



SISTEMA INTEGRADO DE GESTIÓN DE EXPEDIENTES MODULAR (SIGM)

CONFIGURACIÓN DE SIGM PARA LDAP

SIGM v3



Administración Local Soluciones

Control de versiones

Versión	Fecha aprobación	Cambio producido	Autor
01	26-02-2009	Versión inicial	IECISA
02	20-04-2009	Actualización para SIGEM v1.8	IECISA
03	06-07-2009	Establecer el SUPERUSER en el Catálogo de Procedimientos	IECISA
04	08-07-2009	Actualización para SIGEM v1.9 externalización de configuración.	IECISA
05	13-07-2009	Actualización para SIGEM 1.9 con la configuración de LDAP para Archivo.	IECISA
06	27-10-2009	Actualización para SIGEM 1.9 con la configuración de LDAP para Consolidación del Registro Telemático.	IECISA
07	19-11-2009	Actualización para SIGEM DOS con la configuración de LDAP para Archivo.	IECISA
09	04-10-2012	Actualización para SIGM v3.0.	IECISA
10	26-10-2012	Actualización de configuración para SIGM 3.0	IECISA

ÍNDICE

1	INTRODUCCIÓN	4
1.1	VISIÓN GENERAL DEL SISTEMA.....	4
1.2	FINALIDAD DEL DOCUMENTO	4
1.3	DEFINICIONES Y ABREVIATURAS.....	4
2	CONFIGURACIÓN	6
2.1	CAMBIOS EN LA BASE DE DATOS	6
2.2	CAMBIOS EN LAS APLICACIONES WEB	6
2.2.1	<i>IeciTd_LdapConn_Cfg.xml (sigem_estructuraOrganizativaCore)</i>	6
2.3	CAMBIOS DE CONFIGURACIÓN.....	8
2.3.1	<i>Isicres-Configuration.xml (SIGEM_RegistroPresencialWeb)</i>	8
2.3.2	<i>ispac.properties (SIGEM_Tramitacion)</i>	9
2.3.3	<i>ispacdap.properties (SIGEM_Tramitacion)</i>	9
2.3.4	<i>archivo-cfg.xml (SIGEM_ArchivoWeb)</i>	11
2.3.4.1	Establecer la autenticación con LDAP.....	11
2.3.4.2	Definir el sistema de Organización a usar	16
2.3.5	<i>ldapUserAttributes.xml (SIGEM_ArchivoWeb)</i>	16
2.4	CONFIGURACIÓN DE CONEXIÓN LDAP EN LA ADMINISTRACIÓN DE REGISTRO	18
2.5	AUTENTICACIÓN SINGLE-SIGN ON CON EL SISTEMA OPERATIVO DE LA ESTACIÓN CLIENTE..	18
2.6	PROCESO DE CONSOLIDACIÓN DEL REGISTRO TELEMÁTICO PARA LDAP	19
2.6.1	<i>Acciones sobre el servidor LDAP</i>	19
2.6.1.1	Creación de un usuario de consolidación	19
2.6.1.2	Creación de un grupo de consolidación	19
2.6.2	<i>Acciones sobre la Administración de Registro</i>	19
2.6.2.1	Alta de usuario de consolidación	19
2.6.2.2	Creación de oficina	19
2.6.2.3	Selección de oficina preferente para el usuario de consolidación.....	20
2.6.2.4	Asignación de permisos de escritura sobre el libro de entrada.....	20
2.7	DEFINICIÓN DE ÓRGANOS PRODUCTORES DE UN PROCEDIMIENTO CUYOS EXPEDIENTES SE VAN A TRANSFERIR A ARCHIVO.....	21

1 Introducción

1.1 *Visión general del sistema*

AL SIGM es la plataforma de Tramitación Electrónica del MINETUR, solución integral para la tramitación electrónica de los procedimientos administrativos, que fomenta la interoperabilidad entre administraciones mediante su adaptación a estándares de comunicación así como la reutilización de recursos e información pública.

