

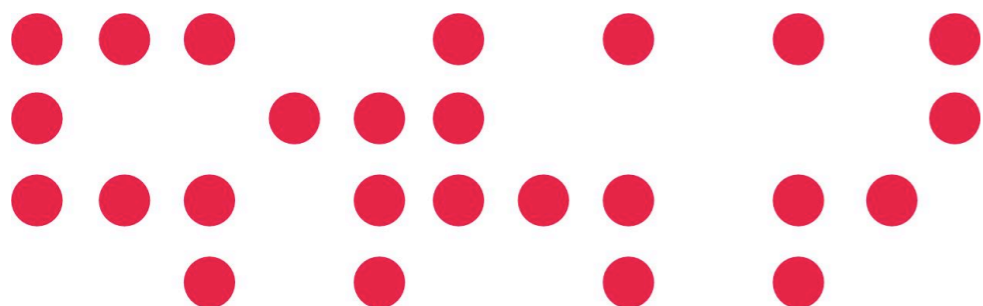


Servicio de Certificados Personales de RedIRIS

SCP

Daniel García - daniel.garcia@rediris.es

1. Estado actual SCS
 - 1.1. Requisitos para acceder al ISC
 - 1.2. Estadísticas
2. Presentación SCP
3. Condiciones de acceso a SCP
4. Planificación SCP



- Requisitos de acceso al ISC

1. Institución dada de alta en el SIR

<http://www.rediris.es/servicios/sir>

- 1.1. Cumplir con la política de atributos de SCS

- **mail**: correo electrónico del usuario
- **ePE**: eduPersonEntitlement indica en rol del usuario
 - urn:mace:rediris.es:entitlement:scs:**req**
 - urn:mace:rediris.es:entitlement:scs:**admin**
- **sHO**: Identificar unívocamente a las instituciones

Los atributos multivaluados se separan con una barra vertical '|'

- Requisitos de acceso al ISC

- 2. Documento de condiciones de uso

- http://www.rediris.es/scs/doc/pdf/scs_cuso.pdf

- 2.1. ID del conector SIR

- <http://www.rediris.es/app/sirdemo/demo/sirdemo.php>

**Pero esto del ID del conector SIR
qué es**

◀ Inicio ▶ Servicios ▶ SIR ▶ Demo de Servidor de Identidad de RedIRIS ▶ SIRdemo

SIRdemo: entorno de pruebas del SIR

Si ha accedido a esta página significa que su proveedor de identidad (IdP) **ha autenticado correctamente** al usuario.

El objetivo de esta aplicación es comprobar que su IdP está enviando los atributos requeridos, tal como se especifica en la [guía](#) para la solicitud de inclusión de IdP en el SIR.

Comprobación de conector

El conector se ha identificado con el siguiente valor:

✓ Conector	newbabia
✓ SHA-1 clave pública	ca636ca2ae9974b7467dd7afb4a60a084fc91e32

ID del conector SIR

Comprobación de atributos

La siguiente lista son los atributos requeridos por el SIR:

✓ ePTI	9ef8e62325ade84eb069e82a5ec93009
✓ ePA	staff
✓ sHO	rediris.es
✓ ePE	urn:mace:rediris.es:entitlement:scs:admin urn:mace:rediris.es:entitlement:wiki:jra5 urn:mace:rediris.es:entitlement:wiki:jra5
✓ sPUC	urn:mace:terena.org:schac:personalUniqueCode:es:rediris:sir:mbid:{md5}749302e9ede903cf76a809cadb90

¡Enhorabuena! Su IdP está enviando todos los atributos que se recomiendan para participar en el SIR. Póngase en contacto con el equipo técnico del SIR para solicitar la inclusión de su IdP en el entorno de producción.

- Requisitos de acceso al ISC

- 2. Documento de condiciones de uso

- http://www.rediris.es/scs/doc/pdf/scs_cuso.pdf

- 2.2. Firmar ambas páginas del CUSO



RedIRIS / Red.es Servicio de Certificados de Servidor. Condiciones de uso

Servicio de Certificados de Servidor de RedIRIS Condiciones de uso - v: 2.1 - 20100311

D./Dña.

como solicitante autorizado de certificados de servidor dentro del servicio SCS de RedIRIS para los servidores cuyos nombres de dominio (FQDN: "Fully Qualified Domain Name") se encuentren en los dominios que se detallan al final de este documento (en adelante, "el Solicitante"), declara que:

