

SCS

Servicio de certificados de RedIRIS

Javi Masa - javier.masa@rediris.es

Antonio Pérez - antonio.perez@rediris.es



GOBIERNO
DE ESPAÑA

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

MINISTERIO
DE CIENCIA
E INNOVACIÓN



Red
IRIS

Valladolid, 29/11/2011

Índice

- 1 **Bienvenida**
- 2 Escenario actual
- 3 Estadísticas
- 4 Perfiles: Personal
Firma de código
- 5 Incidencias
- 6 Ruegos y preguntas



GOBIERNO
DE ESPAÑA

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

MINISTERIO
DE CIENCIA
E INNOVACIÓN



Red
IRIS

- Vídeo

- Mediante Adobe Connect
 - <http://tinyurl.com/czmb3bj>

- Material adicional

- Presentación disponible en
 - <http://www.rediris.es/scs/coord/jt2011/>

Índice

- 1 Bienvenida
- 2 Escenario actual**
- 3 Estadísticas
- 4 Perfiles: Personal
Firma de código
- 5 Incidencias
- 6 Ruegos y preguntas



GOBIERNO
DE ESPAÑA

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

MINISTERIO
DE CIENCIA
E INNOVACIÓN



Red
IRIS

Escenario actual

- **Aumento de instituciones en el servicio**
 - Aumento de solicitantes registrados
 - Aumento de certificados emitidos
- **Aumento de perfiles disponibles**
 - Certificado SSL de servidor
 - Certificado personal (SCP)
 - Certificados de código (manualmente)
- **Disminución del staff**
 - Diego dejó RedIRIS en Octubre
- **Aumento de carga de trabajo**
 - Para los que quedamos

Índice

- 1 Bienvenida
- 2 Escenario actual
- 3 Estadísticas**
- 4 Perfiles: Personal
Firma de código
- 5 Incidencias
- 6 Ruegos y preguntas



GOBIERNO
DE ESPAÑA

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

MINISTERIO
DE CIENCIA
E INNOVACIÓN



Red
IRIS

Estadísticas

- **SSL servidor**

- Instituciones: 92
- Solicitantes registrados: 297
- Certificados emitidos: 3703
- Dominios: 285

- **SCP**

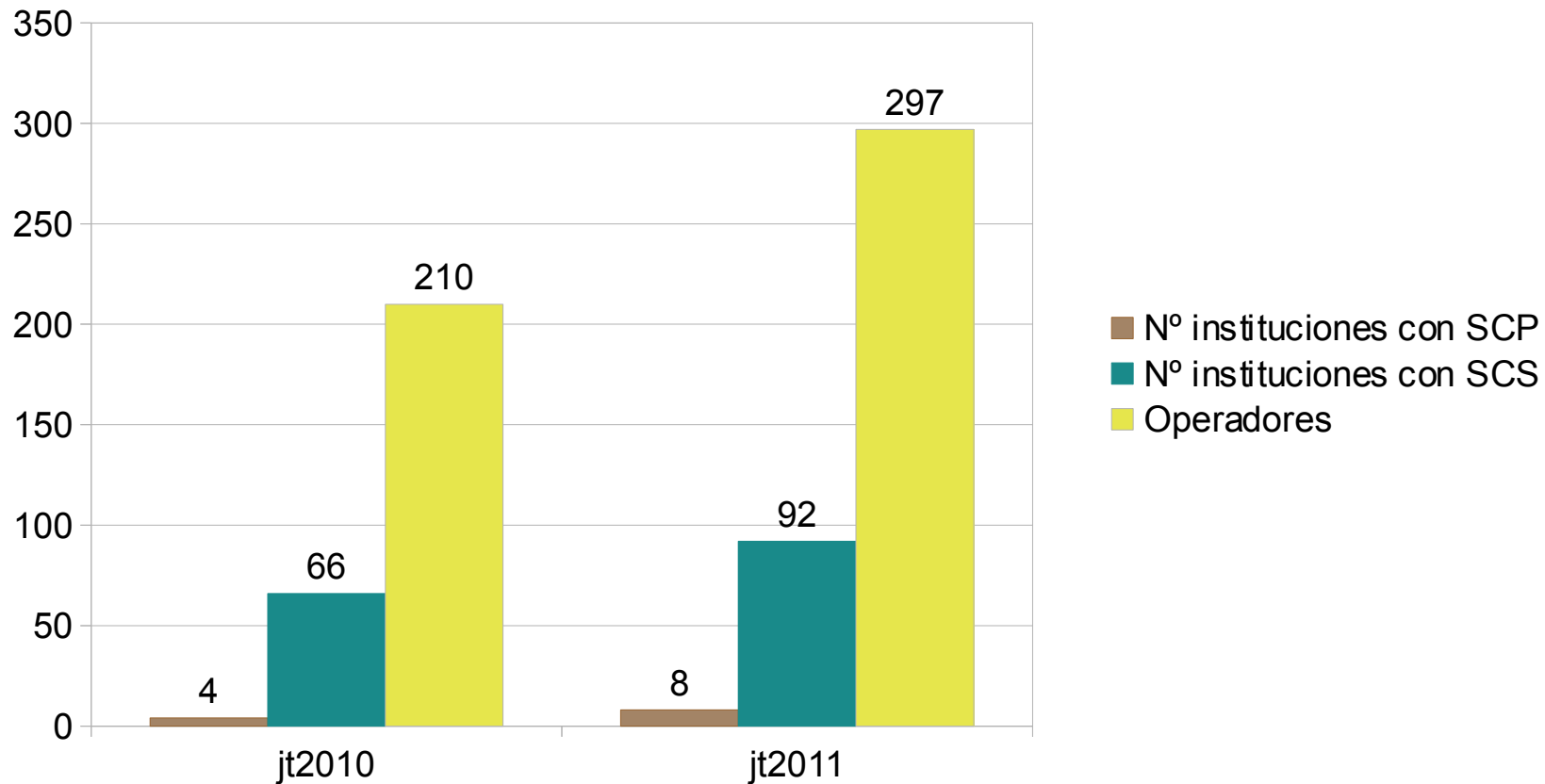
- Instituciones: 9
(BSC, CICA, IVIE, RedIRIS, UC3M, UDC, UPV, URL)
- Certificados emitidos: 123

