PROPUESTA NACIONAL DE GRID IRISGrid

Diseño, Arquitectura y Procedimientos del TestBed de IRISGrid

Ignacio Martín Llorente
Ruben Santiago Montero
Antonio Fuentes Bermejo
Eduardo Huedo

CONTENIDOS

Introducción

¿Qué es un Grid?

Un Grid es un conjunto de recursos hardware y software distribuidos por Internet que proporcionan servicios accesibles por medio de un conjunto de protocolos e interfaces abiertos (gestión de recursos, gestión remota de procesos, librerías de comunicación, seguridad, soporte a monitorización...) y organizados por medio de unos procedimientos y guías de "buenas prácticas" bien definidas. Las organizaciones virtuales que se interconectan por medio de un Grid mantienen sus propias políticas de seguridad y gestión de recursos. Esto significa que la tecnología usada para construir un Grid es complementaria a otras tecnologías para aprovechar los recursos distribuidos en la intranet de una organización.

¿Qué es IRISGrid?

IRISGrid pretende aportar los protocolos, procedimientos y guías de "buenas prácticas" necesarios para construir dentro de España un Grid de investigación coordinando a los diferentes Grupos y Centros interesados en investigación Grid. Esta iniciativa pretende unir recursos distribuidos geográficamente para que los Grupos involucrados tengan un banco de pruebas donde realizar investigación en cualquiera de las áreas Grid.

Este documento no incluye el diseño final de IRISGrid sino el diseño de un primer prototipo. Las experiencias de los primeros usuarios, la evolución de la tecnología de seguridad y las futuras versiones del *middleware* básico que se empleará implicarán hacer revisiones periódicas que serán implementadas por medio de nuevos prototipos.

La gestión de IRISGrid se realizará por medio de la página web irisgrid.rediris.es

¿Qué no es IRISGrid?

IRISGrid no pretende dar servicio técnico, sino fijar las normas, protocolos, procedimientos y guías de "buenas prácticas" que regulen el Grid. El objetivo de IRISGrid será facilitar a los Grupos interesados la unión de sus recursos al Grid. Queremos resaltar que IRISGrid coordinará este Grid estableciendo procedimientos relacionados principalmente con autenticación y monitorización de recursos. La decisión final de qué usuarios podrán usar los recursos será, por supuesto, de los propietarios de los mismos siguiendo sus normas locales. El Grid une dominios de administración sin implicar cambios en las políticas de seguridad o gestión de recursos internas dentro de cada grupo. **Es importante resaltar que realizar la instalación de Globus y configurar su seguridad y los sistemas de información para formar parte del IRISGrid no es un proceso trivial. Los Grupos IRISGrid deberán contar con personal experimentado**. En cualquier caso, en la página web IRISGrid se recomendarán enlaces a sitios con información relevante sobre el tema.

Definiciones

Comité Ejecutivo

Comité encargado de tomar decisiones sobre el futuro de IRISGrid. Este comité estará formado por los Representantes de las diferentes Instituciones o Centros del ámbito científico y académico que formen parte del Grid.

Coordinador

El coordinador es el miembro del Comité Ejecutivo responsable de mantener el servidor web irisgrid.rediris.es con los enlaces a la información de los Centros o Instituciones y los diferentes procedimientos y protocolos, y de recibir las solicitudes de ingreso de nuevas instituciones.

Centro o institución

Grupo de usuarios y recursos que pertenecen a un mismo Centro o Institución, que desarrollan una actividad común y están interesados en unirse a IRISGrid.

Nombre del centro o institución

Una única palabra que identifica cada centro o institución dentro de IRISGrid. Es el modo principal de diferenciar máquinas y usuarios dentro de IRISGrid. Se recomienda que sea breve. Por ejemplo, DACYA-UCM identifica el Departamento de Arquitectura de Computadores y Automática de la Universidad Complutense de Madrid

Representante del centro o institución

Responsable de realizar las comunicaciones con los Representantes de los diferentes centros o instituciones y con el Coordinador e IRISGrid CA. Adicionalmente podrá pertenecer al Comité Ejecutivo IRISGrid.

Responsable técnico

Encargado de administrar los sistemas de un Centro o Institución. Será la persona de contacto para la resolución de problemas técnicos. Podrá realizar comunicaciones con los administradores de otros centros o instituciones.

Usuario de un centro o institución

Usuario de IRISGrid. Únicamente se comunicará con el Representante y Administrador de su Grupo IRISGrid. Persona que usa los recursos de IRISGrid para ámbitos científicos y académicos.

Nombre de Máquina

Es el nombre FQDN (*Full-Qualified Domain Name*) del sistema.

Protocolos de Confianza:

Protocolos para realizar la transferencia de información, vía e-mail, entre los Representantes, Administradores, Coordinador e IRISGrid CA. IRISGrid proporciona los mecanismos para que se puedan realizar comunicaciones de confianza, pero en último

término son los miembros que intervienen en una comunicación los que deben implementar las normas.

Certificados

Son las credenciales X509 de servicios, máquinas, usuarios, Representantes, Administradores, y Coordinador, firmadas por el IRISGrid CA.