- Conoce y asume las normas y procedimientos vigentes, términos y condiciones, y requisitos técnicos establecidos para la solicitud de certificados SCS especificados en <http://www.rediris.es/scs/> y, en especial, las detalladas en la Declaración de Práctica de Certificación (CPS: "Certificate Practice Statement") del servicio. Los solicitantes asumen las condiciones y las modificaciones oportunas de las mismas que se lleven a cabo, y que serán comunicadas con antelación suficiente en el website y a las Personas de Enlace con RedIRIS (en adelante, "PERs") de sus respectivas instituciones.
- Conoce que el incumplimiento de estas normas puede suponer la revocación de los certificados.
- Declara que los datos facilitados en la presente solicitud son ciertos, salvo error u omisión de buena fe.
- Se compromete a mantener siempre actualizada la información facilitada en esta solicitud, comunicando a los PERs cualquier cambio que se produzca, así como a revisar que los certificados son acordes con la solicitud original antes de su utilización. El incumplimiento de esta obligación puede dar lugar a la revocación del/de los certificado/s.
- Asume y conoce que los certificados emitidos deben usarse exclusivamente para el acceso a recursos propios de la institución en tanto en cuanto a sus actividades académicas y de investigación, quedando expresamente excluido su uso para cualquier tipo de transacciones financieras.
- Asume que RedIRIS, en la tramitación de las diferentes actuaciones relativas a la emisión de los certificados de servidor SCS, actuará tomando en consideración los datos comunicados por el Solicitante.
- Es consciente y asume que cualquier falsedad o error en los datos consignados en la presente solicitud podrá ser causa de desestimación de la misma.
- Es consciente y asume que, una vez el sistema le comunique que los certificados han sido emitidos, pueden ser revocados por incumplir los requisitos establecidos al efecto.
- Es consciente y asume que, en caso de grave negligencia técnica, los certificados de servidor pueden ser revocados.

Declara que las solicitudes de certificado sólo serán cursadas cuando, de acuerdo con su conocimiento, el uso de los certificados no violen derechos de terceros.

- Se compromete a que las claves privadas asociadas con los certificados serán tratadas como información confidencial, así como a que los certificados no serán utilizados de manera alguna en caso de revocación de los mismos.
- Asume que el servicio es prestado por RedIRIS en términos no comerciales para sus usuarios de la comunidad investigadora y académica, y que no cabe reclamar responsabilidad a RedIRIS en relación con la prestación de dichos servicios
- Conoce y asume que RedIRIS observará en el tratamiento de los datos personales de las personas y entidades mencionadas lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y normativa de desarrollo, en relación con la solicitud y emisión de certificados de servidor SCS.
- Conoce y asume que los derechos de acceso y rectificación podrán ejercerse de acuerdo con lo dispuesto en la normativa de protección de datos de carácter personal. Los derechos de cancelación y oposición únicamente podrán ejercerse previa revocación del certificado de servidor SCS correspondiente, dado que el tratamiento de los datos personales por parte de Red.es es necesario para la emisión de certificados de servidor SCS.

SCS-CUSO: v.2.1 - 20100311 1 / 2

Firma del solicitante:

Firma del PER:



RedIRIS / Red.es Servicio de Certificados de Servidor. Condiciones de uso

1. Aceptación del Solicitante

En a de de 20

Nombre: Firma:

DNI/pasaporte:

e-mail:

2. Identificación SIR del Solicitante

eduPersonEntitlement (epE): urn:mace:rediris.es:entitlement:scs:

req: operador, admin: administrador

e-mail:

schacHomeOrganization (sHO):

ID del conector SIR:

3. Validación por el PER de la institución

El PER de la institución ha comprobado que el Solicitante puede actuar como responsable técnico del servidor o servidores incluidos en los dominios detallados al final del documento para el/los que queda autorizado para solicitar certificado/s de acuerdo con estas condiciones de uso.

En a de de 20

Nombre: Firma:

DNI/pasaporte:

e-mail:

4. Dominios para los que se podrán solicitar certificados SCS

Lista de los dominios en los que deben encontrarse los FQDN de los servidores para que la solicitud de certificado sea aceptada

1 <input type="text"/>	6 <input type="text"/>
2 <input type="text"/>	7 <input type="text"/>
3 <input type="text"/>	8 <input type="text"/>
4 <input type="text"/>	9 <input type="text"/>
5 <input type="text"/>	10 <input type="text"/>

Por favor utilice mayúsculas para cumplimentar este documento.

SCS-CUSO: v.2.1 - 20100311 2 / 2

Salamanca, 14 de Junio de 2010

7

RedIRIS / Red.es Servicio de Certificados de Servidor. Condiciones de uso

Servicio de Certificados de Servidor de RedIRIS Condiciones de uso - v: 2.1 - 20100311

D./Dña.

como solicitante autorizado de certificados de servidor dentro del servicio SCS de RedIRIS para los servidores cuyos nombres de dominio (FQDN: "Fully Qualified Domain Name") se encuentren en los dominios que se detallan al final de este documento (en adelante, "el Solicitante"), declara que:

1. Conoce y asume las normas y procedimientos vigentes, términos y condiciones, y requisitos técnicos establecidos para la solicitud de certificados SCS especificados en <http://www.rediris.es/scs/> y, en especial, las detalladas en la Declaración de Práctica de Certificación (CPS: "Certificate Practice Statement") del servicio. Los solicitantes asumen las condiciones y las modificaciones oportunas de las mismas que se lleven a cabo, y que serán comunicadas con antelación suficiente en el website y a las Personas de Enlace con RedIRIS (en adelante, "PERs") de sus respectivas instituciones.
2. Conoce que el incumplimiento de estas normas puede suponer la revocación de los certificados.
3. Declara que los datos facilitados en la presente solicitud son ciertos, salvo error u omisión de buena fe.
4. Se compromete a mantener siempre actualizada la información facilitada en esta solicitud, comunicando a los PERs cualquier cambio que se produzca, así como a revisar que los certificados son acordes con la solicitud original antes de su utilización. El incumplimiento de esta obligación puede dar lugar a la revocación del/de los certificado/s.
5. Asume y conoce que los certificados emitidos deben usarse exclusivamente para el acceso a recursos propios de la institución en tanto en cuanto a sus actividades académicas y de investigación, quedando expresamente excluido su uso para cualquier tipo de transacciones financieras.
6. Asume que RedIRIS, en la tramitación de las diferentes actuaciones relativas a la emisión de los certificados de servidor SCS, actuará tomando en consideración los datos facilitados por el Solicitante.
7. Es consciente y asume que cualquier falsedad o error en los datos consignados en la presente solicitud podrá ser causa de desestimación de la misma.
8. Es consciente y asume que, una vez el sistema le comuniqué que los certificados han sido emitidos, pueden ser revocados por incumplir los requisitos establecidos al efecto.
9. Es consciente y asume que, en caso de grave negligencia técnica, los certificados de servidor pueden ser revocados.