1.2 *Finalidad del documento*

El objeto del presente documento es especificar los cambios en la configuración de SIGM para soportar LDAP como gestor de la estructura organizativa para la autenticación y autorización de usuarios.

1.3 *Definiciones y Abreviaturas*

A continuación se expone una tabla con los diferentes acrónimos y abreviaturas utilizados a lo largo del documento, con su correspondiente definición.

Acrónimo / Abreviatura	Definición
MINETUR	Ministerio de Industria, Energía y Turismo
IECISA	Informática El Corte Inglés S.A.
SIGM	Sistema Integrado de Gestión de Expedientes Modular
AL	Administración Local



2 Configuración

2.1 Cambios en la base de datos

La plataforma AL SIGM se proporciona por defecto con una gestión de usuarios propia, para la que se crean elementos de prueba (usuarios, grupos y departamentos) a través de los scripts de inicialización de base de datos proporcionados.

Si se va a configurar AL SIGM con una gestión de usuarios LDAP, previamente se deben eliminar de la bases de datos dichos valores de prueba de la gestión interna.

Para ello, se deben ejecutar los siguientes scripts:

Esquema	Nombre del esquema por defecto	Script a ejecutar
Registro Presencial	registro_000	<ul style="list-style-type: none">registro/00_delete_data_invesdoc_registro_sigemLDAP.sql
Gestión de Expedientes	tramitador_000	<ul style="list-style-type: none">tramitador/00_delete_data_invesdoc_tramitador_sigemLDAP.sql

Se pueden obtener dichos scripts en la distribución de AL SIGM, en el directorio *Aplicaciones\Plantillas BBDD Multientidad\BBDD*, siendo BBDD la base de datos concreta de cada implantación.

2.2 Cambios en las aplicaciones web

Para autenticarse contra LDAP, habrá que realizar los siguientes cambios en el despliegue de las aplicaciones web:

2.2.1 IeciTd_LdapConn_Cfg.xml (sigem_estructuraOrganizativaCore)

Para definir la configuración LDAP es necesario seguir los siguientes pasos:

1. Crear un fichero IeciTd_LdapConn_Cfg.xml con el siguiente contenido:

```
<Configs>
  <Config Entidad="000">
    <Connection>
      <Provider>1</Provider>
      <Pooling>N</Pooling>
      <Pooling_TimeOut>0</Pooling_TimeOut>
    </Connection>
  </Config>
</Configs>
```

```
<Auth_Config>
  <MaxNumTries>3</MaxNumTries>
  <User_Search_By_Dn>N</User_Search_By_Dn>
  <User_Start>CN=Users,DC=sigem,DC=es</User_Start>
  <User_Scope>2</User_Scope>
  <User_Attribute>sAMAccountName</User_Attribute>
  <Group_Start>CN=Users, DC=sigem,DC=es</Group_Start>
  <Group_Scope>2</Group_Scope>
</Auth_Config>
</Config>
</Configs>
```

Hay que crear una sección Config por cada identificador de entidad del sistema y debemos modificar los valores del fichero anterior de la siguiente manera:

- *Connection*
 - **Provider:**
Indica el proveedor de LDAP. Los posibles valores son:
1-SUN
 - **Pooling:**
Indica si se está usando un pool de conexiones. Los posibles valores son: *s* (SI) o *N* (NO).
 - **Pooling_TimeOut:**
Indica el tamaño del pool de conexiones. Si no se utiliza se asigna el valor 0
- *Auth_Config*
 - **MaxNumTries:**
Número máximo de intentos.
 - **User_Search_By_Dn:**
Búsqueda de usuario por DN, valores posibles: *s*(SI) o *N*(NO).
 - **User_Start:**
Nodo a partir del cual se realizan las búsquedas de usuarios.
 - **User_Scope:**
Indica el punto de comienzo de una búsqueda de LDAP y la profundidad desde la base DN a la que la búsqueda podría acceder. Los posibles valores son:
 - 0: BASE. Sólo se busca en el nodo inicial de la BASE DN
 - 1: ONELEVEL. Sólo se busca en los nodos del nivel inferior al nodo inicial de la BASE DN, pero no en este último
 - 2: SUBTREE. Se realiza la búsqueda en todos los nodos a partir del nodo inicial de la Base DN y también en este último
 - **User_Attribute:**
Al autenticarse hay que indicar un nombre y una contraseña. Ese nombre podría corresponder a diferentes atributos Al autenticarse hay que indicar un nombre y una contraseña. Ese nombre podría corresponder a diferentes atributos.
 - **Group_Start:**
Nodo a partir del cual se realizan las búsquedas de grupos.
 - **Group_Scope:**
Indica el punto de comienzo de una búsqueda de LDAP y la profundidad desde la base DN a la que la búsqueda podría acceder. Los posibles valores son:
 - 0: BASE. Sólo se busca en el nodo inicial de la BASE DN

