

# Política para la RA de pkIRISGrid Universidad de Almería

Version	Fecha	Comentario	Autor
1.0	16/10/2009	Redacción del documento	Raúl Martín
1.1	26/06/2013	Revisión	Antonio Casado

Política para la RA de pkIRISGrid Universidad de Almería .....	1
1. Presentación .....	3
2. Operadores de la RA.....	3
3. Cómo solicitar un certificado.....	3
4. Aprobación de solicitudes de certificado .....	3
4.1. Autenticación del solicitante .....	3
4.1.1. Reunión personal.....	3
4.1.1.1 Detalles de la reunión .....	4
4.1.1.2 Documentos Aceptados.....	4
4.1.1.3 Documentación archivada .....	4
4.1.2 Otros métodos.....	4
4.2 Verificación del solicitante .....	4
4.2.1 Descripción del procedimiento para certificado de personas físicas.....	4
4.2.1.1 Verificación en la reunión cara a cara .....	4
4.2.2 Descripción del procedimiento para certificado de servidor.....	5
4.2.2.1 Cambio de administrador para el servidor.....	5
4.2.3 Documentación archivada .....	5
5. Política de revocaciones .....	5
5.1 Solicitud de revocaciones por iniciativa de la RA .....	5
5.2 Solicitud de revocaciones por iniciativa del usuario del Certificado.....	6
5.3 Solicitud de revocación cuando un usuario abandona la institución.....	6

## 1. Presentación

En el presente documento se detalla la política de La Universidad Almería (en adelante UAL) como RA de pkIRISGrid. La política descrita en este documento se aplicará a las solicitudes de certificado recibidas después de la fecha de publicación de este documento.

La UAL, situada en Almería, es una institución dedicada a la educación universitaria y a la investigación.

## 2. Operadores de la RA

Los operadores de la RA de la UAL han de ser personal de la Universidad de Almería con contrato estable, con más de dos años de experiencia en la Universidad de Almería, y con conocimientos medios de informática.

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

Cuándo un operador deja de serlo o abandona la Universidad de Almería, se le quitarán los permisos de acceso a la RA de la UAL a través de SIR (Servicio de Identidad de RedIRIS).

## 3. Cómo solicitar un certificado

En el siguiente enlace se puede solicitar, renovar o revocar un certificado digital para persona física o para un servidor/servicio bajo la UAL como RA de pkIRISGrid:

<https://pki.irisgrid.es/rat37/>

Antes de solicitar el certificado digital es recomendable leer la documentación disponible en <http://pki.irisgrid.es/doc/>

## 4. Aprobación de solicitudes de certificado

La RA de la UAL aprueba solicitudes de certificado, tanto de usuario como de servidor, siempre y cuando se soliciten para el dominio 'ual.es' y el solicitante pertenezca a la UAL.

### 4.1. Autenticación del solicitante

Será obligatoria la autenticación del solicitante, tanto en solicitudes de certificado de usuario como de servidor, siguiendo uno de los procesos que se detallan a continuación.

#### 4.1.1. Reunión personal

La única forma de autenticación del solicitante es mediante la **reunión cara a cara**, para la cual solicitará cita previa mediante el Centro de Atención al Usuario (CAU, <http://cau.ual.es>, 950015999).

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 la Universidad de Almería en la fecha y hora indicadas, presentará uno de los documentos aceptados en el punto 4.1.1.2, 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.

#### *4.1.1.1 Detalles de la reunión*

La RA de la Universidad de Almería está situada en el edificio CITIC (Científico Técnico de Informática y Comunicaciones), despachos 2.22 y 2.23 de planta segunda.

El horario de atención al solicitante es de 12:30 a 15:00, de lunes a viernes. El solicitante dispondrá de un plazo de 7 días hábiles para acudir a la reunión cara a cara después de que el operador de la RA haya contactado con él, si bien los días pueden variar dependiendo de la disponibilidad de los operadores.

#### *4.1.1.2 Documentos Aceptados*

Los documentos aceptados son los siguientes:

- Ciudadanos españoles: **DNI, pasaporte o permiso de conducir**.  
Ni el carné de la Universidad de Almería 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.

#### *4.1.1.3 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.

#### *4.1.2 Otros métodos*

No aplicable.

### *4.2 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.

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

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

El solicitante presentará en la reunión cara a cara con la RA uno de los documentos aceptados en el apartado 4.1.1.2. El documento aceptado 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 la Universidad de Almería deberá presentar un documento, firmado por el responsable de su estancia (director de Grupo de Investigación o Departamento), que le acredite como tal.

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

El solicitante presentará en la reunión cara a cara con la RA uno de los documentos aceptados en el apartado 4.1.1.2. La autenticación del solicitante se describe en el apartado 4.1.

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

##### *4.2.2.1 Cambio de administrador para el servidor*

En caso de que el administrador del servidor pase a ser una persona distinta, será necesario que el solicitante vuelva a repetir el proceso que se describe en el apartado 4.2.2, pero no será necesario volver a solicitar el certificado desde la página de pkIRISGrid.

##### *4.2.3 Documentación archivada*

Descrito en los apartados 4.2.1 y 4.2.2.

## **5. Política de revocaciones**

Las siguientes subsecciones describen en qué casos se puede solicitar la revocación de un certificado. La revocación puede ser realizada por:

- Iniciativa de la RA.
- Iniciativa del usuario del certificado.
- Iniciativa del usuario del certificado cuando éste abandona la institución para la que pidió el certificado inicialmente

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

### ***5.1 Solicitud de revocaciones por iniciativa de la RA***

La RA solicitará la revocación de un certificado por iniciativa propia siempre que se cumpla alguno de los siguientes casos:

- En el caso de un certificado de usuario:
  - Cuando el usuario utilice su certificado para usos ajenos a la Universidad de Almería o de forma indebida.
  - Cuando se detecta que el certificado es usado por varias personas.
  - Cuando se sospecha de un robo de la clave privada.
  - Cuando el usuario comparte su certificado o le da otros usos incompatibles con el objetivo de un certificado digital.
  - Cuando el usuario deja de tener permiso por 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 la Universidad de Almería.
- En el caso de certificados de servicio/servidor:

- Cuando se detecta que la clave privada del servidor se ha visto comprometida.
- Cuando se detecta que el certificado está instalado en varias máquinas, sin ser un sistema de alta disponibilidad.
- Cuando el servicio que ofrecía el servidor para el que se pidió el certificado deja de ofrecerse.

### ***5.2 Solicitud de revocaciones por iniciativa del usuario del Certificado***

La RA solicitará la revocación de un certificado digital de usuario o servidor a petición del usuario siempre que éste se autentique (de acuerdo con la subsección 4.1 sobre autenticación), o lo solicite por teléfono comunicando el pin del certificado.

### ***5.3 Solicitud de revocación cuando un usuario abandona la institución***

Cuando un usuario termine su vinculación con la institución a la que pertenecía y que le daba derecho a solicitar el certificado, deberá informar a la RA de la UAL e iniciar la revocación a iniciativa del usuario.