Declara que las solicitudes de certificado sólo serán cursadas cuando, de acuerdo con su conocimiento, el uso de los certificados no violen derechos de terceros.

10. Se compromete a que las claves privadas asociadas con los certificados serán tratadas como información confidencial, así como a que los certificados no serán utilizados de manera alguna en caso de revocación de los mismos.
11. Asume que el servicio es prestado por RedIRIS en términos no comerciales para sus usuarios de la comunidad investigadora y académica, y que no cabe reclamar responsabilidad a RedIRIS en relación con la prestación de dichos servicios.
12. Conoce y asume que RedIRIS observará en el tratamiento de los datos personales de las personas y entidades mencionadas lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y normativa de desarrollo, en relación con la solicitud y emisión de certificados de servidor SCS.
13. Conoce y asume que los derechos de acceso y rectificación podrán ejercerse de acuerdo con lo dispuesto en la normativa de protección de datos de carácter personal. Los derechos de cancelación y oposición únicamente podrán ejercerse previa revocación del certificado de servidor SCS correspondiente, dado que el tratamiento de los datos personales por parte de Red.es es necesario para la emisión de certificados de servidor SCS.

SCS-CUSO: v.2.1 - 20100311 1 / 2

RedIRIS / Red.es Servicio de Certificados de Servidor. Condiciones de uso

1. Aceptación del Solicitante

En a de de 20

Nombre: Firma:

DNI/pasaporte:

e-mail:

2. Identificación SIR del Solicitante

eduPersonEntitlement (epE): urn:mace:rediris.es:entitlement:scs:
req: operador, admin: administrador

e-mail:

schacHomeOrganization (sHO):

ID del conector SIR:

3. Validación por el PER de la institución

El PER de la institución ha comprobado que el Solicitante puede actuar como responsable técnico del servidor a de de 20

Nombre: Firma:

DNI/pasaporte:

e-mail:

4. Dominios para los que se podrán solicitar certificados SCS

Lista de los dominios en los que deben encontrarse los FQDN de los servidores para que la solicitud de certificado sea aceptada

1	<input type="text"/>	6	<input type="text"/>
2	<input type="text"/>	7	<input type="text"/>
3	<input type="text"/>	8	<input type="text"/>
4	<input type="text"/>	9	<input type="text"/>
5	<input type="text"/>	10	<input type="text"/>

Por favor utilice mayúsculas para cumplimentar este documento.

SCS-CUSO: v.2.1 - 20100311 2 / 2

Firmar aquí!!!

Firma del solicitante:

Firma del PER:

- Requisitos de acceso al ISC

- 3. Registro en el ISC de los usuario

- <http://www.rediris.es/scs/isc/>

- 2.2. Al acceder el ISC hace una re-dirección al formulario de registro, siempre que el usuario tenga permisos para acceder.


◀ [Servicios](#) ▶ [SCS](#) ▶ [ISC](#)

ISC: Interfaz de Solicitud de Certificados Alta de usuario

Acceso no permitido

El acceso a la aplicación de gestión de certificados del Servicio de Certificados Servidor (SCS) de RedIRIS está restringido a usuarios autorizados por el PER de cada institución afiliada a RedIRIS.

Usted puede rellenar el siguiente formulario con el fin de que el PER de su institución le autorize.

Recuerde que es necesario el envío del [Documento de Condiciones de Uso \(sólo para certificados SSL\)](#)  para que sea aceptada su solicitud.

1. *Nombre:

SCSOper

2. *Primer apellido:

Prueba1

3. *Segundo apellido:

Prueba2

4. Correo electrónico:

scsoper@rediris.es

5. *Telefono:

+34 955056623

6. Estado:

urn:mace:rediris.es:entitlement:scs:pending

← **Simplemente indica el estado del usuario**

7. Institution:

TEST

8.

enviar

9. * denotes required field

◀ [Servicios](#) ▶ ◀ [SCS](#) ▶ ◀ [ISC](#)

ISC: Interfaz de Solicitud de Certificados

Alta de usuario

Ha sido añadido correctamente como SCSOper Prueba1 Prueba2

Sus datos son:

- ID: 176
- UID: scsoper
- Common Name: SCSOper Prueba1 Prueba2
- e-mail: scsoper@rediris.es
- Entitlement: urn:mace:rediris.es:entitlement:scs:pending
- Phone: +34 955056623
- Institution: TEST

Comprobar los datos, y si hay alguno erróneo comunicarlo a scs-ra@rediris.es



TEST

◀ [Servicios](#) ▶ ◀ [SCS](#) ▶ ◀ [ISC](#)

ISC: Interfaz de Solicitud de Certificados

Alta de usuario

Ha sido añadido correctamente como SCSOper Prueba1 Prueba2

Sus datos son:

- ID: 176
- UID: scsoper
- Common Name: SCSOper Prueba1 Prueba2
- e-mail: scsoper@rediris.es
- Entitlement: urn:mace:rediris.es:entitlement:scs:pending
- Phone: +34 955056623
- Institution: TEST

Comprobar los datos, y si hay alguno erróneo comunicarlo a scs-ra@rediris.es



Aun no está validado el usuario, por lo que si intentais acceder a cualquier zona del ISC...