- 1: ONELEVEL. Sólo se busca en los nodos del nivel inferior al nodo inicial de la BASE DN, pero no en este último
- 2: SUBTREE. Se realiza la búsqueda en todos los nodos a partir del nodo inicial de la Base DN y también en este último

2. Se debe copiar el fichero anterior (y reiniciar el servidor de aplicaciones) a las siguientes rutas (creando el directorio resources si es necesario):

- /home/sigem/SIGEM/tomcat/webapps/SIGEM_AdministracionWeb/WEB-INF/classes/resources
- /home/sigem/SIGEM/tomcat/webapps/SIGEM_AutenticacionAdministracionWeb/WEB-INF/classes/resources
- /home/sigem/SIGEM/tomcat/webapps/SIGEM_RegistroPresencialAdminWeb/WEB-INF/classes/resources
- /home/sigem/SIGEM/tomcat/webapps/SIGEM_ConsultaExpedienteBackOfficeWeb/WEB-INF/classes/resources
- /home/sigem/SIGEM/tomcat/webapps/SIGEM_CatalogoTramitesWeb/WEB-INF/classes/resources
- /home/sigem/SIGEM/tomcat/webapps/SIGEM_RepositoriosDocumentalesWeb/WEB-INF/classes/resources
- /home/sigem/SIGEM/tomcat/webapps/SIGEM_EstructuraOrganizativaWS/WEB-INF/classes/resources
- /home/sigem/SIGEM/tomcat/webapps/SIGEM_AutenticacionBackOfficeWeb/WEB-INF/classes/resources
- /home/sigem/SIGEM/tomcat/webapps/SIGEM_EstructuraWeb/WEB-INF/classes/resources
- /home/sigem/SIGEM/tomcat/webapps/SIGEM_ConsultaRegistroTelematicoBackOfficeWeb/WEB-INF/classes/resources
- /home/sigem/SIGEM/tomcat/webapps/SIGEM_ArchivoWeb/WEB-INF/classes/resources

2.3 Cambios de configuración

Para autenticarse contra LDAP, habrá que realizar ciertos cambios en la configuración de SIGM. Muchos de estos cambios ya vienen realizados si se genera una configuración personalizada como se especifica en el documento:

SGM_*_*_Manual de Uso Herramienta Configuraciones Básicas

Si no se utiliza la herramienta es necesario realizar a mano los cambios correspondientes, tal como se especifica en los puntos siguientes.

2.3.1 Isicres-Configuration.xml (SIGEM_RegistroPresencialWeb)

Este fichero se encuentra en la ruta ./SIGEM_RegistroPresencial/ISicres-Configuration.xml donde se haya descomprimido el zip de configuración externa.

Se deberá editar el fichero para configurar la política de autenticación para LDAP:

```
<Authentication>
```

```
<AuthenticationPolicy>ieci.tecdoc.sgm.registropresencial.autenticacion.SigemLDAPAuthenticationPolicy
</AuthenticationPolicy>
</Authentication>
```

2.3.2 ispac.properties (SIGEM_Tramitacion)

Este fichero se encuentra en la ruta ./SIGEM_Tramitacion/ispac.properties donde se haya descomprimido el zip de configuración externa.

