Universitat Autònoma de Barcelona

Escola Tècnica Superior d'Enginyeria

ENGINYERIA INFORMÀTICA

1131 – Disseny i implantació d'un directori d'empleats i sistema de login únic

Memòria del Projecte Fi de Carrera d'Enginyeria en Informàtica realitzat per

Roger Sen Montero

i dirigit per

Joan Sorribes

Bellaterra, 10 de Septembre de 2008

Universitat Autònoma de Barcelona

Escola Tècnica Superior d'Enginyeria

El sotasignat, Joan Sorribes

Professor/a de l'Escola Tècnica Superior d'Enginyeria de la UAB

CERTIFICA:

Que el treball a què correspon aquesta memòria ha estat realitzat sota la seva direcció per Roger Sen Montero.

I per tal que consti firma la present.

Signat: Joan Sorribes

Bellaterra, 10 de Septembre de 2008

1 ÍNDICE

2 ÍNDICE DE FIGURAS

3 ÍNDICE DE TABLAS

4 INTRODUCCIÓN

La presente memoria recoge el proyecto de final de carrera de Roger Sen Montero.

Dicha memoria documenta un proyecto real en el que ha trabajado el autor de esta memoria.

4.1 ORGANIZACIÓN DE LA MEMORIA

A continuación se detalla la forma en la que se ha estructurado la memoria del proyecto de movilidad:

Este capítulo (4 INTRODUCCIÓN) tiene como objetivo poner en situación sobre lo que se va a leer. Esto se consigue, tanto con este mismo punto explicando la organización de la memoria, como explicando los objetivos y alcance del proyecto. Finalmente se introduce al lector los conceptos básicos para la comprensión de la memoria como son los relativos al software que se va a usar (Directorio Corporativo como concepto de negocio, LDAP como tecnología de directorio y protocolo y OpenLDAP como producto e implementación del protocolo anterior).

En el capítulo número 5 (ESTUDIO DE VIABILIDAD) se realiza un estudio de viabilidad que demuestra que puede ser llevado a cabo con los recursos dispuestos en el momento de su realización.

En el capítulo 6 (METODOLOGÍA) se explica la metodología usada para el desarrollo e implantación del Proyecto en cada fase.

En el capítulo 7 (REALIZACIÓN DEL PROYECTO) se documenta la realización efectiva del proyecto pasando por las fases necesarias para su ejecución, las cuales han sido definidas en el punto anterior.

En el capítulo 8 (RESULTADOS)se detallan los resultados obtenidos después de la implantación de la solución de movilidad. Es decir, los resultados del proyecto.

El capítulo 9 (CONCLUSIONES) se utiliza para extraer conclusiones posteriores a la realización del proyecto así como hacer un repaso a los problemas encontrados, su solución y a las mejoras futuras del Directorio Corporativo

4.2 OBJETIVOS Y ALCANCE DEL PROYECTO

El objetivo de este proyecto es implantar una solución de directorio de empleados que unifique toda la información de empleados, usuarios, grupos y controles de acceso a aplicaciones de una multinacional farmacéutica.

La necesidad de desplegar un nuevo Porta Corporativo para los empleados de la empresa farmacéutica ha hecho necesario unificar la información de los datos de empleados en un solo repositorio (El directorio de empleados) de forma que el portal de empleados pueda acceder a los mismos a través del protocolo estándar LDAP.

Por esta razón se decide realizar un proyecto basado en cuatro grandes tareas:

- Certificación del software de directorio de empleados (OpenLDAP) como solución técnicamente compatible con el portal de empleados Vignette Portal

  El fabricante del Portal Corporativo (Vignette Portal) no certifica la integración del mismo con el directorio de empleados seleccionado (OpenLDAP). Por esta razón se realizará el proceso de certificación con el fin de asegurar que ambos productos se integran a la perfección.

- Identificación de los atributos necesarios para añadir al esquema de datos del Directorio Coporativo

  Con el fin de personalizar los datos accesibles por el portal de empledos al Directorio Corporativo de empleados, se identificará que datos son útiles para los usuarios en diferentes áreas de la empresa (Finanzas, Ventas, RR.HH., Investigación, Compras…). Estos datos se añadirán al esquema estándar del directorio con el fin de que el portal pueda acceder a ellos respetando su estructura e integridad.

- Identificación de las fuentes maestras de los datos para cargarlos en el Directorio.

  Siguiendo un proceso similar al del punto anterior, se identificarán las fuentes de datos maestras de donde extraerlos y que procesos de transformación y normalización serán necesarios para cargarlos en el directorio de empleados.

- Desarrollo de un proceso de extracción y carga de datos en LDAP.

  A partir del análisis generado por los dos puntos anteriores (identificación de atributos y sus fuentes) se desarrollará un programa que en modo batch realizará las cargas de datos de las fuentes maestras de la empresa al directorio de empleados.

4.3 ¿QUÉ ES UN DIRECTORIO CORPORATIVO?

Un Directorio Corporativo es un servicio que permite la fácil localización de información sobre las personas de una organización.

4.3.1 ¿Qué es un directorio?

Un directorio es una base de datos, pero en general contiene información más descriptiva y más basada en atributos.

La información contenida en un directorio normalmente se lee mucho más de lo que se escribe. Como consecuencia los directorios no implementan normalmente los complicados esquemas para transacciones o esquemas de reducción que las bases de datos utilizan para llevar a cabo actualizaciones complejas de grandes volúmenes de datos. Las actualizaciones en un directorio son usualmente cambios sencillos de todo o nada.

Los directorios están diseñados para proporcionar una respuesta rápida a operaciones de búsqueda o consulta.

Pueden tener capacidad de replicar información de forma amplia, con el fin de aumentar la disponibilidad y fiabilidad, y a la vez reducir tiempo de respuesta. Cuando se duplica la información de un directorio, pueden aceptarse inconsistencias temporales entre la información que hay en las réplicas, siempre que finalmente exista una sincronización.

Hay muchas formas de proporcionar un servicio de directorio. Los diferentes métodos permiten almacenar en el directorio diferentes tipos de información, establecer requisitos diferentes para hacer referencias a la información, consultarla y actualizarla, la forma en que protege al directorio de accesos no autorizados. Algunos servicios de directorios son locales, proporcionando servicios a un contexto restringido. Otros servicios son globales, proporcionando servicio en un contexto mucho más amplio.

4.3.2 ¿Cómo se usa en una organización (corporación)?

El servicio de directorio es un lugar donde se centraliza determinada información sobre las personas de una organización. Sus principales características son:

- Es utilizado como método unificado para la autentificación ante los servicios del usuario mediante la utilización de un único nombre de usuario y contraseña.
- Además de la información sobre las personas almacena datos adicionales sobre las cuentas de correo electrónico de los usuarios e información sobre las listas de distribución.
- La mayor parte de los datos del directorio proceden de sistemas de información corporativos que actualizan éste con la suficiente frecuencia como para mantenerlo constantemente actualizado.
- Las conexiones al servicio de directorio se realizan de forma encriptada, para lo que se requiere la utilización del correspondiente certificado de seguridad.
- Puede ser accedido desde otras aplicaciones, como por ejemplo en las agendas de direcciones de los lectores de correo electrónico o aplicaciones existentes en el ecosistema corporativo que usarán el Directorio de Datos como backend de datos no relacional.

El directorio corporativo recoge la información de todos los posibles usuarios de servicios de la empresa. Esto incluye, además de los empleados, a los clientes y proveedores.

El conjunto de datos que presenta depende del colectivo al que pertenece la persona, pero nunca se presenta información personal, sólo la relacionada con su trabajo.

Además de la información pública indicada, en el Directorio corporativo se encuentra debidamente protegidos la información de cuenta (usuario y clave) de los empleados. Esto permite la implementación de la autenticación única.

El uso de este sistema de autenticación única permite evitar tener que recordar múltiples usuarios y clave para acceder a cada uno de los servicios de la empresa.

La utilización de una clave única permite que múltiples aplicaciones informáticas autentifiquen a los usuarios con la clave almacenada en el Directorio Corporativo, externalizando la función de autenticación a un sistema especializado.

La autenticación única busca unificar el acceso a todos esos servicios con un único usuario y clave. El camino por el que nos lleva esta filosofía es la de identificar a la persona y ofrecer los servicios a cada persona por su relación con la organización en lugar de por el conocimiento de una clave de acceso.

4.4 ¿QUÉ ES UN LDAP?

LDAP ("Lightweight Directory Acces Protocol", en español Protocolo Ligero de Acceso a Directorios) es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio.

Se usó inicialmente como un Front-end o interfaz final para x.500, pero también puede usarse con servidores de directorio únicos y con otros tipos de servidores de directorio.

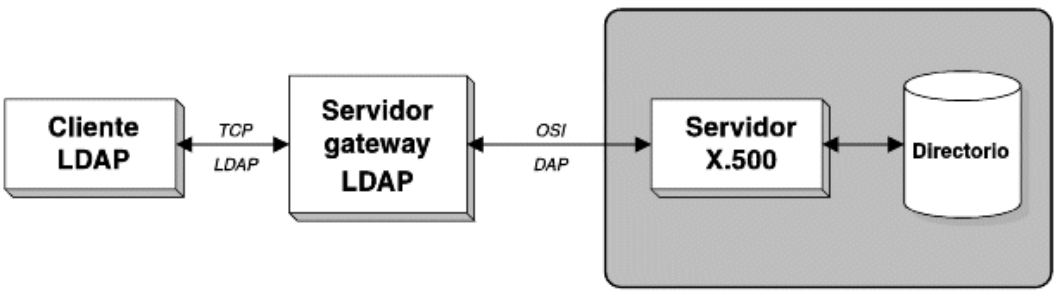

Ilustración a - LDAP como front-end de x.500

LDAP aparece con el estándar de los directorios de servicios. La versión original fue desarrollada por la Universidad de Michigan. La primera versión no llego a usarse y fue en 1995 cuando se publicaron los RFC (Request For Comments) de la versión LDAPv2. Los RFC para la versión LDAPv3 fueron publicados en 1997. La versión 3 incluía características como las listas de acceso (control access lists) y replicación de directorios.

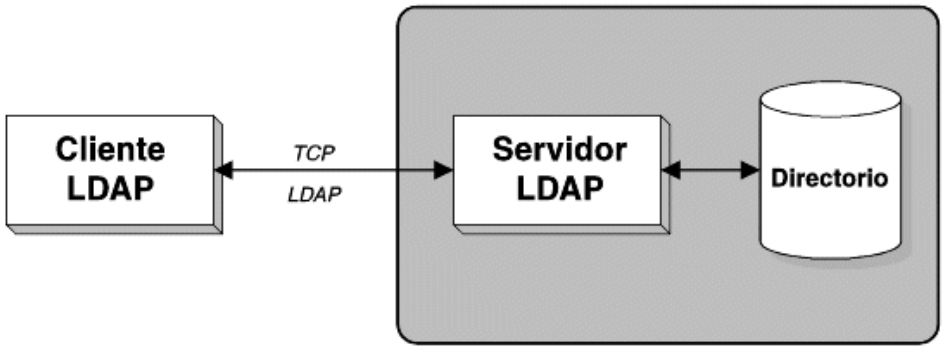

Ilustración b - LDAP como software dedicado

4.4.1 ¿Es un directorio LDAP una base de datos?

El sistema gestor de una base de datos (Database Management System ó DBMS) de Sybase, Oracle, Informix ó Microsoft es usado para procesar peticiones (queries) ó actualizaciones a una base de datos relacional. Estas bases de datos pueden recibir cientos o miles de órdenes de inserción, modificación o borrado por segundo.

Un servidor LDAP es usado para procesar peticiones (queries) a un directorio LDAP. Pero LDAP procesa las órdenes de borrado y actualización de forma mucho más lenta que le lectura.

En otras palabras, LDAP es un tipo de base de datos, pero no es una base de datos relacional. No está diseñada para procesar cientos o miles de cambios por minuto como los sistemas relacionales, sino para realizar lecturas de datos de forma muy eficiente.

4.4.2 Funcionamiento de LDAP

El servicio de directorio LDAP se basa en un modelo cliente-servidor.

Uno o más servidores LDAP contienen los datos que conforman el árbol de directorio LDAP o base de datos troncal, el cliente LDAP se conecta con el servidor LDAP y le hace una consulta. El servidor contesta con la respuesta

correspondiente, o bien con una indicación de donde puede el cliente hallar más información. No importa con que servidor LDAP se conecte el cliente ya que siempre observará la misma vista del directorio; el nombre que se le presenta a un servidor LDAP hace referencia a la misma entrada a la que haría referencia en otro servidor LDAP.

Un directorio LDAP destaca sobre los demás tipos de bases de datos por las siguientes características:

- Es muy rápido en la lectura de datos
- Permite replicar el servidor de forma muy sencilla y económica
- Muchas aplicaciones de todo tipo tienen interfaces de conexión a LDAP y se pueden integrar fácilmente
- Dispone de un modelo de nombres globales que asegura que todas las entradas son únicas
- Usa un sistema jerárquico de almacenamiento de información.
- Permite múltiples directorios independientes
- Funciona sobre TCP/IP y SSL
- La mayoría de aplicaciones disponen de soporte para LDAP
- La mayoría de servidores LDAP son fáciles de instalar, mantener y optimizar.

Dadas las características de LDAP sus usos más comunes son:

- Directorios de información. Por ejemplo bases de datos de empleados organizados por departamentos (siguiendo la estructura organizativa de la empresa) ó cualquier tipo de páginas amarillas.
- Sistemas de autenticación/autorización centralizada. Grandes sistemas donde se guarda gran cantidad de registros y se requiere un uso constante de los mismos.

Por ejemplo:

- Gestionar todas las cuentas de acceso a una red corporativa y mantener centralizada la gestión del acceso a los recursos.

- Sistemas de autenticación para páginas Web, algunos de los gestores de contenidos más conocidos disponen de sistemas de autenticación a través de LDAP.
- Sistemas de control de entradas a edificios, oficinas…
- Sistemas de correo electrónico. Grandes sistemas formados por más de un servidor que accedan a un repositorio de datos común.
- Sistemas de alojamiento de páginas web y FTP, con el repositorio de datos de usuario compartido.
- Grandes sistemas de autenticación basados en RADIUS, para el control de accesos de los usuarios a una red de conexión o ISP.
- Servidores de certificados públicos y llaves de seguridad.
- Autenticación única ó “single sign-on” para la personalización de aplicaciones.
- Perfiles de usuarios centralizados, para permitir itinerancia ó “Roaming”
- Libretas de direcciones compartidas.

Como hemos visto LDAP es una base de datos optimizada para entornos donde se realizan muchas lecturas de datos y pocas modificaciones o borrados.

Por lo tanto es muy importante saber elegir dónde es conveniente usarlo. No será conveniente como base de datos para sitios que realicen constantes modificaciones de datos (por ejemplo en entornos de e-commerce)

Normalmente el tipo de preguntas que debes hacerte para saber si LDAP es conveniente para las aplicaciones son:

- ¿Queremos que los datos estén disponibles desde distintos tipos de plataformas?
- ¿Necesitamos acceso a estos datos desde un número muy elevado de servidores y/o aplicaciones?
- Los datos que almacenamos ¿son actualizados muchas veces?, o por el contrario ¿son sólo actualizados unas pocas veces?
- ¿tiene sentido almacenar este tipo de datos en una base de datos relacional? Si no tiene sentido, ¿puedo almacenar todos los datos necesarios en un solo registro?

4.4.3 Aplicaciones susceptibles de usar un Directorio Corporativo para gestionar su información

- Sistema de correo electrónico

  Cada usuario se identifica por su dirección de correo electrónico, los atributos que se guardan de cada usuario son su contraseña, su límite de almacenamiento (quota), la ruta del disco duro donde se almacenan los mensajes (buzón) y posiblemente atributos adicionales para activar sistemas anti-spam o anti-virus.

  Como se puede ver este sistema LDAP recibirá cientos de consultas cada día (una por cada email recibido y una cada vez que el usuario se conecta mediante POP3 o webmail). No obstante el número de modificaciones diarias es muy bajo, ya que solo se puede cambiar la contraseña o dar de baja al usuario, operaciones ambas que no se realizan de forma frecuente.

- Sistema de autenticación a una red

  Cada usuario se identifica por un nombre de usuario y los atributos asignados son la contraseña, los permisos de acceso, los grupos de trabajo a los que pertenece, la fecha de caducidad de la contraseña…

  Este sistema recibirá una consulta cada vez que el usuario acceda a la red y una más cada vez que acceda a los recursos del grupo de trabajo (directorios compartidos, impresoras…) para comprobar los permisos del usuario.

  Frente a estos cientos de consultas solo unas pocas veces se cambia la contraseña de un usuario o se le incluye en un nuevo grupo de trabajo.

4.4.3.1 Comparación entre LDAP y bases de datos relacionales

Las características de una base de datos relacional (RDBMS o Relational Database Management Systems) son:

- Realizan operaciones de escritura intensivas: las bases de datos relacionales estás preparadas para hacer un uso constante de operaciones orientadas a transacciones, que implican la modificación o borrado constante de los datos almacenados.
- Esquema específico para cada aplicación: las bases de datos relacionales son creadas para cada aplicación específica, siendo complicado adaptar los esquemas a nuevas aplicaciones.
- Modelo de datos complejo: permiten manejar complejos modelos de datos que requieren muchas tablas, foreign keys, operaciones de unión (join) complejas…
- Integridad de datos: todos sus componentes están desarrollados para mantener la consistencia de la información en todo momento. Esto incluye operaciones de rollback, integridad referencial y operaciones orientadas a transacciones.
- Además las transacciones se efectúan siempre aisladas de otras transacciones. De tal forma que si dos transacciones están ejecutándose de forma concurrente los efectos de la transacción A son invisibles a la transacción B y viceversa, hasta que ambas transacciones han sido completadas.
- Disponen de operaciones de roll-back (vuelta atrás). Hasta el final de la transacción ninguna de las acciones llevadas a cabo pasa a un estado final. Si el sistema falla antes de finalizar una transacción todos los cambios realizados son eliminados (roll-back)

Por el contrario, las características de un servidor LDAP son:

- Operaciones de lectura muy rápidas. Debido a la naturaleza de los datos almacenados en los directorios las lecturas son más comunes que las escrituras.
- Datos relativamente estáticos. Los datos almacenados en los directorios no suelen actualizarse con mucha frecuencia.
- Entorno distribuido, fácil replicación
- Estructura jerárquica. Los directorios almacenan la información de forma jerárquica de forma nativa.
- Orientadas a objetos. El directorio representa a elementos y a objetos. Los objetos son creados como entradas, que representan a una colección de atributos.

- Esquema Standard. Los directorios utilizan un sistema standard que pueden usar fácilmente diversas aplicaciones.
- Atributos multi-valor. Los atributos pueden almacenar un valor único o varios.
- Replicación multi-master. Muchos de los servidores LDAP permiten que se realicen escrituras o actualizaciones en múltiples servidores.

4.5 ¿QUÉ ES OPENLDAP?

OpenLDAP es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol (LDAP) desarrollada por el proyecto OpenLDAP. Está liberada bajo su propia licencia OpenLDAP Public License. LDAP es un protocolo de comunicación independiente de la plataforma. Muchas distribuciones GNU/Linux incluyen el software OpenLDAP para el soporte LDAP. Este software también corre en plataformas BSD, AIX, HP-UX, Mac OS X, Solaris, Microsoft Windows (NT y derivados, incluyendo 2000/2003, XP, Vista), y z/OS.

El proyecto OpenLDAP se inició en 1998 por Kurt Zeilenga. El proyecto comenzó como un clon de la implementación LDAP de la Universidad de Michigan, entidad donde se desarrolló originalmente el protocolo LDAP y que también actualmente trabaja en la evolución del mismo.

En abril de 2006, el proyecto OpenLDAP incorpora tres miembros principales: Howard Chu (Arquitecto jefe), Pierangelo Masarati, y Kurt Zeilenga. Hay otros importantes y activos contribuyentes incluyendo Luke Howard, Hallvard Furuseth, Quanah Gibson-Mount, and Gavin Henry.

Los principales lanzamientos funcionales de OpenLDAP incluyen:

- OpenLDAP versión 1 fue una limpieza general de la última versión del proyecto de la Universidad de Michigan (lanzamiento 3.3), y consolidación de cambios adicionales.

- OpenLDAP versión 2.0, lanzada en agosto de 2000, incluyó mejoras importantes incluyendo soporte para LDAP versión 3 (LDAPv3), soporte para Internet Protocol versión 6 (IPv6), y numerosas otras mejoras.
- OpenLDAP versión 2.1, lanzada en junio de 2002, incluyó en backend la base de datos transaccional basada en Berkeley Database o BDB, soporte para Simple Authentication and Security Layer (SASL), y backends experimentales Meta, Monitor, and Virtual.
- OpenLDAP versión 2.2, lanzada en diciembre de 2003, incluyó el motor de "sincronización" LDAP "sync" con soporte de replicación (syncrepl), la interfaz de presentación, y numerosas mejoras funcionales a nivel de base de datos y relacionadas con RFC.
- OpenLDAP versión 2.3, lanzada en junio de 2005, incluyó Configuration Backend (para configuración dinámica), interfaces adicionales incluyendo y numerosas mejoras adicionales...
- OpenLDAP versión 2.4, lanzada en octubre de 2007, introdujo la replicación en N-vías MultiMaster, Stand-by master, y la posibilidad de eliminar y modificar elementos del esquema en tiempo de ejecución, además de más modificaciones.

5 ESTUDIO DE VIABILIDAD

Antes de iniciar el proyecto se efectuó un estudio de viabilidad con el objetivo de evaluar si es posible o no su realización con los medios de los que se dispone y en el contexto en el que se realizará.