TEST

RedIRIS

◀ [Servicios](#) ◀ [SCS](#) ◀ [ISC](#)

ISC: Interfaz de Solicitud de Certificados

SCSOper Prueba1 Prueba2 @ AESIR

Acceso no permitido

Usted ya ha realizado una solicitud de creación de usuario que se encuentra pendiente de validar por los responsbre del ISC de RedIRIS. Si lo desea puede modificar ciertos datos de su solicitud.

1. Correo electrónico:
scsoper@rediris.es
2. *Telefono:
3. Estado:
urn:mace:rediris.es:entitlement:scs:pending
4. Institution:
AESIR
5.
6. * denotes required field

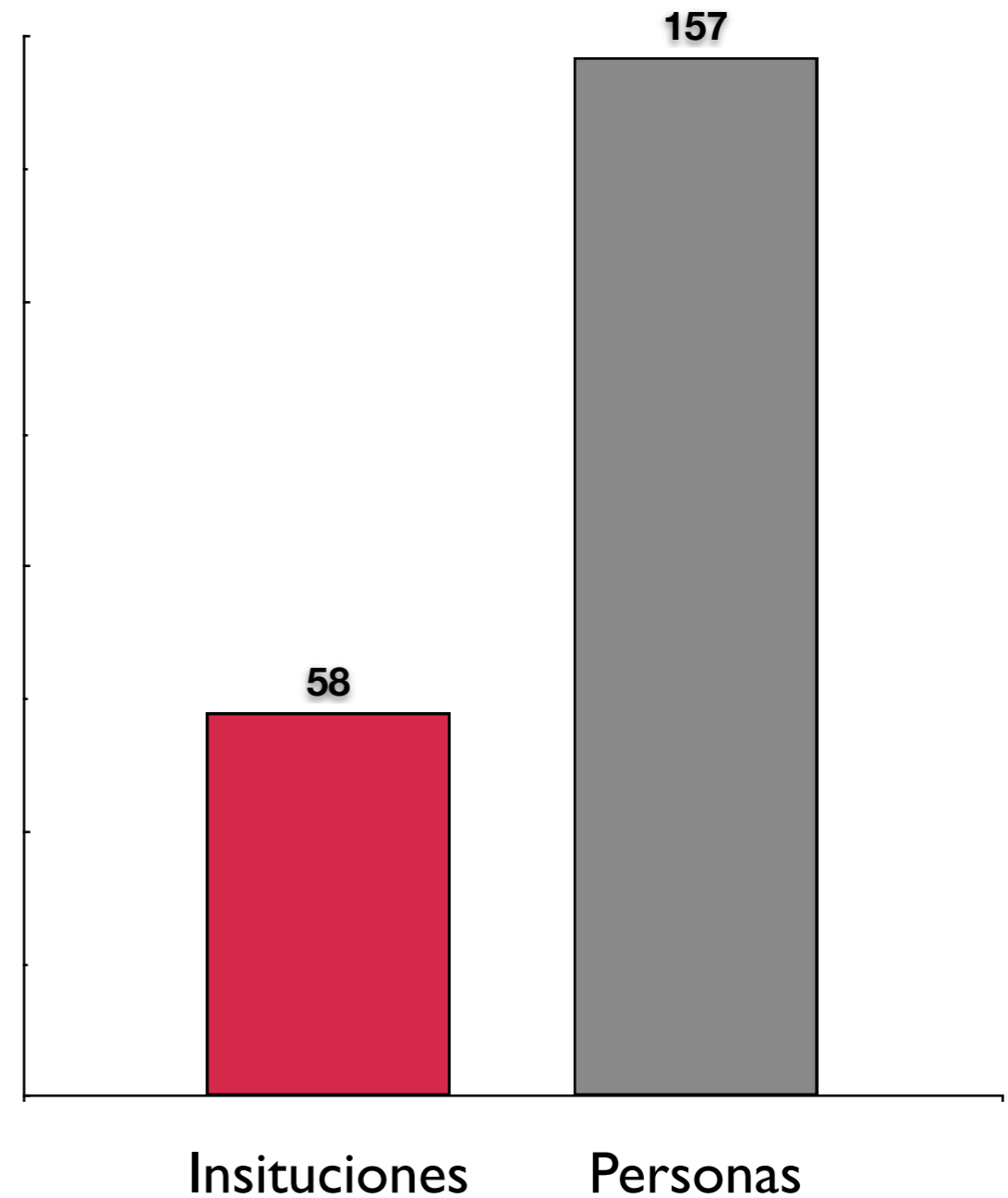
Mapa Web | Contacto | Accesibilidad | Actualizado el 31/05/2010 | © RedIRIS | Red.es

