

# Reunión administradores de autoridades de registro de pkIRISGrid CA

## pkIRISGrid RAdmin 2

Daniel García - [daniel.garcia@rediris.es](mailto:daniel.garcia@rediris.es)

Javi Masa - [javier.masa@rediris.es](mailto:javier.masa@rediris.es)

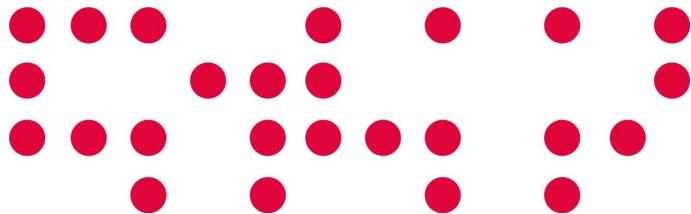


red.es

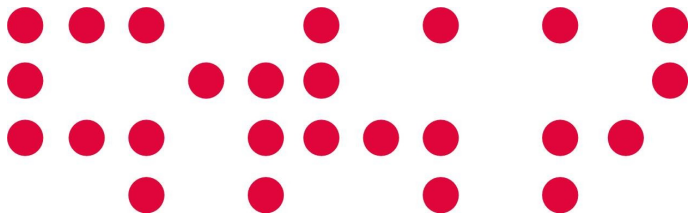


Oviedo, 20 de noviembre de 2007

- 1 Bienvenida**
- 2 Escenario actual
- 3 Mejoras en el servicio
- 4 Política de una RA
- 5 Problemas encontrados
- 6 Futuro
- 7 Ruegos y preguntas



- 1 Bienvenida
- 2 Escenario actual**
- 3 Mejoras en el servicio
- 4 Política de una RA
- 5 Problemas encontrados
- 6 Futuro
- 7 Ruegos y preguntas