Se debe editar el fichero y configurar el sistema de usuarios y organización para LDAP:

1. Establecer el parámetro *SUPERUSER*, que indica el usuario interno que por defecto se asigna para las conexiones de los administradores de SIGEM (este usuario debe existir en LDAP):

```
# Superusuario
SUPERUSER = usuario
```

2. Comentar la línea en la que se indica la clase que implementa el conector de directorio de usuarios para invesDoc:

```
#####
# Invesdoc
#
# Clase que implementa el conector de directorio de usuarios
#DIRECTORY_CONNECTOR_CLASS =
ieci.tdw.ispac.ispac.lib.invesdoc.directory.InvesDocDirectoryConnector
```

3. Descomentar la línea en la que se indica la clase que implementa el conector de directorio de usuarios para LDAP:

```
#####
# LDAP
#
# Clase que implementa el conector de directorio de usuarios
DIRECTORY_CONNECTOR_CLASS = ieci.tdw.ispac.ispac.lib.ldap.directory.LdapDirectoryConnector
```

2.3.3 ispacldap.properties (SIGEM_Tramitacion)

Este fichero se encuentra en la ruta ./SIGEM_Tramitacion/ispacldap.properties donde se haya descomprimido el zip de configuración externa.

Incluye los siguientes parámetros relativos a la configuración LDAP.

Fichero:
ispacldap.properties

Descripción:

Fichero de configuración de la autenticación contra LDAP.

Parámetros:

Nombre	Descripción
LDAP_SERVER	URL de conexión al servidor LDAP.
LDAP_ADMUSER	Usuario de conexión con LDAP.
LDAP_ADMPASS	Clave del usuario de conexión a LDAP.
LDAP_TYPE	Tipo de LDAP: 3 → Active Directory 5 → OpenLDAP
LDAP_ROOTDN	Nombre de dominio raíz en LDAP.
LDAP_GROUPS_ROOTDN	(Opcional) Raíz para la búsqueda de grupos.
LDAP_ORG_ROOTDN	(Opcional) Raíz para la búsqueda en la estructura organizativa.
CN_ATTNAME	Prefijo del nombre común de LDAP.
GUID_ATTNAME	Nombre del atributo de GUID.
MEMBER_ATTNAME	Nombre del atributo de miembro de un grupo.
PERSON_OBJECTCLASS	Nombre del atributo objectClass para usuario.
PERSON_LABEL_ATTNAME	Nombre del atributo que contiene el nombre del usuario. Si está vacío, se coge el valor de CN_ATTNAME
PERSON_LOGIN_ATTNAME	Nombre del atributo que contiene el login del usuario. Si está vacío, se coge el valor de CN_ATTNAME
GROUP_OBJECTCLASS	Nombre del atributo objectClass para grupo.
GROUP_LABEL_ATTNAME	Nombre del atributo que contiene el nombre del grupo. Si está vacío, se coge el valor de CN_ATTNAME
UNIT_OBJECTCLASS	Nombre del atributo objectClass para departamento.
UNIT_LABEL_ATTNAME	Nombre del atributo que contiene el nombre del departamento. Si está vacío, se coge el valor de CN_ATTNAME
ORGANIZATION_OBJECTCLASS	Nombre del atributo objectClass para organización
ORGANIZATION_LABEL_ATTNAME	Nombre del atributo que contiene el nombre de la organización. Si está vacío, se coge el valor de CN_ATTNAME
DOMAIN_OBJECTCLASS	Nombre del atributo objectClass para dominio
DOMAIN_LABEL_ATTNAME	Nombre del atributo que contiene el nombre del dominio. Si está vacío, se coge el valor de CN_ATTNAME

