# El directorio corporativo

## piedra angular de la infraestructura de *middleware*

Victoriano Giralt  José Alfonso Accino

Servicio Central de Informática
Universidad de Málaga

Granada, 17 de noviembre de 2006

# Índice



# Índice



# Índice



# Trabajo coordinado

## Aunando esfuerzos y plantando semillas

Nuestro objetivo inicial fue que el trabajo que hiciésemos le pudiese servir a otros.

# Trabajo coordinado

## Aunando esfuerzos y plantando semillas

Nuestro objetivo inicial fue que el trabajo que hiciésemos le pudiese servir a otros.

- Esquema IRIS

# Trabajo coordinado

## Aunando esfuerzos y plantando semillas

Nuestro objetivo inicial fue que el trabajo que hiciésemos le pudiese servir a otros.

- Esquema IRIS
- Comité del esquema

# Trabajo coordinado

## Aunando esfuerzos y plantando semillas

Nuestro objetivo inicial fue que el trabajo que hiciésemos le pudiese servir a otros.

- Esquema IRIS
- Comité del esquema
- TF-EMC$^2$

# Trabajo coordinado

## Aunando esfuerzos y plantando semillas

Nuestro objetivo inicial fue que el trabajo que hiciésemos le pudiese servir a otros.

- Esquema IRIS
- Comité del esquema
- TF-EMC$^2$
- SCHAC

# Estructura del árbol y los atributos

## Pinos, bonsais y bosques

Puntos destacables del diseño del árbol de información del directorio.

# Estructura del árbol y los atributos

## Pinos, bonsais y bosques

Puntos destacables del diseño del árbol de información del directorio.

- Árbol somero

**Menos ramas, menos problemas**

Estableciendo una rama para cada tipo de objeto y manteniendo el número de éstos bajo, la administración se simplifica enormemente.
Ante todo, los objetos no suelen cambiar de tipo.

# Estructura del árbol y los atributos

## Pinos, bonsais y bosques

Puntos destacables del diseño del árbol de información del directorio.

- Árbol somero
- Rama única para personas

**Las personas son personas**

Independientemente de la relación que tengan con la Universidad en un determinado momento.
Y no es raro que tengan varios tipos de relación.

# Estructura del árbol y los atributos

## Pinos, bonsais y bosques

Puntos destacables del diseño del árbol de información del directorio.

- Árbol somero
- Rama única para personas
- Clasificaciones

**Jerarquías superpuestas**

Asignando códigos de clasificación, un mismo objeto, puede situarse en diversos lugares dentro de jerarquías diferentes, e incluso, dentro de la misma jerarquía.

# Estructura del árbol y los atributos

## Pinos, bonsais y bosques

Puntos destacables del diseño del árbol de información del directorio.

- Árbol somero
- Rama única para personas
- Clasificaciones
- Privacidad

### DNs opacos

Para evitar la fuga de datos personales, hemos utilizados DNs compuestos por datos opacos, que no se pueden asociar a las personas descritas en las entradas: idnc,dc=uma,dc=es, siendo el idnc un UUID generado al crear la entrada.

# Estructura del árbol y los atributos

## Pinos, bonsais y bosques

Puntos destacables del diseño del árbol de información del directorio.

- Árbol somero
- Rama única para personas
- Clasificaciones
- Privacidad

**Mis datos son mios**

El diseño del atributo de privacidad, permite a los usuarios controlar la publicación de determinada información, accesible de forma abierta a cualquiera.

# Estructura del árbol y los atributos

## Pinos, bonsais y bosques

Puntos destacables del diseño del árbol de información del directorio.

- Árbol somero
- Rama única para personas
- Clasificaciones
- Privacidad
- Autorizaciones

### Quién hace qué

La asignación de privilegios por medio de URNs permite un control fino de los niveles de acceso, tanto de las personas a las aplicaciones, como de las aplicaciones a los datos de las personas.

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador?

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador? la última moda

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador? la última moda
- PDI

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador? la última moda
- PDI

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios?

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos?

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC?

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC? . . .

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC? . . .
- Alumnos

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC? . . .
- Alumnos

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC? . . .
- Alumnos ¿ciclo?

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC? . . .
- Alumnos ¿ciclo? ¿movilidad?