- **Firma de código**

- Instituciones: 4
(RedIRIS, UC3M, UPV, UV)
- Certificados emitidos: 7

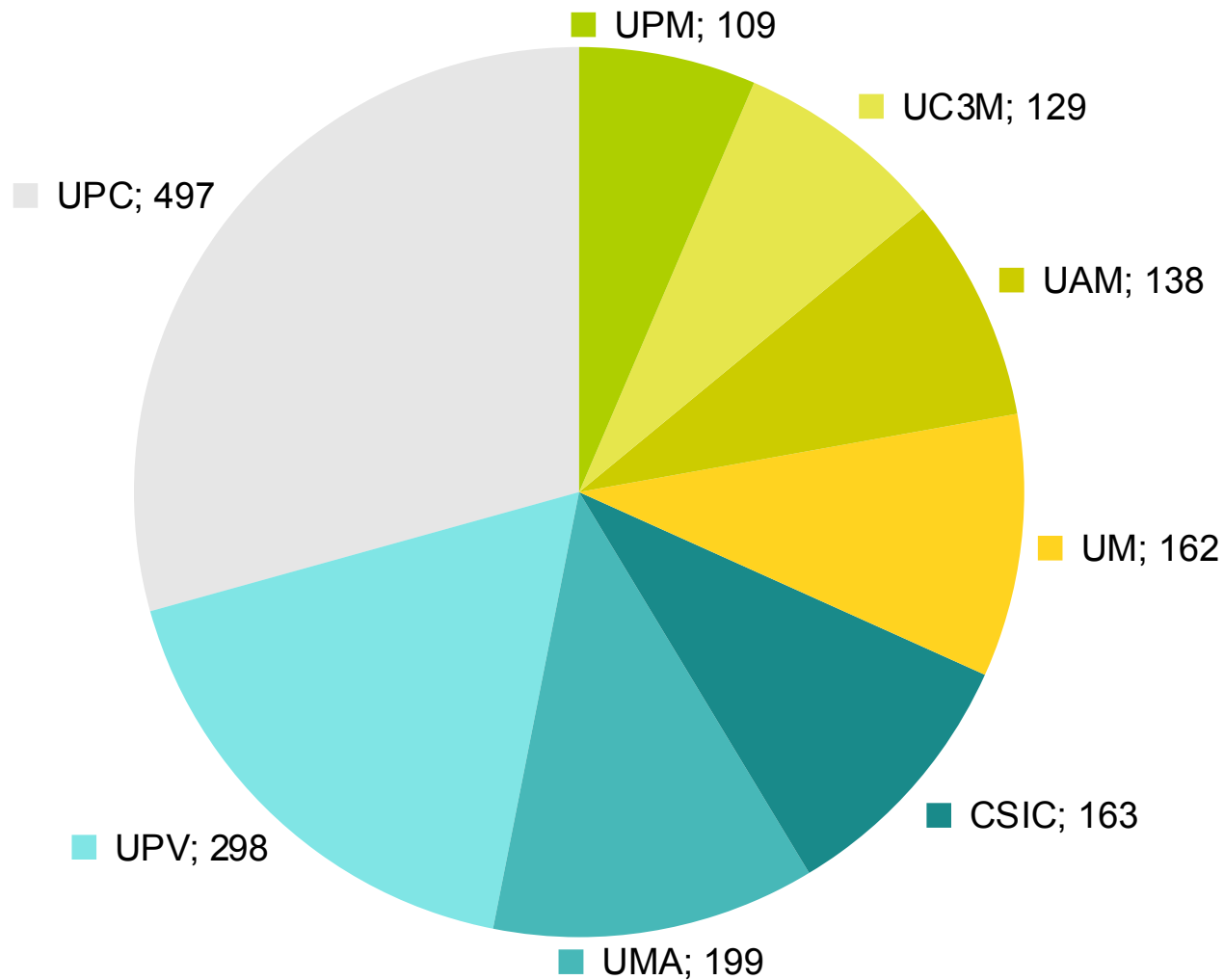
Estadísticas

Instituciones y personas participantes



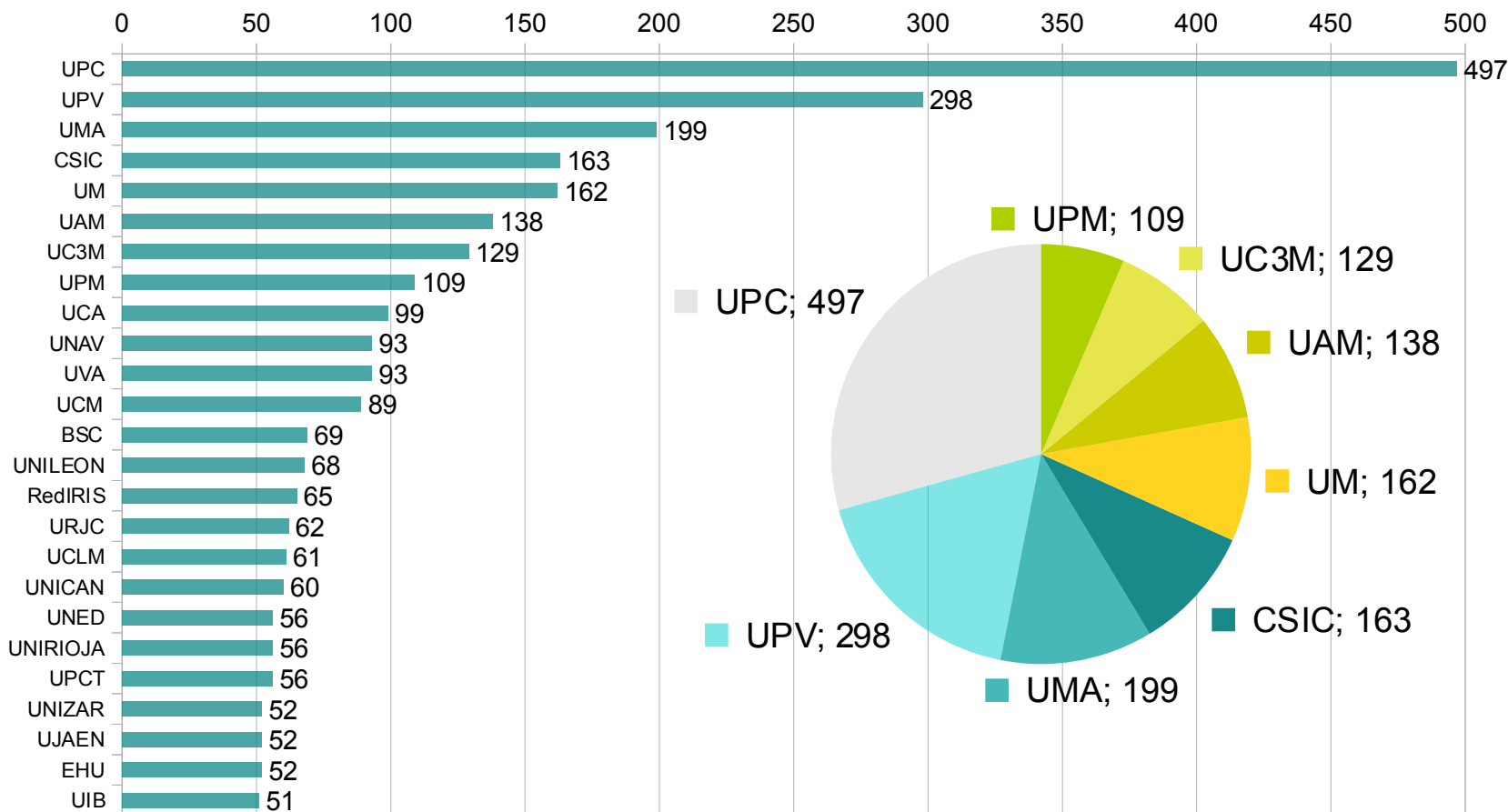
Estadísticas: SCS

Instituciones con más de 100 certificados emitidos



Estadísticas: SCS

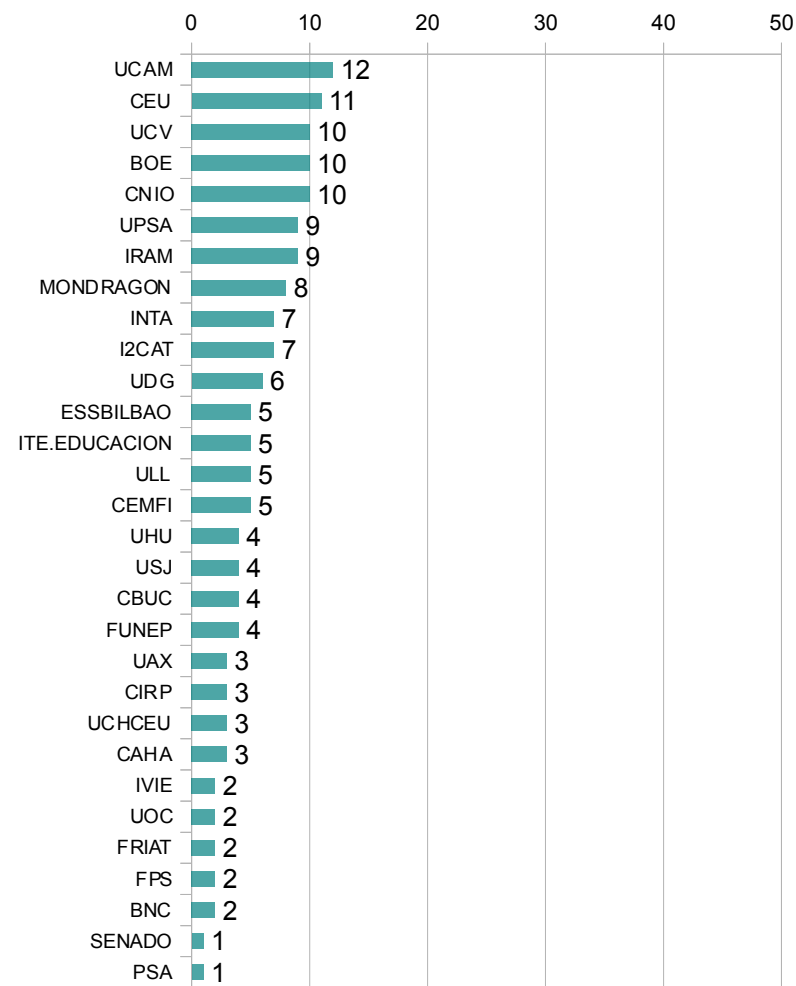
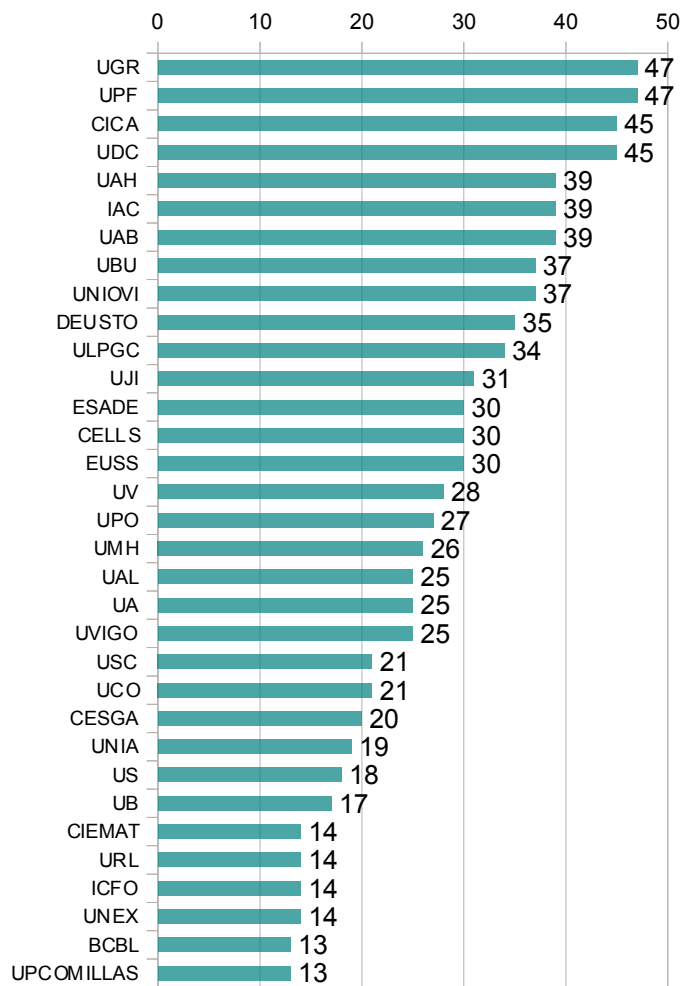
Instituciones con más de 50 certificados emitidos