The screenshot shows the RedIRIS website interface. On the left is a navigation menu with items like 'Sobre RedIRIS', 'La Red', 'Servicios', 'Proyectos', 'Actividades', and 'Difusión'. Below the menu is a Google Custom Search box and a list of links under 'Interfaz de Solicitud de Certificados', including 'Comprobar CSR', 'Solicitar Certificado', 'Revocar Certificado', and 'Gestionar Certs'. The main content area has a breadcrumb trail: 'Servicios < SCS < ISC'. The title is 'ISC: Interfaz de Solicitud de Certificados' with a subtitle 'SCSOper Prueba1 Prueba2 @ AESIR'. A red-bordered box highlights the message 'Acceso no permitido'. Below this, a paragraph explains that the user has created a pending user request and can modify it. A list of details follows: 1. Correo electrónico: scsoper@rediris.es; 2. *Telefono: +34 955056623; 3. Estado: urn:mace:rediris.es:entitlement:scs:pending; 4. Institution: AESIR; 5. An 'enviar' button; 6. * denotes required field. The footer contains 'Mapa Web | Contacto | Accesibilidad | Actualizado el 31/05/2010 | © RedIRIS | Red.es' and the Webbered logo.

- Estadísticas I

- Estadísticas I

Instituciones y Personas participantes

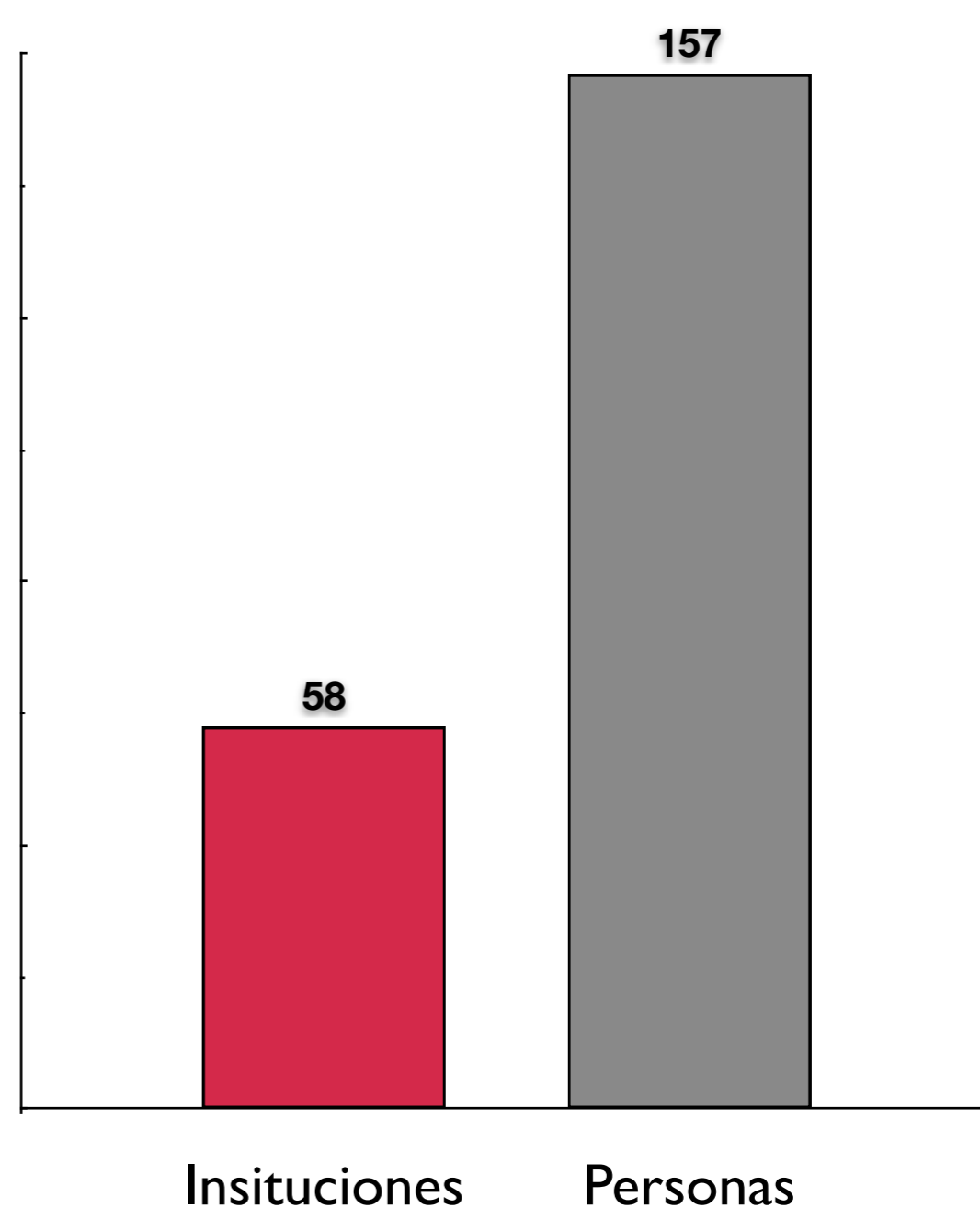


- Estadísticas I

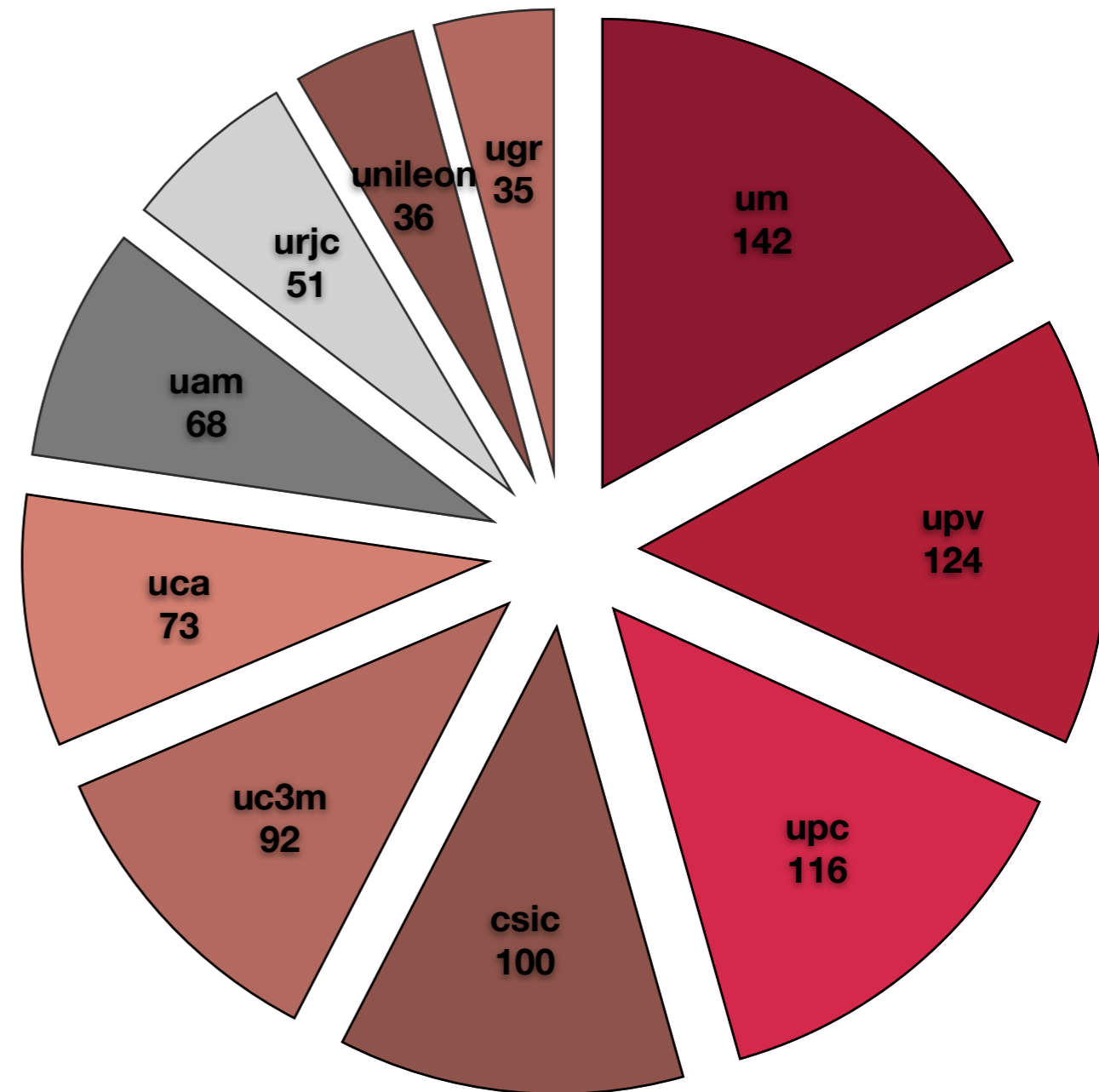
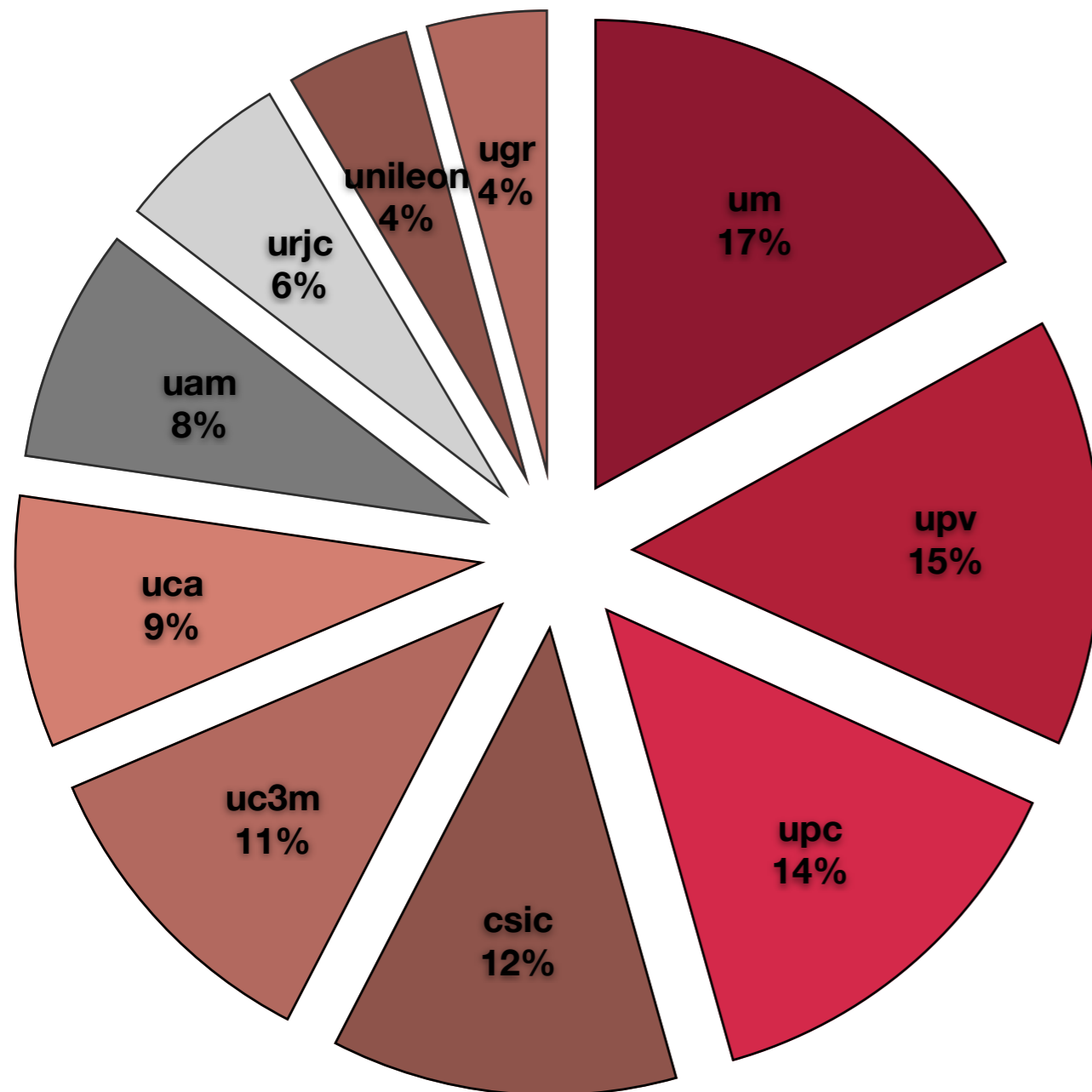
CSR y Certificados procesados