Al finalizar dicho estudio se concluyó que la realización del proyecto de implantación de un directorio corporativo objeto de esta memoria era viable.

5.1 ESPECIFICACIONES DEL SISTEMA Y DE LAS APLICACIONES

Las especificaciones hardware y software del sistema necesario para el proyecto vienen definidas por el producto a instalar, en este caso OpenLDAP. Por ello se utilizó dicha información para adquirir las máquinas necesarias.

Las especificaciones de la aplicación quedaron definidas durante la fase de toma de requerimientos. Se tomó como punto de partida el número de usuarios totales, el número de usuarios conectados concurrentemente y el volumen de datos a almacenar.

A grandes rasgos, el directorio corporativo deberá permitir en una primera fase el almacenamiento de los datos requeridos por el Portal Corporativo y posteriormente la de cualquier aplicación que desee acceder a los datos almacenados en él.

5.2 VIABILIDAD TÉCNICA

Para implantación OpenLDAP se siguieron los requisitos de hardware y software que marca el OpenLDAP por lo que la viabilidad técnica estuvo garantizada.

Se adquirieron dos servidores Intel con los requisitos de frecuencia de procesador y memoria necesarios para la instalación de OpenLDAP.

Uno de los servidores funcionó como master y el segundo servidor como backup del principal para la aplicación LDAP.

Este modelo hace referencia al maestro como servidor principal y al replicado como servidor secundario. Todas las actualizaciones se llevan a cabo en el servidor maestro y se propagan posteriormente al servidor replicado. La base

de datos del servidor replicado contiene una copia exacta de los datos del directorio del servidor maestro.

Los cambios al directorio sólo pueden hacerse en el servidor maestro, que siempre se utiliza para operaciones de escritura en el directorio. El servidor maestro o los servidores replicados pueden utilizarse para operaciones de lectura. Si el servidor maestro original deja de funcionar durante un periodo de tiempo largo, un servidor replicado puede sustituirle para permitir operaciones de escritura en el directorio.

Con el fin de cumplir los requerimientos de seguridad de datos del cliente ambos servidores se conectaron a la infraestructura de backup existente.

5.3 VIABILIDAD OPERATIVA

Para este proyecto se creó un equipo con los siguientes perfiles:

- Gente de cuenta (por parte de la empresa de servicios)
- Consultor OpenLDAP (por parte de la empresa de servicios)
- Gerente de área de infraestructuras (por parte del cliente)
- Técnico de infraestructuras (por parte del cliente)

Al inicio de este proyecto se verificó la disponibilidad de todos los miembros del equipo así como que sus habilidades estaban de acuerdo a los roles del proyecto.

Adicionalmente, la dirección de la compañía transmitió al negocio la importancia de este proyecto y consiguió involucrar a las personas clave en diferentes áreas de negocio para las diferentes fases del proyecto.

Además del componente humano, se dispuso de un espacio físico en la compañía durante el tiempo que dure el proyecto, así como de los medios materiales necesarios para su ejecución.

5.4 VIABILIDAD ECONÓMICA

El proyecto dispuso de presupuesto suficiente para cubrir los diferentes aspectos necesarios para el proyecto:

- Hardware
- Equipo humano
- Dietas y viajes

Los costes de proyecto están reflejados en el capítulo 7.2.3 Presupuesto.

5.4.1 Coste de Hardware

OpenLDAP requiere de un equipo adecuado para poder funcionar. Esto implica servidores adecuados a los requerimientos volumétricos del proyecto. Por esta razón el cliente consiguió una partida presupuestaria para asignar a la compra de hardware.

5.4.2 Equipo humano

El coste del equipo humano que participó en el proyecto se consideró de la siguiente manera:

- Coste de la ayuda experta
- Coste de suplir al personal de la empresa que se encuentre dedicado totalmente al proyecto
- Coste de distraer al personal de la empresa para trabajar con los expertos en sesiones esporádicas
- Coste de capacitación del personal
- Coste de la realización de las pruebas del sistema
- Coste del desarrollo de la documentación

A la hora de calcular el presupuesto se tuvieron en cuenta un porcentaje para desviaciones. De los aspectos enumerados anteriormente el que es susceptible de sufrir las desviaciones más importantes es el ocasionado por el equipo, ya que en caso de retrasarse el arranque de proyecto, crecería con el tiempo.

El cliente disponía una partida presupuestaría para este elemento.

5.4.3 Coste de dietas y viajes

Adicionalmente, el proyecto se realizó en una ciudad diferente a la que es la residencia habitual del equipo de solución, por lo que fue necesario presupuestar un coste de dietas y viajes.

El cliente acepto esta situación y provisionó en su partida presupuestaria esta situación

5.5 VIABILIDAD LEGAL

Al tener que tratar este proyecto con datos de empleados, fue necesaria la autorización del equipo legal del cliente.

Por esta razón el cliente realizó un trabajo previo de consulta a legal y obtención de la autorización necesaria para asegurar que los datos eran tratados con total privacidad y sin incumplir ninguna ley vigente.

5.6 PLANIFICACIÓN

El siguiente gráfico muestra la planificación del proyecto en cada una de sus fases:

Ilustración c - Planificación del proyecto de final de carrera

La planificación estimada de la carga de trabajo fue la siguiente:

- Certificación del software de directorio de empleados (OpenLDAP) como solución técnicamente compatible con el portal de empleados de Vignette
  Dos semanas (10 días/hombre de trabajo)

- Identificación de los atributos y fuentes de datos necesarias para añadir al esquema de datos de LDAP.
  Seis semanas (30 días hombre de trabajo)

- Desarrollo de un proceso de extracción y carga de datos en LDAP.
  Dos semanas (10 días/hombre de trabajo)

- Desarrollo de la memoria y preparación de la presentación.

Tres semanas (15 días hombre). Este último no fue facturado al cliente y es el desarrollo de esta memoria.

6 METODOLOGÍA

Para los proyectos de implantación de software (como es el caso de Directorios Corporativos), la empresa de servicios dispone de una metodología de implantación estándar.

El objetivo de esta metodología es agilizar la implementación de un sistema como un Directorio Corporativo.

Obviamente, la implantación de un Directorio Corporativo tiene algunos requerimientos diferenciales a la implantación de otros paquetes de software (como ERPs, CRMs o aplicaciones verticales), por lo que la metodología que se describe a continuación esta actualizada para tener en cuenta las particularidades de los proyectos de implantación de Directorio Corporativos.

6.1 DESCRIPCIÓN

La metodología usada divide el proceso de implementación en cinco fases que son los principales hitos del proyecto de implementación de un Directorio Corporativo.

Cada una de ellas se compone de:

- Paquetes de trabajo: actividades de las que los equipos del proyecto son responsables.
- Actividades: consisten en tareas que son procesadas por uno o más de un miembro del equipo.
- Tareas: llevadas a cabo por un miembro del equipo de proyecto.

6.2 FASES

La implementación de un directorio corporativo según la metodología establecida se realiza siguiendo las siguientes fases:

- Preparación inicial
- Mapa de datos y procesos
- Implantación
- Preparación final
- Arranque y soporte a post- productivo

La siguiente figura representa el ciclo de vida de un proyecto de implementación de un Directorio Corporativo:

Ilustración d - Ciclo de vida del proyecto de implementación

6.2.1 Preparación inicial

En esta fase se realiza la planificación del proyecto y se sientan las bases para el éxito de la implementación al tomarse las decisiones estratégicas cruciales del proyecto.

- Definir las metas y objetivos del proyecto.

  Tras identificar las personas claves en la compañía, es importante clarificar con ellas los objetivos que se pretenden alcanzar con el proyecto. De esta forma será más sencillo evaluar los resultados al final del mismo.

- Clarificar el alcance de la implementación

  El alcance del proyecto debe quedar claro desde el principio y es imprescindible que quede definido y aceptado por todas las partes. Para ello se crea un documento de especificación de los requerimientos que va a cubrir el proyecto.

  Durante la implantación del proyecto pueden surgir nuevos requerimientos que en caso de ser incluidos podrían retrasar considerablemente el arranque del proyecto. Por ello, es crucial no perder de vista en ningún momento lo que pertenece al alcance del proyecto y lo que debe ser planificado para ser incluido en fases posteriores.

- Definir la planificación del proyecto, el presupuesto y la secuencia de implementación.

  La planificación del proyecto suele venir definida por la propia inercia de la compañía (cierres fiscales, campañas especiales, etc.).

El presupuesto terminará definiendo tanto los recursos como incluso la propia planificación.

- Establecer la organización del proyecto, comités relevantes y recursos asignados.

  El equipo de proyecto estará compuesto por:

  - **Gerente de cuenta** que será la persona que acuda a las reuniones de seguimiento con el negocio y quien gestionará los recursos del proyecto. Será el encargado de dirigir las fases de negocio y asegurar que el plan de proyecto se cumple en fechas y contenidos. También se encargará de gestionar el presupuesto del proyecto.
  - **Equipo de implantación**. Son personas con diferentes roles que se dedicarán a la ejecución efectiva de la solución (programadores, consultores, etc.).

  Seleccionar el equipo que realizará el proyecto es uno de los principales hitos de esta fase ya que será la organización encargada de diseñar, implementar y realizar el soporte de la solución de Directorio Corporativo.

  Es básico en este punto tener claramente asignadas las posiciones clave del gráfico, por ejemplo, el Gerente de cuenta, arquitecto de la solución, profesionales senior y juniors…

  Es el momento también de decidirse entre escoger entre el personal interno o contratar consultores externos para rellenar cada una de las posiciones.

  A parte del equipo de proyecto, estarán involucrados en el mismo diferentes roles del negocio con una aportación puntual en diferentes momentos del proyecto:

  - **Usuarios Clave:**

    Tienen un papel muy importante durante todo el proyecto. Durante la toma de requerimientos, su conocimiento de los

procesos de negocio de la compañía y su visión son cruciales para la asistencia en la creación de la nueva aplicación.

Pero su intervención no termina en la fase previa del proyecto sino que son un pilar muy importante durante las etapas posteriores:

- Participación en las reuniones de toma de requerimientos para explicar procesos en los que están involucrados y que deben aparecer en la aplicación a crear.
- Participación en reuniones en las que se explica el seguimiento del proyecto así como se muestran pequeñas presentaciones de la herramienta para ver su avance.
- Participación en el test de integración con el objetivo de obtener la aprobación de la aplicación una vez terminada y antes de su puesta en productivo.
- Recibir la formación de parte del equipo de IT que realiza la implementación de la aplicación.
- Impartir la formación a usuarios finales.

- **Mandos medios:**

  Acuden a reuniones de seguimiento del proyecto. Entre ellos estará el Director de IT y mandos medios o altos del negocio (responsables de cada área).

  Durante el proyecto se establecen una serie de comités que se dedicarán tanto a vigilar la evolución del mismo como a la toma de decisiones:

  - Comité de dirección (Steering Comitee): Comité de dirección del proyecto al que acuden los mandos medios/altos asignados al mismo y el Project manager. La agenda de este comité consta de:
    - El grado de avance según el plan de proyecto.
    - Progresión de actividades.
    - Problemas importantes surgidos durante la ejecución del proyecto.
    - Discusión sobre puntos pendientes a decidir.
    - Revisión del presupuesto.

  Estas reuniones suelen tener una periodicidad mensual.

- Reuniones con usuarios clave: En estas reuniones el Project manager muestra el avance de la aplicación a los usuarios clave y perfila las funcionalidades según sus requerimientos. La periodicidad es según necesidad del proyecto y sus contenidos suelen ser muy concretos (por funcionalidad, etc.).
- Reuniones seguimiento equipo proyecto: Estas reuniones son semanales y acuden tanto el Project manager como todos los participantes ejecutivos el proyecto (programadores y consultores).

  La agenda de estas reuniones consta de:

  - Grado de avance según plan de proyecto.
  - Revisión de las actividades por integrante del equipo.
  - Problemas durante la ejecución. En este punto se discute tanto el problema como posibles soluciones.
  - Tareas a realizar para reunión siguiente.
  - Pueden revisarse también puntos derivados de la logística de un equipo (vacaciones, horarios, etc.).

6.2.2 Mapa de datos y procesos

El Mapa de datos y procesos documenta los requerimientos de estructura de datos y sus procesos asociados de una compañía. Este documento da una idea general de cómo los datos y procesos existentes en la compañía deben ser representados en el directorio corporativo.

Este mapa documenta en detalle el alcance de los datos, escenarios y procesos de negocio así como los pasos de los procesos.

El mapa de procesos se estructura de la siguiente forma:

- Unidades organizativas.
- Datos maestros.
- Datos concretos.
- Escenarios de negocio.
- Procesos de negocio.
- Pasos de los procesos.

El mapa de datos y procesos se crea después de mantener numerosas entrevistas con los diferentes departamentos involucrados en la solución.

A menudo, estos departamentos están representados en estas reuniones por los que presumiblemente serán los usuarios clave asignados al proyecto.

Ya que este mapa documenta con detalle los requerimientos de la compañía y establece cómo serán implementados en el Directorio Corporativo los datos del negocio, juega un papel muy importante en el acotamiento del alcance del proyecto: la formalización del compromiso que adquiere el equipo de proyecto con el negocio de lo que se va a entregar en la fecha de arranque.

Todo aquello que surja durante la implantación y que no esté contenido en el Mapa de datos y Procesos deberá ser considerado como mejora evolutiva para fases posteriores.

En caso de que un requerimiento no recogido en el Mapa de Datos y Procesos sea crucial para el arranque, deberá ser estudiado para estimar el tiempo necesario para su inclusión. En el comité de dirección se discute si debe ser o no incluido para evaluar el impacto en el proyecto (retraso en la fecha de arranque, necesidad de más recursos, etc.).

6.2.3 Implantación

Esta fase es la de ejecución efectiva del proyecto. Las tareas principales de esta etapa son:

- Configuración de requerimientos.

  Se estudian los requerimientos definidos en el Mapa de datos y Procesos con el fin de detectar que requerimientos no están cubiertos por la funcionalidad estándar del Directorio Corporativo. Para cada uno de ellos se elabora un diseño funcional detallado para que los programadores inicien los desarrollos del proyecto. Estos diseños funcionales formarán parte de la documentación final del proyecto.

  Las funcionalidades estándar del Directorio Corporativo son configuradas en el sistema por los consultores del proyecto. Las configuraciones realizadas en sistema se detallarán en el documento de configuración del proyecto.

- Definición de los test de integración.

  A medida que la aplicación avanza, se debe revisar con los usuarios clave los diferentes escenarios que serán probados durante el test de integración.

Dicho test suele tener lugar algunos meses antes del arranque (dependiendo del tipo de proyecto), por lo que la funcionalidad completa no está lista para dicha fecha. Por ello, es importante negociar lo que se tendrá preparado para el test y qué escenarios serán probados. De esta forma, se evitan falsas expectativas respecto a la herramienta y se dirigen el test hacia objetivos concretos.

Se suelen escoger para el test, los escenarios más críticos para el negocio. De esta forma, en caso de no ser satisfactorio el test, se dispone de tiempo de reacción para cambiar la funcionalidad.

• Documentación del proyecto.

A medida que se avanza en la ejecución del proyecto se va generando mucha documentación que debe ser correctamente clasificada y generada.

- Diseños funcionales: documentan los diferentes desarrollos que se realizan para cubrir funcionalidades no incluidas en el estándar. Constan tanto del requerimiento funcional (definido por el consultor funcional) como de la solución del programador.
- Manual de configuración: las funcionalidades cubiertas por el estándar necesitan de cierta configuración para ajustarlas a las necesidades del negocio. Todos estos cambios se documentan en este manual. En nuestro caso es la documentación de OpenLDAP.
- Manual de uso (manual del administrador): a medida que avanza la aplicación se va construyendo lo que será la guía de referencia a usuarios finales, que en nuestro caso serán los administradores de sistemas. En nuestro caso la definición de los procesos de uso de OpenLDAP (Ver capítulo 11.2 MANUAL DE USUARIO)

6.2.4 Preparación Final

Esta etapa es previa al arranque y las tareas más importantes de las que consta son:

- Completar todas las acciones sobre el sistema (configuraciones y desarrollos).
- Ejecución de test unitarios al finalizar cada una de las funcionalidades.
- Ejecución de test de integración con la participación de los usuarios clave.

- Formación a usuarios finales.
- Resolución de todas las incidencias abiertas.
- Gestión de sistemas, en concreto preparación del entorno de productivo.
- Actividades de corte de operaciones (Cutover).

En esta fase se debe asegurar que todos los prerrequisitos para el arranque del sistema se cumplen.

6.2.5 Inicio y Soporte

Esta es la última fase del proyecto y tiene como eje central la migración de toda la funcionalidad desde el entorno de pre productivo al sistema de productivo. Esta es una actividad crítica para el éxito del proyecto.

Además de esta parte técnica, también en esta etapa se definen la estrategia del soporte a productivo, la monitorización de las transacciones del sistema y la optimización del rendimiento global del sistema.

6.3 METODOLOGÍA ESPECIAL PARA DIRECTORIOS CORPORATIVOS

Los siguientes conceptos son importantes para entender la forma de trabajar en un proyecto de implantación de un Directorio Corporativo utilizando OpenLDAP como software.

6.3.1 Arquitectura de un sistema OpenLDAP

La arquitectura OpenLDAP es cliente/servidor. Para definir este tipo de arquitectura de forma sencilla, podría decirse que incorpora un conjunto de “proveedores de servicios” y de “solicitadores de servicios”.

Este tipo de arquitectura permite distribuir la carga de una aplicación entre varios programas cooperantes. Permite a su vez, separar las tareas de usuario de los datos de la aplicación y las de gestión de esos datos.

Las ventajas de una arquitectura cliente/servidor podrían resumirse en:

- Configuraciones flexibles.
- Distribución de la carga de trabajo.
- Alta escalabilidad.

Las soluciones basadas en el protocolo LDAP son tecnológicamente abiertas. Esto implica que las aplicaciones pueden funcionar sobre múltiples sistemas operativos, múltiples gestores de bases de datos, diferentes fabricantes y protocolos de comunicaciones.

Desde el punto de vista del cliente, el hecho de que el protocolo LDAP sea tecnológicamente abierto, le permite conservar una total independencia de un único fabricante.

La arquitectura de un sistema OpenLDAP se divide en tres capas: la capa de acceso para los clientes, la capa de lógica de datos y la capa de almacenamiento. Cada una de estas capas realiza ciertas funciones y constituye parte del mapa total de un sistema OpenLDAP.

La capa de acceso permite al usuario interaccionar con la aplicación. Este usuario suele ser una aplicación (como un Portal de Empleados, una aplicación desarrollada a medida, un cliente de correo electrónico…) o un usuario a través de comandos estándar desde la línea de comandos o a través de un GUI. Gracias a que LDAP es un protocolo abierto existen múltiples herramientas de diferentes fabricantes para acceder a los datos almacenados en un directorio LDAP.

La capa de lógica de datos es donde OpenLDAP verifica que la estructura (llamada esquema en la tecnología LDAP) es correcta y las relaciones entre los tipos de datos se mantienen al ser actualizados (bien por una inserción, modificación, borrado o renombrado). Esta capa es la que se encarga de las funciones de replicación en un entorno multi-LDAP.

La capa de base de datos es donde OpenLDAP almacena los datos una vez han sido verificados por la capa de lógica de datos. Si bien OpenLDAP hace uso de Sleepycat BDB de formar estándar como sistema de almacenamiento de datos, también puede usar otros sistemas de almacenamiento a través de una arquitectura de plug-ins.

La distribución de funciones de sistema en múltiples capas significa que OpenLDAP es un sistema extremadamente flexible al ser posible personalizar e incluso cambiar las funcionalidades de las capas a través de plug-ins.

Además, con el fin de poder aumentar la disponibilidad y escalabilidad OpenLDAP es capaz de replicar los datos, distribuyendo la carga de trabajo entre múltiples servidores. Esto es posible entre otras cosas gracias a la comunicación de red entre servidores participantes.

Debido a que la arquitectura del sistema OpenLDAP soporta un gran número de plataformas de sistemas operativos y hardware, el software se mantiene lo más independiente posible de las plataformas donde se ejecuta.

6.3.2 Seguridad

En el actual entorno de negocio en el que existe un uso cada vez mayor de redes abiertas y el cruce de relaciones y procesos de negocios entre diferentes empresas, una transferencia de datos segura entre Internet y la intranet de la compañía es una parte crucial del negocio.

OpenLDAP provee de una infraestructura que ofrece funciones en el área de la seguridad en entornos heterogéneos.

Los datos almacenados en el Directorio Corporativo están protegidos ante accesos no autorizados y malos usos. Autorizaciones de acceso y roles determinan quién puede visualizar y procesar datos. Además, aspectos de seguridad respecto al sistema operativo pueden ser considerados de forma separada.

Los aspectos más importantes de la seguridad que deben tratarse incluyen:

- Autentificación de usuario.

  Sólo usuarios autorizados deben tener acceso al sistema. Debe también asegurarse que personas no autorizadas no pueden copiar una identidad.

  Los usuarios pueden ejecutar aquellas tareas para las que han sido autorizados.

- Protección de la integridad.

- Protección de la confidencialidad.

  Los datos y comunicaciones deben estar protegidos de la lectura no autorizada.

- Control y Registro (Logging).

Existe una amplia gama de mecanismos disponibles en OpenLDAP para la autentificación de usuarios:

- ID de usuario y Password.

  Para guardar los passwords, el sistema los convierte con una rutina hash de sentido único en un valor hash que se almacena en la base de datos. El

hecho de que sea de sentido único asegura que desde el valor hash no se puede extraer el password original usando la rutina.