- El resto de instituciones (66) suman 1103 certificados

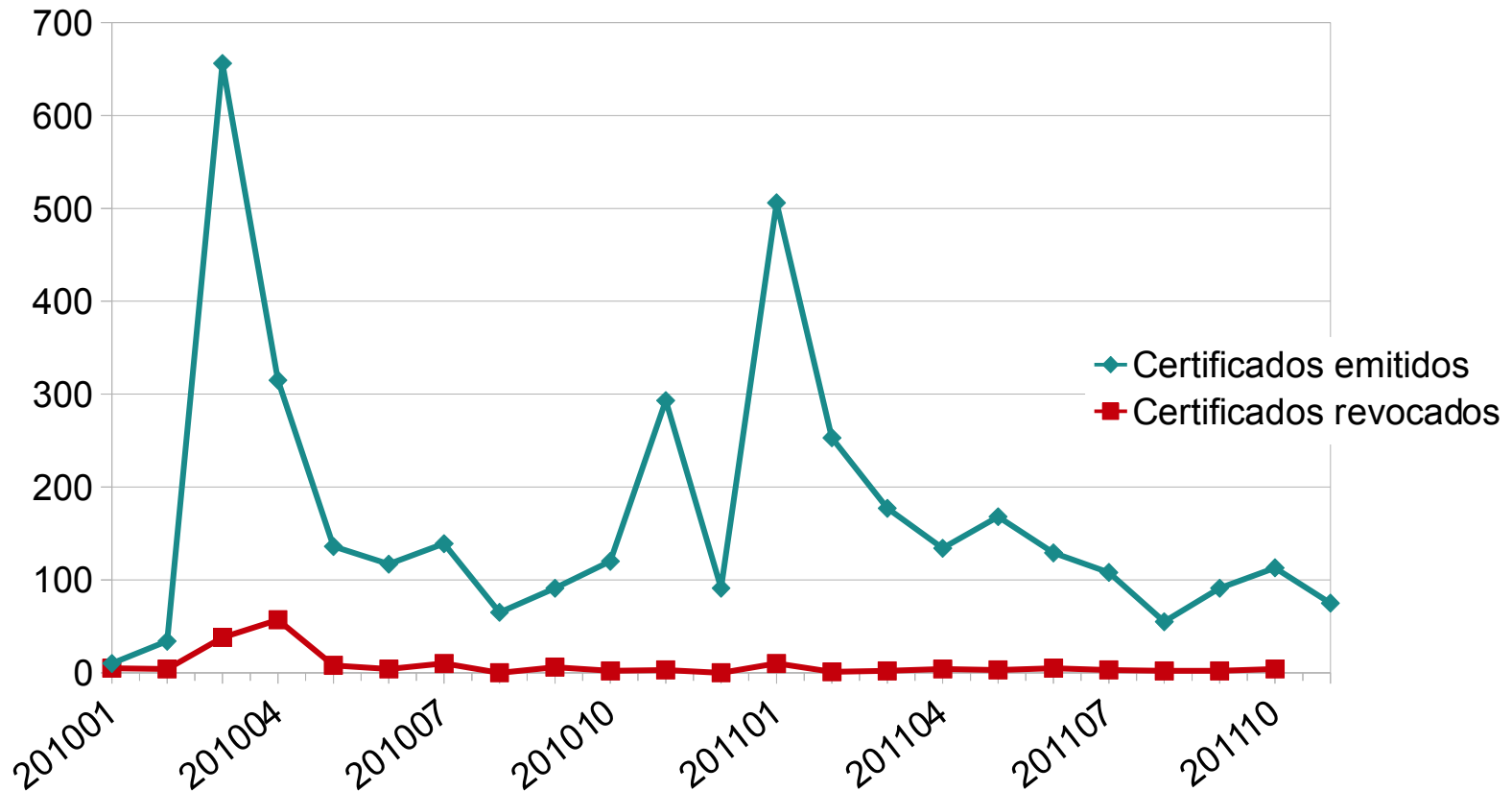
Estadísticas: SCS

Instituciones con menos de 50 certificados emitidos



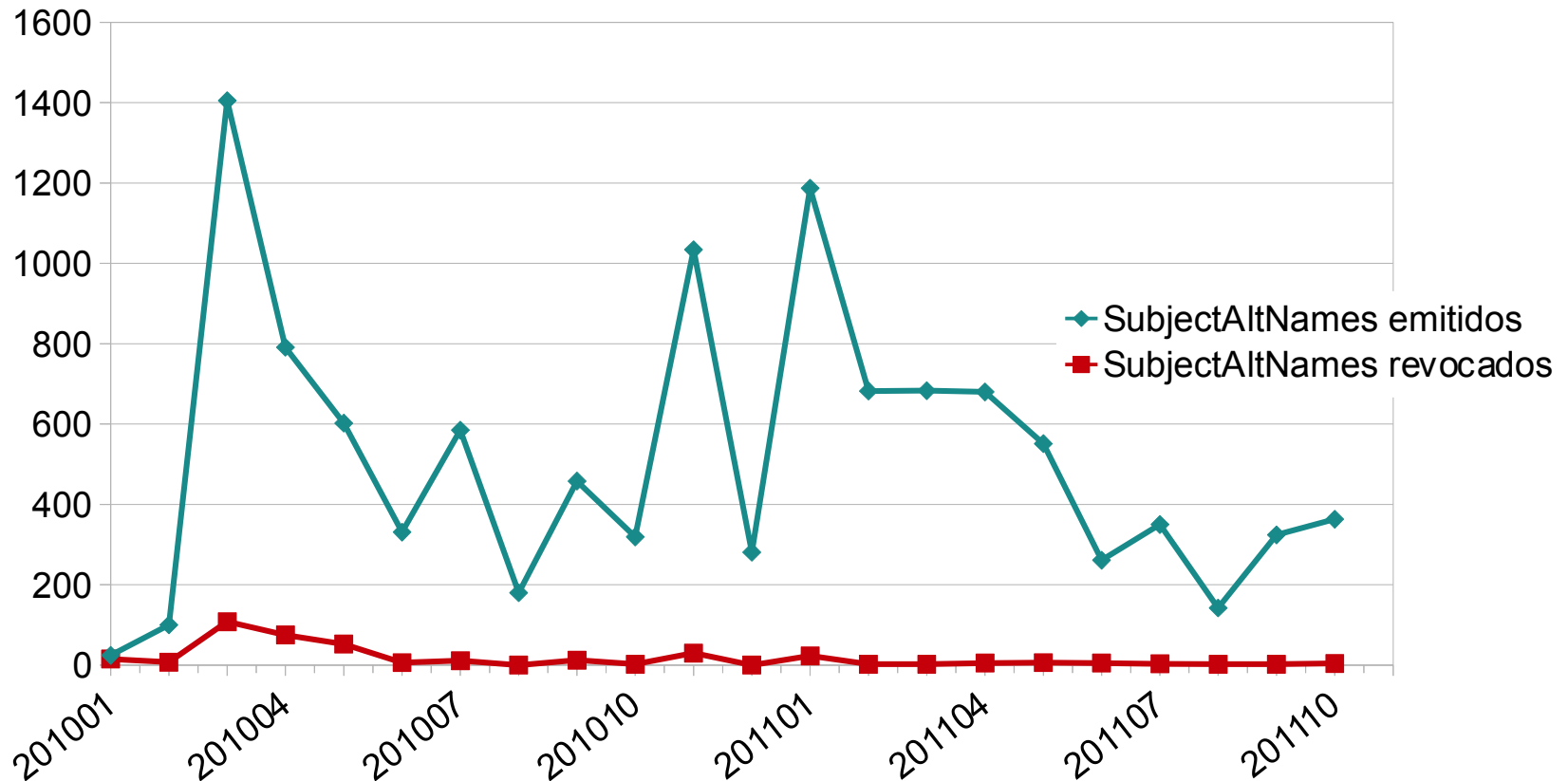
Estadísticas: SSL servidor