Instituciones y Personas participantes

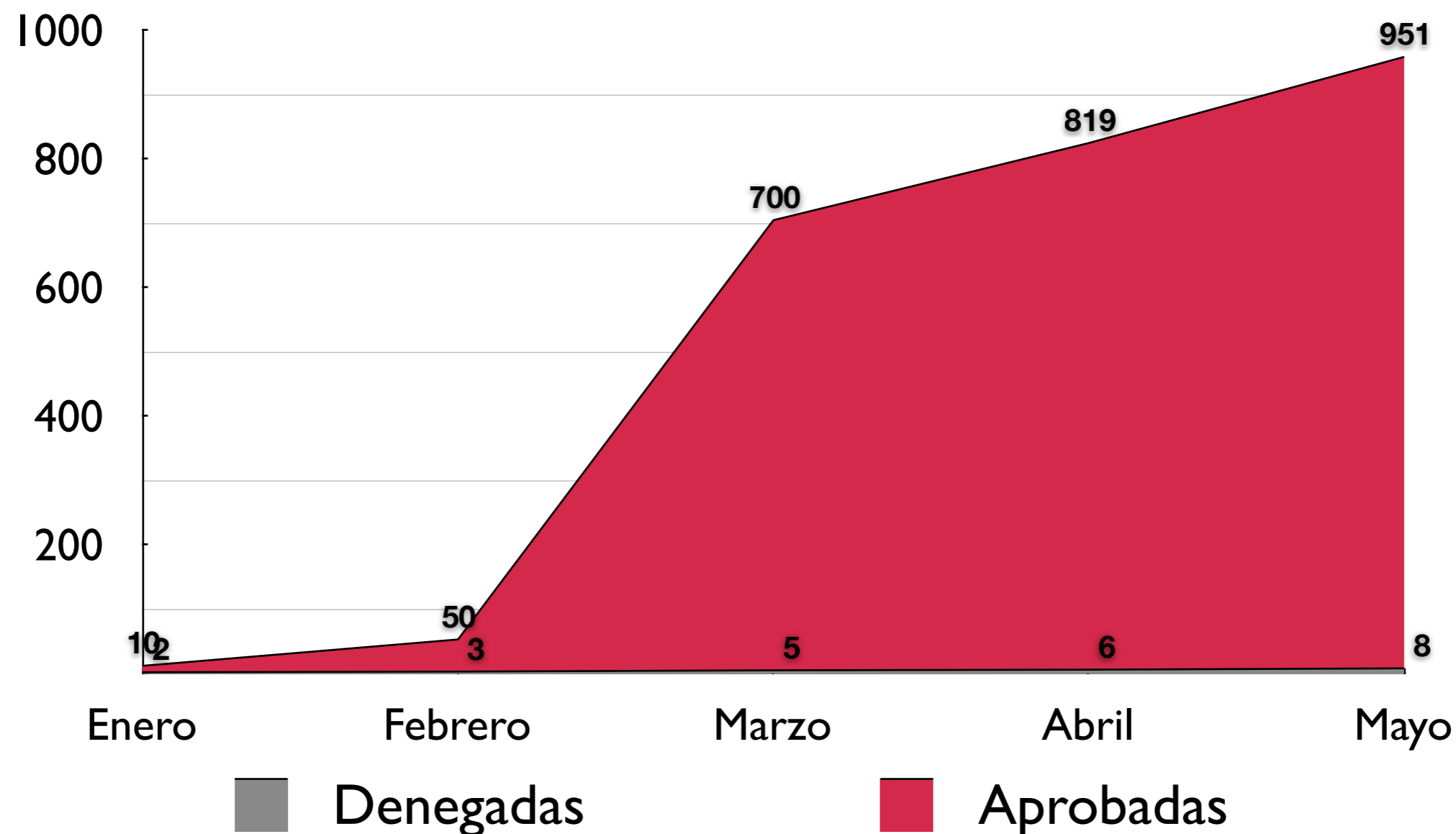


- Estadísticas II
