

# **Política para la RA “RedIRIS” de pkIRISGrid**

v: 1.1.0

Sevilla, 2 de marzo 2009

## Índice de contenido

<b>Historia</b> .....	<b>3</b>
<b>1. Presentación</b> .....	<b>4</b>
<b>2. Operadores de la RA</b> .....	<b>4</b>
<b>3. Aprobación de solicitudes de certificado</b> .....	<b>4</b>
3.1. Autenticación del solicitante.....	4
3.1.1. Reunión cara a cara.....	4
3.1.1.1 Detalles de la reunión.....	5
3.1.1.2 Documentos Aceptados.....	5
3.1.1.3 Documentación archivada.....	5
3.1.2 Otros métodos.....	5
3.2 Verificación del solicitante.....	6
3.2.1 Descripción del procedimiento para certificado de personas físicas.....	6
3.2.1.1 Verificación en la reunión cara a cara.....	6
3.2.2 Descripción del procedimiento para certificado de servidor.....	6
3.2.3 Documentación archivada.....	6
<b>4. Política de revocaciones</b> .....	<b>7</b>
4.1 Solicitud de revocaciones por iniciativa de la RA.....	7
4.2 Solicitud de revocaciones por iniciativa del usuario del Certificado.....	7
4.3 Solicitud de revocación cuando un usuario abandona la institución.....	7

## Historia

02/03/2009	1.1.0	Javi Masa	Incorporación del carné de conducir, NIE y documentos de identidad válidos en países comunitarios como documentos acreditativos de identidad
26/02/2009	1.0.2	Javi Masa	Aclaración sobre el uso del DNI electrónico y la no validez del uso del certificado almacenado en el DNI electrónico como método de autenticación
22/12/2008	1.0.1	Javi Masa	Modificaciones relacionadas con la autenticación del solicitante y el DNI electrónico
20070312	1.0.0	Javi Masa	Revisión y formato.
20061015	0.5.0	Javi Masa	Versión inicial

## 1. Presentación

RedIRIS es la red académica y de investigación española y proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional. Está financiada por el Ministerio de Ciencia e Innovación, e incluida en su mapa de Instalaciones Científico Tecnológicas Singulares. RedIRIS cuenta con más de 350 instituciones afiliadas, principalmente universidades y centros públicos de investigación.

RedIRIS está involucrada tanto en la administración de la pkIRISGrid como en proyectos nacionales e internacionales que requieren el uso de pkIRISGrid. Por ello es necesaria la creación de una RA en RedIRIS.

En este documento se presenta la política de RedIRIS como RA de pkIRISGrid.

## 2. Operadores de la RA

Los operadores de la RA de RedIRIS han de ser personal de RedIRIS, con más de dos años de experiencia en RedIRIS, y con conocimientos medios de informática.

Todos los operadores de la RA de RedIRIS deben haber sido formados para su labor por personal de pkIRISGrid u otros operadores de la RA de RedIRIS.

Cuándo un operador deja de serlo o abandona RedIRIS, los restantes operadores cambian la contraseña de operador.

## 3. Aprobación de solicitudes de certificado.

La RA de la RedIRIS aprueba solicitudes de certificado tanto de usuario como de servidor para sus investigadores.

### 3.1. Autenticación del solicitante

El proceso de autenticación del solicitante de certificados será el mismo tanto para solicitudes de certificado de usuario como de servidor.

#### 3.1.1. Reunión cara a cara

La única forma de autenticación del solicitante de un certificado es mediante la **reunión cara a cara**.

Una vez que ha solicitado su certificado desde su navegador y haya sido contactado por un operador de RA, el solicitante se desplazará a la RA de RedIRIS, presentará un documento de identidad aceptado, y comunicará su pin al operador. Éste procederá a generar la documentación descrita más abajo, archivarla, y aprobará la solicitud.

Una vez aprobada, el operador de la RA enviará la solicitud a la CA en el plazo de dos días laborables.

### 3.1.1.1 Detalles de la reunión

La reunión será acordada mediante correo electrónico con el operador de la RA y se celebrará en alguna de las dependencias de RedIRIS ubicadas en los siguientes centros:

- RedIRIS Sevilla.  
Edificio CICA  
Avenida Reina Mercedes, s/n  
41012 Sevilla
- RedIRIS Madrid.  
Edificio Bronce  
Plaza Manuel Gómez Moreno, s/n - 2ª planta  
28020. Madrid

La no presentación por parte del solicitante en la fecha, hora y lugar acordados, provocará que se desestime la solicitud.

Tanto el solicitante como el operador de la RA informarán con antelación suficiente sobre cualquier impedimento para reunirse en la fecha y lugar acordados. En este caso, se volverá a establecer una nueva reunión.