Certificados emitidos y revocados (por mes)



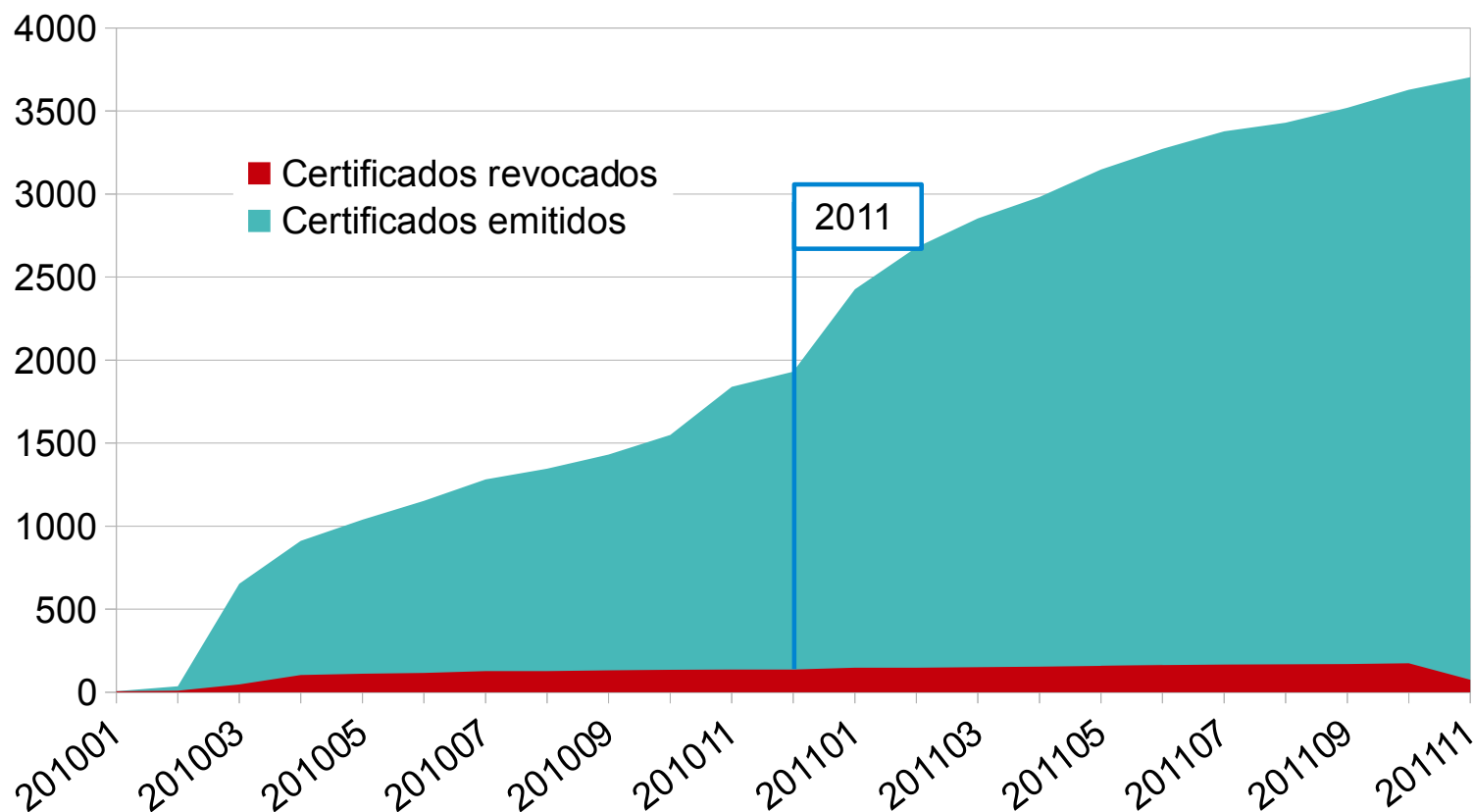
Estadísticas: SSL servidor

SubjectAltNames emitidos y revocados (al mes)



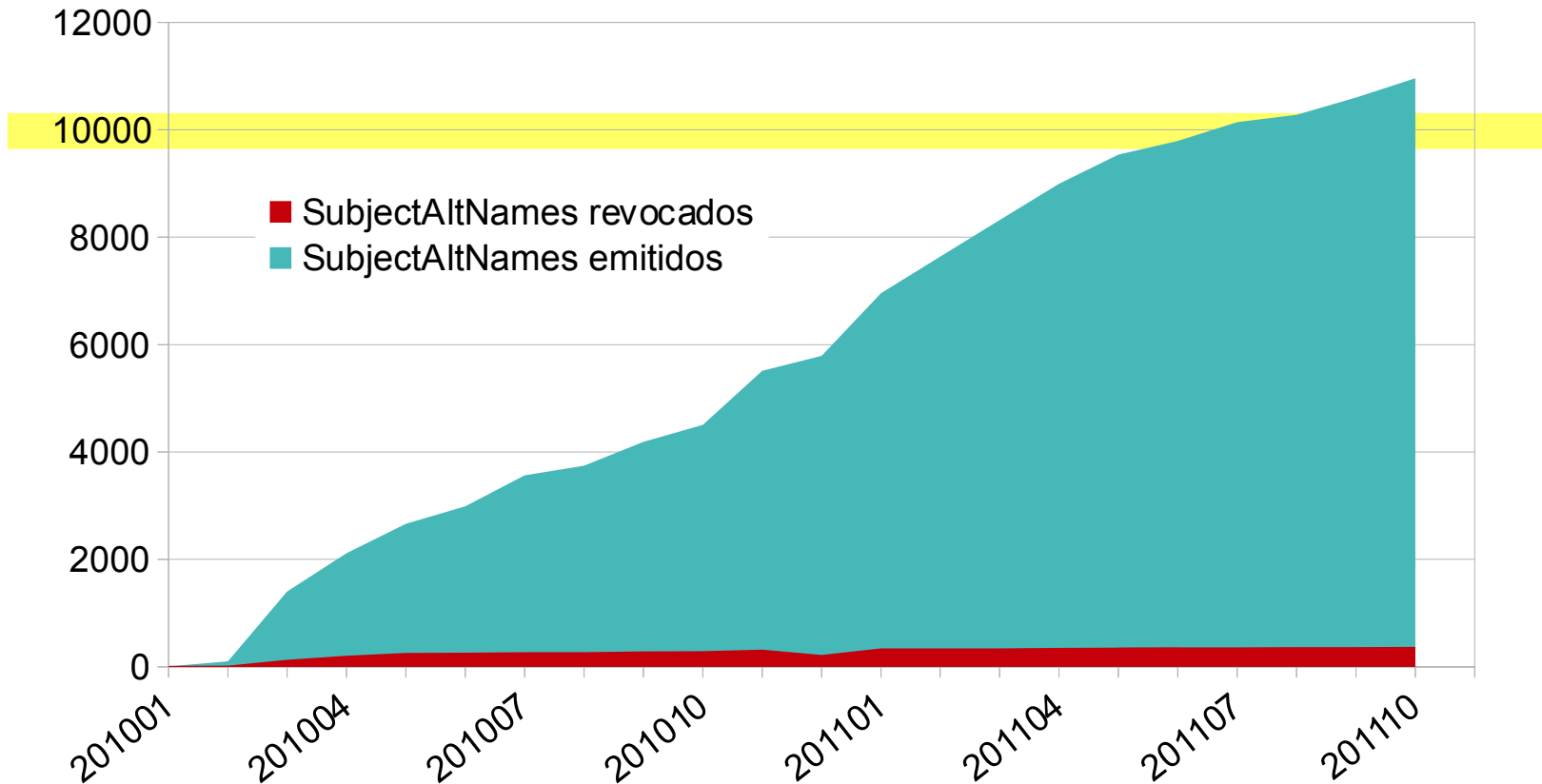
Estadísticas: SSL servidor

Certificados emitidos y revocados (acumulado)