## • RAs

- 29 RAs
- 13 localizaciones

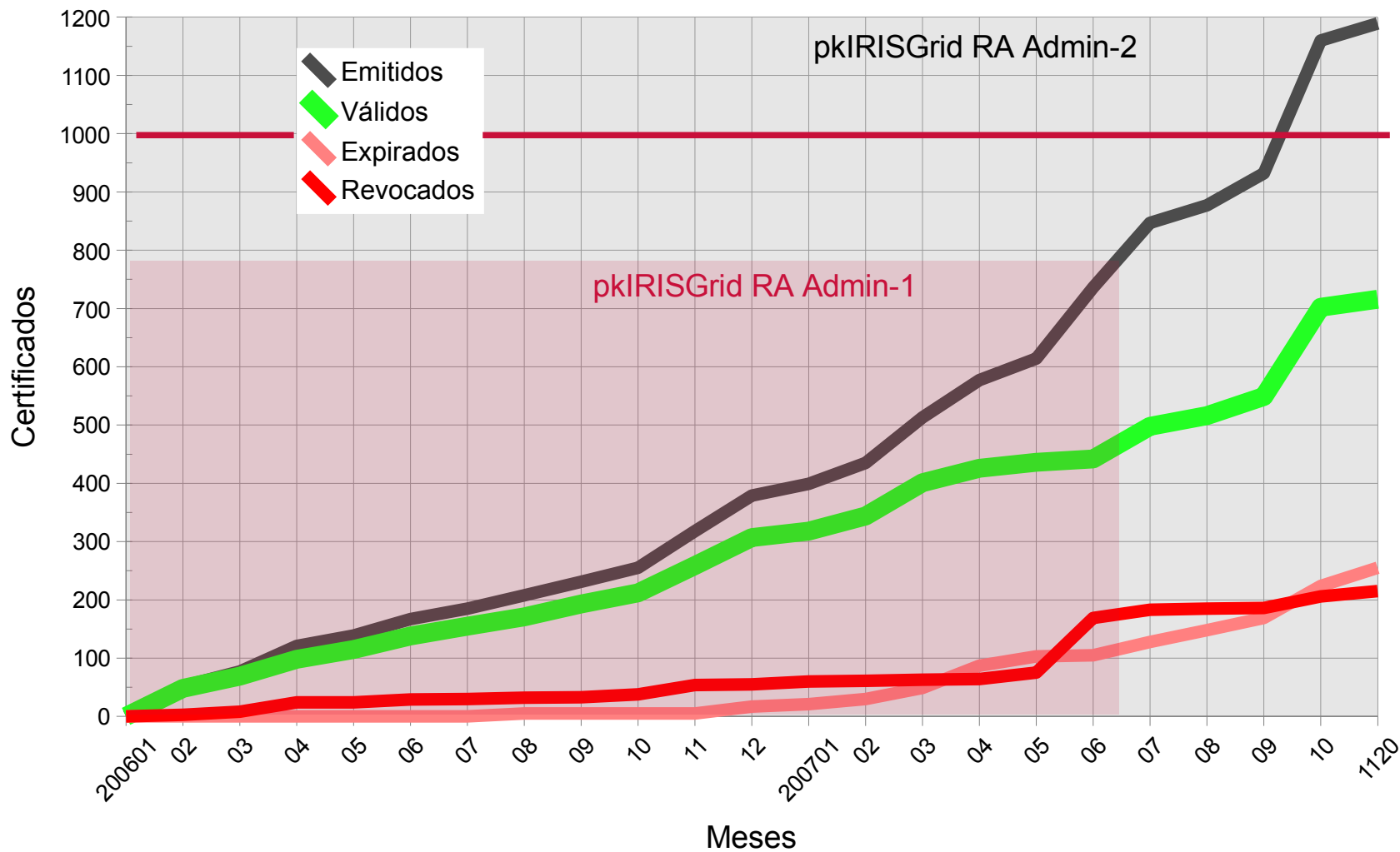
## • Certificados