Se muestra a continuación un ejemplo de configuración:

```
#####
##### CONFIGURACIÓN ACCESO LDAP #####
#####
#
#   Valores para LDAP_TYPE:
#
#   LDAPTYPE_ACTIVEDIR   = 3
#   LDAPTYPE_OPENLDAP   = 5
#
#
# Time-out para las conexiones con el servidor de LDAP
CONNECT_TIMEOUT = 15000
#
# Tipo de LDAP
```

```

LDAP_TYPE = 3

# URL de conexión a LDAP
LDAP_SERVER = ldap://192.168.0.1:389

# Usuario para la conexión a LDAP
LDAP_ADMUSER = CN=usuario,CN=Users,DC=sigem,DC=es

# Clave del usuario para la conexión a LDAP
LDAP_ADMPASS = XXXXXXXX

# Raíz del LDAP
LDAP_ROOTDN = DC=sigem,DC=es

# Raíz para la búsqueda de grupos (opcional)
#LDAP_GROUPS_ROOTDN = CN=Users,DC=sigem,DC=es

# Raíz para la búsqueda en la estructura organizativa (opcional)
#LDAP_ORG_ROOTDN = CN=Users,DC=sigem,DC=es

# Nombre del atributo que contiene el CN
CN_ATTNAME = CN

# Nombre del atributo que contiene el GUID
GUID_ATTNAME = objectGUID

# Atributo de miembro de un grupo
MEMBER_ATTNAME = member

# Valor del atributo objectClass para usuario
PERSON_OBJECTCLASS = person

# Valor del atributo objectClass para grupo
GROUP_OBJECTCLASS = group

# Valor del atributo objectClass para departamento
UNIT_OBJECTCLASS = organizationalUnit

# Valor del atributo objectClass para organización
ORGANIZATION_OBJECTCLASS = container

# Valor del atributo objectClass para dominio
DOMAIN_OBJECTCLASS = domain

```

2.3.4 archivo-cfg.xml (SIGEM_ArchivoWeb)

Este fichero se encuentra en la ruta `./SIGEM_ArchivoWeb/archivo-cfg.xml` donde se haya descomprimido el zip de configuración externa.

Se debe editar el fichero `archivo-cfg.xml` para realizar los siguientes pasos:

2.3.4.1 Establecer la autenticación con LDAP

Para el conector que implementa la autenticación LDAP es necesario añadir los siguientes parámetros de inicialización:

Parámetro	Definición
ENGINE	Indica quién implementa el protocolo LDAP.

	<p>Engines:</p> <table border="1"> <thead> <tr> <th>Valor</th> <th>Definición</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Active Directory</td> </tr> <tr> <td>3</td> <td>Open LDAP</td> </tr> </tbody> </table>	Valor	Definición	1	Active Directory	3	Open LDAP
Valor	Definición						
1	Active Directory						
3	Open LDAP						
PROVIDER	<p>Proveedor de LDAP</p> <p>Providers:</p> <table border="1"> <thead> <tr> <th>Valor</th> <th>Definición</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>SUN</td> </tr> </tbody> </table>	Valor	Definición	1	SUN		
Valor	Definición						
1	SUN						
URL	URL de conexión al servidor de LDAP.						
USER_DEFAULT	Usuario por defecto de LDAP. Para realizar autenticaciones y búsquedas de usuarios, es necesario conectarse previamente a LDAP por lo que es necesario disponer de un usuario.						
PASSWORD_DEFAULT	Contraseña del usuario por defecto.						
USER_START	Nodo a partir del cual se realizarán las búsquedas de usuarios.						
USER_ATTRIBUTE	Atributo a utilizar como nombre de usuario.						

