración 85 Presupuesto por Perfil

Los costes de licencias del producto Identity and Access Management será de 9.500€ (IVA incluido), respetando el número de 500 usuarios que nos indicó HidraUAH. Este precio incluye las licencias, un mes de soporte y la formación.

Licencias ORACLE	9.500 €
TOTAL	426.560,00 €

Ilustración 86 Presupuesto Licencias

Sumando el coste de los recursos y de licencias, el proyecto asciende a 426.560 €.

11. CONCLUSIONES Y TRABAJO FUTURO

Este trabajo de implantación de un sistema de gestión de identidades ha servido para aprender y desarrollar distintas capacidades. Lo primero; la capacidad de instalar y configurar un sistema operativo completamente desconocido para mí, al igual que las herramientas utilizadas. También he aprendido el funcionamiento de un sistema de gestión de identidades y lo que ello implica, con sus dos conceptos más importantes, Autorización y Autenticación. Este trabajo me ha brindado la oportunidad de aprender esta rama de la informática, la cual era totalmente desconocida previamente, y utilizarla en la actualidad en mi día a día.

El enfoque que tendría este trabajo en el futuro, sería la implementación de más herramientas a este sistema. Como por ejemplo:

-Oracle Adaptative Access Manager; este producto añade el segundo factor de autenticación a nuestro sistema. Es un producto que puede enviar tokens de autenticación vía sms o vía correo electrónico para un inicio de sesión OTP (One time pass) más seguro todavía.

-Oracle Business Intelligence; esta herramienta nos permite tomar decisiones eficientes y eficaces mediante los datos que genera nuestro negocio. Ofrece gráficas y análisis visuales junto con aplicaciones analíticas.

12. BIBLIOGRAFÍA.

http://www.gartner.com/technology/home.jsp

http://searchdatacenter.techtarget.com/es/definicion/IAM-o-Sistema-de-gestion-de-accesos-e-identidades

https://technet.microsoft.com/es-es/library/dn271885.aspx

https://www.microsoft.com/es-es/cloud-platform/identity-management

https://www.okta.com/resources/idaas-leader-gartner-magic-quadrant/

https://solutionsreview.com/identity-management/gartner-2016-magic-quadrant-iga/

http://www.oracle.com/us/technologies/linux/linux-for-oracle-database-wp-2068570.pdf

http://searchdatacenter.techtarget.com/tip/Choosing-the-best-server-OS-Linux-vs-Windows-comparisons

https://www.itcentralstation.com/products/comparisons/oracle-linux_vs_windows-server

http://soequipo1.blogspot.com.es/2014/11/ventajas-y-desventajas_26.html

http://oraclebddepn.blogspot.com.es/2013/05/ventajas-y-desventajas.html

http://www.ehowenespanol.com/lista-ventajas-inconvenientes-oracle-database-11g-info_201876/

http://www.oracle.com/technetwork/es/database/enterprise-edition/documentation/caracteristicas-oracle-database-11g-1704852-esa.pdf

http://dbaoracle4hire.blogspot.com.es/2013/11/principales-caracteristicas-de-la-base.html
https://es.wikipedia.org/wiki/Oracle_Database

https://basededatosunounivia.wordpress.com/2015/03/13/oracle-vs-mysql-vs-sql-server-una-comparacion-entre-los-sistemas-gestores-de-bases-de-datos-relacionales-mas-populares/

Universidad de Alcalá
Escuela Politécnica Superior

ESCUELA POLITECNICA
SUPERIOR

Universidad
de Alcalá