



<b>Doc ID:</b>	Primeros_pasos_recursos_grid.doc
<b>Fecha:</b>	25/11/2013 (última modificación)
<b>Actividad:</b>	Actividad
<b>Estado:</b>	BORRADOR
<b>Revisión:</b>	2.0
<b>Ref. proyecto:</b>	UAWP
<b>Repositorio:</b>	CETA-UTC/COORDINACION/CETA-UAWP
<b>Preparado por:</b>	María Botón Fernández, Francisco Prieto Castrillo, Miguel Ángel Díaz Corchero
<b>Aprobado por:</b>	Miguel Ángel Díaz Corchero

# RECURSOS GRID DEL CETA CIEMAT

## Primeros pasos para el acceso

**Resumen:** Este documento pretende ser una guía para los nuevos usuarios/grupos que quieran hacer uso de los recursos Grid del Centro. Se presentan de una forma breve y clara algunos conceptos imprescindibles para entender una infraestructura Grid y el proceso de alta. Además se indica cómo actuar para poder utilizar los recursos que ofrece el Ceta-Ciemat y cómo sería el envío de un primer job/trabajo a la Grid

síntesis

## Información del documento y control de cambios

Revisión	Fecha	Descripción del Cambio	Autor	Aprobado
1.0	12-06-09	Creación del documento	María Botón	SI
1.1	25-11-13	Actualización del documento	Miguel Ángel Díaz	SI

## Tabla de contenidos

<b>1. INTRODUCCIÓN</b>	<b>3</b>
<b>2. CONCEPTOS BÁSICOS</b>	<b>4</b>
2.1 GRID/FEDERACIÓN	4
2.2 EL MIDDLEWARE	4
2.3 ORGANIZACIÓN VIRTUAL	4
<b>3. ACCESO A LOS RECURSOS GRID</b>	<b>5</b>
3.1 CERTIFICADO DIGITAL	5
3.1.1 SOLICITUD DEL CERTIFICADO	6
3.1.2 INSTALACIÓN DEL CERTIFICADO EN EL NAVEGADOR	8
3.1.3 CONVERSIÓN A FORMATO PEM	9
3.2 AFILIACIÓN A UNA VO	9
3.3 CREACIÓN DE CUENTA EN LA UI	10
<b>4. ENVÍO DEL PRIMER TRABAJO</b>	<b>10</b>
4.1 AUTENTIFICACIÓN Y AUTORIZACIÓN	10
4.1.1 CREACIÓN DEL PROXY	11
4.2 LENGUAJE JDL	11
4.3 ENVÍO DE UN TRABAJO	13

## 1. INTRODUCCIÓN

El Centro Extremeño de Tecnologías Avanzadas (CETA-CIEMAT) es un centro del CIEMAT (Centro de Investigaciones Energéticas Medio Ambientales y Tecnológicas), perteneciente al Ministerio de Ciencia e Innovación. Es un centro enteramente público y está dedicado al servicio y desarrollo de las tecnologías de la información, la informática distribuida y las tecnologías Grid para el beneficio de la ciencia y la sociedad. Además, ofrece sus recursos y apoya a investigadores que necesitan para sus proyectos grandes capacidades de cálculo y almacenamiento. Está ubicado en la ciudad de Trujillo, en Extremadura (España). Nuestra sede es el Conventual de San Francisco, construido en el siglo XVI y cedido por el Ayuntamiento de Trujillo para albergar nuestras instalaciones. Actualmente, posee unos 1500 procesadores para el cálculo y 400 TB para el almacenamiento en servidores de disco y cinta, con una conexión redundante de fibra óptica. Este Centro de Proceso de Datos (CPD) es equivalente a unos 500 ordenadores de mesa, 400.000 Gigabytes de almacenamiento y unos 1000 ADSLs domésticos de 10Mbps de capacidad cada uno. Da servicio a investigadores en Europa y en América Latina, potenciando el valor histórico de su ubicación en Extremadura y especialmente en Trujillo.

El CETA-CIEMAT participa en la actualidad en proyectos e iniciativas en distintos ámbitos entre los que se incluyen:

**Climatología**, participamos en el estudio de los efectos de la variación de la temperatura de la superficie de Océano Pacífico en el fenómeno del Niño.