Parámetro	Definición								
USER_SCOPE	<p>Ámbito de búsqueda para los usuarios respecto al nodo inicial definido en USER_START.</p> <p>User Scopes:</p> <table border="1"> <thead> <tr> <th>Valor</th> <th>Definición</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>BASE: Sólo se busca en el nodo inicial.</td> </tr> <tr> <td>1</td> <td>ONELEVEL: Busca en los nodos del nivel inferior al nodo inicial.</td> </tr> <tr> <td>2</td> <td>SUBTREE: Se realiza la búsqueda en todos los nodos a partir del nodo inicial.</td> </tr> </tbody> </table>	Valor	Definición	0	BASE: Sólo se busca en el nodo inicial.	1	ONELEVEL: Busca en los nodos del nivel inferior al nodo inicial.	2	SUBTREE: Se realiza la búsqueda en todos los nodos a partir del nodo inicial.
Valor	Definición								
0	BASE: Sólo se busca en el nodo inicial.								
1	ONELEVEL: Busca en los nodos del nivel inferior al nodo inicial.								
2	SUBTREE: Se realiza la búsqueda en todos los nodos a partir del nodo inicial.								
POOLING	<p>Indica si se está usando un pool de conexiones.</p> <p>Valores:</p> <table border="1"> <thead> <tr> <th>Valor</th> <th>Definición</th> </tr> </thead> <tbody> <tr> <td>S</td> <td>Se está utilizando pool de conexiones</td> </tr> </tbody> </table>	Valor	Definición	S	Se está utilizando pool de conexiones				
Valor	Definición								
S	Se está utilizando pool de conexiones								

	N	No se están utilizando pool de conexiones
POOLING_ TIMEOUT	Indica el timeout del pool de conexiones. Si la propiedad POOLING es N, debería llevar 0.	

Ejemplo de Configuración de sistema LDAP (Active Directory)

```
<Sistema>
  <Id>LDAP-ACTIVE-DIRECTORY</Id>
  <Nombre>Usuarios de LDAP Active Directory</Nombre>
  <Clase>se.autenticacion.ldap.LdapConnector</Clase>
  <init-param>
    <param-name>ENGINE</param-name>
    <param-value>1</param-value>
  </init-param>
  <init-param>
    <param-name>PROVIDER</param-name>
    <param-value>1</param-value>
  </init-param>
  <init-param>
    <param-name>URL</param-name>
    <param-value>
      ldap://10.228.20.177:389/DC=SERVIDOR-GDOC3,DC=iecisa,DC=corp
    </param-value>
  </init-param>
  <init-param>
    <param-name>USER_DEFAULT</param-name>
    <param-value>CN=lucas,CN=Users,DC=SERVIDOR,DC=iecisa </param-value>
  </init-param>
  <init-param>
    <param-name>PASSWORD_DEFAULT</param-name>
    <param-value>secreta</param-value>
  </init-param>
  <init-param>
    <param-name>USER_START</param-name>
    <param-value>CN=Users</param-value>
  </init-param>
  <init-param>
    <param-name>USER_ATTRIBUTE</param-name>
    <param-value>CN</param-value>
  </init-param>
  <init-param>
    <param-name>USER_SCOPE</param-name>
    <param-value>1</param-value>
  </init-param>
  <init-param>
    <param-name>POOLING</param-name>
    <param-value>N</param-value>
  </init-param>
  <init-param>
    <param-name>POOLING_TIMEOUT</param-name>
    <param-value>0</param-value>
  </init-param>
</Sistema>
```

Ejemplo de Configuración con Open LDAP

```
<Sistema>
  <Id>OPEN-LDAP</Id>
  <Nombre>Usuarios de Open LDAP</Nombre>
  <Clase>se.autenticacion.ldap.LdapConnector</Clase>
  <init-param>
    <param-name>ENGINE</param-name>
    <param-value>3</param-value>
  </init-param>
  <init-param>
    <param-name>PROVIDER</param-name>
    <param-value>1</param-value>
  </init-param>
  <init-param>
    <param-name>URL</param-name>
    <param-value>
      ldap://10.228.20.178:389/DC=iecisa,DC=corp
    </param-value>
  </init-param>
  <init-param>
    <param-name>USER_DEFAULT</param-name>
    <param-value>CN=Administrator,DC=iecisa,DC=corp</param-value>
  </init-param>
  <init-param>
    <param-name>PASSWORD_DEFAULT</param-name>
    <param-value>secreta</param-value>
  </init-param>
  <init-param>
    <param-name>USER_START</param-name>
    <param-value>ou=Usuarios</param-value>
  </init-param>
  <init-param>
    <param-name>USER_ATTRIBUTE</param-name>
    <param-value>CN</param-value>
  </init-param>
  <init-param>
    <param-name>USER_SCOPE</param-name>
    <param-value>2</param-value>
  </init-param>
  <init-param>
    <param-name>POOLING</param-name>
    <param-value>N</param-value>
  </init-param>
  <init-param>
    <param-name>POOLING_TIMEOUT</param-name>
    <param-value>0</param-value>
  </init-param>
</Sistema>
```