Entidad de Certificación (IRISGrid CA)

Encargada de firmar los certificados de servicios, máquinas, usuarios, Representantes y Administradores de las diferentes centros e instituciones.

Requisitos para Unirse a IRISGrid

La autorización para usar los sistemas de un Centro o Institución es siempre decisión de los propios centros o instituciones. IRISGrid podrá permitir a un usuario emplear potencialmente los sistemas del Grid por medio de la firma de su certificado. Sin embargo, en último término tendrá que solicitar de forma independiente a cada centro o institución el uso de sus recursos.

Requisitos para Añadir Recursos

Es necesario establecer unos requisitos mínimos para garantizar la disponibilidad del servicio. Es importante resaltar que proveer recursos a IRISGrid conllevará la responsabilidad de proporcionar el nombre de una persona responsable de la administración local de los sistemas que esté localizable durante un horario bien definido. IRISGrid no está en condiciones de proporcionar servicio técnico sobre Globus, por tanto los Grupos deberán contar con un Administrador experimentado en Globus.

Requisitos para Usar Recursos

El único requisito que se exige es la pertenencia a alguna organización pública o privada.

Middleware

Componentes Básicas

El Globus Toolkit es una colección de componentes software que ofrecen la infraestructura básica necesaria para la creación y ejecución de aplicaciones distribuidas, así como para la construcción de Grids. Actualmente, Globus se ha convertido en el estándar de facto para la computación distribuida y será el soporte sobre el que se desarrollará IRISGrid. Globus consta de tres componentes fundamentales: gestión de recursos, servicio de información y gestión de datos; todos ellos usan el protocolo de seguridad GSI para la comunicación y autenticación.

Los componentes anteriores, ya sea de forma independiente o conjunta, facilitan el acceso transparente y seguro a recursos distribuidos geográficamente en diferentes dominios de administración, además de servir como herramientas básicas para implementar las fases de la planificación de trabajos en Grids, a saber: descubrimiento, selección y preparación de recursos; y envío, monitorización, migración y finalización de trabajos. Debido al soporte limitado que prevé ofrecer el equipo de Globus para las versiones del Globus Toolkit (GT) anteriores a la 2.0 y las mejoras que aporta la versión 2.4, la versión que se usará en IRISGrid es la GT2.4. La versión 2.4 es compatible hacia atrás con la 2.0 de la siguiente forma:

- Los clientes 2.4 son compatibles con los servidores 2.0
- Los clientes 2.2 son compatibles con los servidores 2.4 únicamente si han sido actualizados

En el resto de este documento cualquier indicación sobre la configuración del sistema hace referencia a la versión GT2.4.

Gestión de Recursos (GRAM 1.6)

La arquitectura de gestión de recursos de Globus permite el acceso transparente, unificado y seguro a los distintos gestores de recursos locales de cada organización virtual (PBS, Condor, LSF, SGE). Los principales componentes de esta arquitectura son: el lenguaje de especificación de recursos (RSL), el gestor de asignación de recursos (GRAM), y DUROC (*Dynamically-Updated Request Online Coallocator*) para la asignación múltiple de recursos.

La configuración por defecto de Globus asigna al servicio GRAM (gatekeeper) al puerto 2119, todas las máquinas de IRISGrid deben garantizar el acceso desde el exterior a este puerto. **Nota:** un clúster únicamente debe garantizar el acceso al gatekeeper, o a cualquier otro servicio del Grid, en el front-end, y no en cada uno de los nodos computacionales del clúster, que en general se sitúan en una red privada.

El acceso a cada recurso se controla mediante el archivo `/etc/grid-security/grid-mapfile`, que consiste en una serie de asignaciones entre el subject (DN) del certificado de un usuario del Grid que puede usar el recurso, y un usuario local. Cada uno de los centros o instituciones, atendiendo a su propia política de administración, deberá decidir qué usuarios del

Grid tienen acceso a cada recurso; y si estos se asignan al mismo usuario local, o por el contrario si se crea una cuenta local distinta para cada usuario del Grid.

GridFTP

El servidor GridFTP es un protocolo de transferencia de ficheros, seguro y de alto rendimiento, basado en el protocolo FTP y de gran importancia en Grids de datos. El servicio GridFTP se asigna por defecto al puerto 2811, de nuevo todas las máquinas de IRISGrid deben garantizar el acceso a este servicio desde el exterior.

Sistema de Información (MDS 2.4)

El sistema de información de Globus es el *Metacomputing Directory Service* (MDS), que usa el protocolo LDAP para la consulta uniforme de la información referente a los sistemas en el Grid. En particular, mediante el Grid *Resource Information Service* (GRIS), se puede consultar el estado, la configuración, y las prestaciones de cada recurso del Grid. La información suministrada por cada GRIS se agrupa en el *Grid Index Information Service* (GIIS), que ofrece una imagen conjunta y coherente de los recursos del Grid. Por defecto, el servidor LDAP (slapd), tanto para el GRIS como para el GIIS, se asigna al puerto 2135, todas las máquinas en IRISGrid deben garantizar el acceso a este servicio desde el exterior.