**Física de sistemas complejos**, investigamos y desarrollamos herramientas informáticas en la teoría de grafos aleatorios y auto-organización de sistemas dinámicos acoplados. En este ámbito, colaboramos con el *Complex System Laboratory* y el *Complex Networks and Data Communications Group* de la Universidad de Buenos Aires para la optimización de algoritmos de procesos en entornos de computación distribuida basados en la teoría de las redes complejas.

**Física de partículas**, recibimos y procesamos datos del CERN desde Ginebra, el acelerador de partículas con el cual se estudian los orígenes de la materia. En la imagen 9 se puede apreciar el monitor de distribución y proceso de datos del propio CERN.

**Imagen médica**, contribuimos a desarrollar programas informáticos que ayuden a los médicos a detectar patologías como el cáncer de mama.

**Archivística**, desarrollamos servicios para la preservación y conservación de la información digital, especialmente para los manuscritos digitalizados de los archivos históricos.

## 2. CONCEPTOS BÁSICOS

### 2.1 GRID/FEDERACIÓN

**UNA GRID** es una **FEDERACIÓN** de centros que ofrecen **conjuntamente** sus recursos de cálculo y almacenamiento.

**UNA FEDERACIÓN** implica que cada centro (universidades, centros de investigación, empresas, etc.) es **autónomo** en la gestión de sus recursos. Es decir, decide **independientemente** qué recursos adquiere, y cuando los instala y administra según su estrategia, capacidad, oportunidad y presupuesto.

**LOS USUARIOS** acceden a los recursos de manera **análoga a una red eléctrica**. Del mismo modo que accedemos y consumimos potencia eléctrica a través de un enchufe sin saber donde se generó ni como (hidroeléctrica, nuclear, renovable,..), una Grid permite a los usuarios acceder a la potencia de cálculo y capacidad de almacenamiento distribuida en la federación, sin necesidad de saber dónde se realizará su cálculo o se almacenarán sus datos.

### 2.2 EL MIDDLEWARE

**EL MIDDLEWARE** es el software que permite **gestionar la federación**. Por ejemplo, cuando un usuario manda un cálculo a la Grid (a una federación), el middleware determina qué **centro o sitio** de la federación es el más apropiado para realizarlo, dirige el cálculo hacia ese centro, adjunta los datos necesarios, recoge los resultados, etc.

Algunos de los elementos del middleware son:

**WMS** (*Workload Management Service*) recibe las **peticiones de cálculo** (*jobs*) del usuario y **redirecciona** cada una de ellas al centro de recursos más apropiado (según su hardware, aplicaciones instaladas, etc.)

**CE** (*Computing Element*), localizado en cada centro, **recibe jobs del WMS** y los manda a los nodos de trabajo (**working node**) que encuentre disponible

**LFC** (*File Catalog*) es un **catálogo global de ficheros**, indicando donde se encuentra cada fichero, si existen réplicas, etc.

**SE** (*Storage Element*), localizado en cada centro, ofrece **almacenamiento para los archivos** de los usuarios.

### 2.3 ORGANIZACIÓN VIRTUAL

Una **Organización Virtual** (VO) está compuesta por los usuarios de una cierta comunidad, es decir, por los científicos que participan en un mismo experimento, proyecto o disciplina.

**Una VO** negocia con la federación los recursos necesarios para satisfacer los requerimientos de cálculo y almacenamiento de sus usuarios

**Cada Centro** de una federación divide sus recursos entre las VOs a la que da servicio, según sus propios intereses, misión, compromisos, etc.

**Los usuarios** se identifican en los puntos de acceso con certificados digitales emitidos por la autoridad de certificación competente.

**Al identificarse** un usuario, se verifica a qué VO pertenece y se le da acceso al conjunto de recursos negociados por la VO en los distintos centros de la federación.

EL SERVICIO VOMS (VO Management Service) del middleware contiene la lista de usuarios de cada VO y se usa para verificar la pertenencia de usuarios las VOs que sirve.

Para usar los recursos de una federación un usuario debe:

- 1 Obtener un certificado digital solicitándolo a su autoridad de certificación pertinente. Este certificado identificará al usuario en cualquier federación
- 2 Solicitar el alta en la VO de su comunidad o en alguna VO de propósito general
- 3 Solicitar una cuenta en un punto de acceso (User Interface) de la federación.

### 3. ACCESO A LOS RECURSOS GRID

A continuación se especifican los pasos a seguir para acceder a los recursos Grid, de la federación Ibergrid, que España y Portugal ofrece a los diferentes grupos de investigación.