• Comunicaciones de Red Seguras (LDAPS).

LDAPS está disponible para la encriptación de datos cuando se requiere una encriptación completa de todos los datos trasmitidos hacia/desde el Directorio Corporativo. LDAPS es una versión del protocolo estándar LDAP encriptada con una capa SSL/TLS

La infraestructura de la red tiene una importancia primordial en la seguridad del sistema. La red debe soportar las comunicaciones necesarias para la compañía y sus requerimientos para excluir accesos no autorizados.

6.3.3 Gestión de cambios y Migraciones

Todas las aplicaciones requieren de un mantenimiento intensivo a lo largo de la vida del software. Un sistema como un Directorio Corporativo no es una excepción a esta regla y una vez está funcionando en productivo se realizan mantenimientos y mejoras en el sistema.

Sin embargo, por razones de seguridad, los cambios no pueden ser realizados en el entorno de productivo. Se realizan estas modificaciones en un sistema separado de desarrollo.

Esta razón lleva a la definición del mapa de sistemas que es básicamente la disposición de los servidores OpenLDAP.

Idealmente, en un entorno aplicativo, se dispondrá de un mapa con tres sistemas:

• Servidor de Desarrollo (DEV).

En este entorno se realizan todas las configuraciones y desarrollos necesarios para que la aplicación refleje los requerimientos del negocio.

Este entorno no suele tener datos maestros cargados, es decir, en caso de necesitar cualquier dato maestro debe ser creado por el equipo de proyecto.

Una vez que el equipo de proyecto considere que un cambio está terminado, realiza unas mínimas pruebas en este entorno y solicita la transferencia de la modificación al entorno de calidad. Esta transferencia

de configuraciones y desarrollos entre entornos se realiza a través de intervenciones planificadas y controladas.

• Servidor de Integración o Calidad (QAS).

En este entorno se prueban las configuraciones y desarrollos realizados en el entorno de desarrollo.

Este entorno contiene datos maestros reales de la compañía, lo que permite que las pruebas sean fiables y abarcan todos los escenarios posibles.

Una vez que el cambio ha sido probado en este entorno y su funcionamiento es correcto, se solicita la migración de la modificación al entorno de productivo para su uso final.

• Servidor de Productivo (PROD).

Este entorno es en el que se ejecutará la aplicación para su uso real, por lo que lógicamente, contendrá todos los datos maestros de la compañía.

En algunos proyectos se dispone de un cuarto sistema de pruebas llamado SandBox. Este cuarto sistema permite testear la configuración de los procesos de negocio de una compañía, especialmente antes de que el Mapa de datos y procesos se firme, pero el uso más común que se le da a este sistema es de formación del entorno.

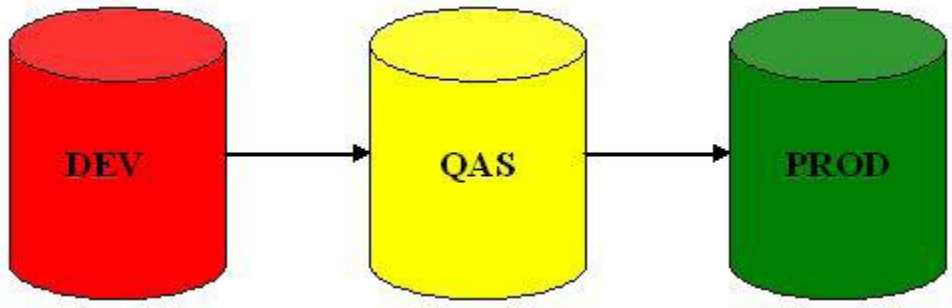

Ilustración e - Esquema de entornos de proyecto

En algunos proyectos se elimina el entorno de calidad y se trabaja sin problemas con dos entornos, el de desarrollo y productivo.

No es ningún problema trabajar de esta forma siempre que en desarrollo se carguen datos maestros reales para las pruebas, y que el equipo de proyecto sea limpio durante la configuración del sistema.

6.3.4 Desarrollos y Configuración

Una vez comprendidos y analizados los requerimientos del cliente, se deben separar los que son cubiertos por el OpenLDAP de forma estándar y aquellos que son una extensión del esquema de datos básico.

6.3.4.1 Configuración

Mediante la guía de administración de OpenLDAP se configura la aplicación para que cubra los requerimientos del cliente.

Esta configuración está pensada para personalizar la instalación de OpenLDAP, así como parametrizar valores del backend de base de datos, la capa de conectividad de red o los parámetros de replicación para una instalación multi-servidor.

6.3.4.2 Desarrollos

Cuando un requerimiento del negocio no está cubierto por el esquema básico de OpenLDAP, y por tanto no puede ser configurado en el sistema, se procede a extender el esquema con un modelo de datos y atributos asociados que requiere el cliente.

Esto se hace a través del fichero de definición de esquemas, el cual utilizando un modelo de *herencia* permite crear extensiones a los esquemas existentes.

Para realizar este trabajo existe un servidor de desarrollo que permite verificar de forma iterativa los cambios que se realizan.

Las principales características de dicho entorno de desarrollo son:

- Soporte de interfaces gráficas comunes y estándar.
- Comunicación transparente con otros sistemas.
- Manejo transparente y abierto del sistema de gestión de la base de datos.
- Comunicación con aplicaciones externas a través de interfaces batch.

6.3.5 Soporte OpenLDAP

Los componentes de cualquier equipo que participa en una implantación de OpenLDAP, cuentan con una serie de herramientas para ayudarles a desempeñar su cometido.

6.3.5.1 Ayuda de OpenLDAP

En la url http://www.openldap.org/faq/ se encuentran, organizada por áreas, información útil sobre el sistema.

De toda esta información es especialmente útil la librería donde usando el buscador se puede encontrar, de forma más o menos sencilla, cómo realizar paso a paso ciertas acciones sobre el sistema para cumplir con los requerimientos.

Forma parte del trabajo diario de las personas que trabajan con OpenLDAP el saber buscar en este repositorio de información.

6.3.5.2 RFCs

Otra fuente de información, tanto a nivel de definición de standard como reglas de implantación son las RFCs (Request for Comments) dedicadas a LDAP.

La mejor fuente de información de RFCs de LDAP está almacenada en http://www.bind9.net/rfc-ldap/

6.3.5.3 Foros de OpenLDAP

Existen varios foros de profesionales dedicados a OpenLDAP en el que se comparten experiencias y conocimientos que pueden ser realmente útiles. Es posible tanto preguntar, cómo simplemente revisar si existe alguna discusión abierta sobre el tema que se necesita. Uno de los más utilizados es http://www.openldap.org/lists/

7 REALIZACIÓN DEL PROYECTO

A continuación se documenta la realización efectiva del proyecto pasando por las fases necesarias para su ejecución.

Para dicha realización se ha adaptado la metodología estándar (ver capítulo 6 METODOLOGÍA) usada por la empresa de servicios propone para una implantación software a un proyecto de implantación de Directorio Corporativo que es más pequeño tanto en tiempo como en alcance y contenido.

7.1 PRESENTACIÓN DEL PROYECTO

Antes de entrar a detallar cada una de las fases de implantación del proyecto Directorio Corporativo introduzcamos el escenario del proyecto.

7.1.1 Cliente

El cliente donde se desarrolló el proyecto es una multinacional dedicada a la producción y comercialización del sector farmacéutico.

Con una facturación de aproximadamente 23.900 millones de dólares anuales, es en su sector una de las más importantes a nivel mundial. Tiene oficinas centrales en Estados Unidos y dispone de 120 filiales, 31 fábricas, además de centros de formación e investigación, además de una potente red de distribución que abarca a más de cien países de todo el mundo y una plantilla de aproximadamente 55.000 empleados.

7.1.2 La empresa de servicios

La empresa de servicios en la que se realizó el proyecto es una multinacional dedicada a los servicios informáticos, trabajando en las áreas de externalización de procesos, aplicaciones e infraestructura.

Con una facturación de aproximadamente 22.100 millones de dólares anuales, es en su sector una de las más importantes a nivel mundial. Tiene oficinas centrales en Estados Unidos y dispone de filiales repartidas en 64 países con una plantilla de aproximadamente 139.000 empelados

7.1.3 Entorno

Como parte de una iniciativa internacional, la filial del cliente en España debía implantar un Portal Corporativo para funcionar como intranet para los empleados de la empresa en España. Este portal requería un Directorio

Corporativo para almacenar los datos de los empleados: cuentas, password, datos personales, atribuciones organizativas…

El cliente no disponía de ningún directorio de empleados y tenía los datos dispersos entre diferentes sistemas (Dominio de Windows, CRM, ERP de RR.HH., ERP de Finanzas…) por lo que era imposible que el Portal Corporativo utilizara los datos de la empresa de forma sencilla.

7.2 PREPARACIÓN INICIAL

7.2.1 Plan de Proyecto

A continuación se muestra el plan de proyecto con las diferentes fases y tareas principales dentro de las mismas:

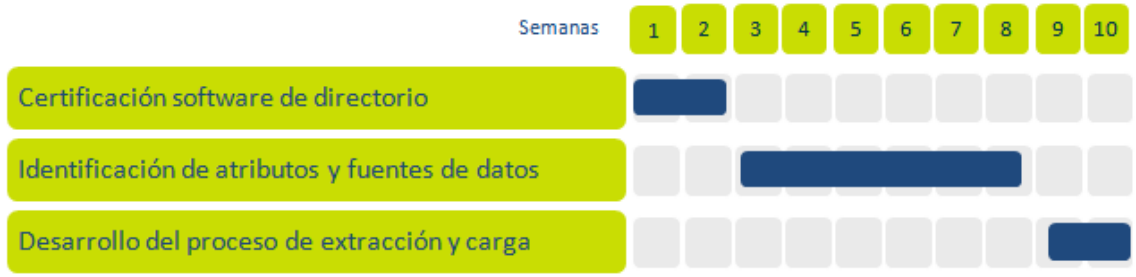

Ilustración f - Plan de proyecto presentado al cliente

El alcance de cada tarea fue la siguiente:

- Certificación del software de directorio de empleados (OpenLDAP) como solución técnicamente compatible con el portal de empleados de Vignette

  Desarrollo de una consultoría con el fin de certificar la correcta funcionalidad de OpenLDAP con el Portal de Empleados de Vignette.

  Se estimó el tiempo necesario para el desarrollo de esta tarea dos semanas.

  El entregable resultante sería un documento de certificación entre ambos software.

- Identificación de los atributos y fuentes de datos necesarias para añadir al esquema de datos de LDAP.

A través de reuniones con las diferentes áreas de negocio, creación de un mapa de datos y procesos para identificar que atributos son necesarios para definir el modelo de datos del Directorio de Empleados, así como el origen de las fuentes de datos de donde provienen esos datos.

Se estimó el tiempo necesario para el desarrollo de esta tarea seis semanas.

El entregable sería una el mapa de datos y procesos.

- Desarrollo de un proceso de extracción y carga de datos en LDAP.

  A partir del entregable de la tarea anterior desarrollo de un programa de extracción y carga de datos de las fuentes de datos existentes al LDAP.

  Se estimó el tiempo necesario para el desarrollo de esta tarea dos semanas.

7.2.2 Equipo

El equipo necesario para implantar la solución Directorio Corporativo estuvo compuesto por los siguientes roles:

- Un gerente de cuenta (por parte de la empresa de servicios)

  Es la persona que gestionará el plan de proyecto y que se asegurará de que se cumplan todos sus hitos.

  Acudirá a todas las reuniones con dirección del negocio y será quien defienda el proyecto en este foro.

- Consultor OpenLDAP (por parte de la empresa de servicios)

  Se trata de un consultor que ha participado en varios proyectos de implantación de directorios corporativos y Portales de Empleados y con experiencia en el sector farma.

  La misión de dicho consultor es diseñar la solución de la forma más eficiente posible usando su experiencia guiando al resto del equipo en la forma que deberá tomar la aplicación.

Escogerá los modelos de datos que cubren los requerimientos del cliente y en caso de existir un requerimiento no cubierto por el estándar, extenderá el esquema tal como sea necesario. El consultor también desarrollará el software para el proceso de extracción y consolidación de datos.

- Gerente de área de infraestructuras (por parte del cliente)

  Equivalente del gerente de cuenta, pero por parte del cliente. Su función es verificar que se cumple el plan de proyecto y asegurar de que se cumplan todos sus hitos.

  También será el encargado de firmar que el proyecto se ha llevado a cabo.

- Técnico de infraestructuras (por parte del cliente)

  Se trata de un técnico de infraestructuras que ha participado en múltiples proyectos en la compañía y conoce sus infraestructuras y responsables de las mismas.

  La misión de dicho técnico es actuar como un facilitador para que el consultor de OpenLDAP pueda trabajar de la forma más eficiente posible.

7.2.3 Presupuesto

La siguiente tabla presenta el presupuesto aproximado para el proyecto en sus 10 semanas de ejecución efectiva.

Contempla tanto el gasto previsto en personal, diferenciando entre los diferentes roles, como en conceptos técnicos (hardware y licencias).

El último apartado (Gastos varios) contempla viajes, hoteles, restaurantes, etc. que deban ser asumidos por el proyecto.

Concepto	Coste para proyecto 10 semanas
Gerente de cuenta (10%)	2.880 €
Consultor Directorio Corp.	22.400 €
Viajes	4.000 €
Hoteles	4.400 €
Dietas	2.500 €
Total:	36.180 €

Tabla i - Costes presupuestados del proyecto

7.3 MAPA DE DATOS Y PROCESOS

7.3.1 Situación

El proyecto cubre la implantación de un Directorio Corporativo para poder ser usada por el Portal de Empleados.

La aplicación será usada por:

• Empleados de la compañía (como usuarios) a través del Portal de Empleados.

• Departamento de IT. Usará la aplicación para tareas de gestión y el mantenimiento.

7.3.2 Sistemas de TI involucrados

Los siguientes sistemas del departamento de tecnologías de la información están involucrados en el proyecto:

- PeopleSoft y META4: ERPs para la gestión de RR.HH.
- JD Edwards: ERP para la gestión de Finanzas.
- Genesys: CRM de ventas.
- DaWa: Data warehouse.
- Vignette Portal: Portal Corporativo para empleados.
- Documentum: Repositorio de gestión documental.
- Executive Information System (EIS): Herramienta de reporting del área de ventas.

7.3.3 Recogida de requerimientos funcionales

Con el fin de recoger la información necesaria para identificar que datos son necesarios almacenar en el Directorio Corporativo se organizaron reuniones con las áreas de negocio implicadas en el proyecto.

El objetivo de la reunión fue identificar que información sobre usuarios y grupos de usuarios deberá ser almacenada en el Directorio Corporativo de modo que pueda ser compartida por toda la organización.

Para cumplir este objetivo, se realizó una reunión por cada aplicación/área que sea candidata a aportar datos al Directorio Corporativo.

A estas reuniones asistieron:

1. Un experto del área de negocio responsable de la aplicación:
   Esta persona aportará el conocimiento de negocio relacionado con el uso de los datos, sin entrar en la problemática técnica del almacenamiento y gestión de los mismos.

2. Un experto del área de desarrollo con conocimientos del modelo de datos de la aplicación:
   Esta persona será la encargada de aportar un conocimiento profundo (técnico, no de negocio) sobre los datos que hace uso la aplicación, complementando la información del experto de negocio.

3. El CSM (Consultant Support Manager, dependiente del departamento de TI):
   Será el encargado de ofrecer una visión global de la aplicación y sus datos, así como seleccionar y coordinar la asistencia de los empleados implicados.

4. El consultor de OpenLDAP:
   Coordinarán y liderarán la reunión, recogiendo la información necesaria y respondiendo a las dudas que puedan surgir en la reunión.

¿Qué se espera del experto del área de negocio?

Ante todo, debe conocer qué datos almacena y trata la aplicación.

Por ejemplo, para una aplicación de gestión de proyectos, el experto de negocio deberá ser capaz de enumerar los datos que se guardan en relación con los usuarios (Nombre, Apellidos, proyectos que lidera, fecha de comienzo de los proyectos...) y con grupos de usuarios (nombre del grupo, líder, área al que pertenece...).

Para una aplicación de RR.HH., sería equivalente al anterior con los valores propios al ese área (Número de empleado, categoría laboral, área a la que pertenece...)

Una vez se disponga de una lista de los datos tratados por la aplicación, el *experto de negocio* deberá indicar, para cada uno de ellos:

- Quién es el propietario del dato — ya que es posible que el programa use el dato, pero que no sea suyo.
- La 'fiabilidad del dato' — para evaluar si es un dato correcto o sólo una aproximación (y puede dudarse de su fiabilidad).
- El ciclo de vida del dato — cada cuanto cambia, y quién y por qué provoca el cambio.
- Quién tiene acceso al dato y en qué condiciones.
- Con qué aplicaciones de que áreas se comparte este dato.

Finalmente, el *experto* deberá indicar que datos le gustaría compartir con otras áreas y a que datos de otras áreas le gustaría acceder. De esta forma se podrán añadir estos datos en el LDAP y facilitar la compartición de los mismos.

El *experto de desarrollo* o el *CSM* deberán ser capaces de complementar los datos del *experto de negocio*, así como proveer de otra información como:

- El formato del dato.
- La facilidad de extracción del dato de la aplicación.
- Entorno en el que se ejecuta la aplicación.
- La existencia de know-how previo para la extracción del dato — si este no se extrae en la actualidad.

Ejemplo de definición de datos tratados:

Tipo de dato	Usuario	Grupo	Propietario	% fiabilidad	Ciclo de vida	Control de acceso	Compartido con...
Número de empleado	Si	No	RR.HH.	100%	Asignado en la contratación. No modificado nunca.	Legible por toda la empresa. Modificable por RR.HH.	Contabilidad, gestión de gastos, gestión de proyectos...
Categoría Laboral	Sí	No	RR.HH.	80%	Asignado en la contratación. Modificado por RR.HH. o por el área del empleado	Legible por toda la empresa. Modificable por RR.HH. o área del empleado.	Desarrollo de carrera profesional
Nombre de equipo de desarrollo	No	Sí	Desarrollo	50%	Creado al crear el equipo, modificado habitualmente durante la vida del mismo.	Legible por el área de desarrollo. Modificable por Dirección del área de desarrollo.	Nadie.
...	...	...	...	...	...	...	...

Tabla ii - Cuestionario de recogida de requisitos

Se realizaron dos rondas de reuniones con los siguientes departamentos:

- TI, desarrollo de software
- Finanzas
- Recursos Humanos
- Ventas Hospitalarias
- Ventas Sanidad CC.AA.
- TI, e-Business
- Marketing
- TI, Seguridad
- TI, Data Warehouse
- Ventas, gestión de delegados (múltiples áreas)

A partir de estas reuniones se definió el siguiente conjunto de requerimientos, modelo de datos y el origen de las fuentes:

7.3.3.1 Requerimientos del cliente

Para el cliente, el Directorio Corporativo es un sistema de agregación de información de fuentes de datos ya existentes.

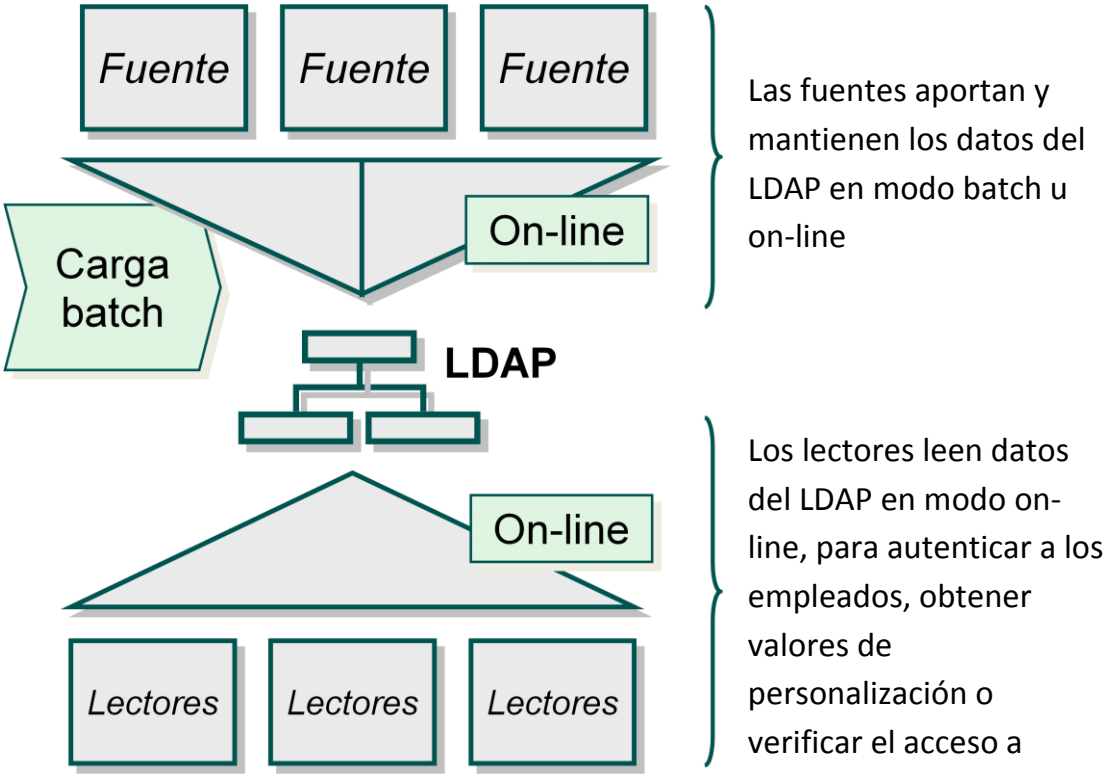

Ilustración g - Modelo general del Directorio Corporativo

Las aplicaciones on-line podrán ser Fuentes y Lectoras simultáneamente.