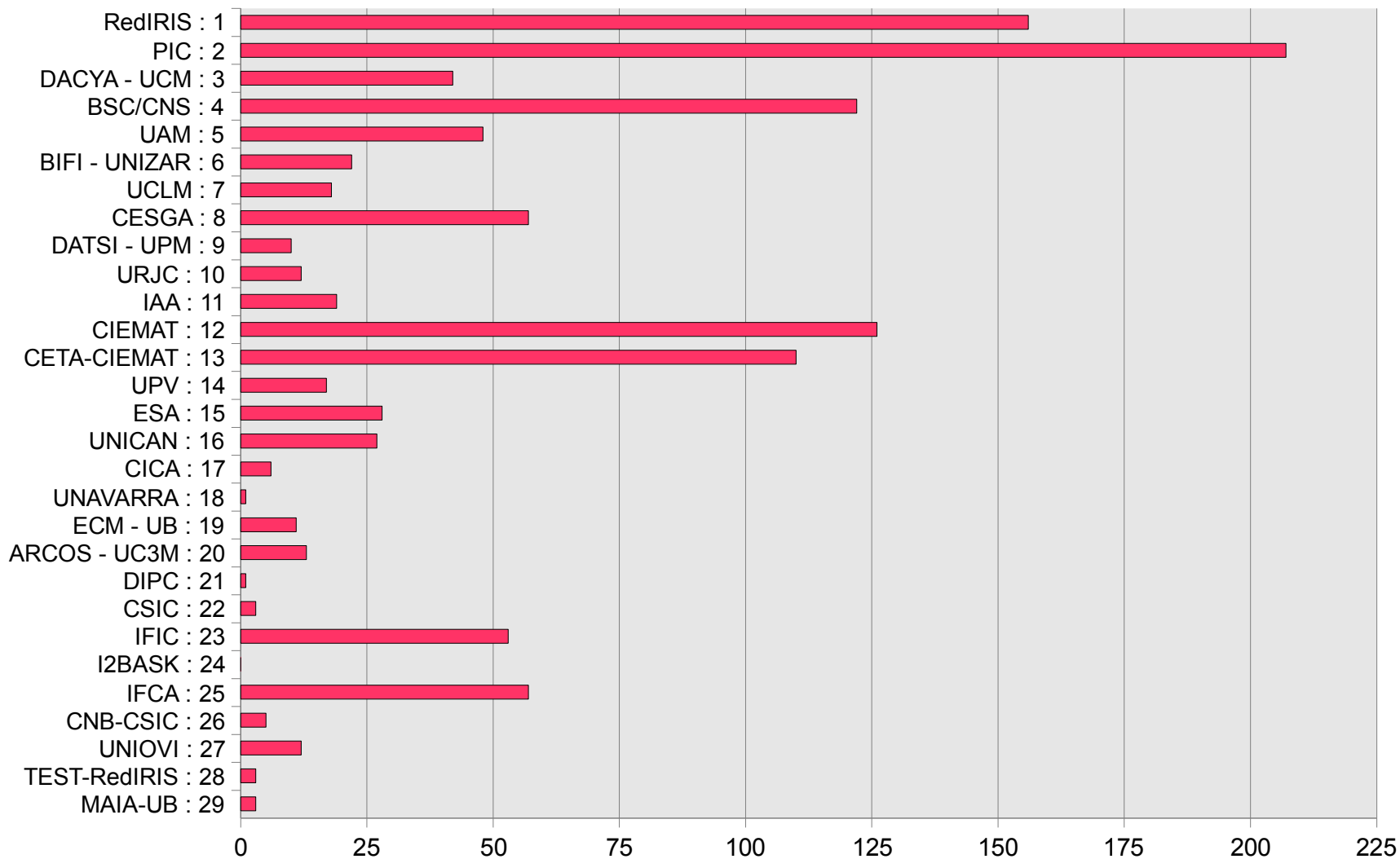
- 1200 emitidos
  - 537 usuario
  - 667 host/servicio