#### 3.1 CERTIFICADO DIGITAL

El certificado digital personal es necesario para identificarte en cualquier federación u organización virtual.

Los certificados digitales los emite en cada país una Autoridad Certificadora (CA) designada por la comunidad académica. En España nuestra CA es pkIRISGrid y para encontrar más información sobre la misma puedes acceder a: [pki.irisgrid.es](http://pki.irisgrid.es)

Si vienes de America Latina, contacta con la CA de tu país para obtener un certificado digital. Si tu país no tiene una CA, puedes obtener un certificado de la CA general para América Latina y el Caribe. En la siguiente dirección encontrarás más información: <https://lacgridca.ic.uff.br>

A modo de resumen, las etapas para solicitar y obtener un certificado son:

- En primer lugar contactar con una Autoridad Certificadora (CA). La solicitud del certificado suele realizarse a través de una interfaz web de la propia CA. Una vez se ha identificado una CA, el segundo paso es elegir una Autoridad Registradora (RA), que actúa como una delegación local de la CA. Por lo general, la CA en su página web proporciona una lista de las diferentes RA con las que se puede contactar. Por ejemplo, en la CA española pkIRISGrid, el CETA-Ciemat actúa como RA siendo su identificador el número 13.
- La RA debe aprobar la solicitud de generación de certificado que realiza el usuario. Para que esto sea así, se debe proporcionar cierta información a la RA (según su política). Para ello, una vez que la RA recibe la solicitud se pondrá en contacto con el

usuario, vía email, para especificarle qué datos debe presentar. Se realiza una segunda aceptación de la solicitud por parte de IRISGrid y, una vez conseguidas ambas, se procede a la generación del certificado. Esta aprobación se notifica al usuario mediante correo electrónico.

- El email que recibe el usuario contiene un link que permite instalar el certificado en el navegador. Para la instalación del certificado se debe utilizar **el mismo navegador** desde el que se realizó la solicitud.
- Una vez que el certificado es instalado en el navegador, se debe exportar a un fichero p12. Por lo general, los navegadores exportan el certificado en formato p12 por lo que, posteriormente, será necesario convertirlo a formato pem.

### 3.1.1 SOLICITUD DEL CERTIFICADO

Como primer paso para acceder a los recursos Grid de un Centro es necesario obtener un certificado personal.

Para solicitarlo se puede proceder solicitándolo a la CA del país al que se pertenece. Éste es el modo de proceder común por todos los grupos de investigación con los que se trabaja. El usuario accederá a la página de la CA correspondiente y solicitará el certificado digital.

En el caso de España, se accedería a la página de pkIRISGrid antes indicada (Figura 1: página principal de pkIRISGrid) y seleccionaríamos una Autoridad Registradora.