Implantar un servicio de directorio cuyo objetivo es dar servicio a las aplicaciones del cliente en:

- Autenticación (Identificar si el usuario y el password de un empleado es correcto)
- Personalización (Crear y mantener grupos de usuarios que comparten características comunes)
- Seguridad (Verificar el acceso de los empleados a diferentes áreas de las aplicaciones)

LDAP no será utilizado por las aplicaciones para:

- Análisis de los datos de empleados (reporting)
- Backend de datos de los sistemas operativos o transaccionales

7.3.3.1.1 Autenticación

Para resolver el problema de unificación de password el cliente decidió utilizar el password de Windows NT como password único de la empresa, por lo que el software elegido (OpenLDAP) no almacena el password en el propio directorio y consulta al dominio de NT cada vez que un usuario desea hacer log-in en el directorio.

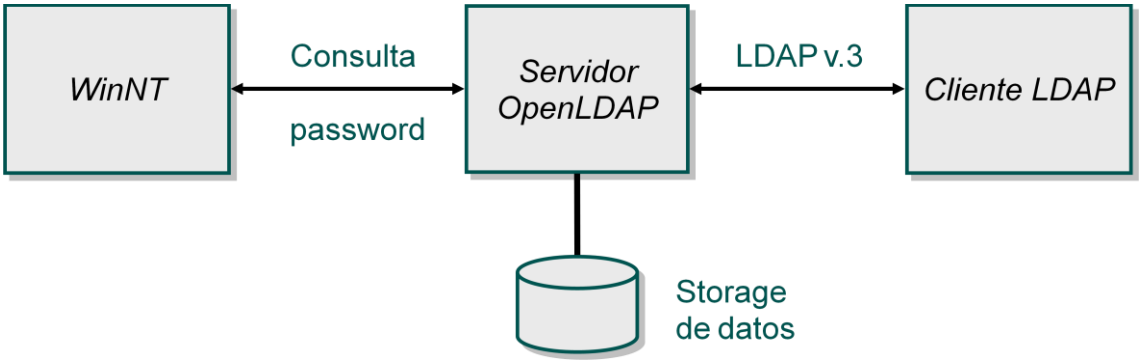

Ilustración h - Modelo de autenticación

7.3.3.1.2 Personalización

Para gestionar la personalización, LDAP crea grupos de empleados que tienen características comunes. Cuando las aplicaciones desean conocer que usuarios tienen esas características, consultan al LDAP la lista de usuarios que pertenecen a ese grupo.

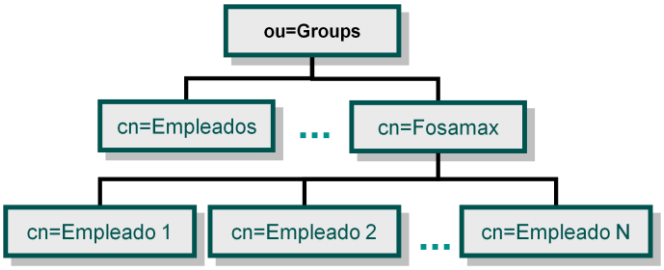

Ilustración i - Jerarquía de personalización

Para saber que empleados tienen alguna relación con un grupo (Fosamax), crearíamos un grupo denominado Fosamax y añadiríamos a todos los empleados relacionados con Fosamax. Toda aplicación que quisiera mostrar datos sobre Fosamax consultaría al Directorio Corporativo que usuarios pertenecen al grupo Fosamax y actuaría sobre esos usuarios.

7.3.3.1.3 Seguridad

Para realizar controles de seguridad, el LDAP contendrá un catalogo de aplicaciones del cliente, donde se almacenarán que usuarios tienen acceso a ellas, los grupos de los que hace uso la aplicación, así como los privilegios (perfiles) de acceso a cada página web correspondientes a cada usuario.

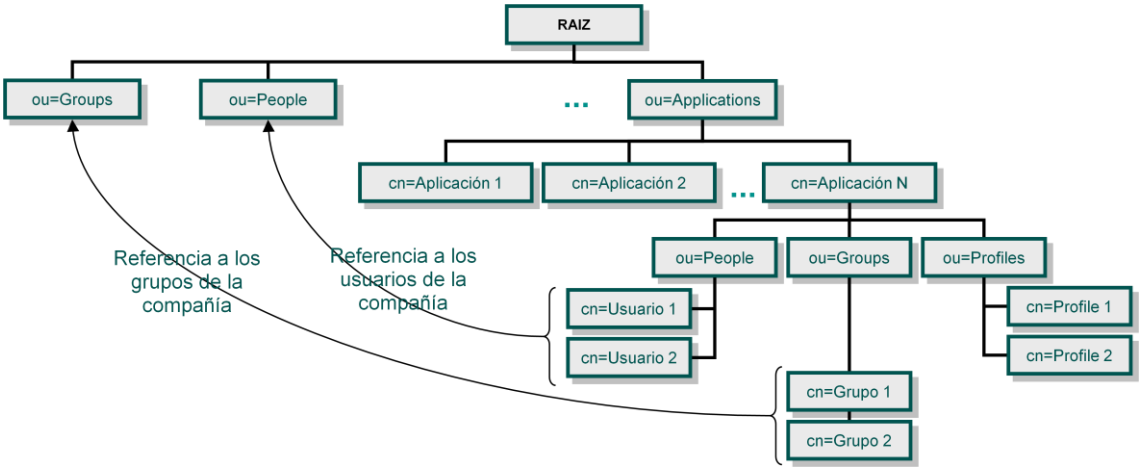

Ilustración j - Jerarquía de seguridad

7.3.3.1.4 Visión general de solución

Modelar tres entidades de datos (datos de empleados, grupos de empleados y aplicaciones) nos obliga a utilizar tres ramas en el Directorio Corporativo. Para empleados y grupos utilizamos las ramas estándar de People y Groups de Directorio Corporativo.

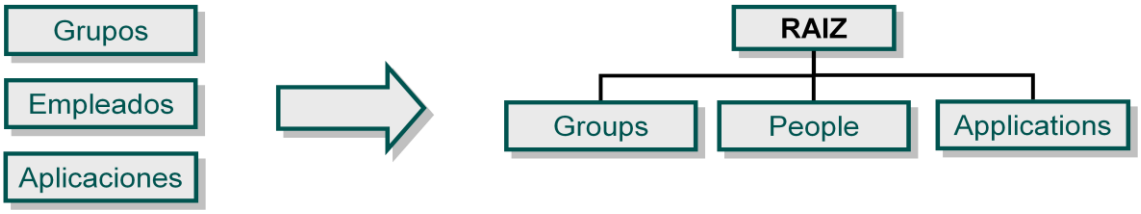

Ilustración k - Fuentes de datos no jerárquicas

Pero cada una de estas entidades carecen de relación entre sus elementos (son planas) y el cliente requiere modelar las relaciones entre grupos en la empresa (Departamentos y red de ventas) y entre los empleados (árbol de posiciones). Por esta razón aparecen las ramas de Departamentos, Fuerza de ventas y Posición, las cuales son jerárquicas:

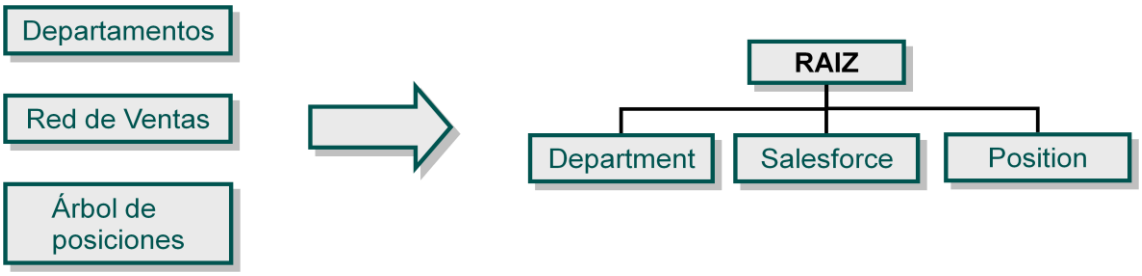

Ilustración l - Fuentes de datos jerárquicas

Para comodidad de las aplicaciones, se define un árbol de contactos de emergencia (a partir del árbol de posiciones) con el objetivo de agrupar a los empleados jerárquicamente según su posición en el árbol de contactos de emergencia.

Ilustración m - Fuentes de datos de posiciones

Finalmente, con el objetivo de disponer del maestro de estructura geográfica (proveniente de IMS) en el Directorio Corporativo para poder cruzar datos de empleados con la estructura geográfica, se modelará esta estructura en el Directorio Corporativo.

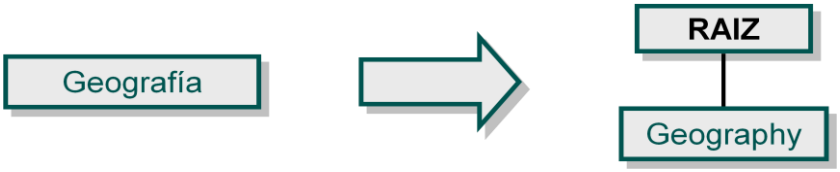

Ilustración n - Fuente de datos de posiciones

7.3.3.1.5 Así pues el modelo general del Directorio Corporativo:

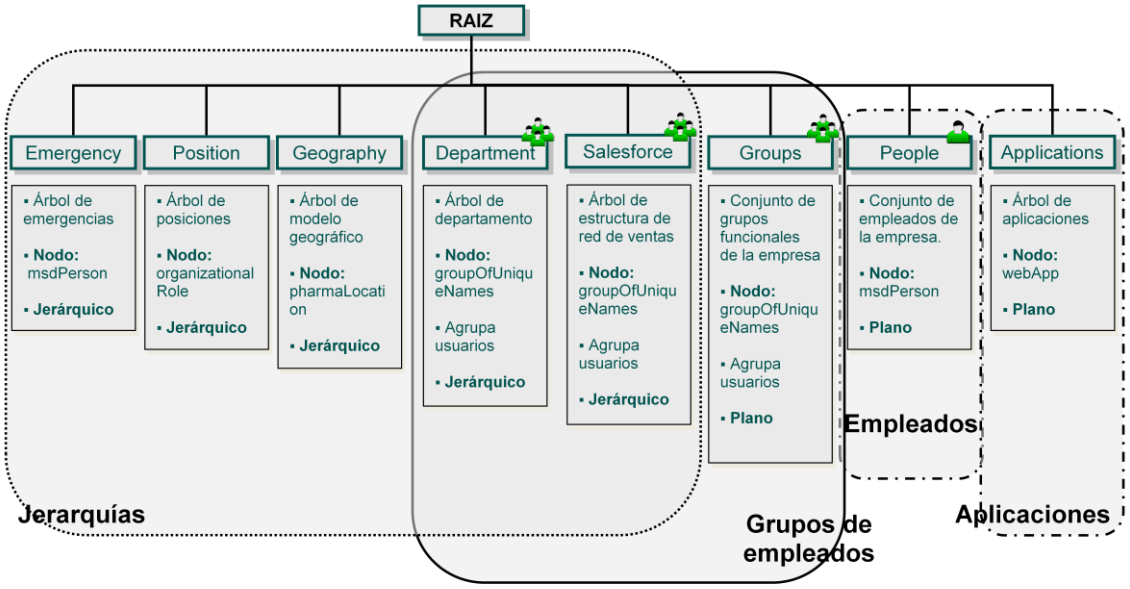

Ilustración o - Modelo de datos general

El modelo para almacenar los datos de los empleados es:

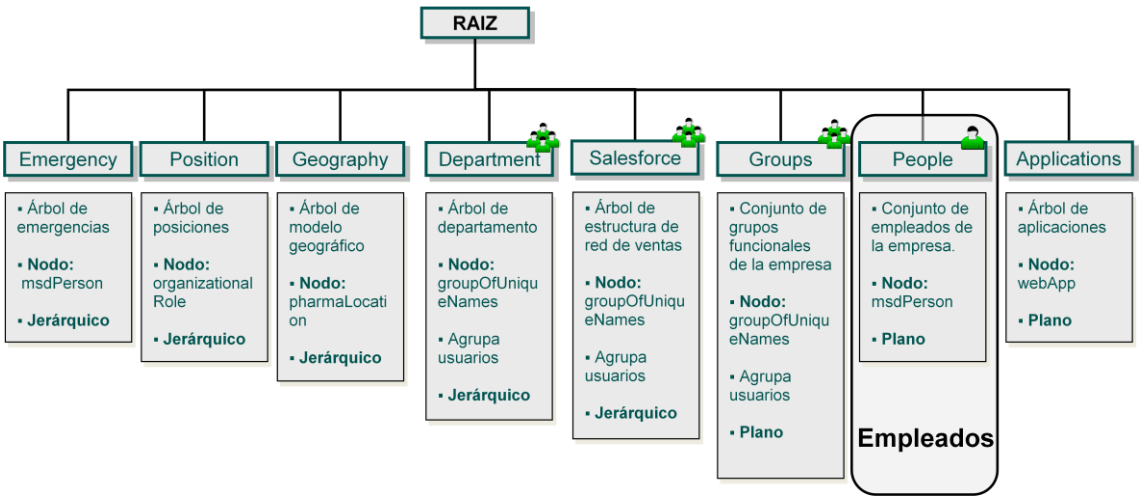

Ilustración p - Modelo de datos de empleados

La extracción de datos de empleados se realizará a partir de los siguientes sistemas:

Los datos de los empleados que no tienen ninguna información jerárquica se obtendrán de tres fuentes: Genesys, J.D. Edwards y Peoplesoft, a través de sus Data Warehouses correspondientes.

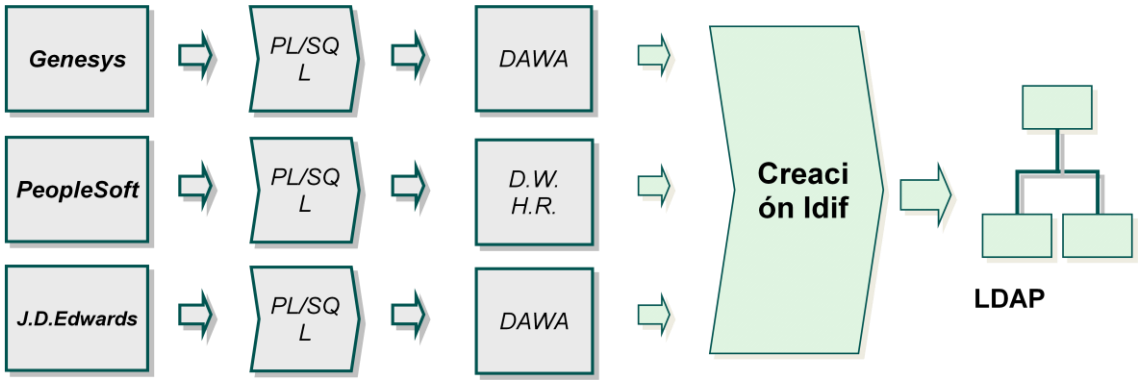

Ilustración q - Procesos de extracción y carga de datos de empleados

Los datos de empleados no podrán ser modificados por las aplicaciones on-line ya que sus aplicaciones maestras son PeopleSoft, J.D. Edwards y Genesys.

El objetivo de almacenar estos datos será almacenar los empleados y sus datos de una forma que permita un sencillo y rápido acceso (Un solo nivel – no recursivo). Estos datos serán de sólo lectura.

El objectclass a utilizar será msdPerson es una especialización de inetOrgPerson al que se le añaden los atributos necesarios para el cliente.

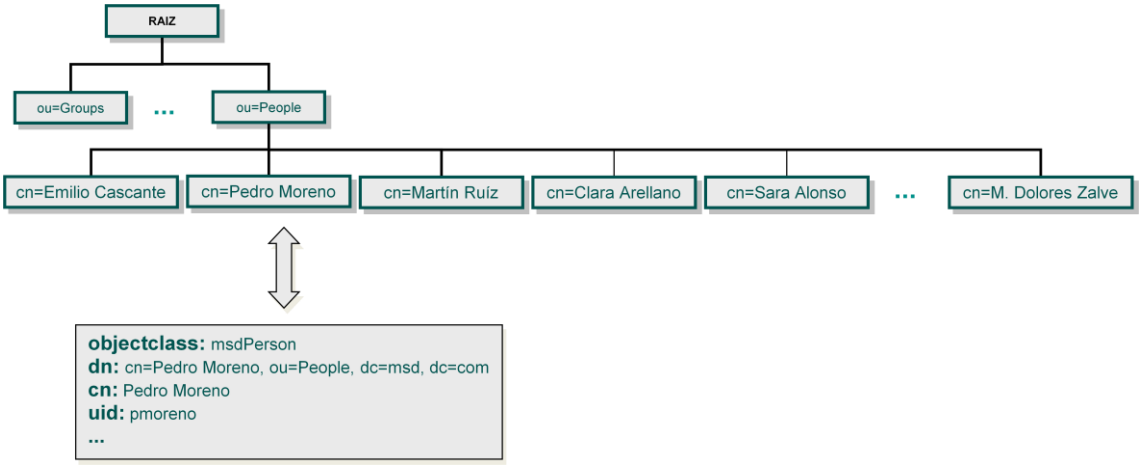

Ilustración r - Esquema msdPerson

Y las familias de atributos de empleados serán:

Ilustración s - Tipos de datos para los esquemas

Y estos atributos serán:

- Multievaluados (que pueden tomar más de un valor):

  Es decir, el departamento puede ser:

  ou: Maintenance & Development

  ou: IT & Business Processes

  ou: Strategy & Business Support

- **Basados en literales:**

  LDAP debe ser usado para guardar los valores como literales, no como códigos.

- **Nulos:**

  Puede que un atributo no tenga valor.

El modelo para almacenar los grupos de los empleados es:

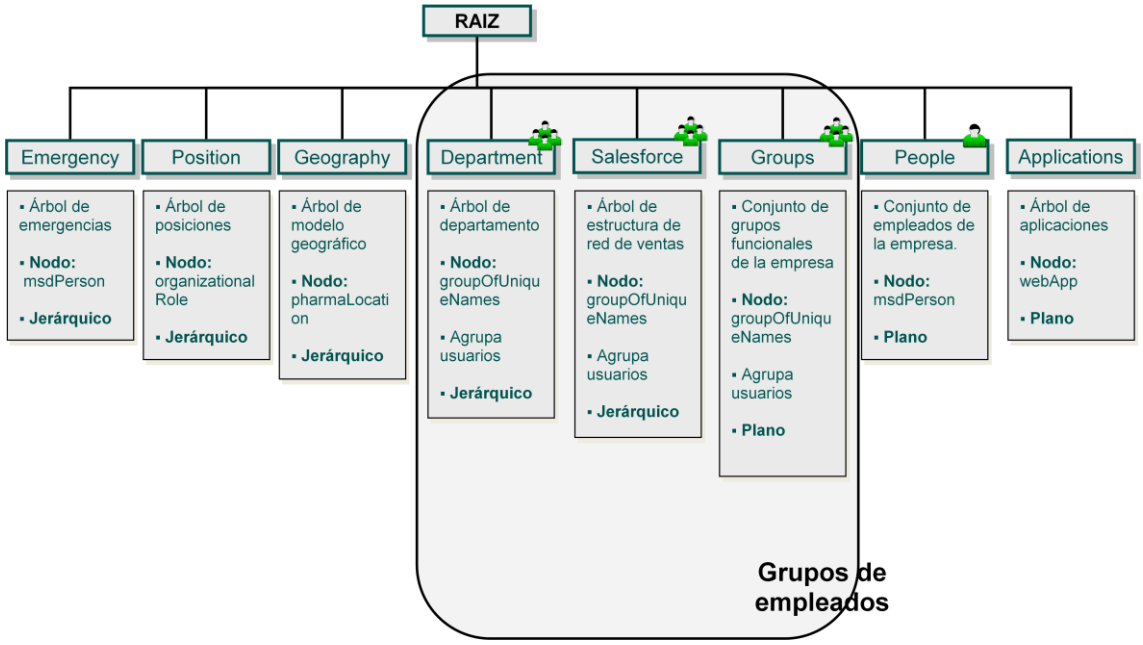

Ilustración t - Modelo de datos de grupos de empleados

Las estructuras de grupos de usuarios son aquellas estructuras que mantienen información sobre las agrupaciones (grupos) de usuarios:

Provenientes en modo Batch de sistemas heredados: Árbol de departamento, árbol de fuerza de ventas, conjunto de grupos de LDAP:

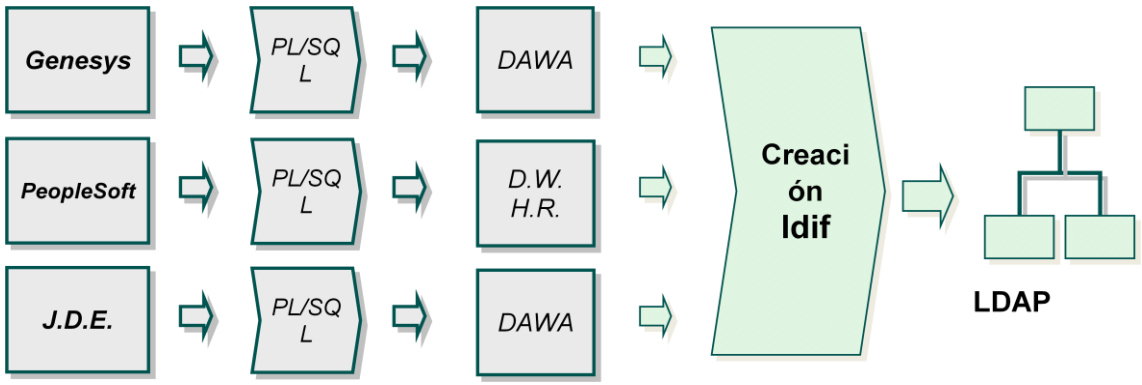

Ilustración u - Extracción y carga de grupos de empleados

Los datos de departamentos y red de ventas no podrán ser modificados por las aplicaciones on-line ya que sus aplicaciones maestras son PeopleSoft y Genesys.