2.3.4.2 Definir el sistema de Organización a usar

Se deben realizar los siguientes cambios:

```
<Sistemas_Externos>
  <!--Sistema>
    <Id>SIGEM</Id>
    <Nombre>Organización SIGEM</Nombre>
  <Clase>se.instituciones.archivo.invesdoc.GestorOrganismoInvesdoc</Clase>
</Sistema-->
  <Sistema>
    <Id>SIGEM</Id>
    <Nombre>Organizacion</Nombre>
    <Clase>se.instituciones.db.DbOrganizationConnectorImpl</Clase>
    <init-param>
      <param-name>DATASOURCE_NAME</param-name>
      <param-value>java:comp/env/jdbc/archivoDS_{0}</param-value>
    </init-param>
  </Sistema>
</Sistemas_Externos>
```

```
<Configuracion_Parametros>
  <parametro>
    <id>MOSTRAR_ADMINISTRACION_ORGANIZACION</id>
    <valor>S</valor>
  </parametro>
</Configuracion_Parametros>
```

2.3.5 ldapUserAttributes.xml (SIGEM_ArchivoWeb)

Este fichero se encuentra en la ruta ./SIGEM_ArchivoWeb/gestores/ldapUserAttributes.xml donde se haya descomprimido el zip de configuración externa.

En este fichero se indican los atributos LDAP que se utilizarán a la hora de dar de alta usuarios en archivo.

Etiqueta	Definición
name	Atributo del sistema LDAP que representa el nombre de usuario.
surname	Atributo del sistema LDAP que representa los apellidos del usuarios.
address	Atributo del sistema LDAP que representa la dirección del usuario.
description	Atributo del sistema LDAP que representa la descripción del usuario.

Ejemplo de configuración:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<attributes xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
xsi:noNamespaceSchemaLocation="..\xsd\ldapUserAttributes.xsd">  
  <name>givenName</name>  
  <surname>sn</surname>  
  <mail>mail</mail>  
  <address>mail</address>  
  <description>distinguishedName</description>  
</attributes>
```

2.4 Configuración de conexión LDAP en la Administración de Registro

Para completar la configuración, habrá que establecer los datos de la conexión con el LDAP a usar desde la herramienta web de *Administración de Registro*.

Para ello consultar el manual *SGM_2012_**_Manual de Usuario Administración Registro*, sección "Configuración de LDAP como gestor de usuarios de registro".

2.5 Autenticación Single-Sign On con el sistema operativo de la estación cliente

Para activar la autenticación *Single-Sign On* con el sistema operativo de la estación cliente, se deberá configurar el parámetro `singleSignOn` en los siguientes ficheros:

- SIGEM_AutenticacionAdministracionWeb\autenticacionAdministracionWebConfig.properties

```
# Para usuarios internos, activar la autenticacion Single-Sign On (true, en caso contrario, desactivada)
singleSignOn=true
```

- SIGEM_AutenticacionBackOfficeWeb/autenticacionBackOfficeWebConfig.properties