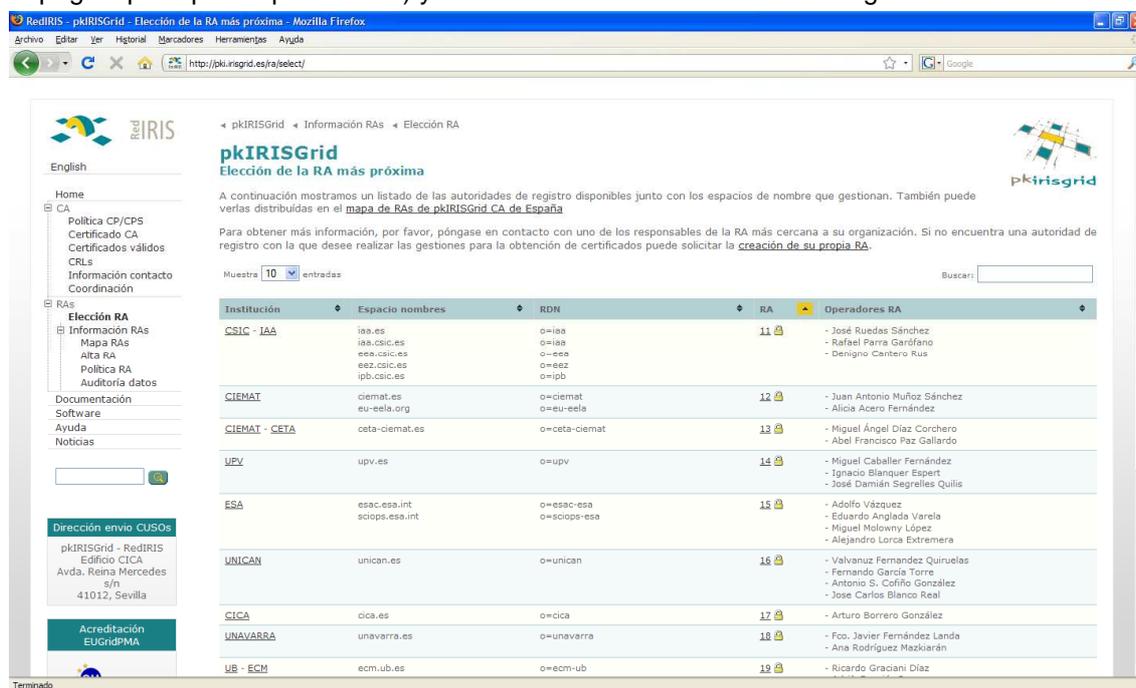


Figura1

Desde la página de la RA se procedería a solicitar el certificado digital (Figura 2: Caso en el que la RA es el CETA-Ciemat)

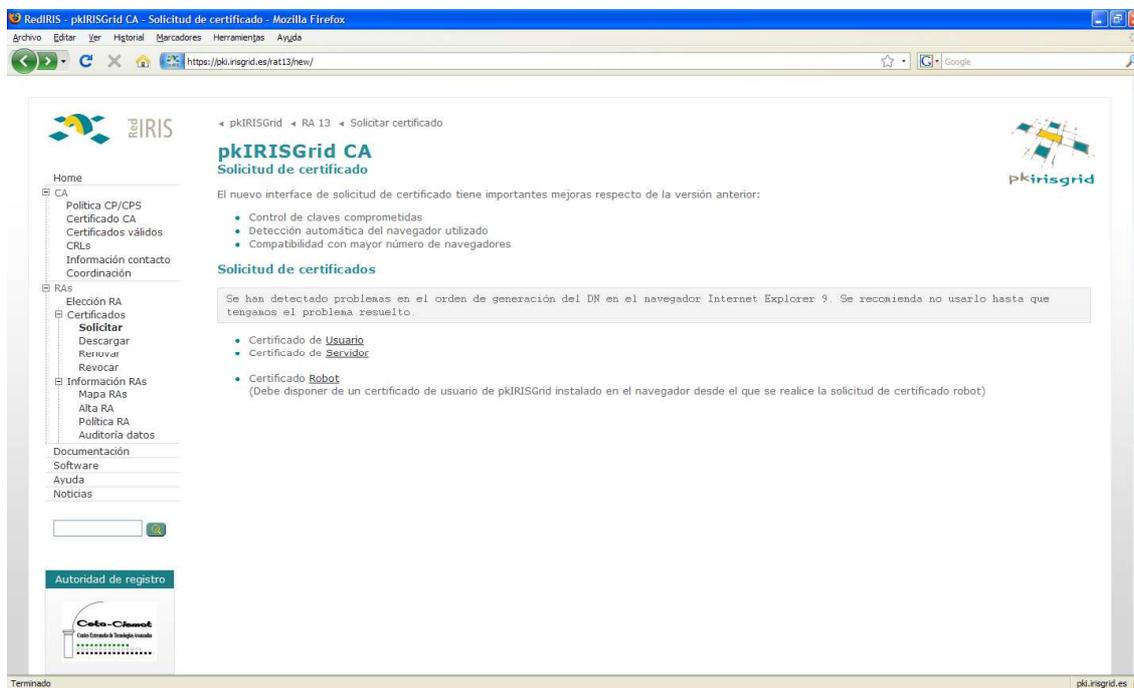


Figura 2

En una nueva ventana aparecerá un formulario a rellenar por el usuario. Una vez esté debidamente cumplimentado se envía, quedando registrada la solicitud. El usuario en ese instante recibirá el documento de su solicitud en formato PDF. Cuando el certificado sea generado se le enviará al usuario a la dirección de correo electrónico que especificó.

Como se ha comentado anteriormente, para que la RA acepte la solicitud por parte del usuario, éste deberá aportar cierta información acreditativa y su solicitud PDF generada por pkIRISGrid. Para saber la forma de proceder de la RA se puede consultar la política de la misma en la página de pkIRISGrid como se puede apreciar en la figura 3.