En el caso del conjunto de grupos de LDAP, estos serán actualizados por las aplicaciones en modo on-line para gestionar los grupos de personalización y seguridad (VAP y aplicaciones a medida)

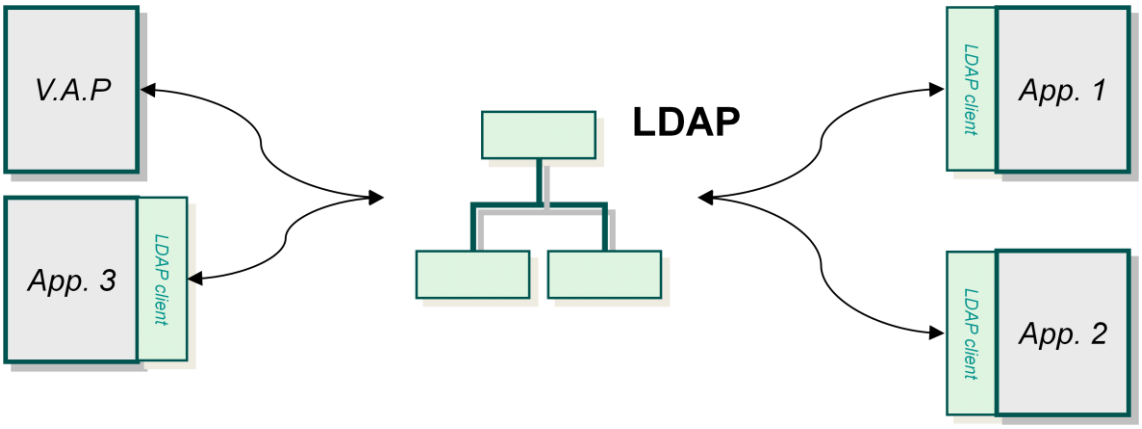

Ilustración v - Acceso on-line de las aplicaciones al Directorio de Empleados

Los datos de grupos podrán ser modificados por la aplicaciones on-line ya que esas aplicaciones on-line son maestras de esos datos.

Para almacenar los grupos de los departamentos el modelo usará los empleados ya existentes el Directorio Corporativo. Esta estructura se extraerá de Peoplesoft. Estos datos serán de sólo lectura.

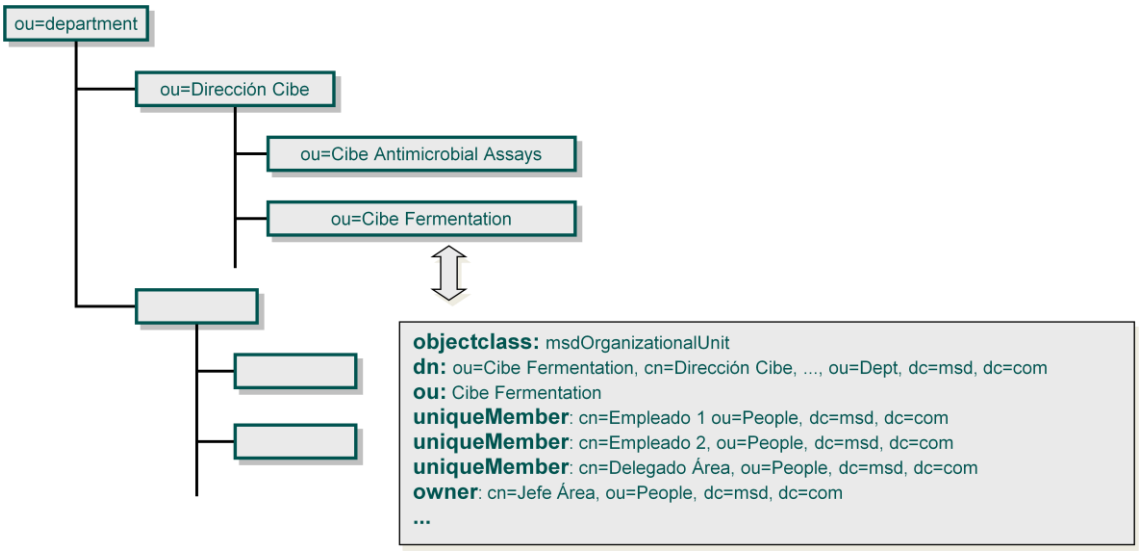

Ilustración w - Esquema de datos msdOrganizationalUnit

Un departamento se modelará a partir del objectclass msdOrganizationalUnit, el cual será una extensión de organizationalUnit, que permite definir departamentos, al cual se le añadirá el atributo uniqueMember con la finalidad de poder incluir personas en la unidad.

Es decir, un departamento no será más que otro grupo de la empresa.

Para modelar la red de ventas en el Directorio se extraerá la estructura de de Genesys.

Estos datos serán de sólo lectura.

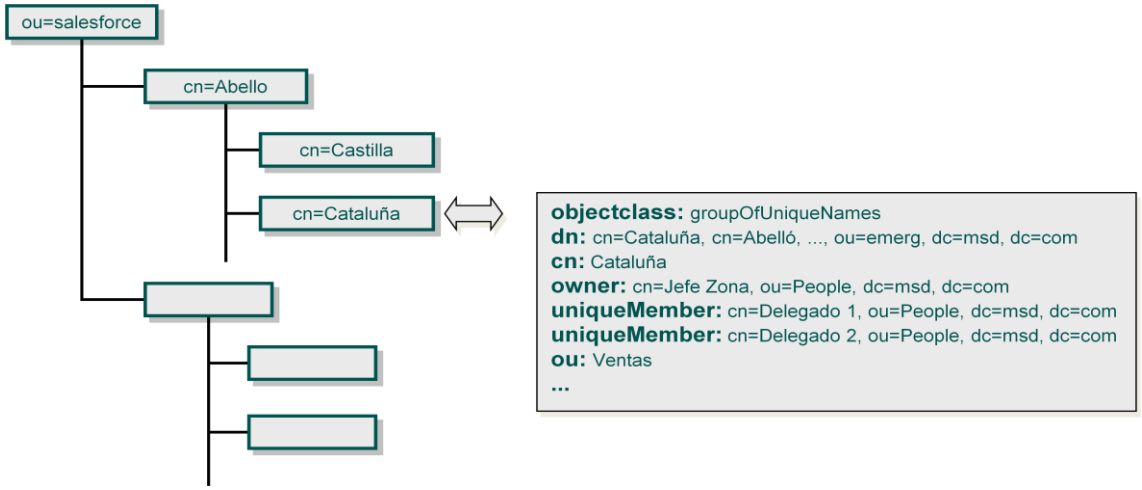

Ilustración x - Esquema de datos de grupos

El modelado de los grupos de negocio se hará a través de agrupaciones de usuarios del negocio, y serán mostradas a las aplicaciones para que hagan uso de ellas.

Estos datos serán de **lectura/ escritura.**

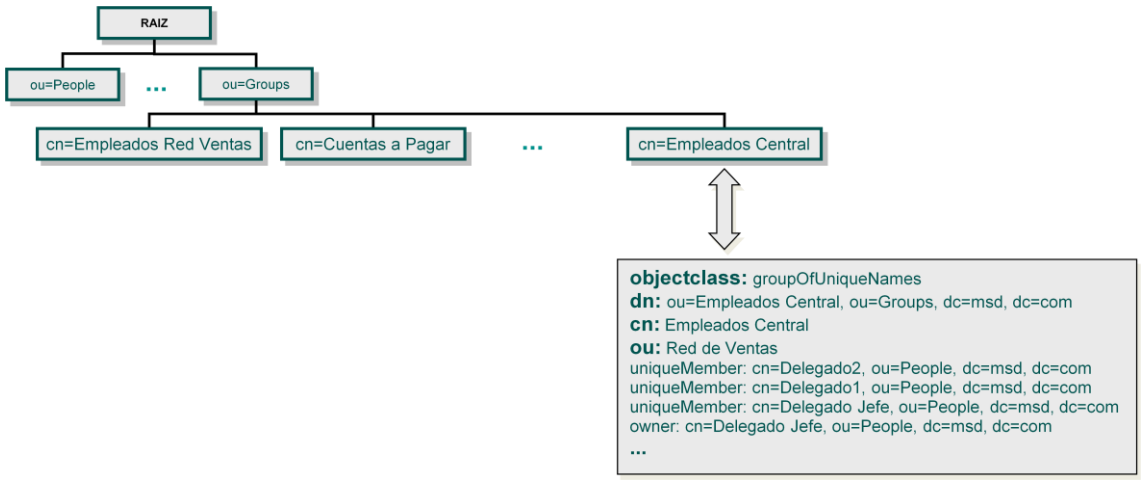

Ilustración y - Atributos del esquema de grupos

Para modelar los grupos se usa el objectclass estándar groupOfUniqueNames, y para facilitar el acceso de aplicaciones existentes, se modelarán en un solo nivel.

Esta forma de modelar los grupos de forma centralizada provoca una nueva situación en los grupos: La aparición del Directorio Corporativo consolida la estructura de grupos en un solo repositorio:

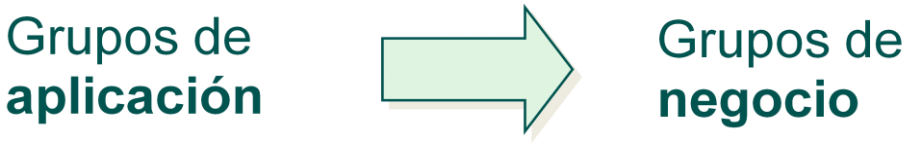

Ilustración z - La consolidación de grupos de usuarios

La transformación de grupos de aplicación a grupos de negocio hace que todas las aplicaciones compartan los mismos grupos, reduciendo la complejidad de administración de cada aplicación.

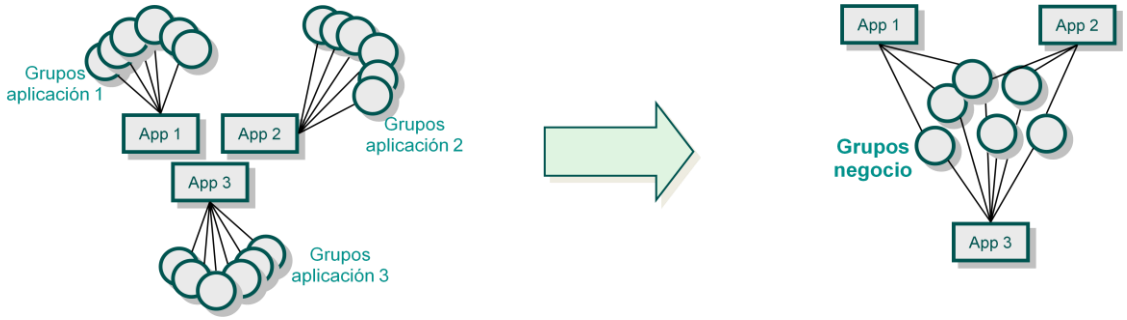

Ilustración aa - De grupos de aplicación a grupos de empresa

Esta pérdida de poder de la aplicación redunda en un beneficio para el negocio, al suprimirse los silos de información inherentes a un sistema de grupos de aplicación.

Esta homogenización de grupos provoca una nueva dificultad en la gestión:

¿Qué define el grupo?

La causa de este problema es que en la empresa existen **diferentes visiones del negocio**. Esto provoca una que dos entidades de igual nombre sean diferentes.

Es decir, la compartición de grupos por diferentes aplicaciones provoca que sea difícil saber **qué** contiene el grupo.

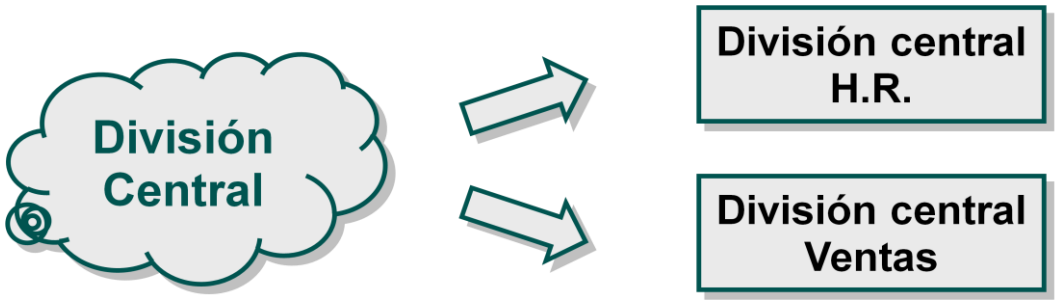

Ilustración bb - Mismo concepto, diferentes visiones

La gestión de grupos requiere de un responsable de cada grupo que defina y mantenga ese grupo.

Los grupos serán la herramienta básica de personalización de contenidos para los usuarios, la cual se realizará de dos formas:

- La pertenencia de un usuario a un grupo, el cual define una característica (Como por ejemplo, pertenecer al grupo Fosamax definiría el interés de un usuario por todo lo relacionado con el producto Fosamax)

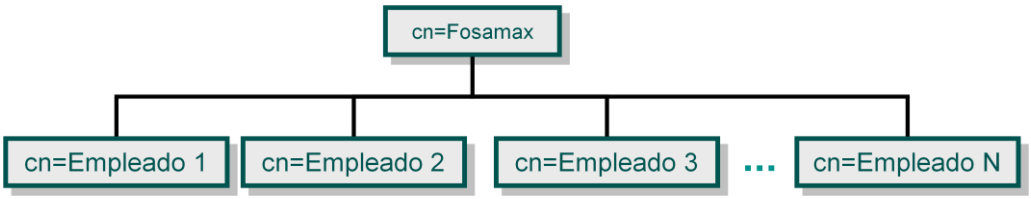

Ilustración cc - Pertenencia jerárquica de usuarios a un grupo

- La existencia de un atributo en la entidad del usuario *(Por ejemplo, la fuerza de ventas a la que pertenece)*

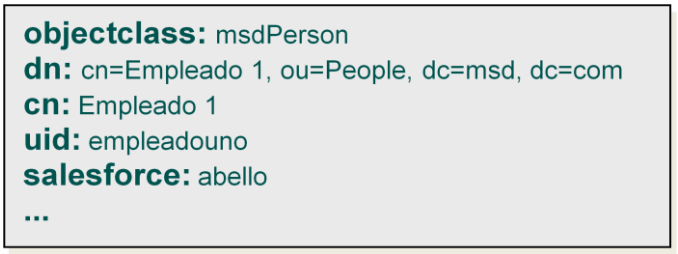

Ilustración dd - Pertenencia por atributo de un usuario a un grupo

Una aplicación desarrollada a medida puede utilizar cualquiera de las dos formas para clasificar a los usuarios, pero las aplicaciones comerciales suelen clasificar a los usuarios por grupos.

Por esta razón la aplicación de carga de datos creará dinámicamente grupos a partir de atributos existentes o condiciones ad-hoc, con el objetivo de facilitar la clasificación de usuarios para las aplicaciones existentes.

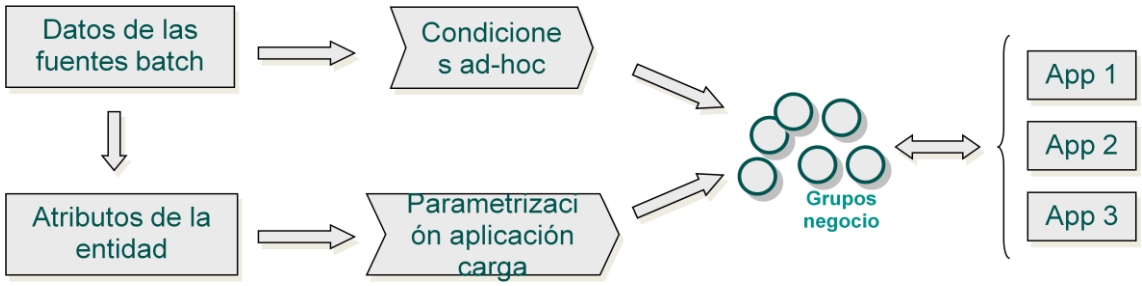

Ilustración ee - Consolidación de datos de múltiples fuentes para crear grupos de negocio

En la fase de implantación de proyecto se definirán, entre otros, los siguientes grupos, y se incluirán a los empleados que pertenecen a ellos:

- Departamentos de PeopleSoft
- Los grupos relacionados con la fuerza de ventas (Genesys), incluyendo:
  - Fuerza de venta, distrito
  - CC.AA., Provincias, Bricks
  - Productos promocionados
- Centros de coste
  - Grupos de centros de coste que puede visualizar un empleado
  - Centros de coste a los que imputa un grupo de empleado
- Pertenencia de un empleado a servicios centrales o red de ventas
- Categoría laboral
- Employee Class del empleado
- ...

Esta definición de grupos es parametrizable en el proceso de carga, y deberá ser objetivo de negocio definir y mantener los grupos de usuarios con el objetivo de poder gestionar el acceso a las aplicaciones y la entrega de contenidos personalizados a los usuarios.

Para la gestión de los árboles jerárquicos se ha seguido el siguiente modelo:

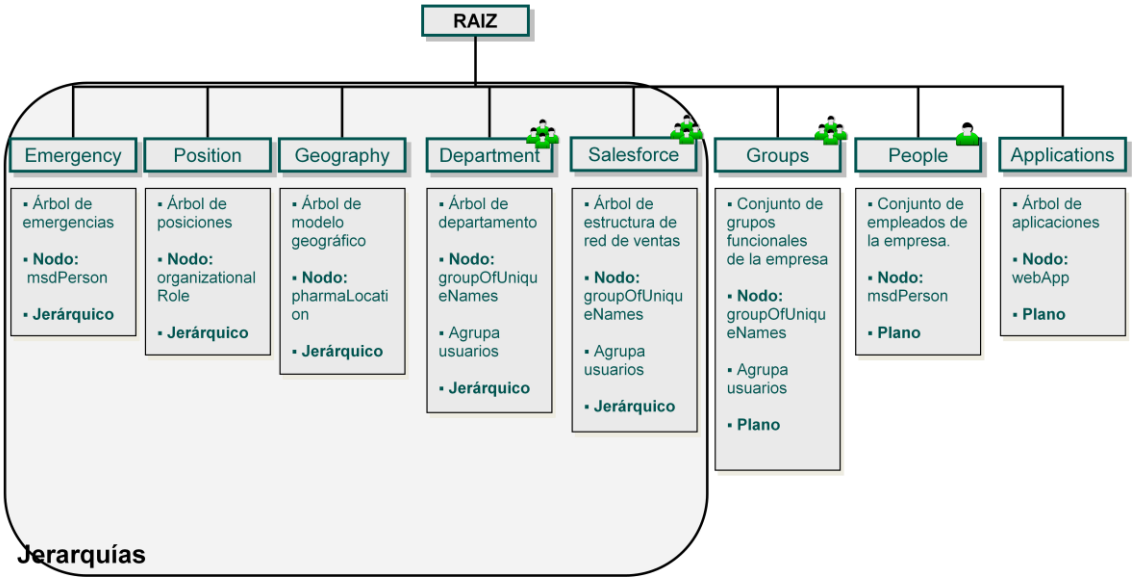

Ilustración ff - Modelo de datos de jerarquía

Los árboles jerárquicos son aquellas estructuras que mantienen **información sobre las relaciones entre diferentes objetos** del directorio:

Provenientes en modo Batch de sistemas heredados: Árbol de posiciones, árbol de emergencias, geografía de ventas.

Ilustración gg - Proceso de carga de datos de jerarquías

Los datos de geografía de ventas, árbol de posiciones y emergencias no podrán ser modificados por las aplicaciones on-line ya que sus aplicaciones maestras son PeopleSoft y Genesys.

El modelado de posición de empleado extrae la estructura de posiciones de recursos humanos a partir de los datos de PeopleSoft. Estos datos serán de sólo lectura.

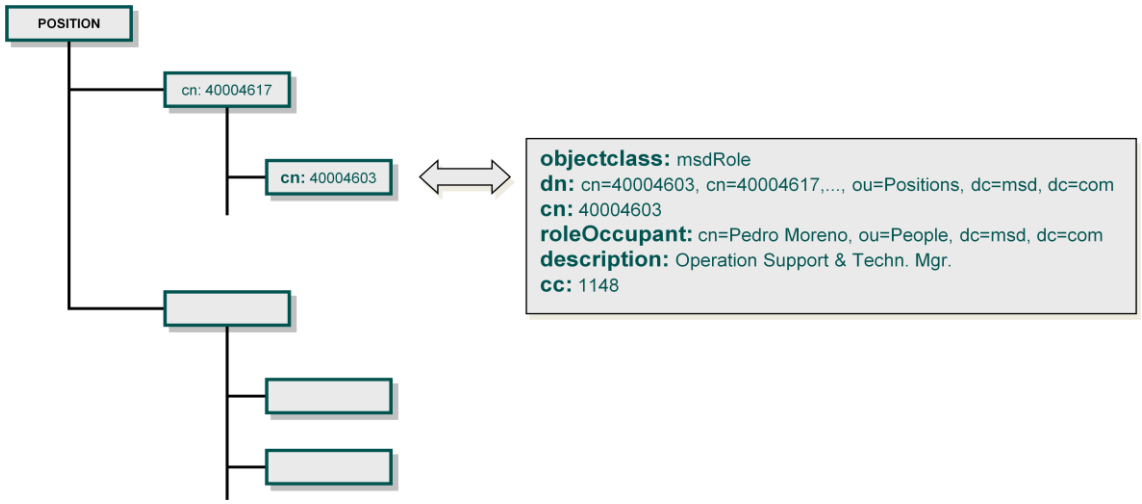

Ilustración hh - Esquema de msdRole

msdRole es una especialización de organizationalRole al que se le añade el centro de coste proveniente de PeopleSoft.

