

# Reunión administradores de autoridades de registro de pkIRISGrid CA

## pkIRISGrid RAdmin 1

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

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



red.es

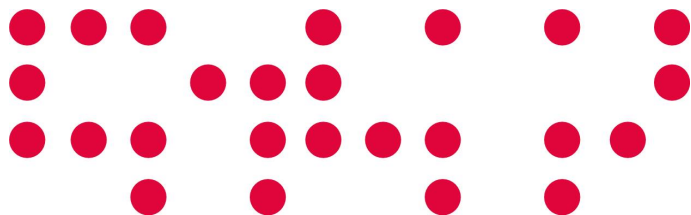


Red IRIS

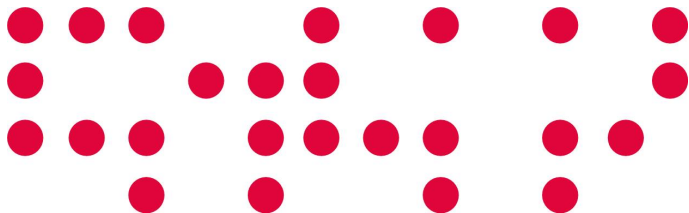


Madrid, 27 de junio de 2007

- 1 Bienvenida**
- 2 Escenario actual
- 3 Coordinación RAs
- 4 Problemas detectados
- 5 Mejoras en el servicio
- 6 Auditoría de RAs
- 7 Ruegos y preguntas



- 1 Bienvenida
- 2 Escenario actual**
- 3 Coordinación RAs
- 4 Problemas detectados
- 5 Mejoras en el servicio
- 6 Auditoría de RAs
- 7 Ruegos y preguntas