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC? . . .
- Alumnos ¿ciclo? ¿movilidad?
- Eméritos

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC? . . .
- Alumnos ¿ciclo? ¿movilidad?
- Eméritos
- Colaboradores

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC? . . .
- Alumnos ¿ciclo? ¿movilidad?
- Eméritos
- Colaboradores
- Inclasificables

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC? . . .
- Alumnos ¿ciclo? ¿movilidad?
- Eméritos
- Colaboradores
- Inclasificables

# Identificar las fuentes

## ¿están todas las que son y son todas las que están?

Todos tenemos claro dónde están los datos de los miembros de nuestra Universidad ¿verdad?

- PAS ¿PAS investigador? la última moda
- PDI ¿becarios? ¿autonómicos? ¿MEC? . . .
- Alumnos ¿ciclo? ¿movilidad?
- Eméritos
- Colaboradores
- Inclasificables

¿de quién . . . es esta dirección de correo?

# Mantenimiento de los datos externos

## Un árbol de hoja perenne

Las entradas se crean, pero no se destruyen

# Mantenimiento de los datos externos

## Un árbol de hoja perenne

Las entradas se crean, pero no se destruyen (salvo casos de grave error).

# Mantenimiento de los datos externos

## Un árbol de hoja perenne

Las entradas se crean, pero no se destruyen (salvo casos de grave error).

- Transiciones de estado

**Las entradas evolucionan**

Los cambios sobre los datos que se almacenan en el directorio, procedentes de sistemas de registro, se cargan como transiciones desde un estado previo a un nuevo estado.

# Mantenimiento de los datos externos

## Un árbol de hoja perenne

Las entradas se crean, pero no se destruyen (salvo casos de grave error).

- Transiciones de estado
- *Triggers* SQL

**Los sistemas de registro trazan sus cambios**

Se han desarrollado *triggers* y funciones que anotan qué tipo de cambio realizan los sistemas de registro sobre los datos que afectan al directorio. Esta traza se almacena en una tabla de estados, con los mismos datos para todas las personas, pero con diferentes transiciones según el sistema.

# Mantenimiento de los datos externos

## Un árbol de hoja perenne

Las entradas se crean, pero no se destruyen (salvo casos de grave error).

- Transiciones de estado
- *Triggers* SQL
- El problema del enlace

### Unir las entradas con su origen

Es fundamental disponer de un código unívoco y diferenciado para enlazar las entradas del directorio con las entradas origen en los sistemas de registro.

El esquema IRIS no tiene este punto bien solucionado, hecho que se ha corregido en SCHAC.

# Cambios en la forma de autenticar

## El directorio como centro de autorización

El camino hacia una auténtica Infraestructura de Autenticación y Autorización.

# Cambios en la forma de autenticar

## El directorio como centro de autorización

El camino hacia una auténtica Infraestructura de Autenticación y Autorización.

- Aplicaciones web

### Antiguas

Hemos desarrollado un mecanismo de autenticación web cásica que valida contra el directorio para el servidor web que usamos, lo que permite usar las aplicaciones basadas en este tipo de autenticación sin modificar.

# Cambios en la forma de autenticar

## El directorio como centro de autorización

El camino hacia una auténtica Infraestructura de Autenticación y Autorización.

- Aplicaciones web

**Nuevas**

Las nuevas aplicaciones utilizan directamente el directorio para autenticar y autorizar a los usuarios, como paso previo al uso de PAPI y otros mecanismos de federación.

# Cambios en la forma de autenticar

## El directorio como centro de autorización

El camino hacia una auténtica Infraestructura de Autenticación y Autorización.

- Aplicaciones web
- Aplicaciones no web

**Validación contra el directorio**

Se usa para aplicaciones convencionales como el acceso a los buzones, el envío de correo autenticado o el acceso a la red inalámbrica.

# El primer gran proyecto

## Asignar un dueño a cada dirección de correo

Este proceso ha sido clave tanto para el avance del directorio como para la depuración de los datos del mismo.

# El primer gran proyecto

## Asignar un dueño a cada dirección de correo

Este proceso ha sido clave tanto para el avance del directorio como para la depuración de los datos del mismo.

- AA

### Identificar y Autorizar

Hemos optado por utilizar usuarios virtuales, lo que permite diversas funcionalidades y, además, permite que los usuarios se identifiquen con cualquiera de sus direcciones de correo electrónico.

Se utiliza tanto para acceder al buzón como para enviar correo autenticado desde cualquier lugar a través del MTA de la Universidad.

# El primer gran proyecto

## Asignar un dueño a cada dirección de correo

Este proceso ha sido clave tanto para el avance del directorio como para la depuración de los datos del mismo.

