tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

357

# GESTIÓN DE IDENTIDAD CORPORATIVA DE LA CC.AA. DE MURCIA

**Celestino Avilés Pérez**
Técnico Responsable
Dirección General de Informática (Comunidad Autónoma Región de Murcia)

**Manuel Escudero Sánchez**
Director General de Informática
Dirección General de Informática (Comunidad Autónoma Región de Murcia)



Volver

**Celestino Avilés Pérez**
**Manuel Escudero Sánchez**

## Palabras clave

*IDECOR, NOVELL IDENTITY MANAGER.*

## Resumen de su Comunicación

*El continuo crecimiento de sistemas y el incremento de la seguridad hace que cualquier persona necesite identificarse para acceder a una aplicación, a un sistema, etc. La gestión de todo ello se hace cada vez más difícil, el usuario debe recordar cada vez más contraseñas por lo que las simplifica, las escribe... Y todo ello hace que la seguridad del sistema se debilite.*

*Es pues imprescindible la creación de un sistema de gestión de identidades que integre y unifique, por una parte el acceso a los sistemas con una única contraseña segura y fiable y por otra simplifique la gestión de entornos complejos a usuarios avanzados. Asimismo el sistema permite la integración de los servicios electrónicos bajo una única plataforma*

*La DGI pone en marcha este proyecto en tres fases:*

*1. Unificación de contraseñas y autenticación de usuarios*
*2. Autorización*
*3. Single Sign On*



Volver

**Celestino Avilés Pérez**
**Manuel Escudero Sánchez**

# GESTIÓN DE IDENTIDAD CORPORATIVA DE LA CC.AA. DE MURCIA

## 1. Justificación

El proyecto de Identidad Corporativa IDECOR nace como respuesta a la necesidad que tiene esta organización de integrar los servicios electrónicos que ofrece en un sistema de acceso único.

Así, la implantación de nuevas plataformas (portal tributario, administración electrónica, portal web, etc.), hace imprescindible abordar un proyecto de gestión de identidad que permita unificar y gestionar de un modo eficaz la autenticación de los usuarios.

Asimismo, el Plan Estratégico de Sistemas, Comunicaciones y Seguridad de la Comunidad Autónoma de la Región de Murcia establece entre sus proyectos la implantación de un sistema de gestión de identidades.

## 2. Alcance.

El proyecto se circunscribe inicialmente a los sistemas de información responsabilidad de la Dirección General de Informática, si bien no se descarta la posibilidad de que una vez implantado y operativo pueda extenderse al resto de Centros Directivos de la CARM.

## 3. Situación actual.

La propia DGI tiene múltiples directorios sobre los que se autentican los usuarios. Así dispone de:

Servicios de directorio de Novell. Utilizado para autenticación y autorización en los servidores de ofimática. Cada edificio tiene un servidor de ofimática, la gran mayoría de las veces Novell Netware. La contraseña caduca de forma periódica.

Servicios de directorio de Microsoft. Utilizado para la granja de servidores de aplicaciones Citrix. La contraseña nunca caduca, y se tiene una por defecto que hasta hace muy poco tiempo no se podía cambiar.

Servicios de directorio basados en LDAP, para autenticación de servicios de Administración Electrónica.

Servicios de directorio basados en LOTUS Domino, para los usuarios de correo electrónico.

Servicios de autenticación en Oracle, en tablas de base de datos para autenticación de usuarios de aplicaciones.

Directorio SAP, para la entrada a los aplicativos en entorno SAP.

## 4. Problemática asociada.

Este conjunto de múltiples directorios y cada uno con una gestión independiente provoca muchísimos problemas, entre los que resaltan los siguientes:

No se encuentran sincronizados, de forma que se tenga toda la información en todos los directorios.

Cada entorno dispone de una contraseña diferente. Un usuario puede tener la misma en todos, pero no es porque el sistema lo haya hecho, sino porque el usuario ha sido lo suficientemente disciplinado para cambiar la contraseña en todos los sistemas y hacerla lo suficientemente segura como para que todos los



Volver

sistemas la acepten como buena.

Es muy difícil recordar o implantar un conjunto de claves tan grande, por lo que el usuario tiende a simplificarlas, o a escribirlas, por lo que los niveles de seguridad bajan.

Política de contraseñas distintas en cada sistema. Cada sistema tiene una política de contraseña diferente (longitud de la clave, caracteres aceptados, consulta a diccionarios internos, etc.), lo que hace complicado disponer de una sola contraseña que reúna los requisitos de todos los sistemas al mismo tiempo.