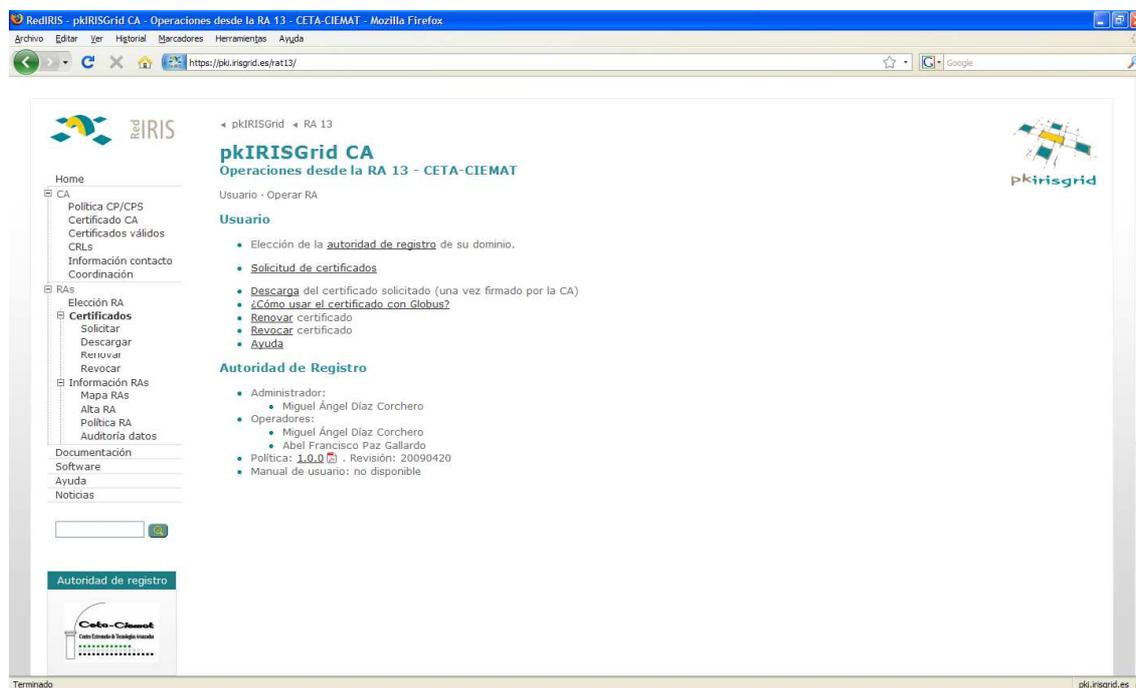


Figura 3

### 3.1.2 INSTALACIÓN DEL CERTIFICADO EN EL NAVEGADOR

Cuando se recibe el certificado digital por correo, el siguiente paso a realizar es la instalación del mismo en el **navegador desde el que se realizó la solicitud**.

**Si el certificado se solicitó a la CA del país**, en el mismo correo se proporciona un link desde el que se puede instalar el certificado en el navegador. Para el caso concreto de pkIRISGrid, al acceder a ese enlace se pide el identificador IRISGrid del usuario (el cual fue especificado en el formulario). En la siguiente ventana se proporciona información del certificado, que se recomienda guardar y copiar en un fichero, y una opción para descargar el certificado (permite almacenarlo en la ubicación que se le indique de tu PC, normalmente se guarda en formato p12).

En caso de estar trabajando con otra CA que no proporcione un link de descarga, se puede exportar el certificado del navegador tras ser instalado en el mismo. Para ello:

Si se utilizó como navegador Internet Explorer. Accedemos a Herramientas → Opciones de internet → etiqueta Contenido. Pulsamos la opción Certificados y seleccionamos la etiqueta Personal. Aparecerá una lista con todos los certificados que hay instalados en el navegador. Seleccionamos el certificado que hemos instalado y escogemos la opción exportar. Se nos pedirá indicar una ubicación para el fichero p12.

Si se utilizó Mozilla. Accedemos a Editar → Preferencias o Herramientas → Opciones (primera opción para Linux, segunda opción para Windows) y seguidamente el icono

“Avanzado”. En “Ver Certificados” nos posicionamos en la pestaña “Sus certificados” y obtenemos una lista con los certificados instalados en ese navegador. Seleccionamos el que acabamos de instalar, pulsamos el botón “Ver” y en la nueva ventana nos vamos a la pestaña “Detalles” Aquí aparece una opción para exportar el certificado. Será necesario indicar una ubicación.