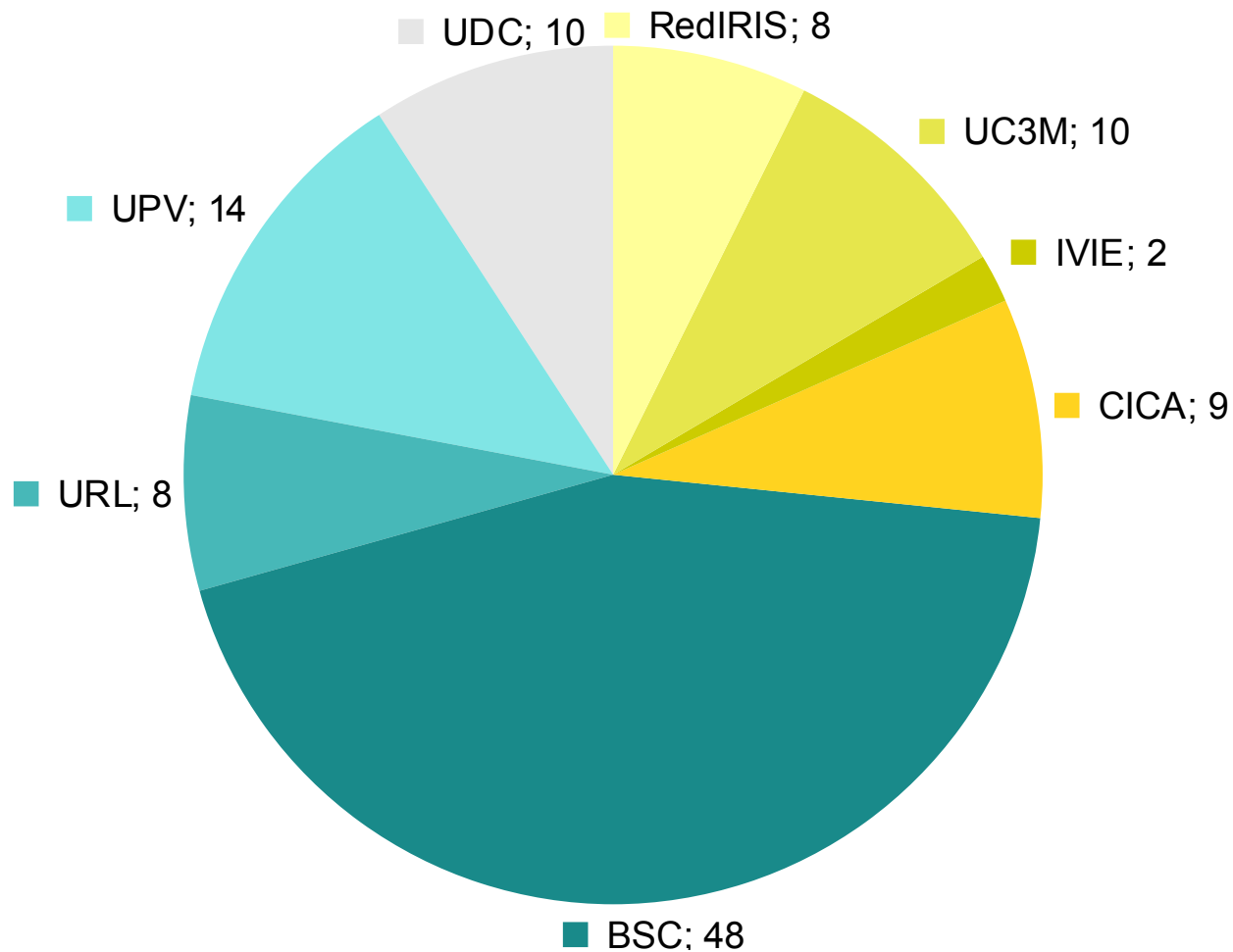
Estadísticas: SSL servidor

SubjectAltNames emitidos y revocados (acumulado)