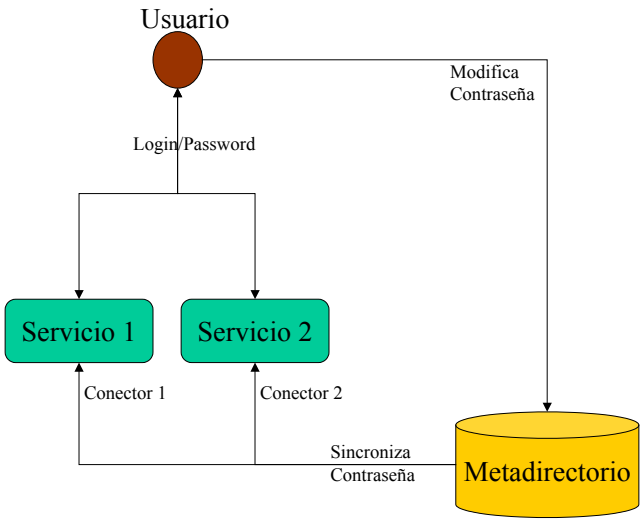
No hay un único entorno en el que cambiar la contraseña de forma que para el usuario sea sencillo tanto su acceso como su gestión.

Es el administrador de sistema el que gestiona la autorización o no de entrar a un sistema o a un servicio, cuando debería ser el responsable de dicho servicio el que se encargara de ello.

Fruto de todas estas reflexiones surge en la DGI el proyecto IDECOR, IDENTIDAD CORPORATIVA, que describimos a continuación

## 5. Descripción del proyecto

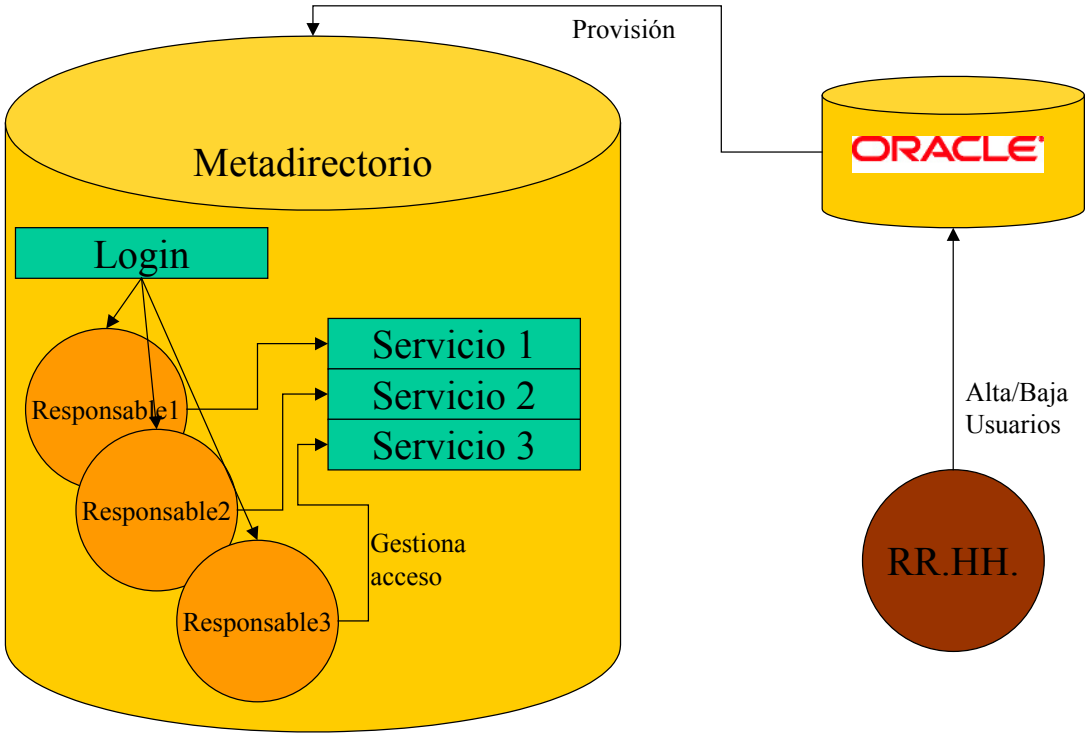
Básicamente el sistema debe funcionar como se indica en la siguiente figura.




- El usuario accede a los sistemas a los que tiene acceso siempre con el mismo login y la misma contraseña.
- La contraseña la puede cambiar siempre que quiera. No en los sistemas, sino en el metadirectorio.
- Es el metadirectorio el que realiza de forma automática los procesos de sincronización con los directorios de cada servicio/sistema.