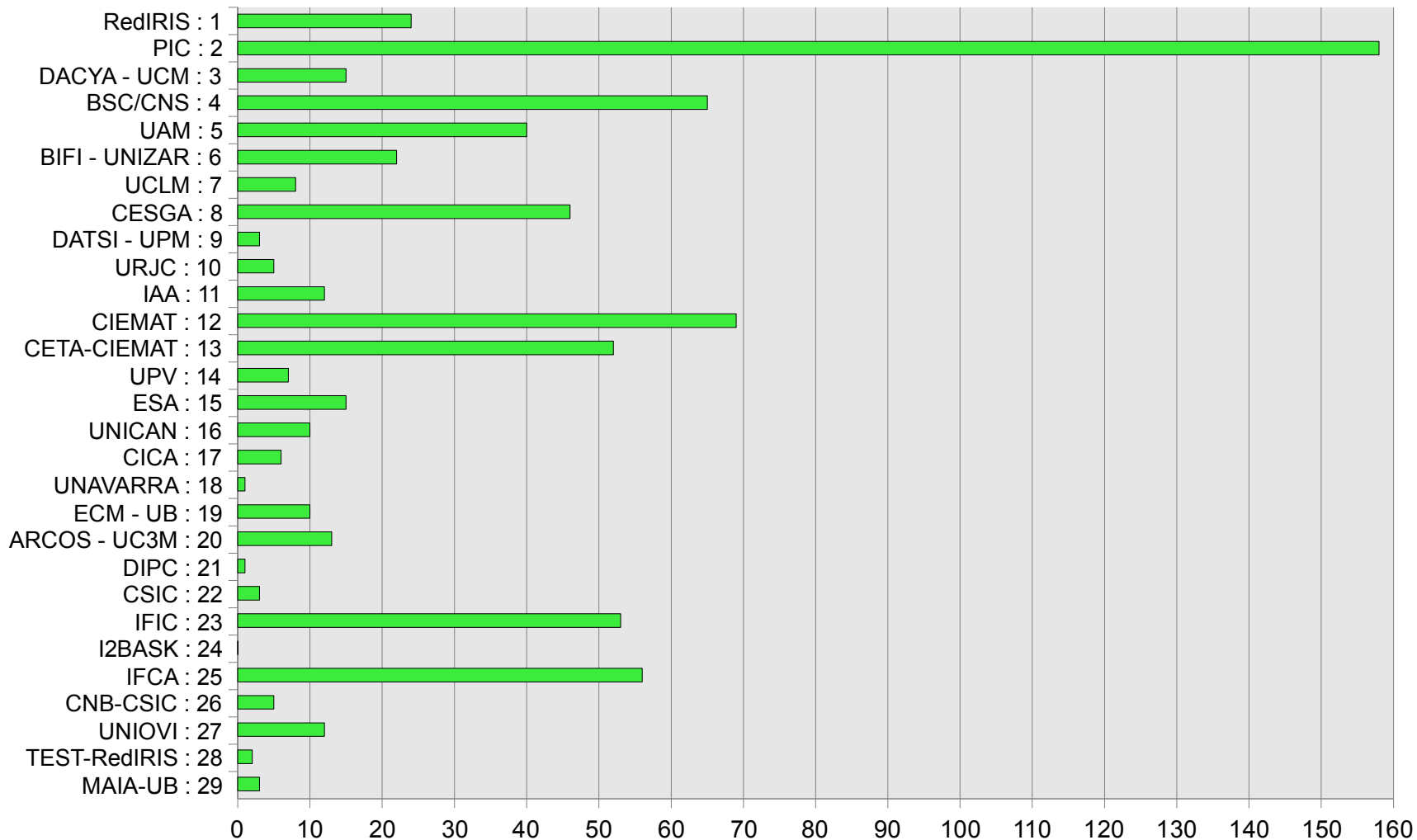
## • CRLs

- 87 emitidas
- 35 Millones descargas

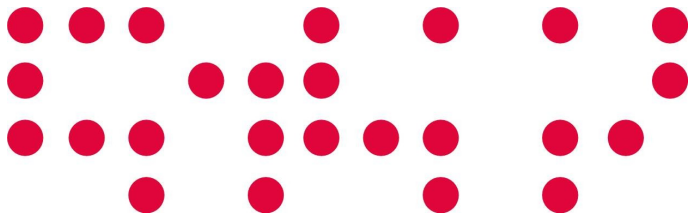








- 1 Bienvenida
- 2 Escenario actual
- 3 Mejoras en el servicio**
- 4 Política de una RA
- 5 Problemas encontrados
- 6 Futuro
- 7 Ruegos y preguntas





- **Procedimientos**

- Documento de condiciones de uso
- Documento de modificación de datos de una RA
- Manual del operador
- <http://www.irisgrid.es/pki/doc>

- **Software**

- Aviso de expiración de certificados
- Aviso de solicitudes pendientes de gestionar (RA)
- Ayuda a la RA para el cumplimiento de algunos requisitos de identificación de solicitantes
  - Documento para el solicitante a presentar en la RA
- Compatibilidad con Opera y Safari

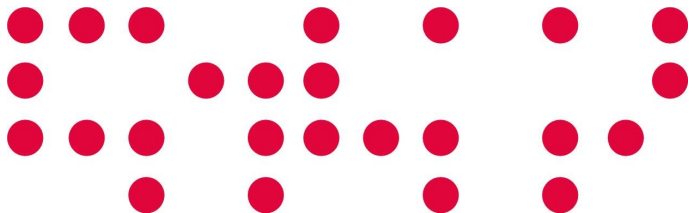
- **Software**

- Uso de "." en los CNs de los usuarios de EGEE/LCG
  - Se ha resuelto esta semana pasada
    - Sólo para gLite v3.0.0
  - Mantendremos el guión por el momento

- **Coordinación**

- Listas de correo con **almacenamiento** de mensajes
  - pkirisgrid-ca@irisgrid.es
  - pkirisgrid-ra@irisgrid.es

- 1 Bienvenida
- 2 Escenario actual
- 3 Mejoras en el servicio
- 4 Política de una RA**
- 5 Problemas encontrados
- 6 Futuro
- 7 Ruegos y preguntas



- A raíz de la auditoría por parte de EUGridPMA
  - Propusimos las auditorias de RA
  - Se nos pidió un guión de auditoría
- Pensamos en que las RAs debían tener una “**Política**”
  - No pretendemos que las RAs tengan un CP/CPS clásico
  - Como tienen las CAs
- Documento de “**Buenas Prácticas de Operación**”
  - Aunque lo llamamos política de RA
  - Buscamos procedimientos, **NO** más burocracia

- **Cómo hemos preparado la “Política” I**
  - Un documento a modo de plantilla
    - Pretendemos que siga la estructura del RFC3647
      - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
      - Es un marco de referencia para redactar el documento CP/CPS de CAs
    - Pero tampoco ser tan estrictos
    - No nos hemos basado en su contenido
    - Nos interesaba el concepto

- **Cómo hemos preparado la “Política” II**
- Contiene en cada punto una ayuda para redactarlo

### 3.1.2. Certificado digital

Este apartado se utilizará en caso de que la RA admita la autenticación del solicitante mediante correo electrónico firmado con un certificado digital a nombre de éste.