```
# Activar la autenticacion Single-Sign On (true, en caso contrario, desactivada)
singleSignOn=true
```

2.6 Proceso de consolidación del Registro Telemático para LDAP

El proceso automático de consolidación se realiza con una periodicidad configurable por el organismo (pueden verse más detalles de este proceso en el documento *SGM_2012_**_Proceso de Consolidación de Registro Telemático*).

Para que se realice dicho proceso cuando el sistema está configurado para usar LDAP, es necesario seguir los siguientes pasos.

2.6.1 Acciones sobre el servidor LDAP

2.6.1.1 Creación de un usuario de consolidación

Definir un usuario específico para el proceso de consolidación. Puede crearse un usuario nuevo o utilizar uno ya existente. Es aconsejable crear uno nuevo y utilizarlo solamente para este proceso.

Este usuario se utilizará para validarse en el registro presencial al realizar la consolidación.

 El usuario que vaya a ser usado para la consolidación ha de configurarse en el fichero de propiedades *consolidacion.properties*.

Para más información, consultar el documento *SGM_2012_**_Proceso de Consolidación de Registro Telemático*.

2.6.1.2 Creación de un grupo de consolidación

Definir un grupo específico para el proceso de consolidación. Puede crearse un grupo nuevo o utilizar uno ya existente. Es aconsejable crear uno nuevo y utilizarlo solamente para este proceso.

El usuario creado en el paso anterior debe pertenecer a este grupo.

2.6.2 Acciones sobre la Administración de Registro

2.6.2.1 Alta de usuario de consolidación

Se debe dar de alta como usuario de registro el usuario LDAP creado para la consolidación, asignándole el perfil de *superusuario*, y cumplimentando los datos obligatorios del mismo (nombre, primer apellido...).

2.6.2.2 Creación de oficina

Se debe crear una oficina de registro telemático con el **código 999**, asociada al grupo del usuario de consolidación.

2.6.2.3 Selección de oficina preferente para el usuario de consolidación

Se debe marcar la oficina creada en el paso anterior, como oficina preferente del usuario de consolidación.

2.6.2.4 Asignación de permisos de escritura sobre el libro de entrada

Se deben dar permisos de creación (Consultar + Crear + Modificar), a la oficina creada anteriormente (código 999), sobre el libro de entrada en el que se vayan a consolidar los registros telemáticos.

2.7 Definición de Órganos Productores de un procedimiento cuyos expedientes se van a transferir a Archivo

El módulo de *Gestión de Expedientes*, cuando está configurado para hacer uso de LDAP, debe utilizar un conector específico a la hora de obtener los productores de sus procedimientos, en la aplicación de *Catálogo de Procedimientos*, para aquellos procedimientos cuyos expedientes vayan a ser transferidos al módulo de Archivo.

En concreto, dicho conector recupera la información de los órganos productores definidos en el módulo de Archivo.

Para ello, habría que realizar los siguientes pasos:

1. Modificar los orígenes de datos en el fichero server.xml para las aplicaciones SIGEM_CatalogoProcedimientosWeb y SIGEM_TramitacionWeb, para añadir la conexión con el esquema de base de datos del módulo de Archivo.

Por ejemplo, en Tomcat habría que cambiar:

```
<!-- Habilitar cuando se active el conector de órganos productores de procedimientos contra archivo -->
<!-- <ResourceLink global="jdbc/archivoDS_000" name="jdbc/archivoDS_000" type="javax.sql.DataSource"/> -->
```

Por:

```
<!-- Habilitar cuando se active el conector de órganos productores de procedimientos contra archivo -->
<ResourceLink global="jdbc/archivoDS_000" name="jdbc/archivoDS_000" type="javax.sql.DataSource"/>
```

2. En el fichero ispac.properties, realizar la siguiente modificación:

- Descomentar las líneas en las que se indica el conector con el sistema de productores de Archivo:

```
#####
# CONFIGURACIÓN DEL CONECTOR DE ÓRGANOS PRODUCTORES
#####

# Conector de órganos productores de procedimientos (por defecto)
#PRODUCERS_CONNECTOR_CLASS = ieci.tdw.ispac.ispac.lib.producers.ProducersConnectorImpl

# Conector de órganos productores de procedimientos contra archiDoc
PRODUCERS_CONNECTOR_CLASS = ieci.tdw.ispac.ispac.lib.producers.ProducersConnectorArchiDocImpl
# Etiqueta de la raíz del árbol de productores
PRODUCERS_CONNECTOR_ARCHIDOC_ROOT_NAME = ROOT
# Nombre del datasource de los datos de productores
PRODUCERS_CONNECTOR_ARCHIDOC_DATASOURCE_NAME = java:comp/env/jdbc/archivoDS
```