Los contactos de emergencia (relación de empleados en caso de emergencia) se modela a partir del árbol de posiciones extraído de PeopleSoft. Estos datos serán de sólo lectura.

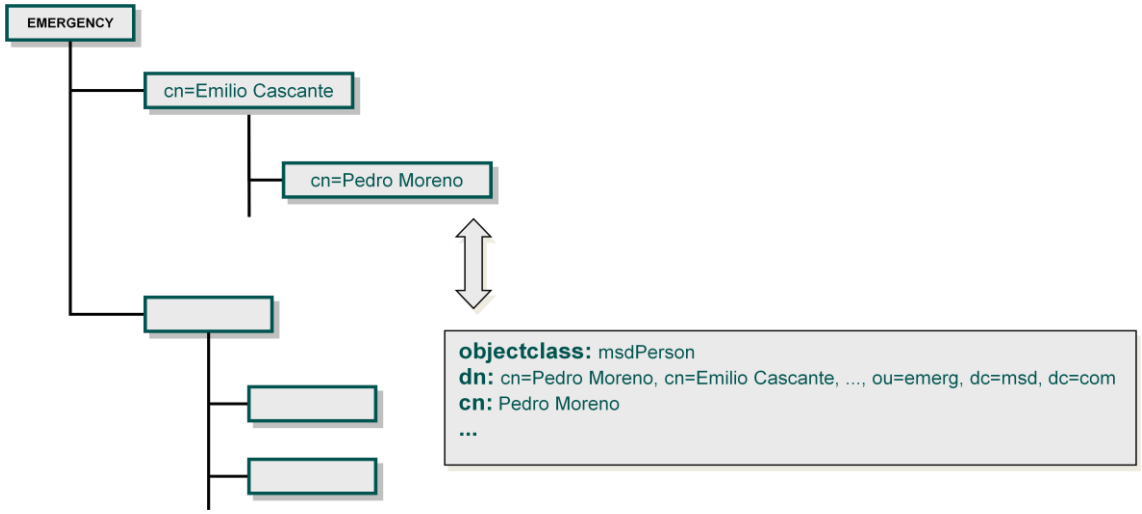

Ilustración ii - Esquema de msdPerson para contactos de emergencia

msdPerson es una especialización de inetOrgPerson al que se le añaden los atributos necesarios para el cliente.

La integración con la API en java permitirá que fácilmente sea posible obtener las relaciones entre los empleados en el árbol de emergencia.

Para la estructura geográfica de IMS se extraerán los datos de Genesys. Estos datos serán de sólo lectura.

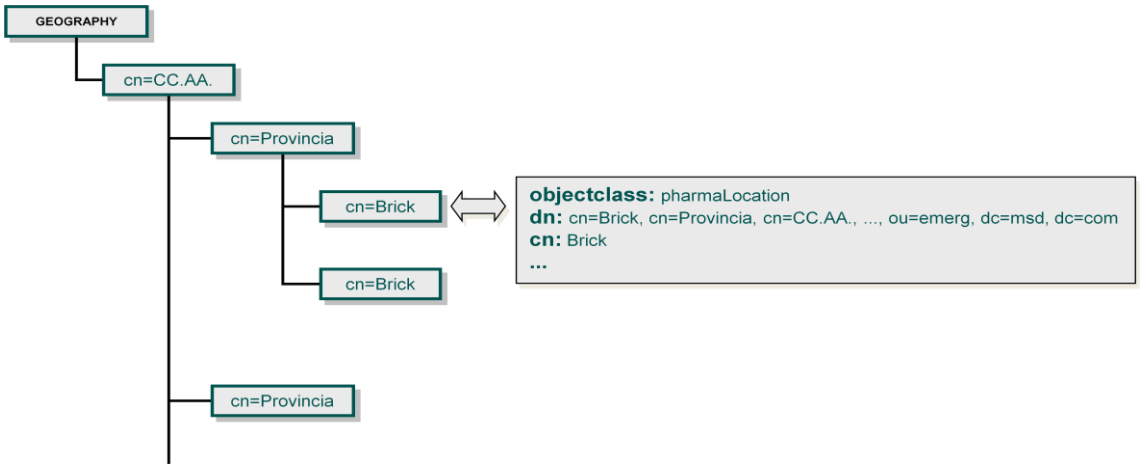

Ilustración jj - Esquema de datos geográficos

Las estructuras de geografía red de ventas se modelarán a partir del objectclass pharmaLocation y su estructura será: estructura será Zona, CC.AA., Provincia, Brick.

También se han modelado las aplicaciones en el Directorio Corporativo con la siguiente estructura:

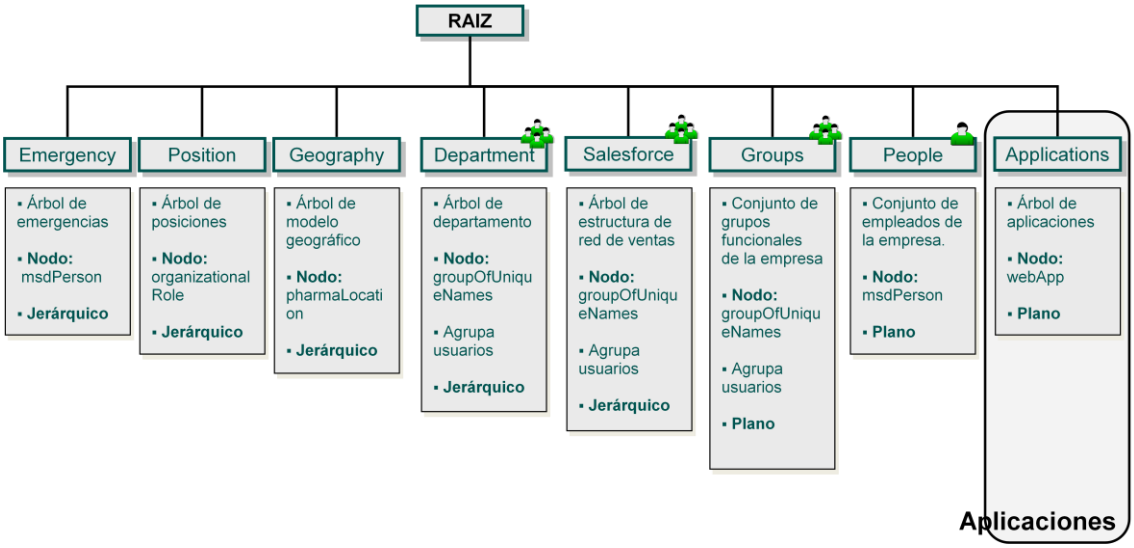

Ilustración kk - Modelo de datos de aplicaciones

Los datos que las aplicaciones deseen utilizar para controlar el acceso o personalizar los contenidos del usuario serán guardados en esta rama del Directorio Corporativo.

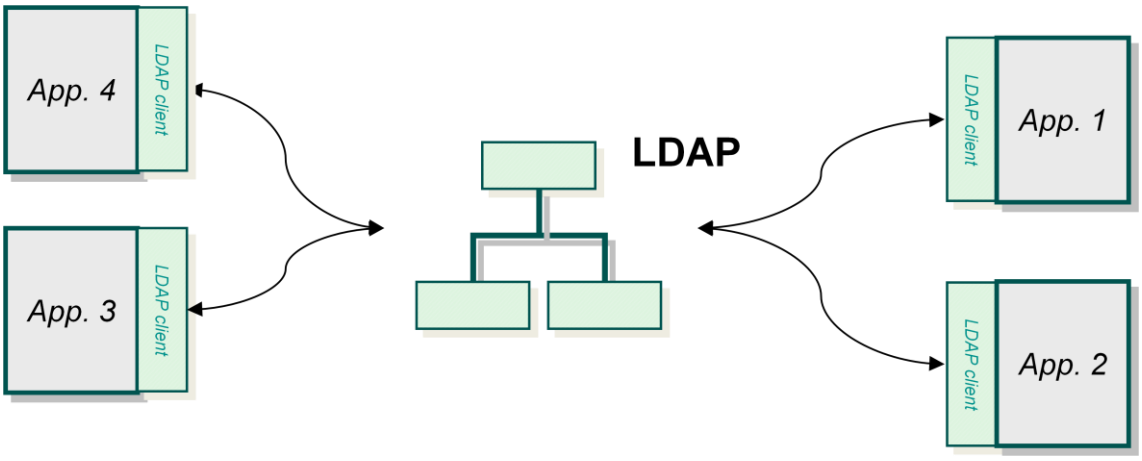

Ilustración ll - Acceso on-line de las aplicaciones al Directorio Corporativo

Los datos de aplicaciones podrán ser creados y editados por la aplicaciones on-line ya que esas aplicaciones on-line son maestras de esos datos. No se alimentarán datos *de aplicación* desde fuentes batch.

El objetivo es modelar las aplicaciones existentes en el negocio, así como los usuarios que pueden acceder a ellas y los perfiles de acceso de esos usuarios.

Estos datos serán de lectura/ escritura.

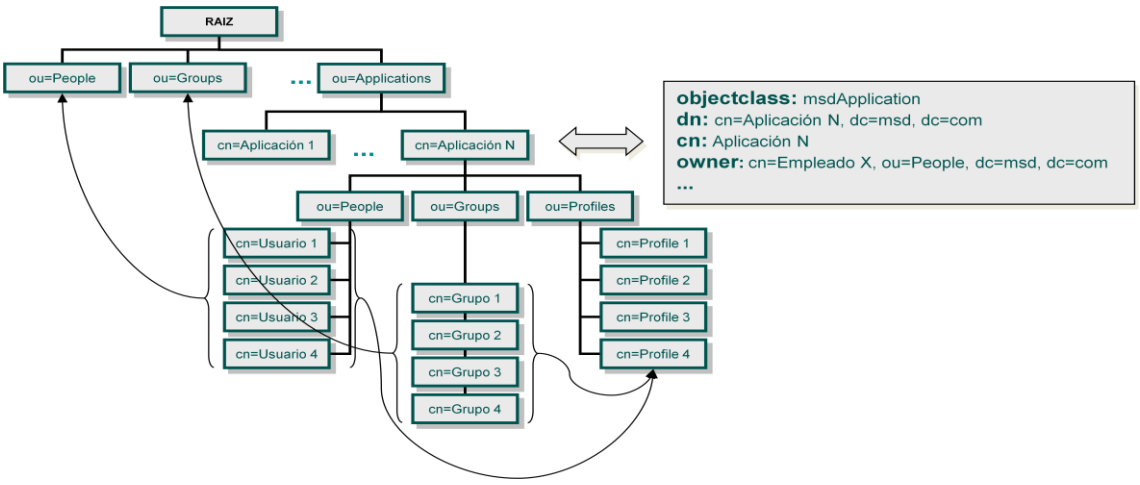

Ilustración mm - Relaciones entre las entidades de datos de las aplicaciones

Para modelar las aplicaciones se usa el objectclass msdApplication, junto con msdApplicationUser y msdApplicationProfile para modelar los usuarios y sus perfiles en la aplicación.

El modelo de datos para las aplicaciones permitirá la gestión de usuarios, grupos de usuarios y perfiles de forma que, una aplicación podrá:

- Almacenar usuarios y grupos particulares a cada aplicación, referenciado los existentes en las ramas de People y Groups, de forma que controle el acceso de los usuarios y grupos de la empresa a la aplicación.
- Asociar a esos usuarios y grupos de usuarios, independientemente a aplicación, de forma que esos usuarios o grupos tienen unas características propias que permiten a la aplicación controlar el acceso a diferentes áreas o personalizar el contenido del usuario/grupo.
- Filtrar el acceso a la aplicación para usuarios concretos, permitiendo excluir de acceso a la aplicación a usuarios concretos.

Así pues, la visión general del árbol es la siguiente:

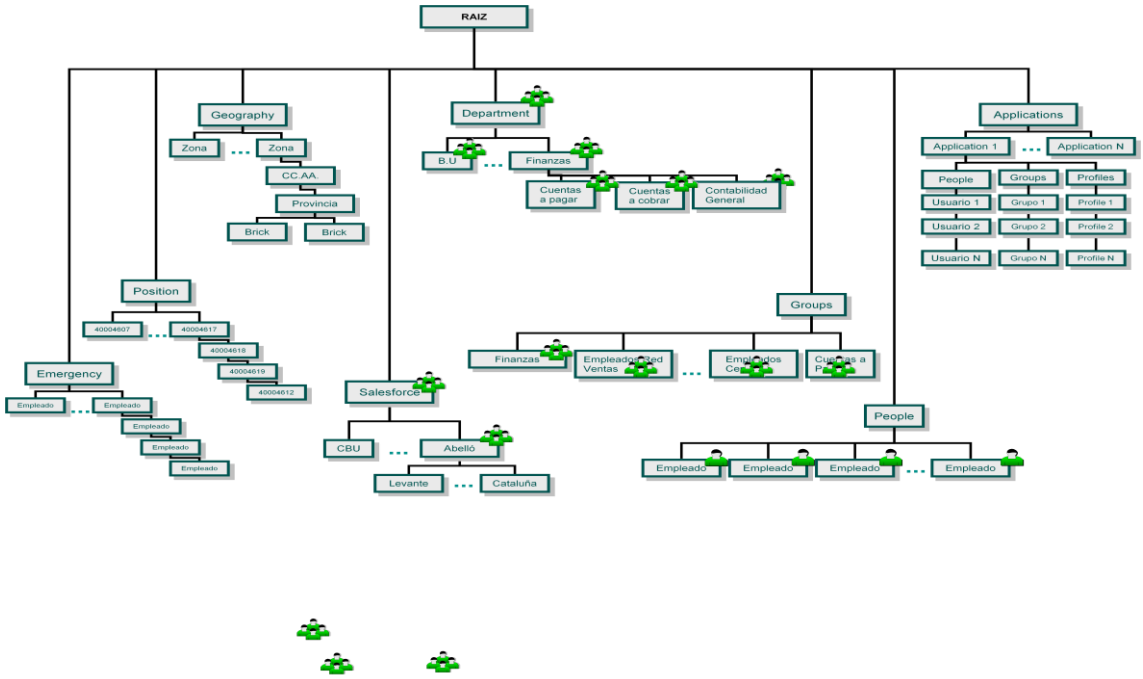

Ilustración nn - Modelo general del Directorio Corporativo

7.3.3.1.6 ¿Qué implica el Directorio Corporativo para el área de sistemas del cliente?

La llegada del LDAP provoca que aparezcan algunos nuevos procesos en la empresa y otros se vean modificados:

- Procesos de actualización y uso de datos del LDAP
  - Carga batch de datos provenientes de fuentes de datos existentes
  - Uso del LDAP por parte de aplicaciones
  - Actualización de los datos desde fuentes de datos existentes
  - Proceso de modificación de esquema
  - Crear objectclass nuevo o añadir un atributo a un objectclass existente

    - Re arrancar el servicio
    - Añadir el proceso de carga de datos de la nueva fuente
- Procesos de desarrollo
    - Crear la estructura de la aplicación en el LDAP
    - Uso del LDAP por parte de las aplicaciones para controlar acceso y personalizar contenidos
- Procesos de modificación del esquema
    - Modificar un objectclass o crear uno nuevo
    - Reiniciar el servidor de LDAP
    - Modificar el proceso de carga para añadir esta nueva fuente
- Procesos de adquisición de software
    - Verificación que el software hace uso del LDAP
    - Verificación que el software puede usar el esquema del cliente.

7.3.4 Interfaces y procesos de carga de datos

Se necesitaron usar interfaces para cargar datos iníciales y para mantener el Directorio Corporativo sincronizado:

- DaWa:

  Durante las reuniones de análisis se identificó que la gran mayoría de datos necesarios pasaban a través del Data Warehouse de la compañía.
  Afortunadamente este Data Warehouse era una instancia de BB.DD. Oracle con acceso a través del cliente de Oracle utilizando consultas SQL estándar.
  Esto permitió definir una forma de acceso sencilla y directa a los datos de interés, sin tener que desarrollar complejos interfaces.
  Desafortunadamente, la frescura de datos estaba limitada al ciclo de refresco de datos en el Data Warehouse, que no siempre era la más ideal para el Directorio Corporativo.

- Dominio de Windows

  Adicionalmente fue necesario definir un interface al dominio de Windows con el fin de verificar que el password introducido era el

correcto. El acceso al password de Windows se realizaba en modalidad on-line y el Directorio no almacenaba el password, si no que accede directamente al Dominio de Windows cada vez que un usuario necesita hacer login en el Portal Corporativo.

7.3.4.1 Actualización y usos de datos

La actualización y uso del Directorio Corporativo se basa en tres grandes procesos:

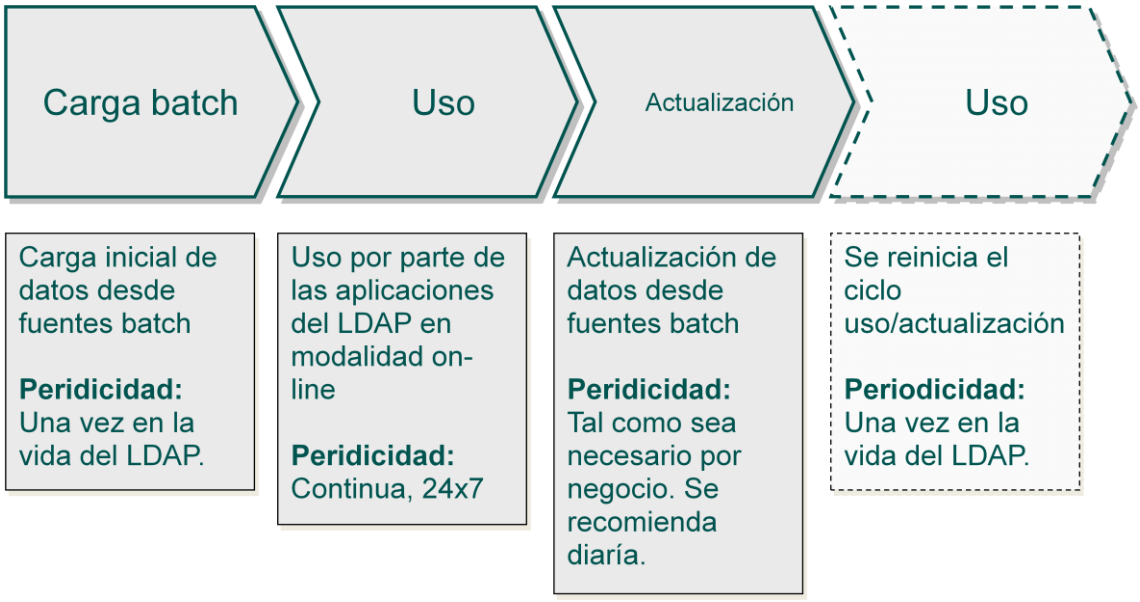

Ilustración oo - Procesos de actualización y uso de datos

7.3.4.1.1 Carga Batch

- El proceso de carga batch es el encargado de cargar contenidos el LDAP por **primera vez**.
- Este proceso vuelca los datos de las aplicaciones aportadoras que no tienen interface directo con LDAP.
- Para esto, EDS desarrollará un proceso de carga de datos.
- Este proceso deberá lanzarse una sola vez.