*El usuario puede solicitar que se le apruebe la solicitud autenticándose mediante un correo firmado con un certificado digital.*

*Hay que recalcar que este certificado debe haber sido emitido a nombre del solicitante. Por motivos obvios, no se admitirá una solicitud firmada por el certificado de un tercero.*

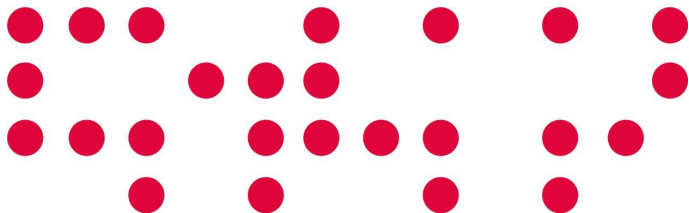
- Primer borrador disponible
- URL: <http://www.irisgrid.es/pki/doc/pkirisgrid-ra-policy-template.pdf>

- **Cómo hemos preparado la “Política” III**
  - Una guía de ayuda a la redacción de la **Política**
    - Es un ejemplo sobre una RA ficticia
    - Explica lo que hay decir en cada apartado
    - No es una guía exhaustiva
  - Primer borrador disponible
    - URL: <http://www.irisgrid.es/pki/doc/pkirisgrid-ra-policy-example.pdf>



- La idea de política debe ser colaborativa
  - Queremos que participéis en la mejora de los borradores
  - Para obtener un mejor documento que entregar a próximas RAs

- 1 Bienvenida
- 2 Escenario actual
- 3 Mejoras en el servicio
- 4 Política de una RA
- 5 Problemas encontrados**
- 6 Futuro
- 7 Ruegos y preguntas



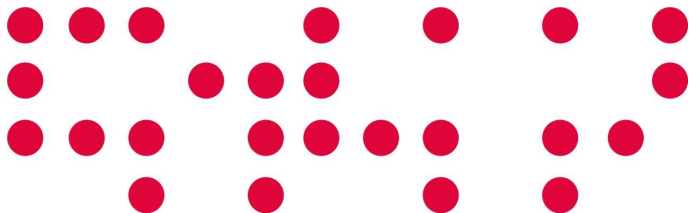
- **Usuario final**

- Cambio de responsable del certificado de host/servicio
  - Creación de figura responsable administrativo
- Cambio de datos del certificado de un usuario
  - Revocar certificado
- MS Internet Explorer 7 sobre Windows Vista y otros navegadores

- RA
  - Comprobación de datos de la solicitud
    - CN
      - Comprobar Nombre y Apellido
    - Email
      - En muchos casos se está **certificado** la dirección de correo
      - Debe existir ya que a esa dirección llegarán los avisos de expiración
    - FQDN
      - No certificamos direcciones IP
      - No se emiten certificados con wildcard
        - \*.subdominio.dominio
  - Cambio de PIN de usuario
    - Captura de pantalla
    - Veámoslo en el interfaz web

- CA
  - Revocaciones en período de renovación
- ¿Más problemas?
  - Por favor comentadlos ahora

- 1 Bienvenida
- 2 Escenario actual
- 3 Mejoras en el servicio
- 4 Política de una RA
- 5 Problemas encontrados
- 6 Futuro**
- 7 Ruegos y preguntas



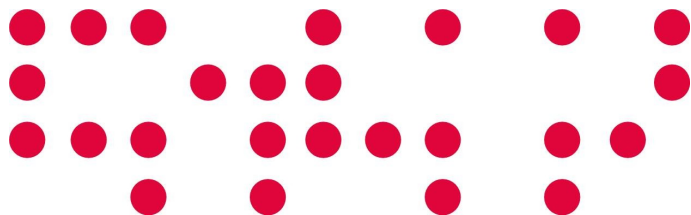
- **A corto plazo**

- Creación de nuevas listas por cada RA
  - pkirisgrid-ratN-admin@ (administradores de la RA N)
  - pkirisgrid-ratN-users@ (usuarios de la RA N)
- Realizar auditoría pkIRISGrid-CA
  - También alguna auditoría a alguna de las RAs
- Estadísticas de uso de la RA
  - Solicitudes aprobadas/denegadas
  - Certificados emitidos/válidos/revocados

- **A medio plazo**
  - Especificación de duración del certificado (en días)
    - Modificar la política
  - Soporte de Subject Alternative Name
- **A largo plazo**
  - Importación de CSRs externas
  - Soporte de múltiples certificados



- 1 Bienvenida
- 2 Escenario actual
- 3 Mejoras en el servicio
- 4 Política de una RA
- 5 Problemas encontrados
- 6 Futuro
- 7 Ruegos y preguntas**





red.es

Edificio Bronce  
Plaza Manuel Gómez Moreno s/n  
28020 Madrid. España

Tel.: 91 212 76 20 / 25  
Fax: 91 212 76 35  
[www.red.es](http://www.red.es)

RedIRIS. Edificio CICA  
Avenida Reina Mercedes s/n  
41012. Sevilla. España

Tel: 95 505 66 00  
Fax: 95 505 66 27