- **RA**s

- 25 RAs
- 12 localizaciones

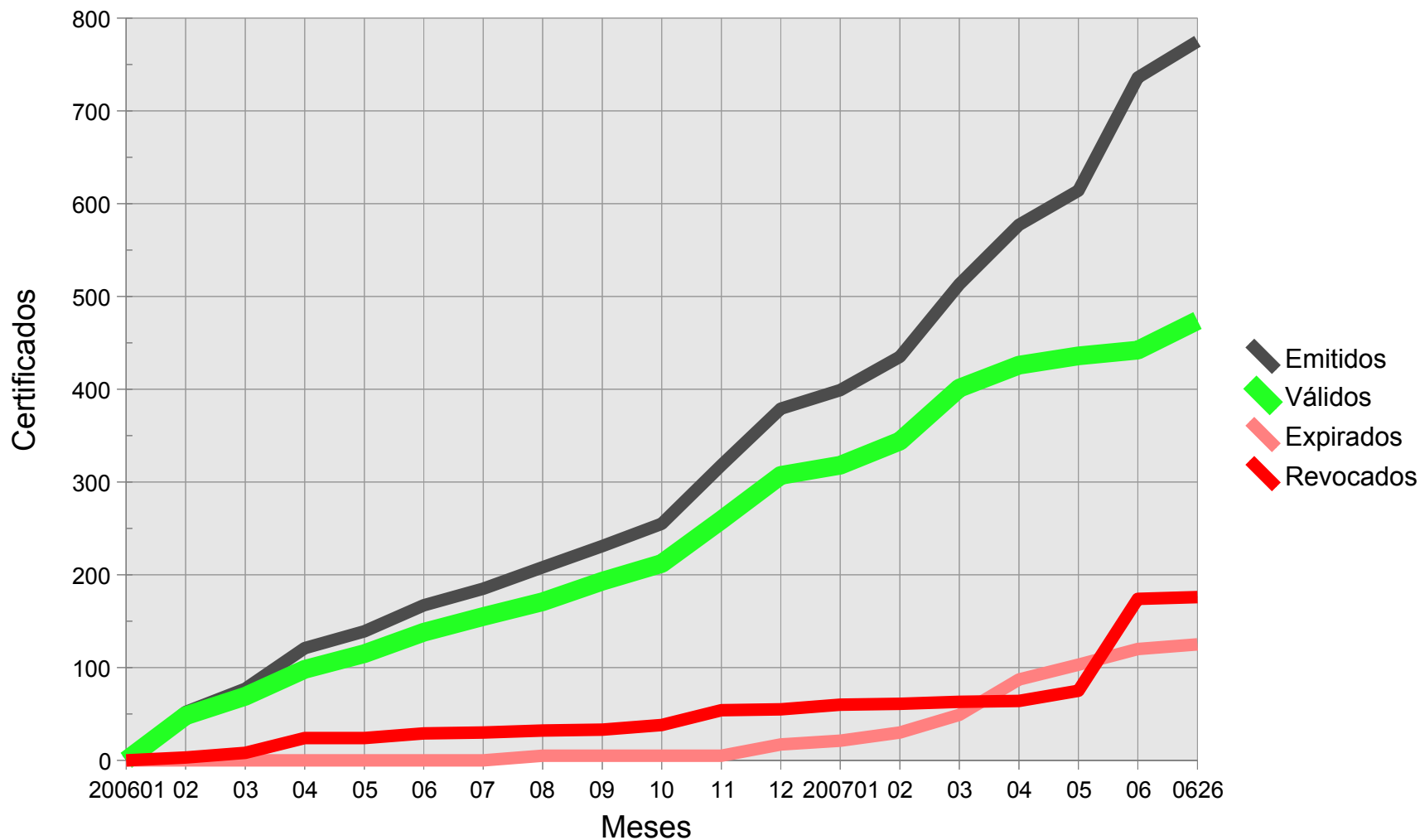
- **Certificados**

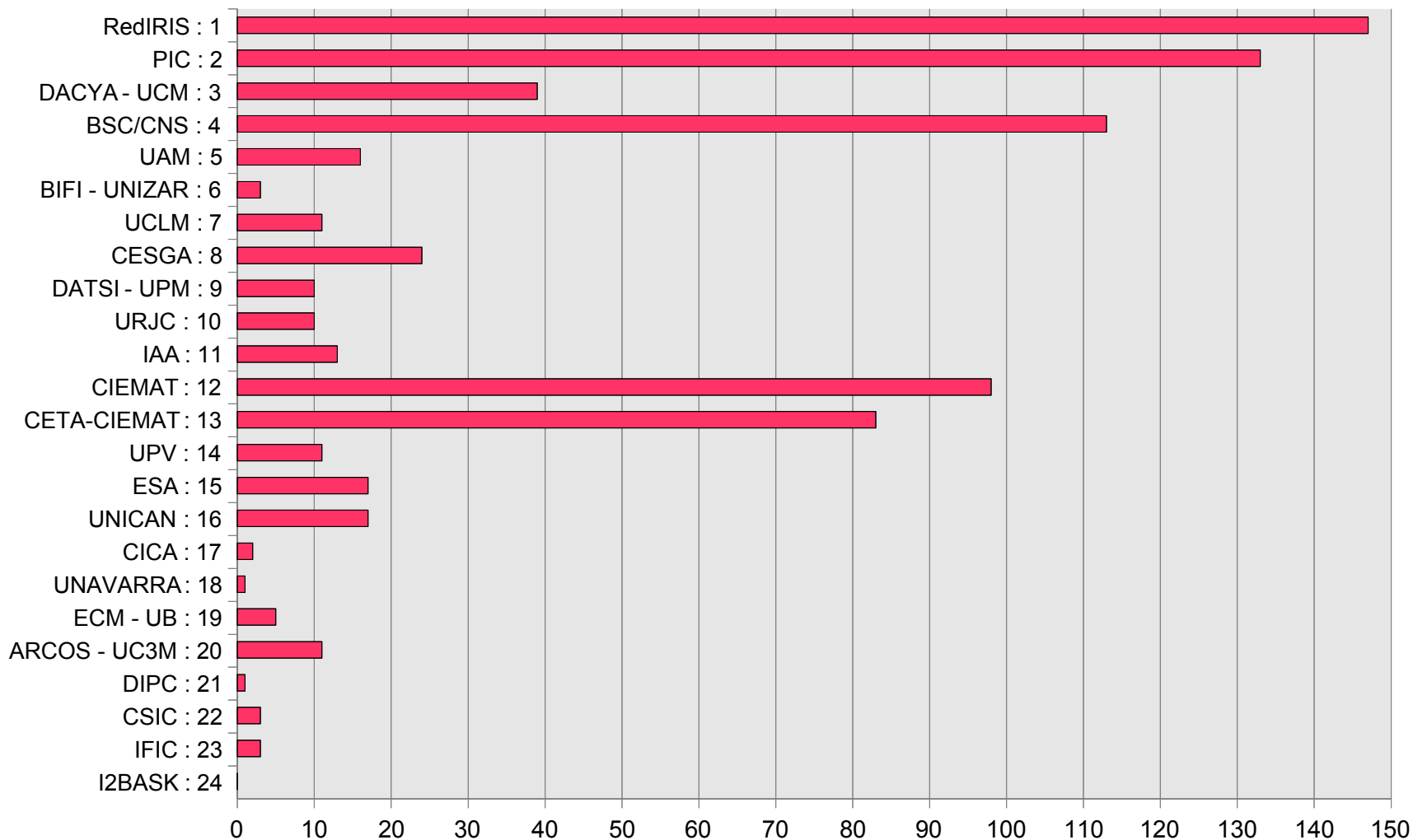
- 775 emitidos
  - 357 usuario
  - 418 host/servicio