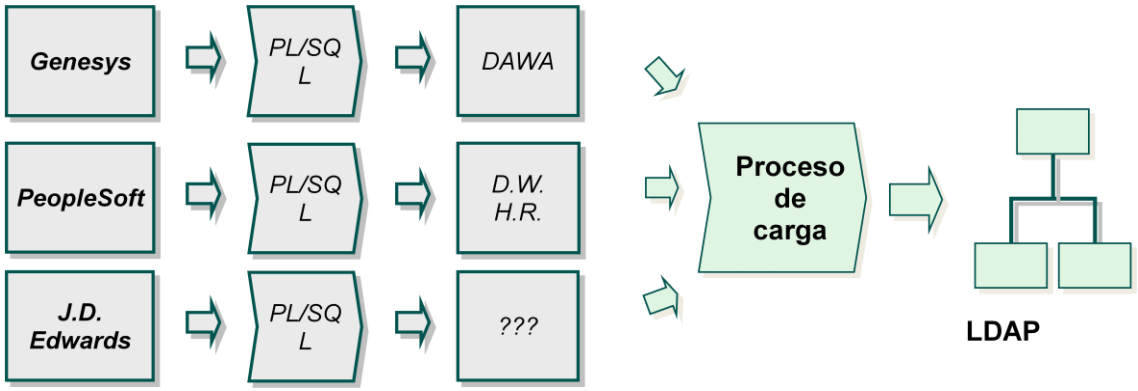

Ilustración pp - Proceso de carga de datos

7.3.4.1.2 Uso

El proceso de uso on-line se divide en diferentes **subprocesos**:

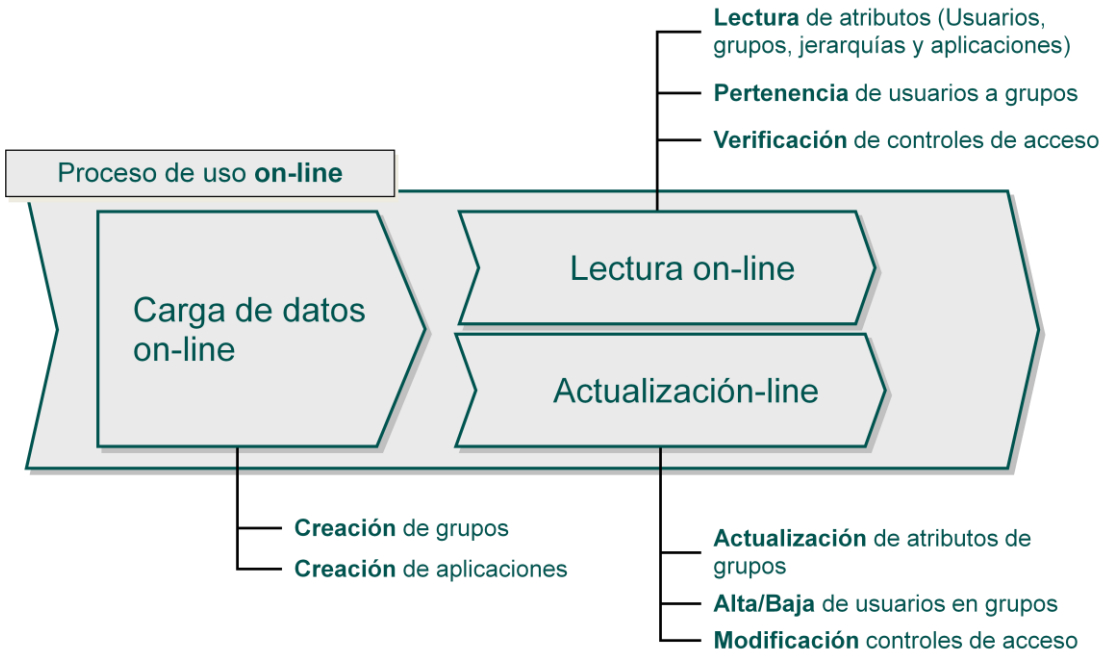

Ilustración qq - Procesos de uso del Directorio Corporativo

El proceso de actualización es el encargado de refrescar los datos contenidos en el LDAP.

Las premisas principales son:

- Las jerarquías y usuarios no son modificables por las aplicaciones on-line.
- Las aplicaciones no son modificables por los procesos batch.

Pero... ¿qué ocurre con los datos (los grupos) cargados en batch y que pueden ser modificados por las aplicaciones on-line?

El responsable del grupo define cual es el sistema primario: la aplicación batch, la aplicación que actualiza los datos en LDAP o si van a trabajar 'agregados'

En caso que el primario sea batch, se restauran los usuarios del grupo en el LDAP tal como están en el sistema batch, sobrescribiendo los cambios realizados por el on-line. (o se define el grupo como sólo lectura para on-line)

Ilustración rr - Carga de datos batch

En caso de que el primario sea el sistema on-line, se realizará una carga inicial desde batch y no se actualizarán los usuarios desde batch.

Ilustración ss - Carga de datos on-line

En caso de que se deseen agregar datos, el proceso batch no agregará los usuarios borrados por el on-line, pero añadirá los nuevos usuarios que lleguen desde el sistema batch.

Ilustración tt - Carga de datos agregando batch y on-line

7.3.4.1.3 Proceso de modificación del esquema

El proceso de uso on-line se divide en diferentes **subprocesos**:

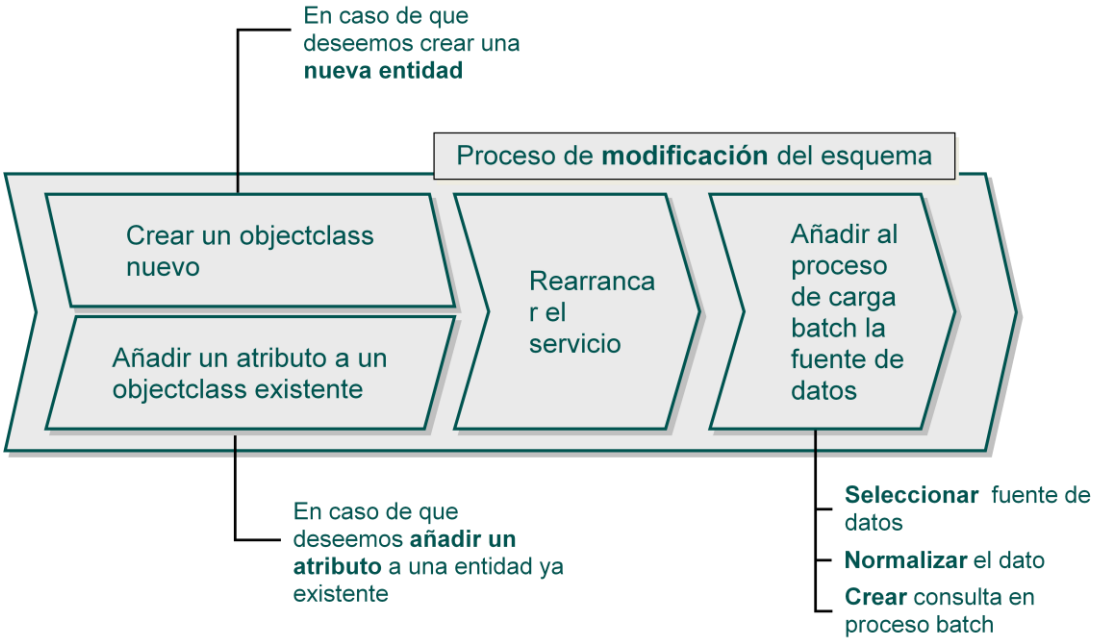

Ilustración uu - Proceso de modificación del esquema

7.3.4.2 Procesos de desarrollo

Que procesos debe seguir desarrollo para usar el Directorio Corporativo.

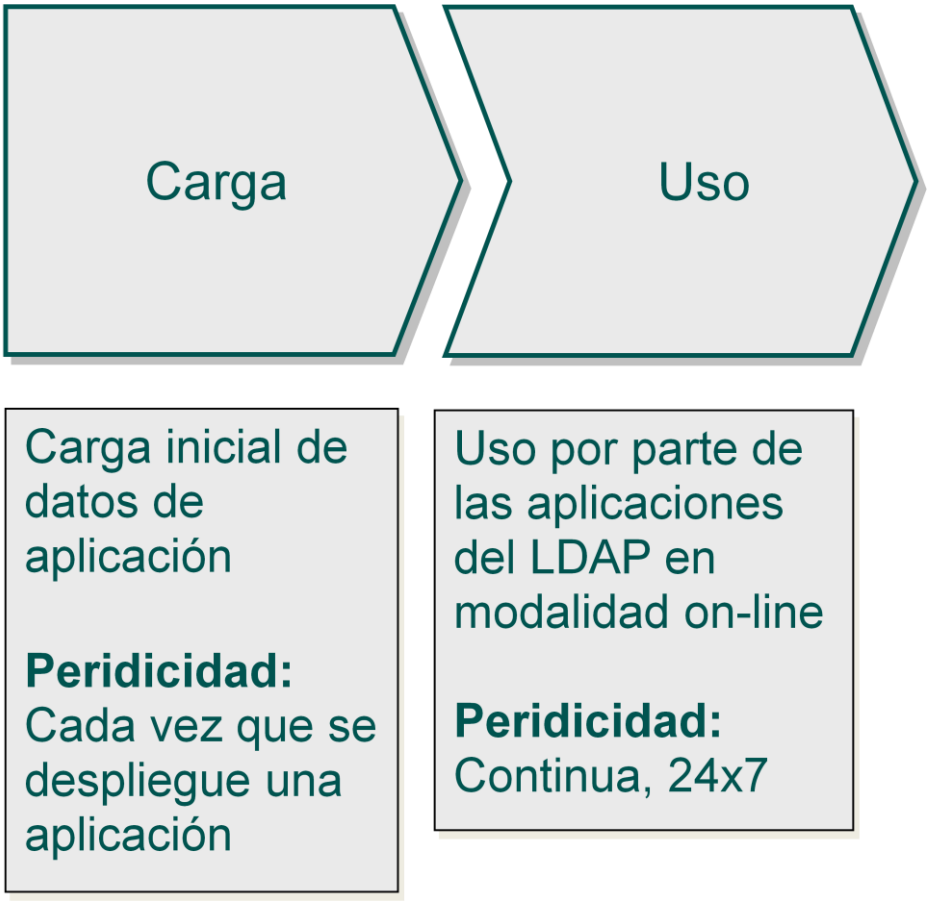

Ilustración vv - Procesos de desarrollo

El proceso de carga es el encargado de crear las estructuras necesarias para que una aplicación haga uso del LDAP. Esto se podrá realizar a través de la API entregada o directamente con un browser de LDAP.

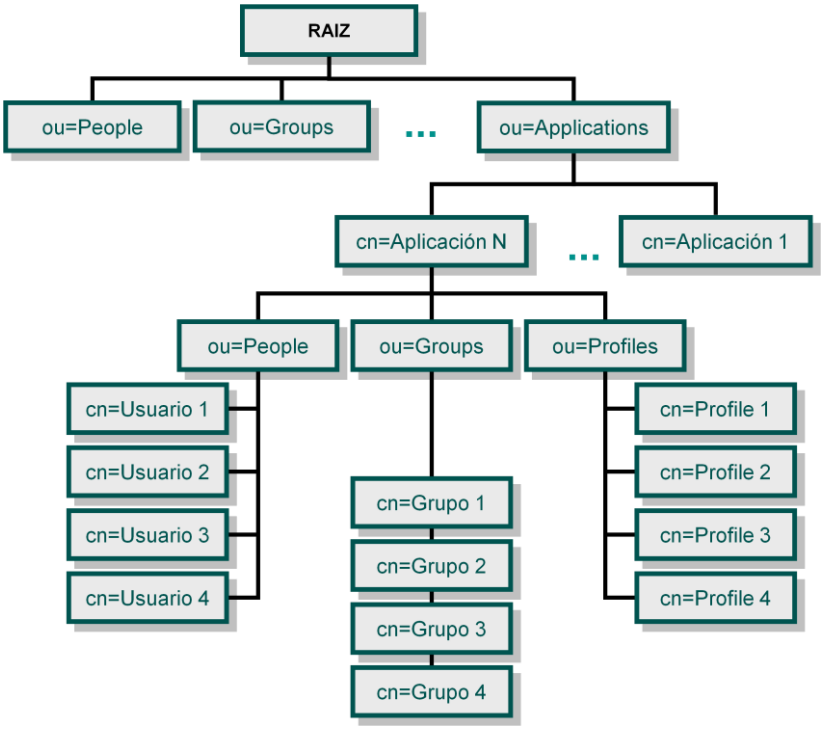

Ilustración ww - Modelo de datos para aplicaciones

Las acciones son a realizar son:

- Crear la aplicación con sus atributos descriptivos
- Crear las ramas de usuarios, grupos y privilegios
- Añadir usuarios, grupos y privilegios

7.3.4.2.1 Proceso de uso online de desarrollo

El proceso de uso on-line para desarrollo se divide en diferentes subprocesos:

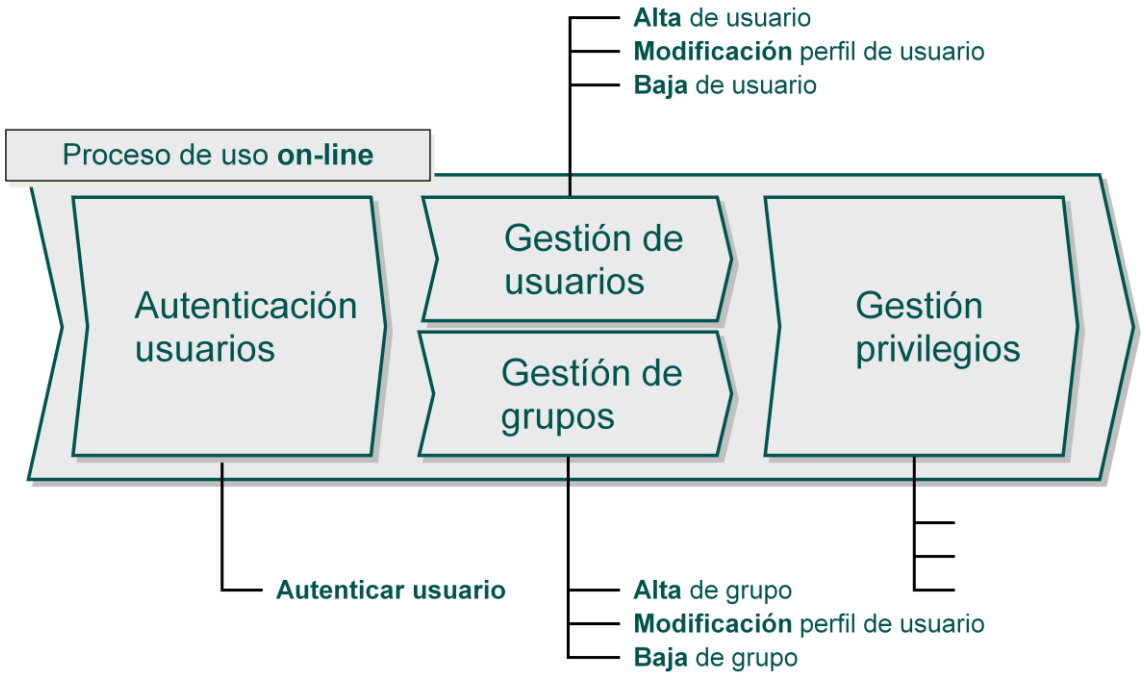

Ilustración xx - Modelo de uso de datos on-line para desarrollo

7.3.4.2.2 Proceso de adquisición de software

El proceso de adquisición de software que requiera acceso al directorio se divide en dos subprocesos.

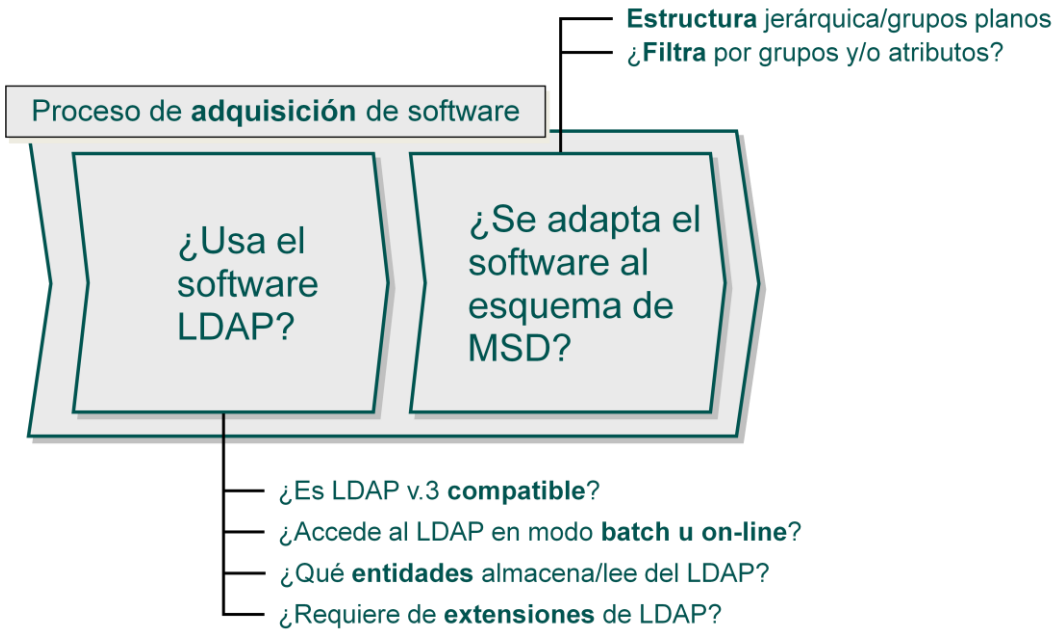

Ilustración yy - Proceso de adquisición de software

7.3.4.3 Proceso de gestión de externos (personal no contratado)

Durante el análisis se ha detectado que los empleados externos deben ser incluidos en el LDAP, pues hacen uso de aplicaciones y servicios de igual forma que un empleado.

No existe ninguna fuente de datos fiable de donde obtenerlos, ni ninguna aplicación pensada para gestionar ese tipo de datos, por lo que la única posibilidad es unificar diferentes fuentes:

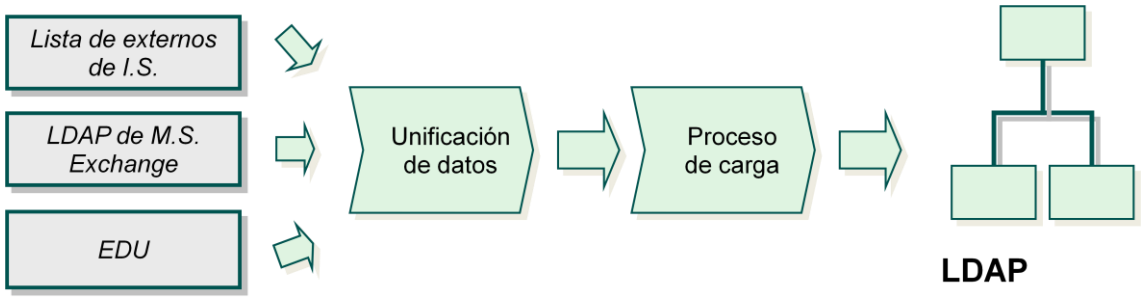

Ilustración zz - Proceso de incorporación de datos de empleados externos

Aún así ninguna solución tecnológica será satisfactoria si el cliente no acepta la realidad de este tipo de empleados en toda su complejidad:

- Aceptar la necesidad de gestionar este tipo de dato
- Definir una fuente de datos autoritativa o usar LDAP como fuente primaria de datos para externos
- Negocio debe liderar este objetivo

7.3.5 Seguridad

Para el modelo de seguridad se utilizó el modelo por defecto de OpenLDAP basado en ACLs (Access Control Lists) para cada elemento almacenado en LDAP.

Este modelo permite que todos los usuarios puedan acceder a los datos de los demás, pero no modificarlos.

El password es una excepción a esta regla. El único usuario que puede cambiar el password es el propietario del mismo. Todo el resto de usuarios tienen vetado este acceso.

El administrador del sistema puede realizar cualquier modificación sobre el directorio.

Las ACLs son atributos del LDAP.

Adicionalmente, toda la infraestructura física fue hospedada en el centro de datos del cliente, con control físico de acceso.

7.4 IMPLANTACIÓN

En este proyecto se decidió trabajar con tres entornos: desarrollo, test y producción.

Todas las modificaciones del sistema, desarrollos y configuraciones, se realizan en el entorno de desarrollo.

Cada vez que se realiza una modificación en este entorno, esta se documenta y proceduriza en un proceso llamado cambio de entorno. Lo común es organizar los cambios de entorno de tal forma que se tenga el control absoluto de lo que contiene cada una de ellos. De esta forma, cuando llegue el momento de mover las modificaciones a otros entornos (test, productivo) se reduce el riesgo de problemas.

Estos cambios de entorno suelen gestionarse con una hoja Excel donde se especifica al menos la siguiente información:

- Código del cambio de entorno.
- Descripción.
- Sistema al que se aplicará.
- Tipo (Personalización, desarrollo, anotación)
- Estado.

La forma de trabajar a partir de este momento es la descrita en el apartado 3.3.3 Gestión de Cambios y Transportes.

Se realizan unas pruebas unitarias mínimas en el entorno de desarrollo y para unas pruebas más completas, con datos reales, se mueve el cambio a test.

Siguiendo el Mapa de Datos y Procesos se van detallando las modificaciones que son necesarios (aquellos requerimientos no cubiertos por el estándar) y se crea para cada uno de ellos un diseño funcional. Esto no es más que un documento para los analistas de datos en los que se explica el requerimiento con detalle suficiente. No se mueve todo a productivo hasta la fase de preparación final.

7.5 PREPARACIÓN FINAL

7.5.1 Formación a usuarios Clave

Estos usuarios tiene un papel muy importante durante todo el proyecto ya que (tal y como se explica anteriormente) participan en las siguientes tareas:

- Participación en las reuniones de toma de requerimientos para explicar procesos en los que están involucrados y que deben aparecer en la aplicación a crear.
- Participación en reuniones en las que se explica el seguimiento del proyecto así como se muestran pequeñas presentaciones de la herramienta para ver su avance.
- Participación en el test de integración con el objetivo de obtener la aprobación de la aplicación una vez terminada y antes de su puesta en productivo.
- Recibir la formación de parte del equipo de IT que realiza la implementación de la aplicación.
- Impartir la formación a usuarios finales.

Los usuarios clave, por su implicación en todas las fases del proyecto, son usuarios “avanzados” en la nueva solución de movilidad. Son usuarios que viven la evolución de la aplicación por lo que su formación es más concreta que para los usuarios finales que no la han visto nunca.

Además son usuarios que juegan con la aplicación durante el test de integración por lo que su formación es ciertamente continuada en el tiempo.

Para la formación a los usuarios clave es necesario disponer de una documentación que, pese a no ser la guía de usuario, se acercará mucho. Se crearán lo siguientes soportes para dicha formación:

- Presentación para ser proyectada durante la formación. Este soporte nos servirá para presentar la idea global de la aplicación, los conceptos más importantes, flujos de forma visual, etc.
- Manual de la aplicación. Es un manual de usuario donde por capítulos se explican todos los menús y submenús de la aplicación por procesos de negocio.

• Quick Guide. Fichas que de un vistazo muestran el flujo para realizar los procesos de ventas de los vendedores.