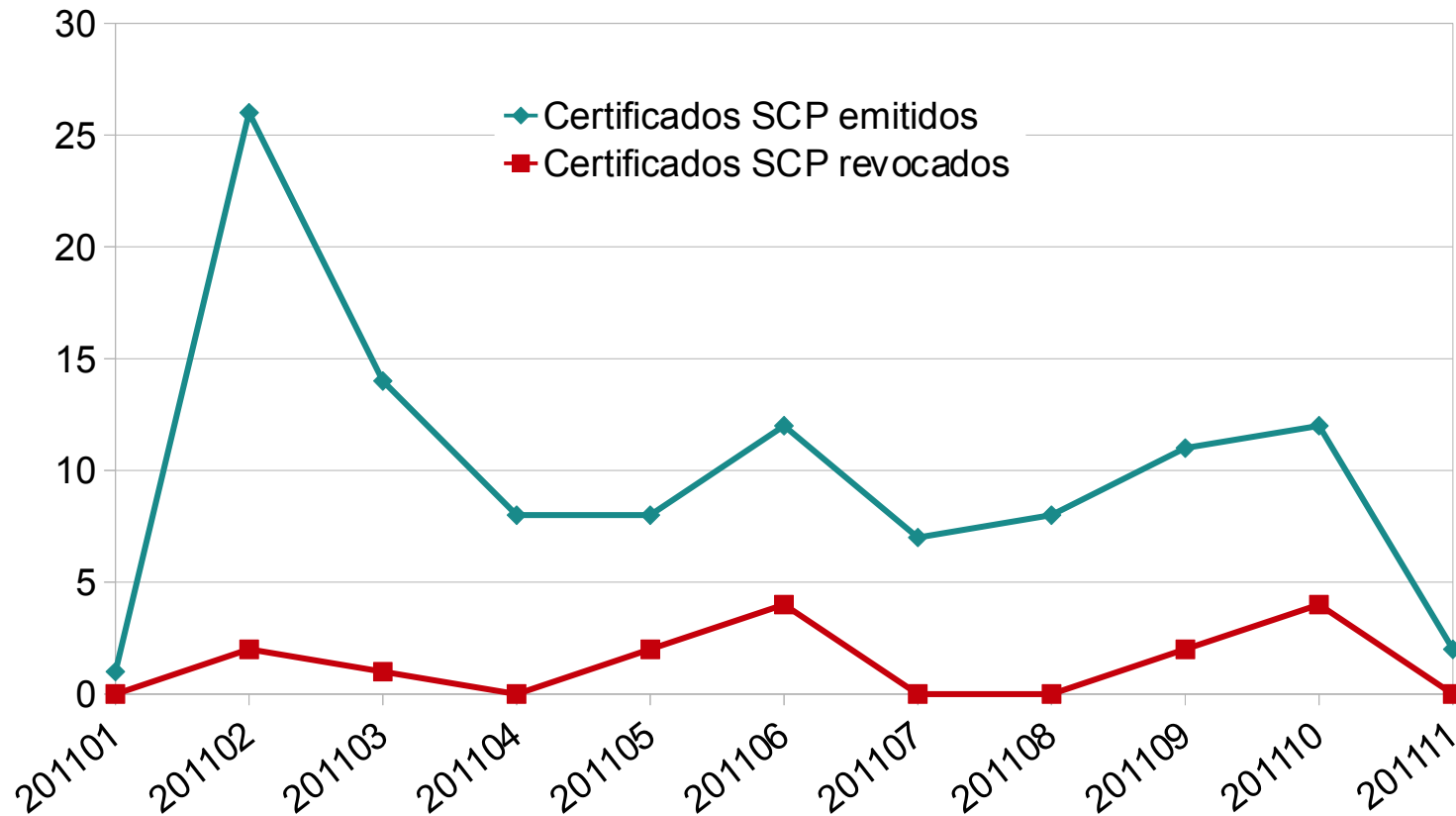
Estadísticas: SCP

Certificados emitidos



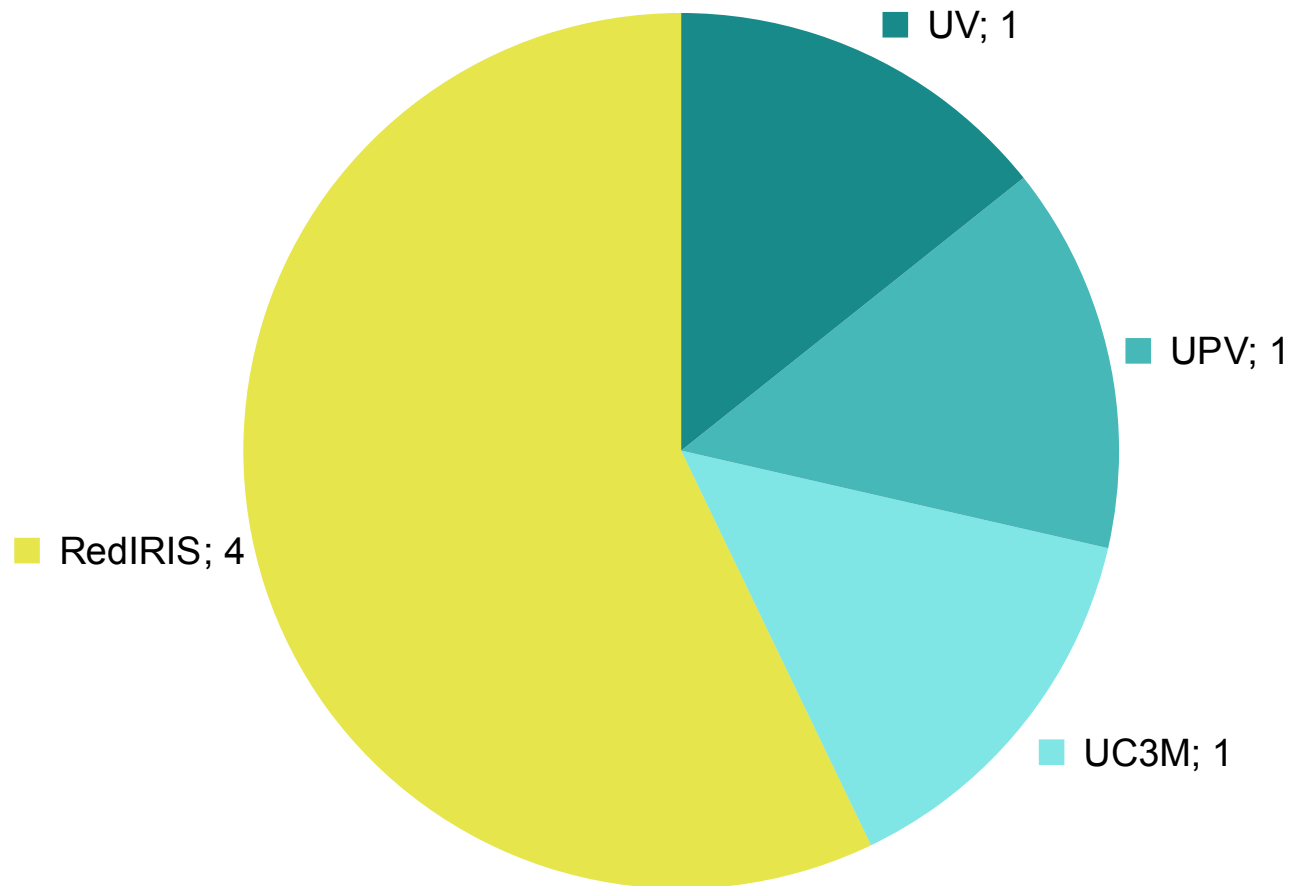
Estadísticas: SCP

Certificados emitidos y revocados (al mes)



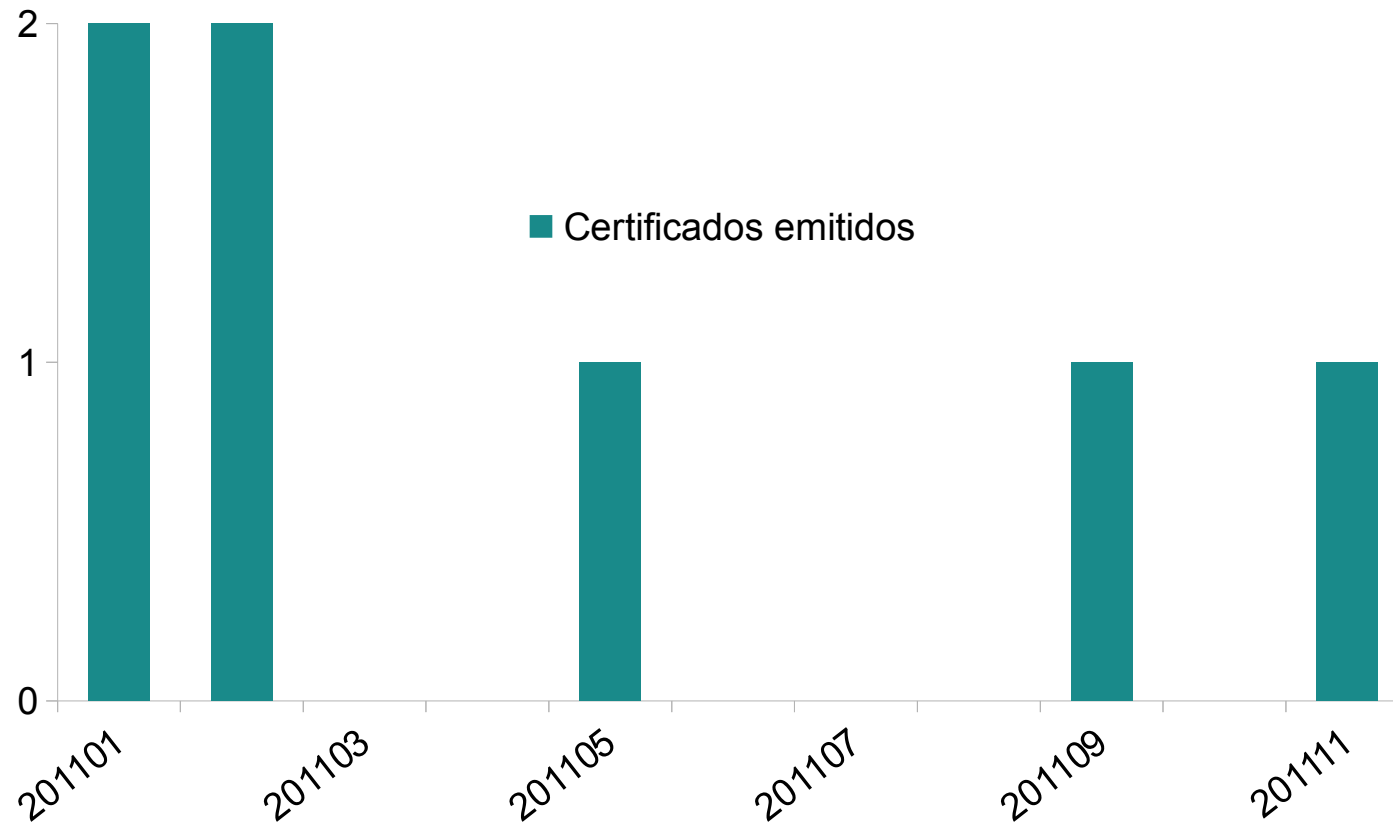
Estadísticas: Firma de Código

Certificados emitidos



Estadísticas: Firma de Código

Certificados emitidos (al mes)



Índice

- 1 Bienvenida
- 2 Escenario actual
- 3 Estadísticas
- 4 **Perfiles: Personal**
Firma de código
- 5 Incidencias
- 6 Ruegos y preguntas



GOBIERNO
DE ESPAÑA

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

MINISTERIO
DE CIENCIA
E INNOVACIÓN



Red
IRIS

- ¿Cómo se da de alta la institución en el servicio SCP?
 - Un operador de SCS debe enviar un mail a scs-ra@rediris.es
 - Identificador del conector SIR
 - Dirección de correo corporativa de la institución dedicada a dar soporte a sus usuarios
 - URL explicativa del servicio para los usuarios finales de la institución.
 - RedIRIS comprueba que esas direcciones funcionan
 - Se activa SCP para la institución