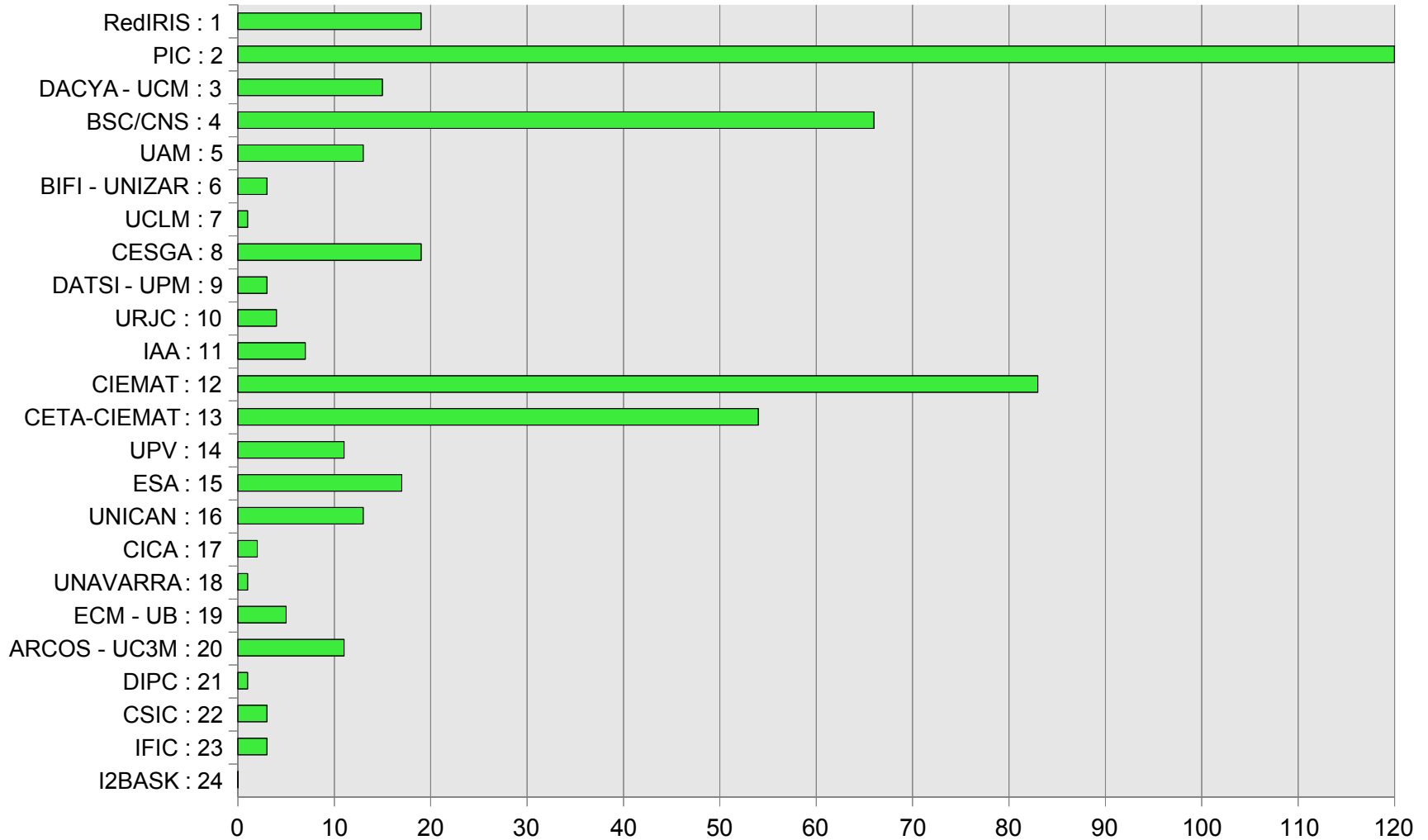
- **CRL**s

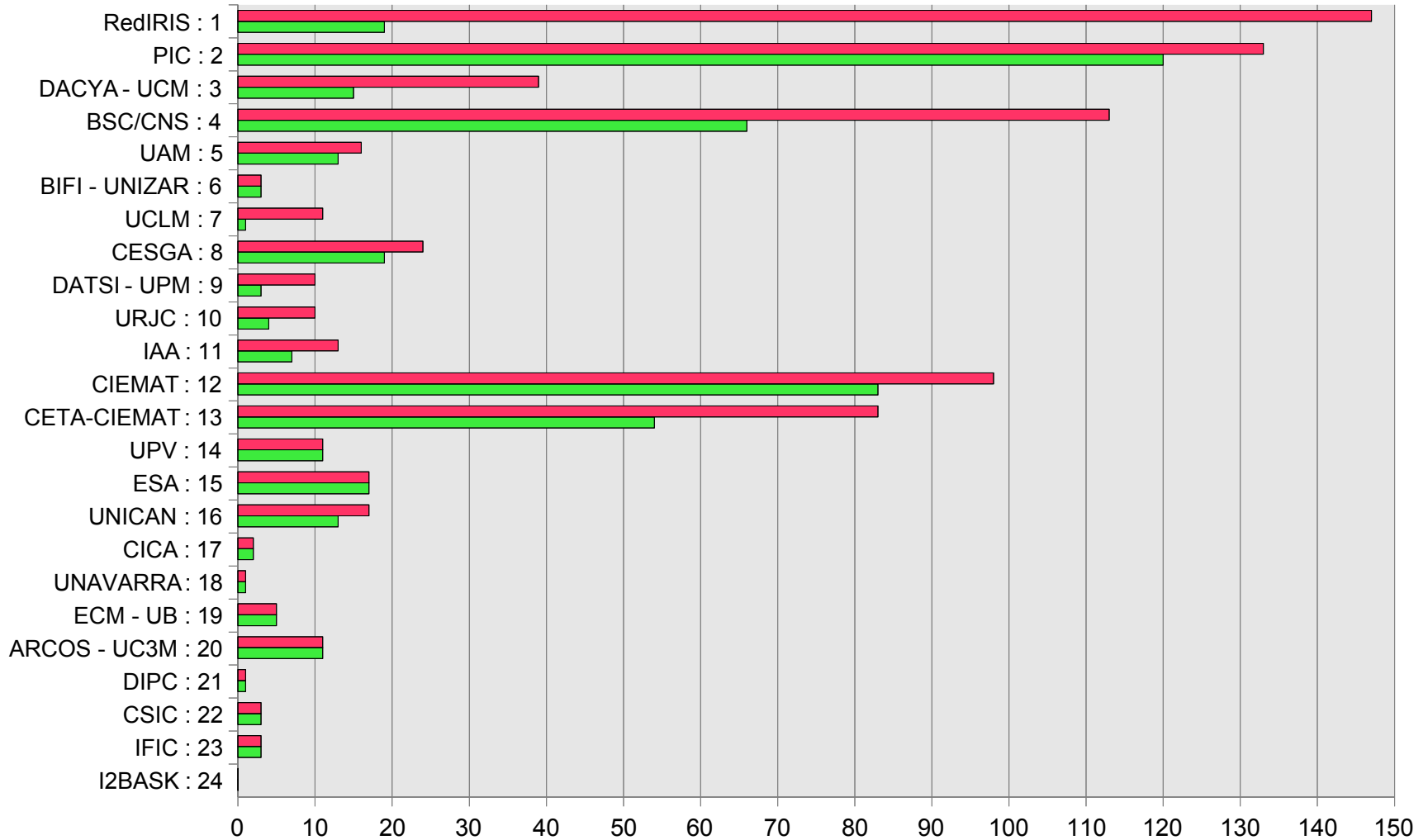
- 67 emitidas
- 24 Millones descargas



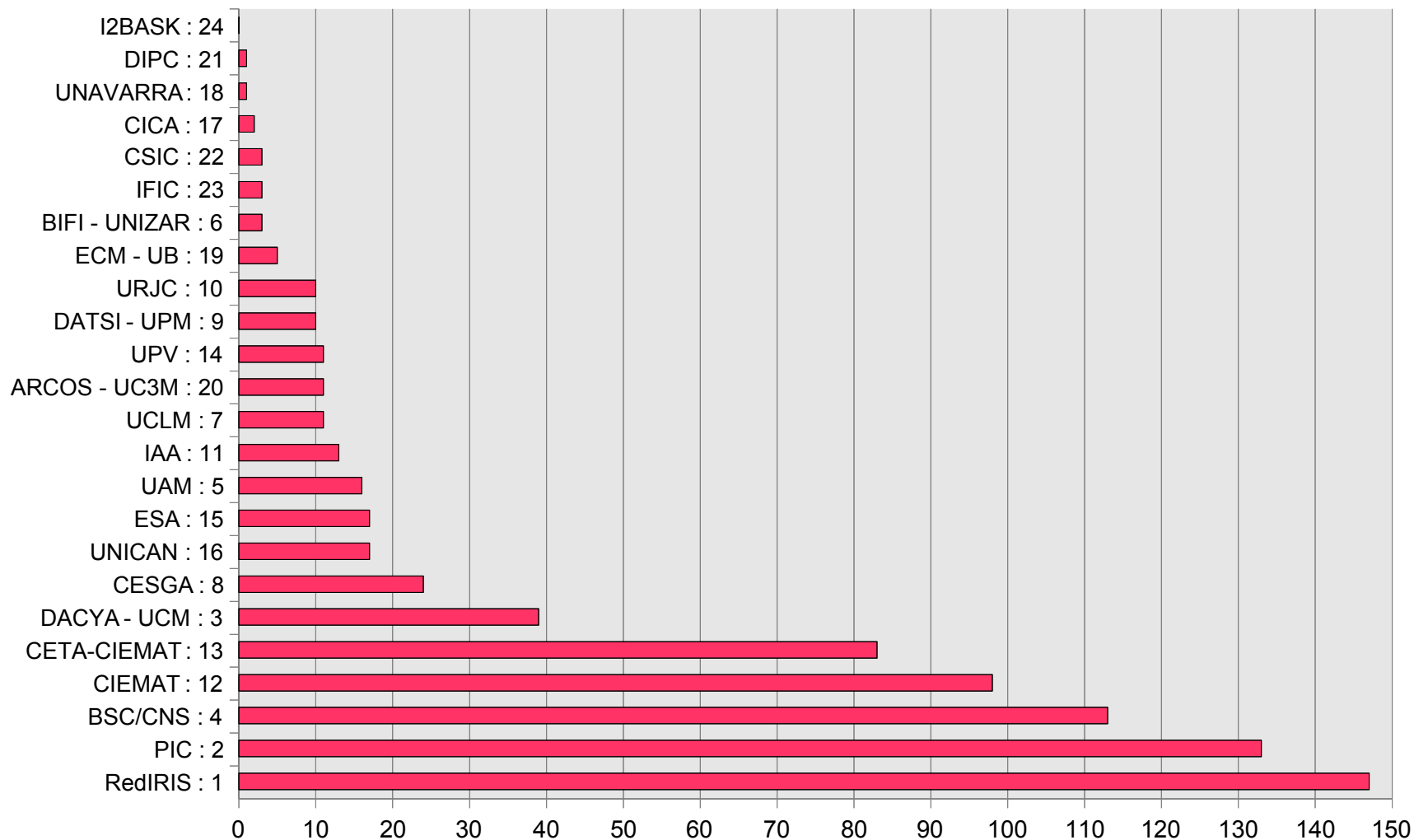


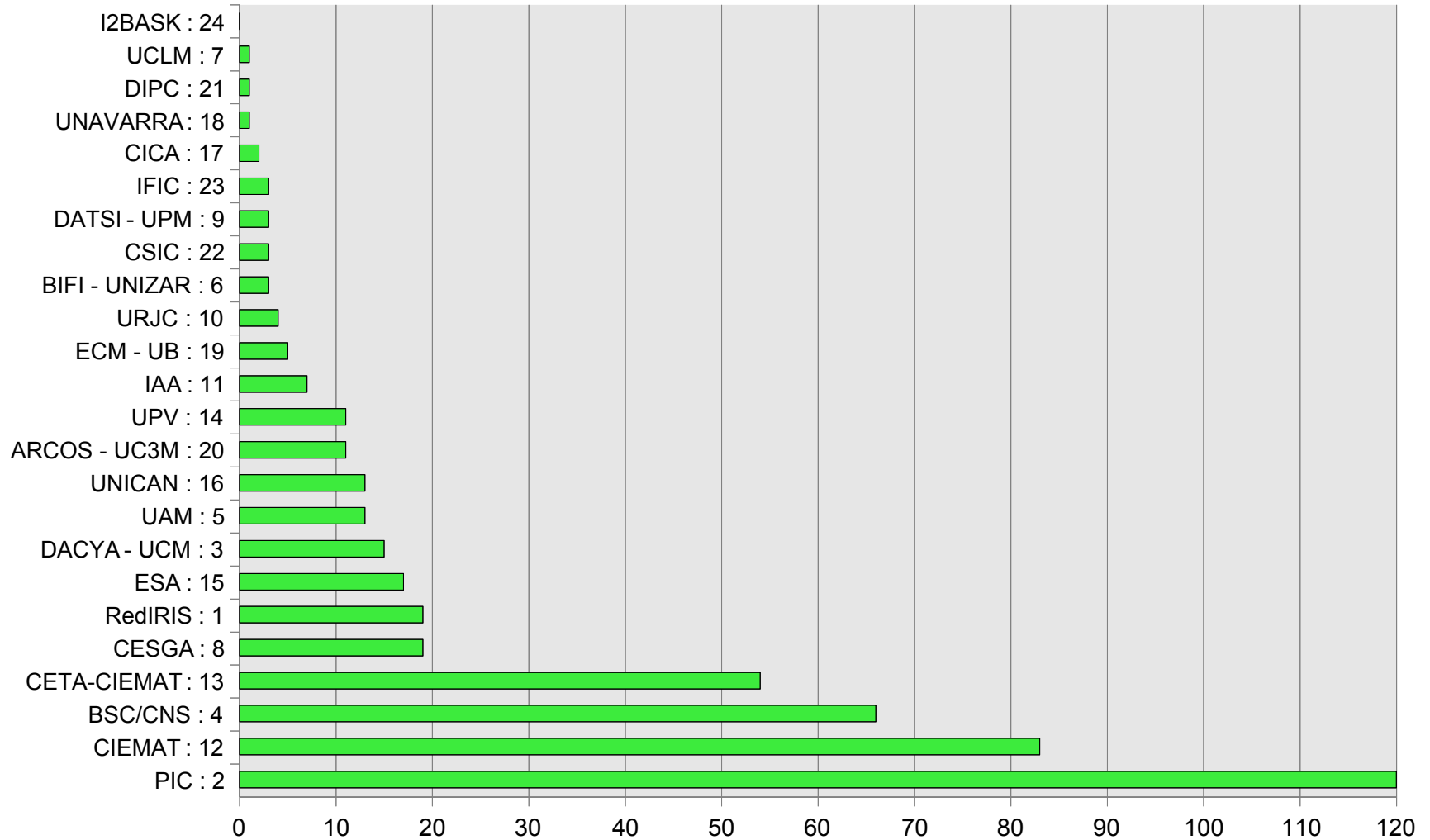


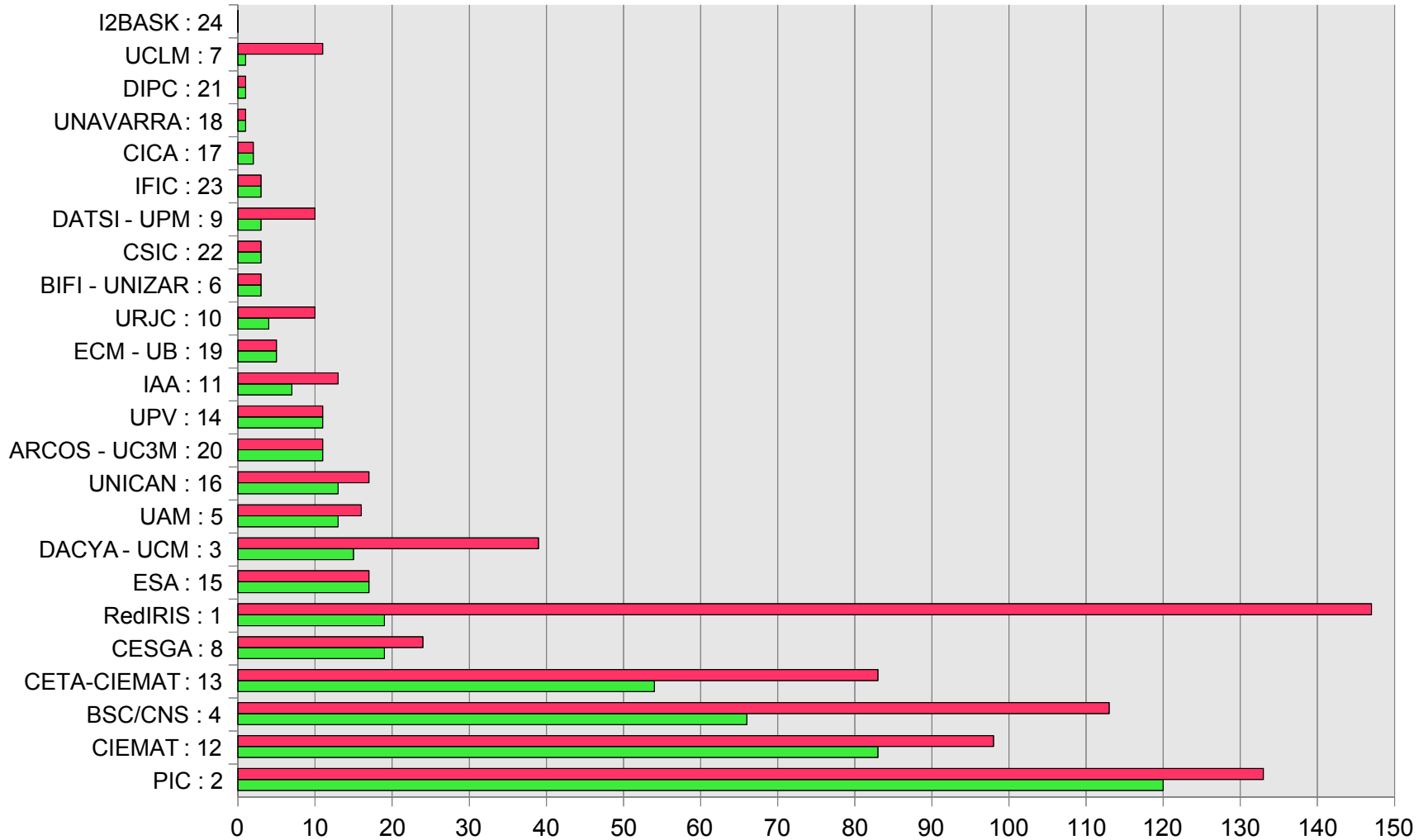




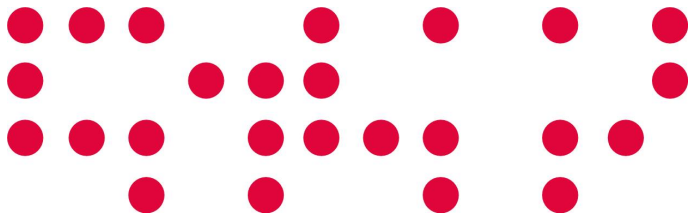








- 1 Bienvenida
- 2 Escenario actual
- 3 Coordinación RAs**
- 4 Problemas detectados
- 5 Mejoras en el servicio
- 6 Auditoría de RAs
- 7 Ruegos y preguntas

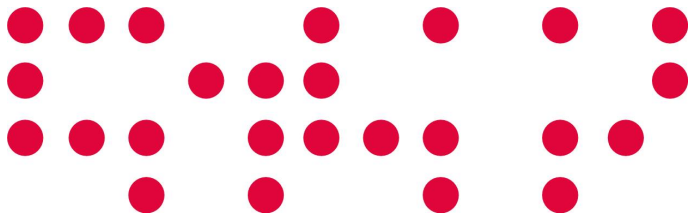