• Hoja de evaluación de la formación. De esta forma se evalúa la forma de dar la formación, tanto en contenidos como en formato. Cualquier comentario es útil para mejorar la formación cara a los usuarios finales.

7.5.2 Documentación

La documentación definitiva que se entrega con el proyecto es:

• Manual de usuario (para administradores) y configuración

Este manual es una guía de referencia para los usuarios de todos los procesos que podrá realizar con la nueva herramienta. Pretende ser un apoyo para ser usado, sobretodo, hasta que el usuario se habitúe a trabajar con la nueva aplicación. Se utiliza de apoyo también durante las formaciones.

Adicionalmente, todos los cambios que se realizan en el sistema quedan documentados en este manual para facilitar el posterior mantenimiento.

A menudo, el equipo que realiza el proyecto de implantación no es el equipo que realizará el mantenimiento de la aplicación. Por esto es tan importante que este manual sea completo y organizado.

7.5.3 Test de Integración

Una vez finalizada la configuración del sistema de tal forma que todos los requerimientos definidos en la fase inicial se han cubierto, se realiza con los usuarios clave el test de integración.

El objetivo de dicho test es analizar la viabilidad de la aplicación, es decir, si es posible funcionar o no con la herramienta tal y como ha sido configurada. La misión de los usuarios clave durante el test de integración es probar todos los flujos de negocio definidos y evaluar si la herramienta los ejecuta correctamente o si por lo contrario echa de menos algún proceso o alguna parte de alguno.

Para la ejecución del test de integración se debe crear la siguiente documentación:

- Presentación del test de integración.
  Permite situar a todos los asistentes al test de integración en el objetivo a alcanzar al final del mismo.

- Manual rápido de usuario.
  Para ayudar al usuario en la agilidad de la ejecución del test de integración. Suelen ser en forma de fichas que el usuario puede luego llevar en sus primeros días con la herramienta.

- Scripts de test.
  Definirán paso a paso cada uno de los procesos. En cada uno de esos pasos se espera que el usuario rellene los resultados obtenidos y en caso de ser distintos a los esperados se reporte la incidencia.

- Lista de Incidencias.
  Durante el test aparecerán algunas incidencias que deben ser documentadas al máximo detalle para ser resueltas en el mínimo tiempo posible. Dichas incidencias deben ser priorizadas y catalogadas para su fácil manejo.

  En esta lista aparece al menos la siguiente información:

  - Número de incidencia.
  - Package (cuando un desarrollador libera una modificación del esquema este se clasifica dentro de un la jerarquía de datos, denominada package)
  - Descripción.
  - Tipo (Desarrollo, Customizing, Nuevo Requerimiento).
  - Prioridad.
  - Status.
  - Comentarios.
  - Reportado por.
  - Responsable del Testing.
  - Desarrollador responsable.

- Evaluación del test de integración.

  Es un documento en el que, al final de cada sesión de test, los implicados expresan su opinión.

- Documento de aceptación de la aplicación.

  Al final del test de integración, los usuarios clave que han participado desde el inicio del proyecto deben elaborar un documento en el que "firmen" la aceptación de la aplicación desarrollada. Es decir, afirmen en este documento que tal y como ha sido desarrollada es válida para el trabajo de los vendedores en su trabajo diario.

7.6 INICIO Y SOPORTE A POST PRODUCTIVO

7.6.1 Migración inicial

Es necesario cargar en el Directorio Corporativo una primera carga de datos con el que alimentar el mismo. Como decisión de arquitectura se decidió no crear un proceso de migración diferenciado al de migración incremental. Por esta razón se utilizó el mismo software que se desarrolló para las cargas incrementales. Esta decisión permitirá replataformar desde cero la solución en caso de desastre con el mismo programa que se usa para las cargas incrementales, reduciendo el coste de formación de administradores y mantenimiento de la solución.

7.6.2 Formación a usuarios

Esta formación corre a cargo de los usuarios clave que son las personas que más fácilmente pueden hacer llegar el mensaje a los usuarios finales. Pese a eso el departamento de IT encargado de la creación de la aplicación debe proporcionar soporte y apoyo en dicha formación.

A diferencia de los usuarios clave, los usuarios finales son personas que no han visto jamás la aplicación, a quienes no se les ha explicado el por qué del cambio y en definitiva quienes más van a "sufrirlo".

Es frecuente que este grupo de usuarios, debido a los motivos expuestos anteriormente, muestren una resistencia lógica al cambio de aplicación. Por ello es crucial que el mensaje le llegue desde los usuarios clave y no desde el

departamento de IT ya que serán capaces de hablar el mismo "lenguaje" que el usuario final para explicar los beneficios del cambio.

La estrategia de formación a usuarios depende en gran medida del negocio, que es quien define de cuántas y qué personas puede prescindir simultáneamente para ser formados. La formación del usuario final estuvo fuera del ámbito del proyecto.

7.6.3 Corte de operaciones

Se entiende por Corte de operaciones (CutOver) el proceso de transición de un sistema a otro nuevo.

Al ser este proyecto una nueva aplicación no fue necesario aplicar el corte de operaciones.

7.6.4 Arranque

El Arranque (Go Live) de la aplicación se realizó en un solo paso (Big Bang).

El requerimiento de total funcionalidad impuesto por el Portal Corporativo obligó a tener el portal disponible antes del arranque de la fase de pruebas del Portal Corporativo.

7.6.5 Soporte a productivo

Después del arranque se define una estrategia de soporte de la aplicación a los usuarios (en nuestro caso, a los administradores y aplicaciones) que lo están usando. En este tipo de arranque escalonado hay dos soportes diferenciados:

- Soporte a los usuarios clave que realizan el primer arranque.
- Soporte después del despliegue masivo de la aplicación.

7.6.5.1 ¿Qué se hace?

Durante el funcionamiento de la aplicación pueden surgir errores que no han sido detectados durante las distintas fases de desarrollo del proyecto. El usuario que detecta un error lo pondrá en conocimiento con el equipo de proyecto

proporcionando el máximo detalle posible para una posible reproducción del

problema.

El equipo de proyecto categoriza y prioriza el error según unos criterios objetivos y según esta clasificación inicia la investigación y posterior resolución.

En las primeras fases de un arranque es común que los usuarios reporten errores que finalmente no lo son. Si de la investigación se deriva que el usuario no sabe realizar un proceso o no entiende el funcionamiento de la solución en un área determinada, se informará de la necesidad detectada de formación. Es posible que cuando se detecta una necesidad de este tipo no sea únicamente para un usuario sino que varios de ellos reporten lo mismo.

En caso de realmente ser un error se diseñará la mejor solución y se implementará siguiendo el flujo normal.

7.6.5.2 ¿Cómo se organiza?

Los usuarios que detectan un error en la aplicación tienen un teléfono disponible del equipo de proyecto para llamar y realizar la consulta. El consultor que recoge el posible error debe ser una persona capaz de solucionar el problema si es solucionable inmediatamente y en caso de no serlo, se le solicita al vendedor que envíe un mail a una dirección de soporte genérica del proyecto para su investigación.

En este e-mail, el usuario deberá enviar la máxima información posible sobre el error detectado y el detalle de los pasos para la reproducción del problema.

Con toda esta información, en una herramienta corporativa destinada a tareas de soporte, se abre una incidencia. La información necesaria para abrir una incidencia es:

- Persona que lo reporta (nombre y número de vendedor).
- Fecha y Hora.
- Descripción corta del problema.
- Descripción larga.
- Pasos para reproducir el error.

Esta incidencia queda grabada en dicha herramienta y después de comunicar la referencia al usuario y asignar la incidencia a una persona del equipo de proyecto, se inicia el proceso de resolución:

- Diseño.
- Implementación / Programación.
- Test.
- Documentación.
- Entrega a los usuarios.

8 RESULTADOS

El resultado más importante obtenido fue que el arranque del proyecto se realizó en la fecha prevista y dentro del presupuesto establecido.

El primer día de la integración entre el portal de empleados fue capaz de conectarse con el directorio corporativo sin ninguna incidencia. Durante un periodo de 30 días el equipo del portal de empleados (ajeno al proyecto) realizó las pruebas de carga y de integración con las aplicaciones desarrolladas a medida sobre el Portal Corporativo.

Tras este periodo se realizó un piloto de 30 días con un área de negocio para realizar las pruebas finales de usuario, verificar que la solución se adaptaba a las necesidades de los empleados de negocio y realizar la formación a los empleados.

Finalmente se arrancó el portal de empleados integrado con el Portal Corporativo recibiendo 800 usuarios el primer día de uso sin ninguna incidencia achacable al Portal Corporativo.

Tras una semana de periodo crítico se dio como finalizado el proyecto tras haberse realizado la formación técnica al equipo de desarrollo.

Durante el tiempo que se dio soporte a la aplicación, el número de incidencias fue muy reducido (inferior a 1 al mes). La mayoría se debía a problemas de calidad de datos que al provenir de terceras fuentes no cumplían los requerimientos definidos.

Con respecto a la aplicación de carga de datos, esta funciona de forma correcta en las cargas diarias de datos y desde la implantación del proyecto los administradores de sistemas son capaces de parametrizar la aplicación para incorporar nuevas fuentes de datos sin tener que modificar la aplicación.

9 CONCLUSIONES

Al finalizar un proyecto, es importante extraer conclusiones con el fin de no repetir los errores cometidos nos hacen aprender para el siguiente proyecto.

La metodología utilizada en este proyecto tiene una fase opcional de *post-mortem* que desafortunadamente no fue utilizada para este proyecto por petición expresa del cliente.

Afortunadamente, fuimos capaces de identificar los éxitos y errores del proyecto con el fin de reducir los errores y asegurar un mayor éxito en siguientes proyectos.

9.1 OBJETIVOS CUMPLIDOS

Los cuatro objetivos principales expresados en el apartado de Objetivos y alcance del proyecto se consiguen al finalizar el proyecto:

- Se obtiene la certificación del software de directorio de empleados (OpenLDAP) como solución técnicamente compatible con el portal de empleados de Vignette. El set de pruebas que establece la compatibilidad entre el portal de empleados y el directorio de empleados es ejecutado correctamente y sin incidencias.

- Se identifican y añaden los atributos necesarios para añadir al esquema de datos de LDAP, de forma que el directorio de empleados es capaz de almacenar específica al cliente y a su sector.

- Se identificación las fuentes maestras de los datos para cargarlos en el LDAP. De esta forma que se puede mantener actualizado el directorio de empleados con los datos fidedignos.

- Se desarrolla un software de extracción y carga de datos en LDAP en Python el cual es extensible por los administradores del sistema sin necesidad de tener que modificar el código del programa.

9.2 PROBLEMAS SURGIDOS

A lo largo de la ejecución del proyecto han aparecido varios problemas de diferente índole. Unos han sido fácilmente solucionados y otros han necesitado más esfuerzo por parte del equipo. Ninguno ha sido lo suficientemente crítico para parar

el proyecto ni para retrasarlo, razón por lo que el proyecto fue considerado un éxito por el cliente.

- El equipo de aplicaciones existente en la empresa estaba acostumbrado a trabajar con fuentes de datos relacionales y no con la estructura jerárquica de LDAP, lo que supuso un fuerte shock cuando tuvieron que acceder a una fuente de datos carente de un equivalente al JOIN relacional.

- El rendimiento de los procesos de carga se veía fuertemente penalizado por el modelo de datos del Data Warehouse, el fue diseñado para realizar análisis de datos más que para ser una fuente de extracción de los mismos.

- Algunas fuentes de datos eran sistemas heredados cuyo acceso a los datos era 'no standard', bien por no estar documentado, por tener problemas de rendimiento o por requerir un acceso a los datos de forma exclusiva incompatible con el nivel de servicio de la aplicación.

9.3 FUTURAS MEJORAS Y AMPLIACIONES

Durante la ejecución del proyecto, en varias reuniones, fueron surgiendo nuevos requerimientos que quedaron registrados en un de mejora.

Estos nuevos requerimientos fueron estimados por el equipo de proyecto y priorizados por el negocio para crear futuras fases de ampliación de la funcionalidad.

Los proyectos más destacables son:

- Curso de familiarización y uso del directorio corporativo para el equipo de desarrollo.

- Creación de un bus Standard corporativo para dotar al cliente de una solución de intercambio de datos distribuida en tiempo real en lugar de la existente en batch (a través del Data Warehouse). Este proyecto es de especial importancia para aquellos sistemas heredados donde el acceso a los datos era costoso.

- O bien la mejora del modelo de datos del Data Warehouse con el fin de permitir una más rápida extracción y carga de datos del Data Warehouse en el directorio corporativo o bien la modificación de los scripts de carga de datos del Data Warehouse para que generen datos que puedan ser cargados directamente en el directorio corporativo.

10 BIBLIOGRAFÍA

Understanding and deploying LDAP directory services

Timothy A. Howes, Ph. D., Mark C. Smith, and Gordon S. Good

MacMillan Technical Publishing, 1999

OpenLDAP Software Administrator's Guide

The OpenLDAP Project <http://www.openldap.org/>

http://www.openldap.org/doc/

The OpenLDAP Project <http://www.openldap.org/>

Referrals Within the LDAPv2 Protocol

University of Michigan

http://www.openldap.org/pub/umich/ldap-ref.html

University of Michigan

Los RFCs básicos asociados con LDAP son:

RFC1777 - Lightweight Directory Access Protocol. (Obsoletes RFC1487)

RFC1778 - The String Representation of Standard Attribute Syntaxes

RFC1779 - A String Representation of Distinguished Names (Obsoletes RFC1485)

RFC1823 - The LDAP Application Program Interface

RFC1960 - A String Representation of LDAP Search Filters (Obsoletes RFC1558)

RFC 2251 - Lightweight Directory Access Protocol (v3)

RFC 2252 - LDAPv3 Attribute Syntax Definitions

RFC 2253 - UTF-8 String Representation of Distinguished Names

RFC 2254 - The String Representation of LDAP Search Filters

RFC 2255 - The LDAP URL Format

RFC 2256 - A Summary of the X.500 (96) User Schema for use with LDAPv3

RFC2829 Authentication Methods for LDAP.

RFC2830 - Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security.

Otros RFCs relacionados:

RFC1274 - The COSINE and Internet X.500 Schema

RFC1279 - X.500 and Domains

RFC1308 - Executive Introduction to Directory Services Using the X.500 Protocol

RFC1309 - Technical Overview of Directory Services Using the X.500 Protocol

RFC1617 - Naming and Structuring Guidelines for X.500 Directory Pilots (Obsoletes RFC1384)

RFC1684 - Introduction to White Pages services based on X.500

RFC2079 - Definition of an X.500 Attribute Type and an Object Class to Hold Uniform

11 ANEXOS

11.1 GLOSARIO

Cross-Selling: Venta cruzada.
Customer Relationship Management (CRM): Gestión de la relación con los clientes.
Cutover: Corte de operaciones.
Final Preparation: Preparación final.
Firewall: Cortafuegos.
Go Live: Arranque proyecto.
GUI: Graphical User Interface, en español interfaz gráfico para usuarios.
Help: Ayuda.
Off-line: Sin línea. Para que la aplicación pueda funcionar en los pcs de forma autónoma, sin Internet.
Package: Paquete.
Partners: Socios.
Password: Contraseña.
Plugin: Adaptador.
Project Preparation: Preparación inicial.
Prospect: interesado.
Query: Consulta.
Quick Guide: Guía Rápida.
Realization: Implantación.
Reporting: Informes.
Retail: Venta al detalle.
Script: Guión.
Steering Comitee: Comité de dirección.
Support: Soporte.
TI: Tecnologías de la información
Workflow: automatización de etapas de un flujo.

11.2 MANUAL DE USUARIO

A continuación se describen los documentos entregados para los administradores de sistemas que sirvieron como manual de usuario:

11.3 Arranque LDAP

Versiones:

Versión	Fecha	Redactor	Cambios aplicados
1.0	2003-08-10	Roger Sen Montero	Redacción principal

Objetivo del proceso:

El objetivo de este proceso es arrancar el servicio de directorio.

Requerimientos:

Elemento
Disponer del servidor de LDAP instalado. Disponer de las herramientas clientes de LDAP instaladas. Estar loggado como root en la máquina que tiene el LDAP instalado.

Acción:

1. Verificar que el servidor está parado ejecutando:

```
# /etc/rc.d/init.d/ldap status
```

2. Si el servidor está parado, arrancar el servidor:

```
# /etc/rc.d/init.d/ldap start
```

3. Finalmente, verificar que el servidor está arrancado ejecutando:

```
# /etc/rc.d/init.d/ldap status
```
o
```
# /etc/rc.d/init.d/ldap monitor
```

Notas adicionales a la acción:

En caso de que el paso 3 indique que el servidor no esta arrancado, los logs de OpenLDAP en los ficheros (##A definir en el proceso de instalación##)

Comentarios:

Comentarios

11.4 Parada LDAP

Versiones:

Versión	Fecha	Redactor	Cambios aplicados
1.0	2003-08-10	Roger Sen Montero	Redacción principal

Objetivo del proceso:

El objetivo de este proceso es parar el servicio de directorio.

Requerimientos:

Elemento
Disponer del servidor de LDAP instalado.
Estar loggado como root en la máquina que tiene el LDAP instalado.

Acción:

1. Verificar que el servidor está arrancado ejecutando:

```
# /etc/rc.d/init.d/ldap status
```

2. Si el servidor está arrancado, parar el servidor:

```
# /etc/rc.d/init.d/ldap stop
```

3. Finalmente, verificar que el servidor está parado ejecutando:

```
# /etc/rc.d/init.d/ldap status
```

4. Si el servidor sigue ejecutándose, matar el proceso con:

```
# killall slapd
# killall slapd
```

5. Si después del punto 4 el servidor sigue vivo, ejecutar:

```
# killall -9 slapd
# killall -9 slapd
```

Notas adicionales a la acción:

No hay notas adicionales.

Comentarios:

Comentarios

11.5 Monitorización LDAP

Versiones:

Versión	Fecha	Redactor	Cambios aplicados
1.0	2003-08-10	Roger Sen Montero	Redacción principal

Objetivo del proceso:

El objetivo de este proceso es monitorizar el servicio de directorio.

Requerimientos:

Elemento
Disponer del servidor de LDAP instalado.
Disponer de las herramientas clientes de LDAP instaladas.
Estar loggado como root en la máquina que tiene el LDAP instalado.

Acción:

1. Para monitorizar el servicio de directorio, ejecutar:

```
# /etc/rc.d/init.d/ldap monitor
```

2. En caso que se desee monitorizar desde una herramienta externa, se puede lanzar una consulta contra el LDAP utilizando como basedn="cn=Monitor" y recuperandose los atributos que cuelgan de ese "cn=Monitor".
Algunos atributos de interés son:

DN del atributo	Significado del atributo
"cn=Total,cn=connections,cn=monitor"	Conexiones totales
"cn=Completed,cn=Operations,cn=monitor"	Operaciones completadas
"cn=Bytes,cn=Statistics,cn=monitor"	Bytes transferidos
"cn=Add,cn=Completed,cn=Operations,cn=monitor"	Operaciones de añadir registros completadas
"cn=Modify,cn=Completed,cn=Operations,cn=monitor"	Operaciones de modificar registros completadas
"cn=Search,cn=Completed,cn=Operations,cn=monitor"	Operaciones de busqueda completadas
"cn=Compare,cn=Completed,cn=Operations,cn=monitor"	Operaciones de comparación completadas
"cn=Delete,cn=Completed,cn=Operations,cn=monitor"	Operaciones de borrar registros completadas
"cn=Bind,cn=Completed,cn=Operations,cn=monitor"	Operaciones de conexión completadas
"cn=Unbind,cn=Completed,cn=Operations,cn=monitor"	Operaciones de desconexión registros completadas

Notas adicionales a la acción:

No hay notas adicionales.

Comentarios:

Comentarios

11.6 Backup LDAP

Versiones:

Versión	Fecha	Redactor	Cambios aplicados
1.0	2003-08-10	Roger Sen Montero	Redacción principal
1.1	2003-08-13	Roger Sen Montero	Añadido Restore

Objetivo del proceso:

El objetivo de este proceso es realizar el backup y restore de los datos del directorio.

Requerimientos:

Elemento
Disponer del servidor de LDAP instalado.
Disponer de las herramientas clientes de LDAP instaladas.
Estar loggado como root en la máquina que tiene el LDAP instalado.

Acción:

Para realizar el backup:

1. Parar el directorio:

```
# /etc/rc.d/init.d/ldap stop
```

2. Copiar los datos del directorio a un directorio de backup

```
# tar cvf /var/backup/ldap/`date +%Y-%m-%d`.tar \
  /var/spool/ldap/msd-data/*
```

3. Realizar el backup con la herramienta corporativa

4. Arrancar el directorio:

```
# /etc/rc.d/init.d/ldap start
```

Para restaurar el backup:

1. Parar el directorio:

```
# /etc/rc.d/init.d/ldap stop
```

2. Realizar el restore con la herramienta corporativa

3. Copiar los datos del directorio de backup al directorio de datos del LDAP

```
# tar xvf /var/backup/ldap/<filename.tar> \
  /var/spool/ldap/msd-data/
```

4. Arrancar el directorio:

```
# /etc/rc.d/init.d/ldap start
```

Notas adicionales a la acción:

Este procedimiento supone parar el directorio corporativo para realizar el backup. Si no se desea parar el servicio, existen dos alternativas:

1. Realizar replica de datos en un segundo directorio y realizar el backup sobre este directorio.
2. Realizar el backup a nivel de Berkeley DB. Ver más información en: http://www.openldap.org/faq/data/cache/738.html

Comentarios:

Comentarios