En IRISGrid, las consultas a los servidores GRIS y GIIS se realizarán de forma anónima. En futuras versiones del prototipo para no comprometer la seguridad de las máquinas del Grid deberá emplearse el acceso no anónimo a los servidores GRIS y GIIS. Nota: MDS-2.4 usa el mismo fichero `grid-mapfile` que el servicio GRAM. El esquema LDAP que se propone para MDS es el estándar de MDS.

Se configurará un host (que será albergado por RedIRIS) como nodo raíz para el acceso superior GIIS, que a su vez preguntará a los servidores GIIS de cada centro o institución con su nombre. Con el fin de simplificar su gestión, todos los grupos, respecto a IRISGrid, están al mismo nivel independientemente de si pertenecen a la misma institución o ubicación geográfica. Internamente los diferentes centros o instituciones podrán estar a su vez organizadas jerárquicamente. El Apéndice B, recoge los pasos fundamentales para configurar los servidores GIIS y GRIS.

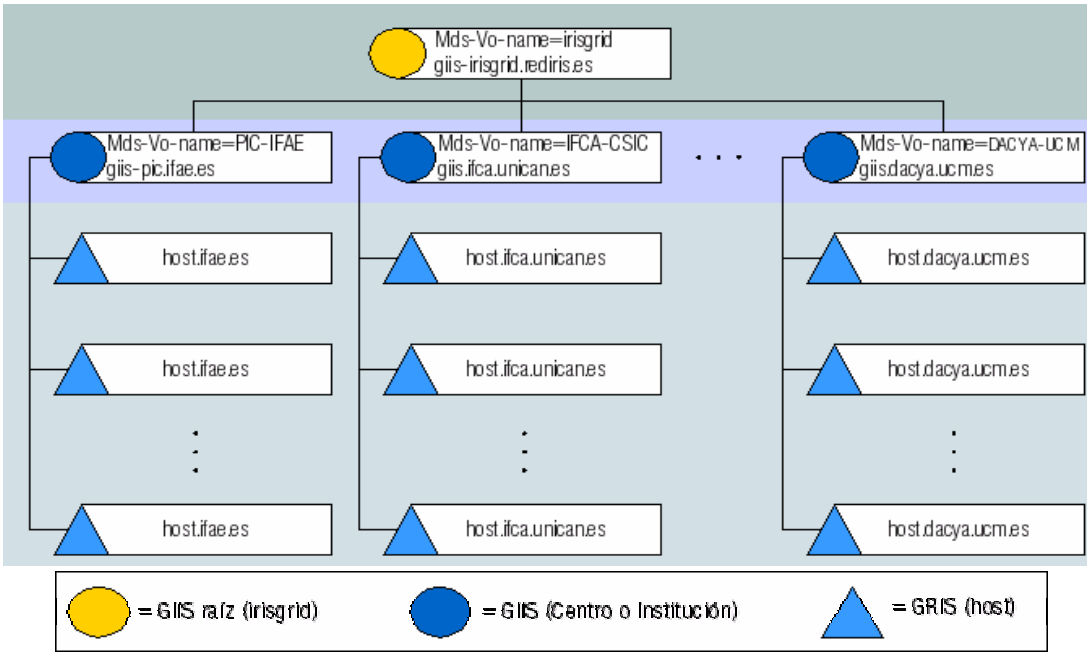

Figura 1: Estructura jerárquica del servicio de información (MDS) de IRISGrid.

Gestión de la Seguridad

Visión Global

La gestión de la seguridad es la componente más importante de un Grid. Debemos establecer procedimientos y políticas de seguridad lo suficientemente robustas como para que en el futuro IRISGrid se pueda convertir en un Grid de producción.

Introducción a la Seguridad en Globus

Autenticación

La infraestructura de seguridad seguida por Globus está basada en PKI (Public Key Infrastructure) por medio del uso de criptografía asimétrica con claves públicas y privadas. La información encriptada por medio de una clave privada sólo puede ser desencriptada por su clave pública y viceversa. La clave privada (`userkey.pem`) sólo es accesible a los usuarios y a las máquinas que desean autenticarse mientras que la clave pública es accesible para todos. La clave pública se distribuye por medio de un certificado X509 (`usercert.pem`) que lleva un identificador único o DN (Distingued Name) correspondiente a un usuario, máquina o servicio, y que está firmado por una CA (Certification Authority). De este modo, cuando un usuario se autentica envía su certificado X509 y su identidad es reconocida si está firmado por una CA de confianza (todo esto se realiza de forma transparente para el usuario por medio del protocolo SSL).

Autorización

Mientras que la autenticación implica demostrar quién se asegura ser, autorizar implica definir el acceso del usuario al sistema. Globus implementa la autorización por medio de un fichero de mapeo que asigna DNs a cuentas UNIX locales. Es importante resaltar que el hecho de que un usuario tenga un certificado X509 firmado por una CA válida, no

implica que esté autorizado a acceder al sistema. Esta decisión es interna a cada centro o institución que es responsable de la gestión de sus propios recursos.