- **Objetivos**

- Mantenimiento de los lazos de confianza entre CA y RAs
  - Reunión presencial con los administradores de las RAs
  - NIF, pgp, ...
- Colaboración en la formalización de procedimientos
  - Altas de RA
    - Actualización de los requisitos mínimos para la incorporación de nuevas RAs
  - Políticas de RA
  - Auditorías de RA
- Análisis de requisitos de las RAs y sus usuarios
  - Para la mejora de pkIRISGrid CA
- Resolución de problemas encontrados

- **Reuniones periódicas presenciales**
  - 2 reuniones anuales
    - Grupos de trabajo de junio
    - Jornadas Técnicas de noviembre
- **Listas de correo**
  - Mayor uso de la lista pkirisgrid-ra@
    - Poca actividad
    - Se enviarán todas las cuestiones recibidas en nuestros buzones personales a la lista
- **Auditorías**
  - Reunión/Visita a alguna de las RAs para verificar sus procedimientos

- 1 Bienvenida
- 2 Escenario actual
- 3 Coordinación RAs
- 4 Problemas detectados**
- 5 Mejoras en el servicio
- 6 Auditoría de RAs
- 7 Ruegos y preguntas



- **Usuario final**

- Uso de "." en los CNs de los usuarios de EGEE/LCG
  - Solución CERN
    - <https://savannah.cern.ch/bugs/?19878>
  - Solución temporal de RedIRIS
    - Usar "-" en el cn: nombre-apellido
- Cambio de datos del certificado de un usuario
  - Revocar certificado
- Cambio de responsable del certificado de host/servicio
  - Tratar individualmente

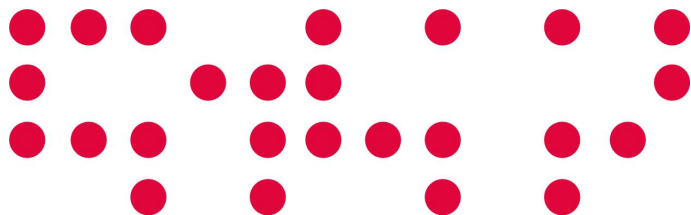


- RA

- Inexistencia documento de condiciones de uso de RA
- Comprobación de datos del solicitante
  - email
- Servicio ofrecido a usuarios de institución no autorizada (In)
  - ¿A quien podemos darle servicios de PKI?
    - A las instituciones **afiliadas** a RedIRIS
  - ¿Podría ofrecer servicios a instituciones no afiliadas?
    - Por defecto no
    - Si una institución/empresa no afiliada quiere usar la PKI tendrá que sentarse con nosotros y firmar un convenio para establecer en qué términos hacemos eso
    - Pero puede que se decida no darle el servicio