### 3.1.3 CONVERSIÓN A FORMATO PEM

Este paso será necesario para aquellos usuarios que hayan solicitado el certificado a la CA de su país y el certificado digital lo tengan en formato p12 (pkcs12).

Para realizar la conversión se puede hacer uso de un script proporcionado en la siguiente URL <http://pki.irisgrid.es/software/pkcs12toglobus.sh>. Por medio de este script el usuario generará los ficheros *userkey.pem* y *usercert.pem*, correspondientes a las claves públicas y privadas obtenidas a partir del certificado de usuario en formato p12. Para ello se ejecuta el script con los siguientes parámetros por línea de comandos:

```
[...] $ sh pkcs12toglobus.sh -c usercert.pem -k userkey.pem nombrecertificado.p12
```

La contraseña que nos pide, es la que impusimos cuando exportamos el certificado desde el navegador.

También es posible realizar esta conversión haciendo uso de unos comandos:

Creamos el fichero *userkey.pem*

```
[...]$ openssl pkcs12 -nocerts -in nombrecertificado.p12 -out userkey.pem
```

Creamos el fichero *usercert.pem*

```
[...]$ openssl pkcs12 -clcerts -nokeys -in nombrecertificado.p12 -out usercert.pem
```

### 3.2 AFILIACIÓN A UNA VO

Una vez que se tiene un certificado instalado en el navegador, el siguiente paso consiste en afiliarse a una de las VO que gestiona el centro, que son:

Proyecto	VO	HomePage
Gisela	Prod.vo.eu-eela.eu	<a href="http://www.e-science.unam.mx">http://www.e-science.unam.mx</a>
ALICE	Alice	<a href="http://aliceinfo.cern.ch">http://aliceinfo.cern.ch</a>
IBERGRID	Phys.vo.ibergrid.eu	<a href="http://ibergrid.lip.pt/USP">http://ibergrid.lip.pt/USP</a>
(12 VOs)	Chem.vo.ibergrid.eu	
	...	
DRHIM	Drihm.eu	<a href="http://www.drihm.eu/">http://www.drihm.eu/</a>

Si pertenece a alguno de los proyectos indicados, lo conveniente es afiliarse a la VO asociada al proyecto pero, si por el contrario, no pertenece a ningún proyecto se recomienda la afiliación a IBERGRID (Federación Grid española y portuguesa)

### 3.3 CREACIÓN DE CUENTA EN LA UI

Una vez que el usuario ha obtenido un certificado digital y se ha afiliado a una VO, deberá indicar al CETA-Ciemat que ya tiene el certificado y la afiliación a la VO, para que el centro le cree una cuenta en un servidor que actuará como Interfaz de Usuario (UI) de la Grid. El CETA-Ciemat procederá a crearle la cuenta y le mandará los datos de acceso para acceder a la infraestructura Grid.

## 4. ENVÍO DEL PRIMER TRABAJO

En este apartado se van a especificar los pasos a realizar para poder hacer uso de los recursos Grid una vez se nos habilita acceso a los mismos.

Recordad que se utilizan los datos de la cuenta que se creó en el último subapartado anterior y que fueron enviados por correo.

### 4.1 AUTENTIFICACIÓN Y AUTORIZACIÓN

Accedemos a la máquina con nuestra cuenta de UI indicando por la línea de comandos/consola de nuestro ordenador:

```
[...] ssh nombreusuario@nombremaquina
```

Una vez estamos en nuestro directorio home de la UI, cuyo nombre será nombreusuario, debemos crear un directorio llamado “.globus” (el “.” antes del nombre indica que el directorio será oculto, para verlo a la hora de listar los directorios por línea de comandos utilizaremos “ls -la”).

```
[...] $ mkdir .globus
```

A continuación copiamos en este directorio los ficheros pem de nuestro certificado haciendo uso del comando scp. Esta sentencia se realiza por línea de comandos desde nuestro ordenador, no desde la UI, por lo que se recomienda hacerlo desde una segunda ventana de consola.

```
[...] $ scp *.pem nombreusuario@nombremaquina:/home/nombreusuario/.globus
```

Una vez que tenemos los ficheros userkey.pem y usercert.pem copiados en el directorio .globus debemos modificar los permisos de los mismos. Para ello, nos colocamos dentro del directorio y los modificamos:

```
[...] $ cd .globus  
[...] $ chmod 400 userkey.pem  
[...] $ chmod 644 usercert.pem
```

Ya tenemos nuestros certificados correctamente instalados en el directorio .globus. Esta acción solo será necesaria realizarla la primera vez y cuando se renueven los certificados, es decir, una vez al año.