- ¿Qué usuarios pueden solicitar certificados?
 - Uso del atributo **ePA** (*eduPersonAffiliation*) en la aserción
 - Este atributo es utilizado para realizar el control de acceso a la solicitud de certificados personales. Los valores aceptados para este atributo son:
 - student: Estudiantes
 - faculty: PDI
 - staff: PAS
 - employee: staff & faculty
 - member: staff, faculty & student
- Guía del servicio
 - <http://www.rediris.es/scs/perfiles/personal/guia.html>

- Formato de un DN

- **C=ES, O=Inst, CN=Name, unstructuredName=ID_OpenID**

CN	Depende de los atributos que envíe el IdP de la institución a la que pertenece el usuario
----	---

unstructuredName	Identificador traceable, único y persistente del propietario del certificado en el ámbito del IdP de la institución a la que pertenece. http://www.rediris.es/sir/howto-openid.html
------------------	--

<http://yo.rediris.es/soy/uid@sHO/>
<http://eu.rediris.es/son/uid@sHO/>
<http://jo.rediris.es/soc/uid@sHO/>
<http://ni.rediris.es/uid@sHO/naiz/>

SCS: perfil Personal

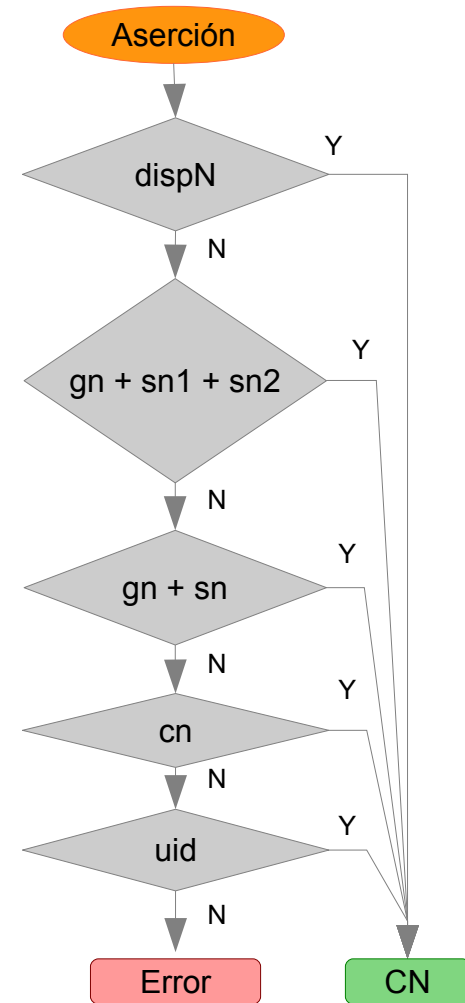
• Composición del CN

- Se genera a partir de los atributos codificados según SIR
 - dispN, gn, sn1, sn2, sn, cn, uid
http://www.rediris.es/sir/docs/attr_map.html
- Usando el proceso de composición
www.rediris.es/scs/perfiles/personal/guia.html#subjectdn

1. dispN
2. gn + sn1 + sn2
3. gn + sn
4. cn
5. uid

• Composición del unstructuredName

- <prefijo>/uid@sHO/< sufijo>



SCS: perfil Personal - Ejemplos

- **cn=Javier Fariñas Alvariño, uid=javier.farinas**
 - C=ES, O=upv.es, CN=**Javier Fariñas Alvariño**,
unstructuredName=<http://yo.rediris.es/soy/javier.farinas@udc.es/>
- **cn=Miguel MacÃ-as EnguÃ-danos, uid=mimaen**
 - C=ES, O=upv.es, CN=**Miguel MacÃ-as EnguÃ-danos**,
unstructuredName=<http://yo.rediris.es/soy/mimaen@upv.es/>
- **cn=Observatorio Sie, uid=obsersie**
 - C=ES, O=ivie.es, CN=**Observatorio Sie**,
unstructuredName=<http://yo.rediris.es/soy/obsersie@upv.es/>
- **cn= Unidad De Formación Pas Rrhh**
 - C=ES, O=upv.es, CN=**Unidad De Formación Pas Rrhh**,
unstructuredName=<http://yo.rediris.es/soy/rrhh06@upv.es/>

SCS: perfil Firma de código

- Por ahora “disponible de forma manual”
 - No integrado en el ISC
- ¿Cómo es el proceso para la obtención?
 - RedIRIS accede a un interface de solicitud que nos da COMODO
 - Introducimos los datos que nos debéis proporcionar
 - Nuestro navegador genera la clave clave privada y envía la CSR
 - COMODO nos envía el certificado
 - Lo instalamos en nuestro navegador y lo exportamos a PKCS #12
 - Os enviamos el PKCS #12 por mail
 - Eliminamos ese certificado de nuestro navegador
 - Hay que “confiar” en RedIRIS

SCS: perfil Firma de código

- ¿Cómo solicitarlo?

- Datos del certificado
 - Duración del certificado: 1 a 5 años
 - eMail de contacto que aparecerá en el certificado (opcional)
- Datos de la institución
 - Nombre oficial de la institución
 - Departamento (opcional)
 - Dirección postal
 - Código postal, Ciudad y Provincia
- Datos del contacto
 - Nombre, Apellidos
 - eMail
 - Teléfono

Índice

- 1 Bienvenida
- 2 Escenario actual
- 3 Estadísticas
- 4 Perfiles: Personal
Firma de código
- 5 Incidencias**
- 6 Ruegos y preguntas



GOBIERNO
DE ESPAÑA

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

MINISTERIO
DE CIENCIA
E INNOVACIÓN



Red
IRIS

Incidencias - ISC de RedIRIS

- Acceso por SIR

- Cambios en direcciones de correo
- Compromiso de la clave del usuario en la institución
 - Permite solicitar un certificado desde otra máquina y descargarlo
 - ¿Avisar por mail/SMS cuando se emite un certificado?

- SCS

- Avisos del alta de usuarios en el ISC a RedIRIS
 - Se automatizará el aviso para agilizar la validación de usuarios
- Fecha 1970-01-01 en los estados de los certificados
 - Se ha enviado la solicitud validada a COMODO pero todavía no ha sido firmada. Tenemos que arreglar el mensaje mostrado

Incidencias - ISC de RedIRIS

- **SCS** (continuación)
 - Sede electrónica
 - COMODO no es un prestador reconocido según las leyes 59/2003 y 11/2007 y, por tanto, sus certificados no tienen reconocimiento jurídico.
 - <https://www11.mityc.es/prestadores/busquedaPrestadores.jsp>
 - Pero COMODO es reconocido por los navegadores
 - Solicitados para: UM (José Fco. Hidalgo), UPV, USAL, URJC
 - Certificados wildcard
 - Actualmente no soportado
 - Futuro: ¿uso para dominios que sigan la regla de los tres puntos?
 - Tipo *.subdomain.domain.tld, por ejemplo *.blog.rediris.es

- SCP

- Los administradores no pueden ver los certificados emitidos bajo sus dominios
- Cambios de nombre, codificación UTF-8
- ¿Cómo identificar a un usuario?
 - Diferentes correos para un usuario
 - iMMa (irisMailMainAddress)
 - iMAA (irisMailAlternateAddress)
 - mail
 - Uso de sPUC?
<http://www.rediris.es/sir/docs/spuc.html>

Incidencias - COMODO

- Avisos

- Avisos de expiración de certificado llegan a RedIRIS
- No envían avisos de emisión de certificados SCP

- Retrasos en la firma de certificados

- Validación de control de dominios (DCV)

DCV (Domain Control Validation)

Verificación de la autoridad sobre el FQDN

- Problema

- Solicitantes no autorizados (por no ser dueños de los FQDNs) consiguieron validar solicitudes y se emitieron los certificados.