- AA
- Encaminar

**Entregar el correo a su destinatario**

Hemos aplicado las recomendaciones de uso del esquema IRIS para encaminar correo, lo que ha conferido una gran flexibilidad al sistema.

# El primer gran proyecto

## Asignar un dueño a cada dirección de correo

Este proceso ha sido clave tanto para el avance del directorio como para la depuración de los datos del mismo.

- AA
- Encaminar
- Almacenar

### Un buzón permanente

Para evitar dependencias de atributos que pueden cambiar por motivos diversos, hemos utilizado el entryUUID para identificar los buzones asociados a las entradas, personales o no, lo que permite modificar y mover la entrada como se desee, sin perder nunca la conexión con su almacen de correo.

# Organizar a las personas
## de formas variadas

Estamos trabajando en varias clasificaciones en este momento.

# Organizar a las personas
## de formas variadas

Estamos trabajando en varias clasificaciones en este momento.
Existe poca información automatizada.

# Organizar a las personas
## de formas variadas

Estamos trabajando en varias clasificaciones en este momento.
Existe poca información automatizada.

- Guía de comunicación

# Organizar a las personas
## de formas variadas

Estamos trabajando en varias clasificaciones en este momento.
Existe poca información automatizada.

- Guía de comunicación
- Departamentos

# Organizar a las personas
## de formas variadas

Estamos trabajando en varias clasificaciones en este momento.
Existe poca información automatizada.

- Guía de comunicación
- Departamentos
- Localización geográfica

# Organizar a las personas
## de formas variadas

Estamos trabajando en varias clasificaciones en este momento.
Existe poca información automatizada.

- Guía de comunicación
- Departamentos
- Localización geográfica
- Áreas temáticas

# No todas las ramas están sanas

## podar e injertar

Hemos conseguido un nivel razonable de salud en la rama de personas.

# No todas las ramas están sanas

## podar e injertar

Hemos conseguido un nivel razonable de salud en la rama de personas.
Aún queda trabajo por hacer en la ramas con entradas no personales.

# No todas las ramas están sanas

## podar e injertar

Hemos conseguido un nivel razonable de salud en la rama de personas.
Aún queda trabajo por hacer en la ramas con entradas no personales.

- Definir claramente los roles de la Universidad.

# No todas las ramas están sanas

## podar e injertar

Hemos conseguido un nivel razonable de salud en la rama de personas.
Aún queda trabajo por hacer en la ramas con entradas no personales.

- Definir claramente los roles de la Universidad.
- Trasladar las entradas no personales a sus ubicaciones definitivas.

# No todas las ramas están sanas

## podar e injertar

Hemos conseguido un nivel razonable de salud en la rama de personas.
Aún queda trabajo por hacer en la ramas con entradas no personales.

- Definir claramente los roles de la Universidad.
- Trasladar las entradas no personales a sus ubicaciones definitivas.
- Eliminar las ramas transitorias.

# Los esquemas no son estáticos
## mejoran con el tiempo

Nuestro objetivo es aplicar los nuevos desarrollos que estimamos valiosos.

# Los esquemas no son estáticos
## mejoran con el tiempo

Nuestro objetivo es aplicar los nuevos desarrollos que estimamos valiosos.

- Migrar el esquema de IRIS a SCHAC, donde sea aplicable.

# Los esquemas no son estáticos
## mejoran con el tiempo

Nuestro objetivo es aplicar los nuevos desarrollos que estimamos valiosos.

- Migrar el esquema de IRIS a SCHAC, donde sea aplicable.
- Mejorar la gestión de autorizaciones. ¿eduPermissions?

# Los esquemas no son estáticos
## mejoran con el tiempo

Nuestro objetivo es aplicar los nuevos desarrollos que estimamos valiosos.

- Migrar el esquema de IRIS a SCHAC, donde sea aplicable.
- Mejorar la gestión de autorizaciones. ¿eduPermissions?
- Desarrollar un registro de URNs

# Resumen

- El directorio es el más vivo de los servicios

# Resumen

- El directorio es el más vivo de los servicios

# Resumen

- El directorio es el más vivo de los servicios, un proyecto sin fin.

# Resumen

- El directorio es el más vivo de los servicios, un proyecto sin fin.
- Las personas son personas.

# Resumen

- El directorio es el más vivo de los servicios, un proyecto sin fin.
- Las personas son personas.
- Las clasificaciones permiten organizar el directorio de muchas formas.