Desde el punto de vista de la administración, el sistema funciona tal y como se explica en la siguiente figura:

**Celestino Avilés Pérez**
**Manuel Escudero Sánchez**




- Los departamentos de recursos humanos gestionan el alta y baja de usuarios que trabajan en la CARM, y disponen de las herramientas que permiten dar de alta en sistemas de bases de datos Oracle para proporcionar un login único y una dirección de correo normalizada.
- Se establecen mecanismos de carga desde Oracle al metadirectorio, con objeto de tenerlo actualizado.
- Dentro del metadirectorio, los usuarios responsables de cada servicio son los que establecen la posibilidad o no de autenticarse en los mismos.

## 6. Objetivos del proyecto

Los objetivos a cumplir con la implantación del proyecto son:

- Racionalizar los recursos electrónicos.
- Integrar los servicios electrónicos bajo un mismo directorio.
- Reducir el tiempo dedicado a la Administración de usuarios
- Incrementar la seguridad en los procesos de autenticación, autorización y auditoría.
- Consolidar la información de los usuarios en un repositorio.
- Facilitar la administración con la creación de roles genéricos de acceso.
- Delegación de las responsabilidades de autorización de acceso en los responsables de cada servicio o persona en quien delegue.
- Aplicación unificada de mecanismos de control de acceso.
- Integrar en el modelo diferentes servicios.
- Desarrollo homógeneo de las políticas de autenticación y autorización.
- Autenticación única de acceso a servicios.

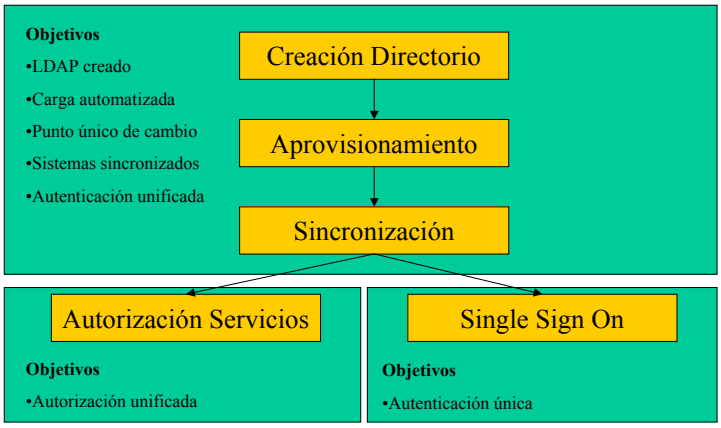
**Celestino Avilés Pérez**
**Manuel Escudero Sánchez**

## 7. Fases del proyecto

Dado que se buscan resultados concretos, consideramos que el proyecto se puede acometer en tres fases diferenciadas.

Así, la primera fase finalizaría en la sincronización con los sistemas. Las otras dos fases pueden realizarse de forma independiente, y cada una en un momento diferente o las dos al mismo tiempo.

Fases reales




### Fase 1.- Metadirectorio. Creación, aprovisionamiento y sincronización.

Tras la finalización de esta fase, se dispondría de:

- Un metadirectorio creado e implantado, flexible, escalable y extensible a toda la Organización
- Unos sistemas de carga automática de los datos desde donde se originan.
- Un aplicativo Web que permita a un usuario cambiar la contraseña.
- Unos procedimientos y programas de sincronización con los servicios que se consideren,
- Un modelo para seguir creciendo en sincronización de servicios extensible a otros Centros Directivos.
- Un sistema completo de autenticación unificada.

### Fase 2.- Autorización de Servicios.

Tras esta fase, dispondríamos de:

- Un aplicativo Web que permita gestionar, para cada programa, las autorizaciones en un entorno homogéneo.
- Un modelo escalable a todos los servicios y aplicativos que se consideren.

### Fase 3.- Single Sign-On.

Al finalizar los trabajos se habrían conseguido cubrir los siguientes objetivos:

- Una plataforma unificada para autenticarte frente a los sistemas y aplicativos.
- Un modelo desplegable al resto de la Organización.
- Un modelo extensible a nuevos servicios.

**Celestino Avilés Pérez**
**Manuel Escudero Sánchez**

## 8. Conclusiones

El proyecto IDECOR nos va a permitir fundamentalmente tres cosas:

Incrementar la seguridad en los sistemas, al tener una única contraseña y forzar a que la misma sea robusta.

Simplificar la actividad al usuario, que solo debe recordar una contraseña.

Optimizar y delegar en los responsables de cada servicio la administración del mismo.