- Solución

- Verificación de la autoridad sobre el FQDN antes de validar la solicitud
- COMODO exige prueba de que el solicitante es la persona que tiene el control sobre el FQDN que se desea certificar
 - Uso del mecanismo DCV
 - Envío de un correo electrónico con un código necesario para una validación posterior vía web



DCV (Domain Control Validation)

Verificación de la autoridad sobre el FQDN

- Descripción del procedimiento DCV

- De la CSR se extrae el dominio a validar
- Se presenta una lista de direcciones al usuario para que elija donde recibir el código de validación. La lista se genera en base a
 - Datos obtenidos del Whois +
 - Lista de 5 nombres (decididos por Google, MS y Mozilla) por cada subdominio

admin@

administrator@

hostmaster@

postmaster@

webmaster@

- COMODO envía el código a esa dirección
- El usuario recibe el código y valida el dominio vía web
- COMODO valida la solicitud y emite el certificado al instante



DCV y tipos de certificado

- **Certificados con un dominio**

- Se usa DCV
 - Se envía un mensaje

- **Certificados con varios dominios**

- Se usa DCV para cada dominio
 - Se enviará un mail por cada dominio
 - No se emite el certificado hasta que se han validado todos los dominios
- Se intentará crear grupos de dominios con el mismo TLD para disminuir el número de mensajes.
 - a1b1.rediris.es, a1b2.rediris.es, a1b3.rediris.es
 - a2b1.rediris.com, a2b2.rediris.com
- Estamos probando con el interface de COMODO para ver opciones de implementación



DCV para www.rediris.es

Y otros 17 dominios más

Domain Control Validation for order 10982032 Close Window

Domain Name	DCV Email Address	DCV Progress	
		Sent	Valid
www.eduroam.es	webmaster@eduroam.es	<input type="button" value="Set For All"/> <input type="button" value="Whols"/> <input type="button" value="Remove"/>	✓
pk.irisgrid.es	webmaster@irisgrid.es	<input type="button" value="Whols"/> <input type="button" value="Remove"/>	✓
www.irisgrid.es			
pki.irisgrid.es			
www.rediris.com			
cmwebber.rediris.es	www.eduroam.es	<input type="button" value="Set For All"/> <input type="button" value="Whols"/> <input type="button" value="Remove"/>	✓
eu.rediris.es		<input type="button" value="Whols"/> <input type="button" value="Remove"/>	✓
intranet.rediris.es	pk.irisgrid.es	<input type="button" value="Whols"/> <input type="button" value="Remove"/>	✓
www.rediris.es	www.irisgrid.es	<input type="button" value="Whols"/> <input type="button" value="Remove"/>	✓
yo.rediris.es	www.irisgrid.es	<input type="button" value="Whols"/> <input type="button" value="Remove"/>	✓
sir.rediris.es	pki.irisgrid.es	<input type="button" value="Whols"/> <input type="button" value="Remove"/>	✓
wiki.rediris.es	www.rediris.com	<input type="button" value="Whols"/> <input type="button" value="Remove"/>	✓
stats.rediris.es	cmwebber.rediris.es	<input type="button" value="Whols"/> <input type="button" value="Remove"/>	✓
scs.rediris.es	eu.rediris.es	<input type="button" value="Whols"/> <input type="button" value="Remove"/>	✓
jo.rediris.es	administrator@rediris.es	<input type="button" value="Whols"/> <input type="button" value="Remove"/>	✓
ni.rediris.es	administrator@rediris.es	<input type="button" value="Whols"/> <input type="button" value="Remove"/>	✓
papi.rediris.es	administrator@rediris.es	<input type="button" value="Whols"/> <input type="button" value="Remove"/>	✓
www.rediris.net	administrator@rediris.net	<input type="button" value="Whols"/> <input type="button" value="Remove"/>	✓

DCV para www.rediris.es

Y otros 17 dominios más

De: Comodo Security Services <noreply@trust-provider.com>

Asunto: **Demonstrate domain control and approve 12 domains for SSL/TLS certificate order #10982032**

Fecha: 23 de noviembre de 2011 20:12:01 GMT+01:00

Para: administrator@rediris.es

Dear administrator@rediris.es,

We have received a request to issue an SSL certificate for
cmwebber.rediris.es
eu.rediris.es
intranet.rediris.es
jo.rediris.es
ni.rediris.es
papi.rediris.es
scs.rediris.es
sir.rediris.es
stats.rediris.es
www.rediris.es
www.rediris.es
yo.rediris.es.

Please ignore this email if neither you nor a trusted colleague made this request for a certificate.

Otherwise, please browse to

<https://secure.comodo.net/products/EnterDCVCode?orderNumber=10982032>


and enter the following "validation code":






DCV para www.rediris.es

Y otros 17 dominios más

	<i>« networking the networkers »</i>
Please do not use your browser's BACK and FOR	
Domain Control Validation (Part 2)	
Please enter your "validation code" for Order #10982032, then click "Next"	
<input type="text"/>	<input type="button" value="Next >"/>

	<i>« networking the networkers »</i>
Please do not use your browser's BACK and FORWARD buttons	
Thank you	
You have entered the correct Domain Control Validation code for this Domain. Your certificate will be issued once the remaining domains have been validated. Please close this window now.	
<input type="button" value="Close Window"/>	



Solicitud de certificado usando DCV para CN=prueba.upc.edu



The screenshot shows the RedIRIS ISC interface. On the left is a navigation menu with 'Servicios' selected. The main content area has a breadcrumb trail: 'Servicios < SCS < Beta < Oper'. The title is 'ISC: Interfaz de Solicitud de Certificados' by 'Javier Masa Marin @ RedIRIS'. There are two dropdown menus: 'Validez del certificado:' set to 'Un año' and 'Tipo de servidor:' set to 'OTHER'. Below is a 'CSR - Certificate Signing Request:' section containing a long alphanumeric string. At the bottom, there is a text input for 'Dirección de correo:' with 'javier.masa@rediris.es' and a 'Solicitar' button.

RedIRIS

Sobre RedIRIS
La Red
Servicios
Proyectos
Actividades
Difusión

Google Custom Search

SCSBeta SSL
Comprobar CSR
Solicitar Certificado
Revocar Certificado
Gestionar Certs

SCSBeta Personal
Solicitar certificado
Revocar certificado
Gestionar certificado

◀ Servicios ◀ SCS ◀ Beta ◀ Oper

ISC: Interfaz de Solicitud de Certificados

Javier Masa Marin @ RedIRIS

Validez del certificado:

Tipo de servidor:

CSR - Certificate Signing Request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC0jCCABoCAQAwODELMAkGA1UEBhMCRVMxEDAoBgNVBAoTB1J1ZElSSVMxZAV
BgNVBAMTDnBrLmlyeXNncmlkLmVzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAnOKzwgnown9lmi8d3rDQk1Xdyo3V1rDCD7ANBYWMScwe+jpjyhEZ1H0r
RbiNb1ZMKELqT0zA7JES/Pogf7kR6+wn5L/fDIS7/YkAkU4WqfDmJNMIa29Vr17
J3G6khoUwXNk0mqWYJwbamaDz1833bjbjXpcAk/Pec2h88T19+oU90b2pEsFR7EA
8IaHfx0X5RWHpoJgdhT22P++NtxIa+yiXJXs9dqDyMz82b0I6uGY94T0umhOQ4JW
U8eOHg/tFoDY8ebgYu1MT/GKbaTpBtde2A2PA1Kb98f60/tJapmgJ6V0C9Sa1QQA
6q3kxax5NKNNGdfmrWge5Jp4ynyuGDwIDAQABOFUwUwYJKoZIhvcNAQKOMUYwRDAJ
BgNVHRMEAJAAMAsGAlUdDwQEAwIFoDAQBgNVHREIzAhgg5way5pcmlz23Jp2C5l
c4IPcGtpLmlyeXNncmlkLmVzMAOGCSqGSIb3DQEBAQUAA4IBAQCOTnCNdrfTPmm9
focFKZYWcY4kTb3s3myRIJnDLPE+JOxzvehWwF3WgCtgc+uYPvakG0BrZU2NVabX
pAvh/xLR5ugnJk+q20wGI dwBVcl1EFqrrgEQQ9HPWQvCAP8EX0pwvqhXOfokMEbt
6iY6rRtLNh77k7qtRMQ76bsXWdX2uDeM9GNIRANFT0JX0532bnDXhhOjmaOpJMLM
HP+WEUnVzQKlm+ke3nSZH77heOwH/VftEWAuPyfcU9i6sBDQ780Hr1P923TQGL1f
EmqNfOlxcSBmItU/ZS00z90aakkP5z9K65pEJk3xo3uC6W+pdwrJ5ge+87PiHTkz
```

Dirección de correo:

Índice

- 1 Bienvenida
- 2 Escenario actual
- 3 Estadísticas
- 4 Perfiles: Personal
Firma de código
- 5 Incidencias
- 6 Ruegos y preguntas**



GOBIERNO
DE ESPAÑA

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

MINISTERIO
DE CIENCIA
E INNOVACIÓN



Red
IRIS

¡Muchas gracias!



Red IRIS

Más de 20 años al servicio de la investigación



GOBIERNO
DE ESPAÑA

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

MINISTERIO
DE CIENCIA
E INNOVACIÓN



Red IRIS