Tras estas operaciones ya tenemos todo lo necesario para generar un proxy de nuestro certificado.

### 4.1.1 CREACIÓN DEL PROXY

El certificado está en el directorio .globus dividido en dos ficheros, los cuales se corresponden con las claves públicas y privadas que serán utilizadas en la conexión de autenticación.

El paso de generación del un proxy del certificado, es una medida de seguridad que puede ser equiparable al paso de login a la Grid ya que sin éste paso son muy pocas las acciones que se pueden realizar en la infraestructura.

El comando para generar un proxy es:

```
[...] voms-proxy-init --voms <nombre de vo>
```

La contraseña que nos pide, es la que impusimos cuando exportamos el certificado desde el navegador.

El proxy tiene una duración, tiempo de vida, de 12 horas por cuestiones de seguridad. Sin embargo, es probable que tus trabajos necesiten más tiempo para finalizar la ejecución. En esos casos, el proxy expira antes de que el trabajo termine provocando que falle. Para evitar esto, hay un mecanismo de renovación del proxy para mantener el proxy del job válido el tiempo que sea necesario. El servidor MyProxy es el componente que proporciona proxies de larga duración.

1. Crear el proxy normalmente en la UI  
**voms-proxy-init -voms <vo a la que estás afiliado>**
2. Se puede chequear que el proxy fue almacenado con éxito  
**voms-proxy-info**

## 4.2 LENGUAJE JDL

Para ejecutar trabajos en la Grid se hace uso de JDL (Job Description Lenguaje), un lenguaje específico que sirve para describir las características de los trabajos que se quieren ejecutar.

A continuación se van a comentar los argumentos, pertenecientes a este lenguaje, que más se utilizan para indicar las especificaciones de un trabajo. Para más información se puede consultar el capítulo 6 "Workload Management" de la guía de gLite que se proporciona junto a éste documento.

#### TYPE

Este atributo contiene un string que representa el tipo de requisito descrito mediante JDL.

**Type**="Job";

#### JOBTYPE

Contiene una cadena o lista de cadenas que representan el tipo de trabajo descrito en el JDL. Este atributo tiene sentido utilizarlo cuando en el atributo anterior se especificó "Job".

**Jobtype**="Normal";

#### EXECUTABLE

Contiene una cadena que representa el nombre del comando ejecutable.

**Executable**="/bin/sh";

#### INPUTSANDBOX

Contiene una cadena o una lista de cadenas con los ficheros necesarios para ejecutar el trabajo en los Worker Node (WN) y, que además, necesitan ser transferidos desde la UI hacia los WNs.

**InputSandbox**="hostname.sh";

#### ARGUMENTS

Contiene todos los comandos que son necesarios indicar por línea de comandos.

**Arguments**="hostname.sh";

#### STDOUTOUTPUT

Contiene el nombre del fichero donde queremos guardar la salida estandar del trabajo.

**Stdoutput**="hostname.out";

#### STDERROR

Contiene el nombre del fichero donde se quiere guardar los errores estándares del trabajo. Funciona como el anterior.

**Stderror**="hostname.err";

#### Ejemplo: hostname.jdl

*Type* = "Job";

*JobType* = "Normal";

*Executable* = "/bin/sh";

*Arguments* = "hostname.sh";

*StdOutput* = "hostname.out";

*StdError* = "hostname.err";

*InputSandbox*={"hostname.sh", "in"};

*OutputSandbox* = {"hostname.err", "hostname.out"};

**Ejemplo: hostname.sh**

```
#!/bin/sh
```

```
hostname -f
```

```
id
```

## 4.3 ENVÍO DE UN TRABAJO

Los comandos básicos para el envío y gestión de los jobs son:

**Envío del job:** `glite-wms-job-submit -o jobid -a hostname.jdl`

El fichero `jobid` será donde se almacene el identificador del job que se manda, para poder realizar la monitorización del mismo. El nombre de este fichero es elección del usuario

**Monitorización estado del job:** `glite-wms-job-status -i jobid -v 2`

**Recuperación de los salidas del job:** `glite-wms-job-output --dir <dir. donde descargarlos> -i jobid`

Para más información consultar la guía de usuario de gLite 3.1.