Protocolos de Comunicación Segura

Los certificados certificados X509 emitidos para los usuarios del Grid (grid-cert-request) se usarán, además de para la explotación segura del grid, para garantizar las comunicaciones entre representantes, administradores, coordinador e IRISGrid CA. Para convertir el certificado del formato **`pem`** usado por Globus al formato **`pkcs12`** usado por los clientes de mail comunes (Netscape y Microsoft OutLook) se puede usar el siguiente comando:

```
openssl pkcs12 -export -in usercert.pem -inkey userkey.pem -out cert.p12
```

el fichero de salida cert.p12, puede importarse fácilmente con el gestor de correo. Establecemos los siguientes dos niveles de seguridad, que los gestores de correo habituales implementan de forma automática:

- **Nivel 1**: Integridad y Autenticación del emisor del mensaje: El emisor realizará un resumen del mensaje que encriptará con su clave privada. Este protocolo garantiza que el e-mail no ha sido manipulado y además que el emisor es realmente quien dice ser.

- **Nivel 2**: Confidencialidad: Además de satisfacer el nivel anterior, el e-mail se encriptará con la clave pública del receptor. De este modo, la información viajará por la red encriptada.

Canales de Comunicación

- **Canal de gestión.**

  Los representantes sólo se podrán comunicar con otros Representantes, con el coordinador y con IRISGrid CA. Este canal está destinado a:

  - Realizar peticiones de firma de certificados X509 de nuevos usuarios del Grid (Nivel 1 de seguridad)

  - Realizar peticiones de firma de certificados X509 de nuevos recursos del Grid (Nivel 1 de seguridad)

  - Solicitar autorización en sistemas (Nivel 1 de seguridad), cuando sea necesario comunicar alguna contraseña se empleará el Nivel 2 de seguridad

- **Canal técnico**

  Los administradores se comunicarán entre sí para solventar aspectos técnicos. Cuando un usuario de un centro o institución tenga problemas, se lo comunicará a su Administrador que se pondrá en contacto con el Administrador del centro o institución al cual pertenece la máquina remota. Por defecto para estas comunicaciones se requiere un Nivel 1 de seguridad. Los problemas de seguridad observados también se reportarán por medio de este canal (Nivel 2 de seguridad).

- **Canal interno**

  Es el usado por los usuarios de un centro o institución para comunicarse con su Administrador y Representante, los protocolos de comunicación y niveles de seguridad de este canal dependen de las políticas propias de cada centro o institución.

Resaltar que los puntos anteriores indican un conducto reglamentario de obligado cumplimiento. Un usuario, por ejemplo, no podrá contactar con Representantes y Administradores de otros centros o instituciones. Sin embargo, existe la posibilidad de que una persona desempeñe varios roles (Usuario, Representante o/y Administrador).

Requisitos de IRISGrid CA

La entidad de certificación de IRISGrid es responsable de:

- Crear y mantener una lista de certificados revocados (CRL). La CRL deberá actualizarse inmediatamente después de cada revocación y 7 días antes de su caducidad, que deberá ser de no más de 30 días. Cada centro o institución es responsable de actualizar sus copias locales de la CRL. La CRL se publicará en la página irisgrid.rediris.es
- La CA publicará en irisgrid.rediris.es su política de certificación (Certificate Policy Statement, CPS), de acuerdo a la plantilla del rfc2527
- La CA publicará sus credenciales en irisgrid.rediris.es

La máquina usada para emitir los certificados debe satisfacer los siguientes requisitos:

- Debe ser una máquina dedicada
- La ubicación de la máquina ha de ser segura
- Debe ser administrada por personal cualificado
- La clave privada de la CA, y sus copias, han de permanecer siempre en un entorno seguro
- La clave privada ha de ser encriptada con una *pass phrase* no inferior a 10 caracteres y sólo puede conocerla la persona encargada de emitir (firmar) los certificados
- No puede estar conectada a ninguna red pública.