- CA
  - CRL
    - Enlaces a directorios incorrectos
      - Un fin de semana sin CRL
  - Renovación
    - Certificados que no podían renovarse
      - No contenían dirección de correo porque fueron solicitados durante los primeros meses de existencia de la pkIRISGrid CA
      - Problema con la renovación el mismo día en el que expiraba el certificado
      - Certificados no marcados como expirados en nuestra base de datos
- ¿Más problemas?
  - Comentadlos ahora por favor

- 1 Bienvenida
- 2 Escenario actual
- 3 Coordinación RAs
- 4 Problemas detectados
- 5 Mejoras en el servicio**
- 6 Auditoría de RAs
- 7 Ruegos y preguntas



- **Aportaciones de los usuarios finales**
  - Herramientas desarrolladas
    - Actualizador CRL, ...
- **Aportaciones de las RAs**
  - Documentación accesible desde su web
    - Política de uso de la RA
    - Manuales de uso de la RA



- **A corto plazo**

- Herramienta de ayuda a la RA para el cumplimiento de los requisitos de identificación de solicitantes
  - Formulario para el solicitante a presentar en la RA
- Estadísticas de uso de la RA
  - Solicitudes aprobadas/denegadas
  - Certificados emitidos/válidos/revocados
- Reestructuración listas de correo
  - En el servidor de listas de RedIRIS
    - `pkirisgrid-ca@listserv.rediris.es`
    - `pkirisgrid-ra@listserv.rediris.es`
  - Creación de nuevas listas por cada RA
    - `pkirisgrid-ratN-admin@` (administradores de la RA N)
    - `pkirisgrid-ratN-users@` (usuarios de la RA N)

- **A corto plazo**

- Aviso de solicitudes pendientes (RA)
- Aviso de expiración de certificado (User)
  - Plantilla por RA
  - 1 mes, 1 semana, 1 día

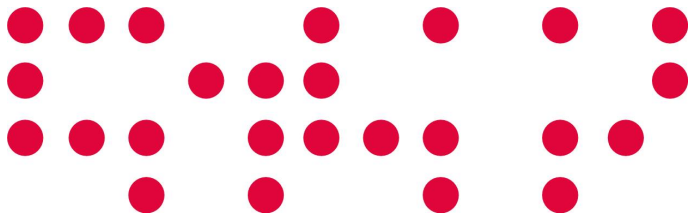
- **A medio plazo**

- Especificación de duración del certificado (en días)
  - Modificar la política
- Soporte de Subject Alternative Name

- **A largo plazo**

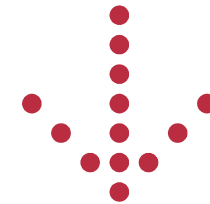
- Importación de CSRs externas
- Soporte de múltiples certificados

- 1 Bienvenida
- 2 Escenario actual
- 3 Coordinación RAs
- 4 Problemas detectados
- 5 Mejoras en el servicio
- 6 Auditoría de RAs**
- 7 Ruegos y preguntas



## • Problema

- Las *relying parties* (dueñas de las máquinas que os prestan servicio) han solicitado a la EUGridPMA que se realice un mayor control sobre el usuario final



## • Solución

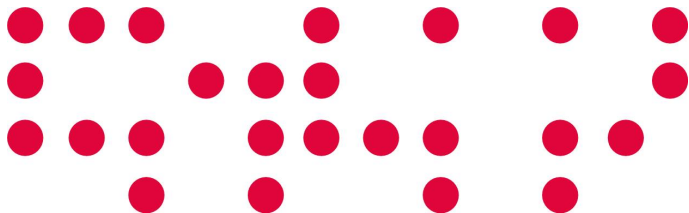
- Auditoría de las CAs
- Auditoría de las RAs
- Mecanismos de control sobre el proceso que realizan las RAs en la verificación de los solicitantes
  - Política de uso de la RA



- Creación de una política por cada RA
  - Os presentaremos un borrador con los requisitos mínimos que os sirva de guía
- Los usuarios deben aceptar la política de su RA antes de terminar la solicitud de certificado
  - Incluiremos un checkbox en el formulario de solicitud
- Presentación de la política en una reunión RAdmin
- La política debe incluir
  - Procedimiento que usa cada RA para la validación de los solicitantes de certificado

- **Procedimiento de validación de los solicitantes**
  - Identidad del solicitante
    - Cara a cara
    - Presentación de identificación fotográfica
  - Pertenencia a la organización
  - Administrador del servicio/servidor
    - Documento firmado por el responsable que identifique al administrador del servicio/servidor
- **Mantener en formato auditable el tipo de verificación realizada**

- 1 Bienvenida
- 2 Escenario actual
- 3 Coordinación RAs
- 4 Problemas detectados
- 5 Mejoras en el servicio
- 6 Auditoría RAs
- 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: 91 505 66  
Fax: 91 505 66