### 3.1.1.2 Documentos Aceptados

Los documentos aceptados son los siguientes:

- Ciudadanos españoles: **DNI** (tradicional, electrónico), **pasaporte** o permiso de **conducir**.  
Ni el carné de RedIRIS ni cualquier otro documento similar será aceptado para la autenticación aunque tengan fotografía.  
En el caso de uso del DNI electrónico deberá mostrarse en la reunión cara a cara al operador de la RA. No será válido el envío de un correo electrónico firmado con el certificado incluido en el DNI electrónico para evitar la reunión cara a cara.
- Ciudadanos comunitarios: **Pasaporte** o bien el documento de **identidad legal en su país** de origen, siempre que contenga fotografía.
- Ciudadanos extranjeros: **Pasaporte** o **NIE** (carné de Número de Identificación de Extranjeros). No se aceptarán NIE en tramitación, sólo definitivos con la tarjeta que muestre la fotografía

### 3.1.1.3 Documentación archivada

En el proceso de autenticación del solicitante el operador de la RA contrastará los datos de la solicitud del certificado con los del documento de identidad presentado. Si los datos son correctos, se fotocopiarán tanto el documento de identidad presentado como el documento con los datos de la solicitud de certificado que el usuario imprimió al realizar la misma, y se guardarán para futuras auditorías.

### 3.1.2 Otros métodos

No aplicable.

## **3.2 Verificación del solicitante**

Tras la autenticación del solicitante, se ha de verificar la autoridad de éste para solicitarlo antes de aprobar la solicitud. En todos los casos se verificará la dirección de correo electrónico.

### **3.2.1 Descripción del procedimiento para certificado de personas físicas**

#### **3.2.1.1 Verificación en la reunión cara a cara**

El solicitante presentará en la reunión cara a cara con la RA su carné de RedIRIS. El carné se fotocopiará y se guardará junto a las fotocopias de los documentos que se hicieron en la fase de autenticación.

Se verificará el correo electrónico pidiendo al solicitante que responda al correo con el que se le cita a la reunión cara a cara, antes de acudir a ella.

En caso de que el solicitante sea personal visitante de RedIRIS deberá presentar un documento, firmado por el director de la institución, que le acredite como tal.

#### **3.2.2 Descripción del procedimiento para certificado de servidor**

La persona solicitante deberá presentar un documento firmado por el responsable de la máquina que autoricen al solicitante a pedir un certificado de servidor. Este documento o documentos se guardarán junto con los documentos generados en la fase de autenticación.

#### **3.2.3 Documentación archivada**

Descrito en los apartados 3.2.1 y 3.2.2.

## 4. Política de revocaciones

Las siguientes subsecciones describen en qué casos la RA puede solicitar la revocación de un certificado. En todas las solicitudes de revocación se generará un informe con los datos del operador que la solicitó, la circunstancias que provocaron la solicitud, la fecha, y otros documentos justifiquen dicha decisión, como los datos de autenticación en caso de iniciativa del usuario, o informes que muestren el mal uso de los certificados.

### 4.1 Solicitud de revocaciones por iniciativa de la RA

La RA solicitará la revocación de un certificado por iniciativa propia cuando:

- En el caso de un usuario:
  - Está usando los servicios a los que tiene acceso con su certificado para usos ajenos a la RedIRIS o de forma indebida.
  - Se detecta que el usuario tiene instalado el certificado en un ordenador al que tienen acceso varias personas.
  - Se detecta un robo de la clave pública.
  - El usuario comparte su certificado o le da otros usos incompatibles con el objetivo de un certificado digital.
  - El usuario deja de tener permiso de la institución que lo avaló para usar el certificado.
  - Otros usos del certificado que el operador estime incorrectos o que puedan dañar la imagen o la reputación de pkIRISGrid o de RedIRIS.
- En el caso de certificados de servicio/servidor:
  - Se detecta que la clave privada del servidor se ha visto comprometida.
  - Se detecta que el certificado está instalado en varias máquinas, sin ser un sistema de alta disponibilidad.
  - El servicio que ofrecía el servidor para el que se pidió el certificado deja de ofrecerse.

### 4.2 Solicitud de revocaciones por iniciativa del usuario del Certificado

La RA solicitará la revocación de un certificado a petición del usuario siempre que éste se autentique (de acuerdo con la subsección 3.1 sobre autenticación), o lo solicite por teléfono comunicando el pin del certificado.

### 4.3 Solicitud de revocación cuando un usuario abandona la institución

La secretaría de recursos humanos de la RedIRIS informa a la RA siempre que hay una baja de personal, ya sea local o visitante. La RA procede entonces a emitir la solicitud de revocación de certificado.