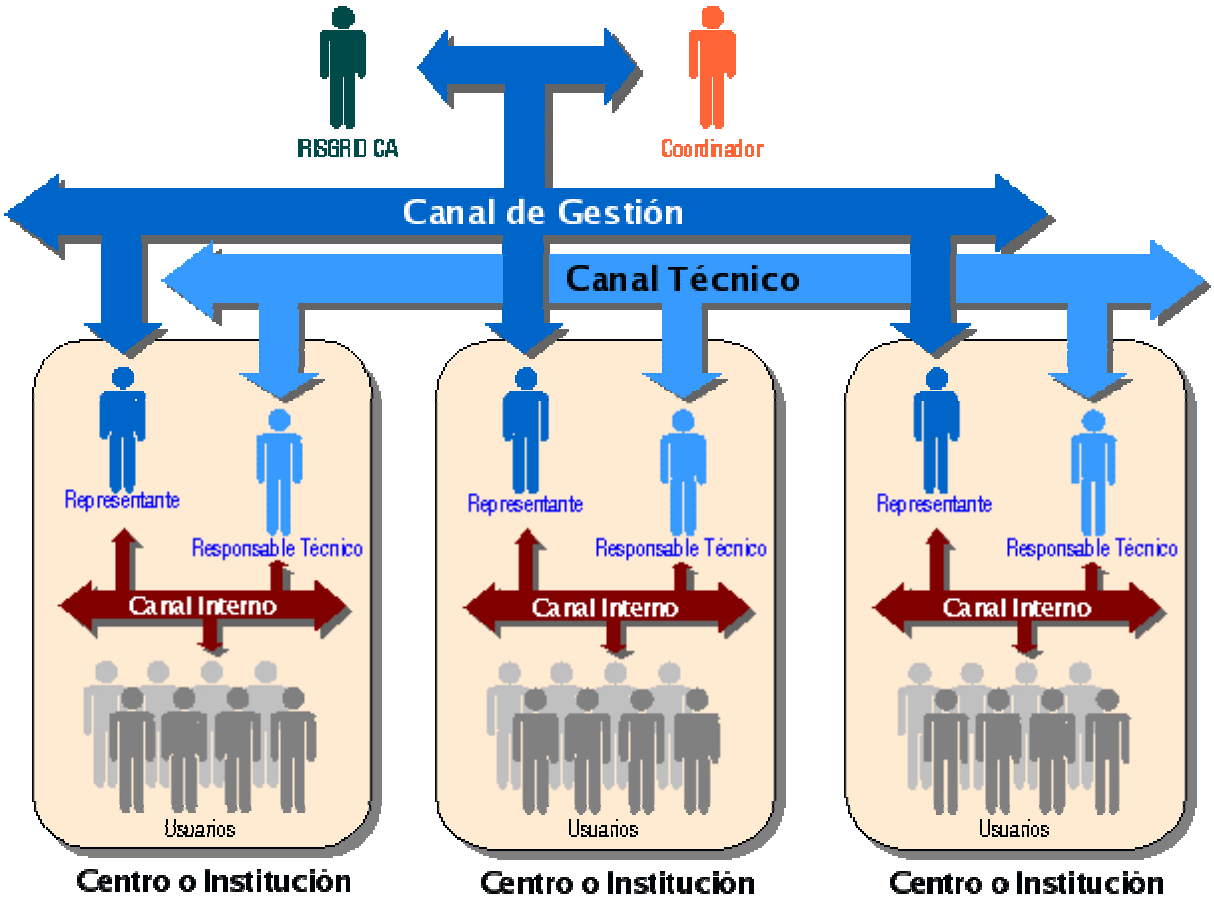

Figura 2: Esquema de los distintos canales de comunicación empleados en IRISGrid.

Procedimientos

Procedimiento para el alta en IRISGrid de instituciones o centros

Las instituciones o centros que deseen participar en la iniciativa IRISGrid deberán seguir los siguientes pasos, independientemente de si la institución o centro incluya únicamente recursos o recursos y usuarios.

Solicitud de nombre institución o centro.

1. Crear una página Web que incluya la siguiente información (ver ejemplos):
   - **Nombre propuesto del institución o centro.**
   - **Representante** (Nombre, teléfono y email).
   - **Responsable Técnico** (Nombre , teléfono, y email).
2. **El representante deberá solicitar el alta de su centro o institución enviado un email al Coordinador de IRISGrid con un enlace a la página Web descrita en el punto anterior.**

Configuración y Solicitud de las Credenciales.

1. El coordinador de IRISGrid enviará la solicitud (Nivel 1 de seguridad) a todos los miembros del Comité Ejecutivo para su evaluación durante un periodo máximo de un día hábil y comprobará que el nuevo centro o institución cumple los requisitos mínimos. El coordinador comunicará al representante del centro o institución candidata el resultado de la evaluación del Comité Ejecutivo.
2. Instalar los paquetes de la CA de IRISGrid mediante la secuencia de comandos:

```
$GPT_LOCATION/sbin/gpt-build \ globus_simple_ca_41d1861c_setup-
0.12.tar.gz <flavor>
$GPT_LOCATION/sbin/gpt-postinstall
$GLOBUS_LOCATION/setup/globus_simple_ca_41d1861c_setup/setup-gsi
```

donde *flavour* definen las opciones de instalación para el centro o institución, por ejemplo, gcc32dbg, vendorcc32dbg, etc.

3. Una vez instalado, modificar el fichero `/etc/grid-security/certificates/globus-user-ssl.conf.41d1861c`:

```
...
[ req_distinguished_name ]
# BEGIN CONFIG
countryName                     = Country Name (2 letter code)
countryName_default             = ES
countryName_min                 = 2
countryName_max                 = 2
0.organizationName              = Level 0 Organization
0.organizationName_default      = IRISGrid
0.organizationalUnitName        = Level 0 Organizational Unit
0.organizationalUnitName_default = DACYA-UCM
commonName                      = Name (e.g., John M. Smith)
commonName_max                  = 64
```

```
emailAddress                    = Email Address
emailAddress_max                = 40
...
```

4. Crea un nuevo certificado X509 para el Representante y otro para el Responsable Tecnico. El DN final debe tener la forma:

```
/C=ES/O=IRISGrid/OU=Nombre_Centro/CN=Nombre Completo/Email=mail
```

Para solicitar los certificados, usar el comando:

```
grid-cert-request -ca -int
```

Se creará, entre otros, el archivo `$HOME/.globus/usercert_request.pem`, ejecutar el siguiente comando para obtener el *fingerprint* de la solicitud (anotar el resultado para comprobarlo posteriormente con IRISGrid CA).

```
openssl dgst -c -sha1 $HOME/.globus/usercert_request.pem
```

La figura del Responsable Técnico es necesaria, aunque el centro o institución solo incluya usuarios, para implementar el Canal Técnico.

5. Añadir IRISGrid CA como CA válida en la herramienta de correo electrónico descargando los ficheros adecuados.

6. El Representante enviará la solicitud a IRISGrid CA quien se pondrá en contacto por teléfono con el con el fin de comprobar la validez de los certificados comparando los *fingerprints* de las solicitudes. Una vez comprobados, IRISGrid CA enviara los certificados firmados al Responsable. (Nivel 1 de seguridad).

7. El Responsable Técnico actualizara la pagina web con los enlaces a los certificados firmados.

   - Nombre del Centro o Institución
   - Representante (Nombre, teléfono, e-mail y certificado X509 firmado por IRISGrid CA
   - Responsable Técnico (nombre, teléfono, e-mail y certificado X509 firmado por IRISGrid CA)

Los certificados deben publicarse en la pagina web en formato `der`, para exportarlos ejecutar el siguiente comando:

```
openssl x509 -outform der -in $HOME/.globus/usercert.pem -out
$HOME/.globus/usercert.der
```

8. El Representante y Responsable Técnico importaran los certificados en su gestor de correo para implementar los canales de seguridad descritos en la sección de seguridad. Los certificados pueden convertirse en formato `pkcs12` (aceptado por los gestores de correo habituales) mediante el comando:

```
openssl pkcs12 -export -in usercert.pem -inkey userkey.pem -out
usercert.p12
```

Procedimiento para Solicitar el Alta de Nuevos Recursos

El siguiente procedimiento supone la existencia de un centro o institucion dado de alta de acuerdo al procedimiento anterior.

1. Cuando se añaden nuevos recursos es necesario crear certificados para las máquinas y sus servicios. Estos certificados se crean con el DN recomendado por Globus pero siempre usando el formato:

   ```
   /C=ES/O=IRISGrid/OU=Nombre_Centro/CN=host/FQDN maquina
   ```

   para generar el certificado ejecutar el comando:

   ```
   grid-cert-request -ca -host FQDN
   ```

2. Actualizar la página web para que incluya información del sitio (ver ejemplos):
   - Nombre del Centro o Institución
   - Representante (Nombre, teléfono, e-mail y certificado X509 firmado por IRISGrid CA
   - Responsable Técnico (nombre, teléfono, e-mail y certificado X509 firmado por IRISGrid CA)
   - Credenciales de su CA si es diferente a IRISGrid CA
   - Sistemas conectados al Grid (nombre, arquitectura, sistema operativo, y componentes Globus instalados).
3. El Representante deberá solicitar la firma de los nuevos certificados enviándolos por mail a IRISGrid CA (Nivel 1 de seguridad), que firmara los certificados y los devolverá en un e-mail al Representante (Nivel 1 de seguridad). El Responsable Técnico instalará los certificados de los nuevos recursos.

Procedimiento para Solicitar el Alta de Nuevos Usuarios

El siguiente procedimiento supone la existencia de un centro o institucion dado de alta de acuerdo al procedimiento anterior.

1. Crea un nuevo certificado X509 para el usuario. El DN final debe tener la forma:

   ```
   /C=ES/O=IRISGrid/OU=Nombre_Centro/CN=Nombre Completo/Email=mail
   ```

   Para solicitar los certificados, usar el comando:
   ```
   grid-cert-request -ca -int
   ```

2. El Representante deberá solicitar la firma de los nuevos certificados enviando un mail a IRISGrid CA. Es importante resaltar que el Representante es el encargado de autenticar internamente dentro de su institucion o centro a los usuarios. Todos los nuevos usuarios deberán enviar firmado (primero por fax y luego por correo) el documento de compromiso de seguridad de IRISGrid (ver la sección de Documentos) a la dirección postal de IRISGrid CA. IRISGrid CA firmara los certificados y los enviara en un e-mail de vuelta al Representante (Nivel 1de seguridad).

Procedimiento para Solicitar la Autorización para el uso de Recursos

IRISGrid proporciona autenticación. Sin embargo, la autorización se realiza de forma totalmente independiente dentro de cada institucion o centro. Para solicitar la autorización a usar un sistema gestionado por una institucion o centro se seguirán los siguientes pasos:

1. En la pagina web de cada institucion o centro se describe la información necesaria que se deberá enviar a su Representante. Siempre será el Representante de cada institucion o centro el que solicite autorización a otro Representante (Nivel 1 de seguridad).

2. Cada institucion o centro decidirá si autoriza el uso de sus máquinas y los procedimientos que deberá utilizar el solicitante, así como las políticas y procedimientos de seguridad internos que deberá respetar. En tal caso podrá (si es necesario) enviar la contraseña del nuevo usuario al Representante que lo solicito (Nivel 2 de seguridad).

Procedimiento para Dar de Baja un Usuario

El Representante de cada institucion o centro debe llevar un registro de todas las cuentas que ha solicitado para los usuarios de su institucion o centro. Cuando un usuario no vaya a usar el Grid, el Representante debe informar a los Responsables Técnicos de todas las instituciones o centros donde el usuario tenia cuenta. Además deberá informar a IRISGrid CA para añadirlo en la CRL.

Preguntas Frecuentes (FAQ)

¿Qué ocurre si tengo mis sistemas y mis usuarios de alta en otro Grid (DataGrid, CrossGrid...)?

En tal caso, los certificados tanto de las máquinas como de los usuarios estarán firmados por la CA de, por ejemplo, DataGrid. Para evitar líos, estas máquinas y usuarios no necesitarían volver a crear nuevos certificados firmados por IRISGrid CA y podrían mantener los existentes. Lo importante es que estos sistemas deben configurar la CA de IRISGrid como de confianza y además los centros o instituciones que quieran usar estas máquinas deberán declarar la CA de DataGrid como de confianza. Los Grupos IRISGrid que usen una CA diferente a IRISGrid deberán poner en su página web las credenciales de esta. Sin embargo, el Representante y Administrador del Grupo deberán tener certificados firmados por IRISGrid CA para poder implementar los canales de comunicación segura.

¿Puede un usuario pertenecer a varios centros o instituciones?

Si, un usuario puede mantener certificados firmados por diferentes CAs e incluso con centros o instituciones diferentes en su directorio `$HOME/.globus`. Cuando se crea el proxy de certificación, el usuario debe indicar el certificado que pretende usar (`grid-proxy-init -cert <certfile> -key <keyfile>`).

Apéndice A

Compromiso de Uso de los Sistemas de IRISGrid

El siguiente documento describe las reglas de uso para los recursos informáticos (computadores, servidores, dispositivo de red, programas, base de datos, sistema de almacenamiento, etc) dentro de IRISGrid. El objetivo de este documento es asegurar que todos los usuarios del Grid usan los recursos de un modo efectivo, eficiente, ético y dentro del marco legal actual.

Reglas Generales

- El Representante de nuestro centro o institución nos dará la cuenta de usuario y nos indicará a qué recursos podemos acceder. Está prohibido acceder a un recurso si no hemos recibido un permiso explícito
- Las cuentas solo se pueden utilizar para el propósito para el cual fueron solicitadas y nunca se podrán utilizar para actividades no relacionadas con la investigación.
- Los usuarios son los responsables de proteger la información que tienen dentro de sus cuentas, por ejemplo ficheros fuente sobre los que se trabaja temporalmente en caso de un proyecto confidencial. Esta protección implica tanto evitar que sea leída, como modificada o borrada
- Los usuarios deberán informar al responsable de seguridad de cualquier vulnerabilidad que observen
- Los usuarios no deberán intentar acceder ni a información ni a sistemas para los cuales no se les ha dado permiso explícito
- Esta terminantemente prohibido hacer copias de software propietario protegido con copyright, excepto si hay permiso del propietario del copyright
- El usuario no puede copiar ni transmitir por la red ficheros de configuración del sistema (por ejemplo /etc/passwd)
- El usuario no puede copiar ni transmitir por la red información confidencial
- El usuario no debe realizar acciones que fastidien innecesariamente a otros usuarios, degraden el rendimiento de los sistemas, o circunvalen mecanismos de seguridad o auditoria.
- No se podrá enviar ni almacenar dentro de los equipos información fraudulenta u obscena.
- El usuario no podrá bajar de la red ni instalar herramientas relacionadas con seguridad que revelen vulnerabilidades en los sistemas
- En caso de detectar incidencias de seguridad se deberá informar rápidamente a su Administrador, y éste al Administrador del centro o institución donde se detectaron las incidencias

Criterios de selección de contraseñas y planificación de envejecimiento

Las contraseñas se deben modificar cada dos meses siguiendo las siguientes normas:

- No se debe escribir la contraseña
- Está prohibido almacenar la contraseña en el sistema sin encriptar
- Nunca se enviará la contraseña por mail
- Nunca se comunicará por teléfono

- Nunca una sola cuenta puede ser compartida entre varios usuarios
- No usar palabras de diccionario (aunque le añadamos números)
- No usar combinaciones de letras de nuestro nombre, usuario o apodo (un cracker tarda segundos en averiguar que la contraseña es nuestro nombre al revés)
- No usar combinaciones de letras de personajes famosos
- No usar combinaciones de letras de nombres de esposa, hijos, novia, mascota, ... (un atacante que le conozca puede obtener la contraseña fácilmente)
- No usar números con significado especial (NIF, teléfono, matrícula, ...)
- No usar solo dígitos o toda la misma letra
- No usar una contraseña de menos de 6 caracteres
- Usar contraseñas que combinen mayúsculas y minúsculas
- Evitar combinaciones lineales del teclado (pueden ser observadas fácilmente)
- Usar contraseñas con caracteres especiales ^, +, %, &, $, ...
- Usar una contraseña que se pueda escribir rápidamente (pueden ser observadas fácilmente)

El no cumplimiento de alguna de estas reglas constituirá una violación de la seguridad y la baja permanente en IRISGrid; y en función de su importancia incluso actuaciones legales. El abajo firmante ha leído y entendido todas y cada una de las normas arriba expuestas.

Nombre del usuario: DNI:

Nombre del Centro o Institución:

Firma del usuario Firma del Representante Fecha

Apéndice B

Configuración jerárquica del MDS

En el siguiente ejemplo supondremos los siguientes hosts:

- `draco.dacya.ucm.es`, máquina perteneciente a la `VO DACYA-UCM`, con su servidor GRIS
- `ursa.dacya.ucm.es`, máquina perteneciente a la `VO DACYA-UCM`, con su servidor GRIS y actuará como servidor GIIS de la VO DACYA-UCM

A continuación se detallan los pasos para configurar ambas máquinas

`draco.dacya.ucm.es (sólo GRIS)`

- Comentar o eliminar las siguientes líneas del archivo `$GLOBUS_LOCATION/etc/grid-info-slapd.conf`:

```
# database        giis
# suffix          "Mds-Vo-name=site, o=Grid"
# conf            /usr/local/globus/etc/grid-info-site-giis.conf
# policyfile      /usr/local/globus/etc/grid-info-site-policy.conf
# anonymousbind   yes
# access to * by * write
```

- Modificar el archivo `$GLOBUS_LOCATION/etc/grid-info-resource-register.conf`:

```
# registrar el GRIS de draco al servidor GIIS de DACYA-UCM (ursa)
dn: Mds-Vo-Op-name=register, Mds-Vo-name=DACYA-UCM, o=grid
regtype: mdsreg2
reghn: ursa.dacya.ucm.es
regport: 2135
regperiod: 600
type: ldap
hn: draco.dacya.ucm.es
port: 2135
rootdn: Mds-Vo-name=local, o=grid
ttl: 1200
timeout: 20
mode: cachedump
cachettl: 30
```

- Modificar las variables de entorno en el archivo `$GLOBUS_LOCATION/etc/grid-info.conf`:

```
GRID_INFO_HOST="draco.dacya.ucm.es"
GRID_INFO_PORT="2135"
GRID_INFO_BASEDN="Mds-Vo-name=local, o=grid"
GRID_INFO_ORGANIZATION_DN="Mds-Vo-name=IRISGRID, o=grid"
GRID_INFO_ORGANIZATION_ADMIN_DN=""
GRID_INFO_TIMEOUT="30"
```

- Reiniciar el demonio slapd

ursa.dacya.ucm.es (GRIS + GIIS de DACYA-UCM)

- Modificar el archivo `$GLOBUS_LOCATION/etc/grid-info-slapd.conf`, para añadir una nueva entrada para el GIIS de DACYA-UCM:

```
# Configuración del servidor GRIS de ursa (permite binding anonimo)
database    ldif
suffix            "Mds-Vo-name=local,o=grid"
conf        /usr/local/globus/etc/grid-info-resource-ldif.conf
anonymousbind   yes
access to * by * write

# Configuracion del servidor GIIS de la VO: DACYA-UCM GRIIS
database        giis
suffix          "Mds-Vo-name=DACYA-UCM,o=grid"
conf            /usr/local/globus/etc/grid-info-site-giis.conf
policyfile      /usr/local/globus/etc/grid-info-site-policy.conf
anonymousbind   yes
access to * by * write
```

- Modificar el archivo `$GLOBUS_LOCATION/etc/grid-info-resource-register.conf`:

```
# Registrar el servidor GIIS de DACYA-UCM al servidor GIIS de IRISGRID
dn: Mds-Vo-Op-name=register, Mds-Vo-name=IRISGRID, o=grid
regtype: mdsreg2
reghn: giis-IRISGrid.ifae.es
regport: 2135
regperiod: 600
type: ldap
hn: ursa.dacya.ucm.es
port: 2135
rootdn: Mds-Vo-name=DACYA-UCM, o=grid
ttl: 1200
timeout: 20
mode: cachedump
cachettl: 30

# Registrar el servidor GRIS de ursa al servidor GIIS de DACYA-UCM
(ursa)
dn: Mds-Vo-Op-name=register, Mds-Vo-name=ASDS-DACYA, o=grid
regtype: mdsreg2
reghn: ursa.dacya.ucm.es
regport: 2135
regperiod: 600
type: ldap
hn: ursa.dacya.ucm.es
port: 2135
rootdn: Mds-Vo-name=local, o=grid
ttl: 1200
timeout: 20
mode: cachedump
cachettl: 30
```

- Modificar las variables de entorno en el archivo `$GLOBUS_LOCATION/etc/grid-info.conf`:

```
GRID_INFO_HOST="ursa.dacya.ucm.es"
GRID_INFO_PORT="2135"
GRID_INFO_BASEDN="Mds-Vo-name=local, o=grid"
GRID_INFO_ORGANIZATION_DN="Mds-Vo-name=IRISGRID, o=grid"
GRID_INFO_ORGANIZATION_ADMIN_DN=""
GRID_INFO_TIMEOUT="30"
```

- Reiniciar el demonio slapd