 - Certificados por institución

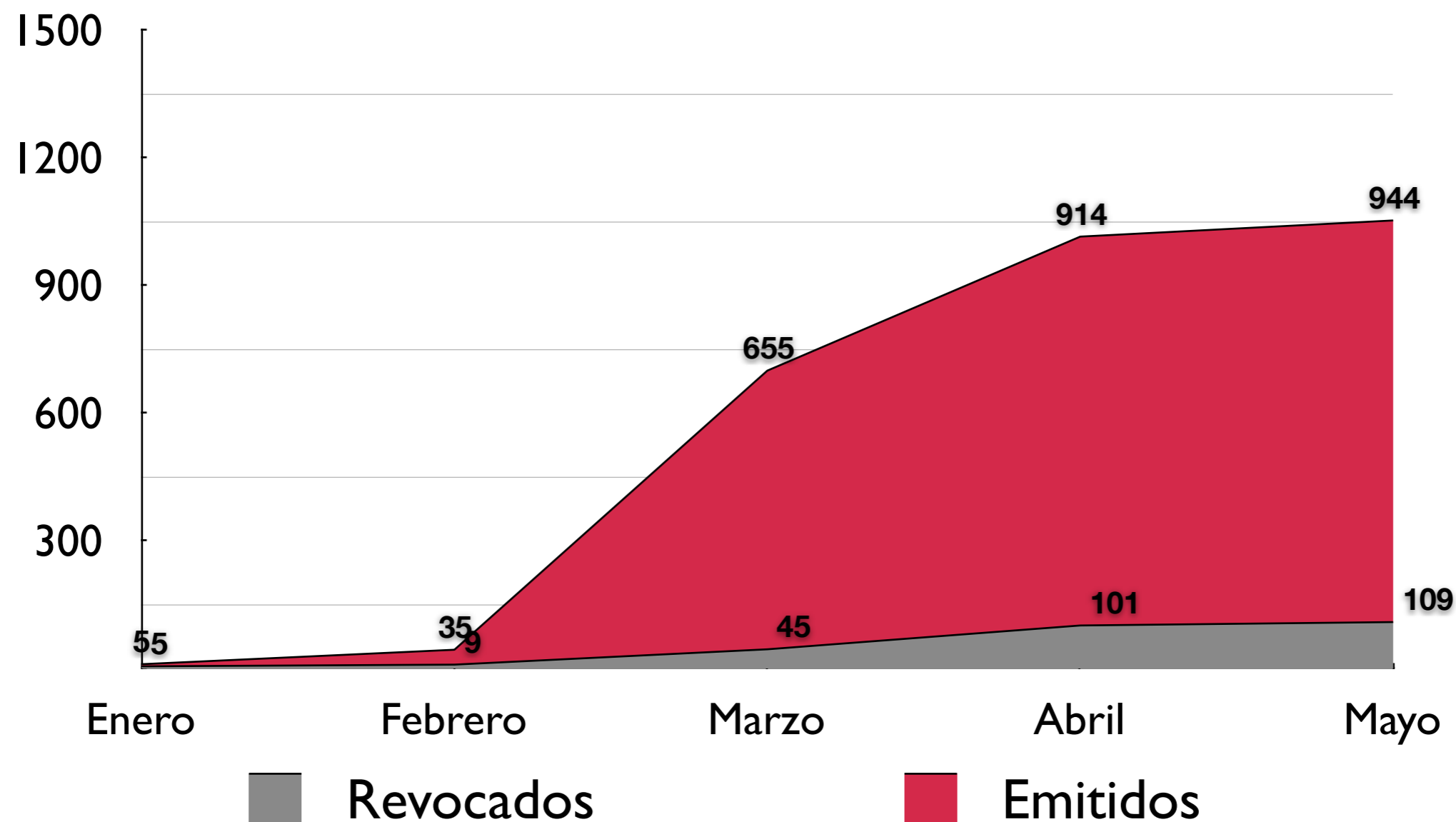


- Estadísticas III

- Distribución temporal de CSRs

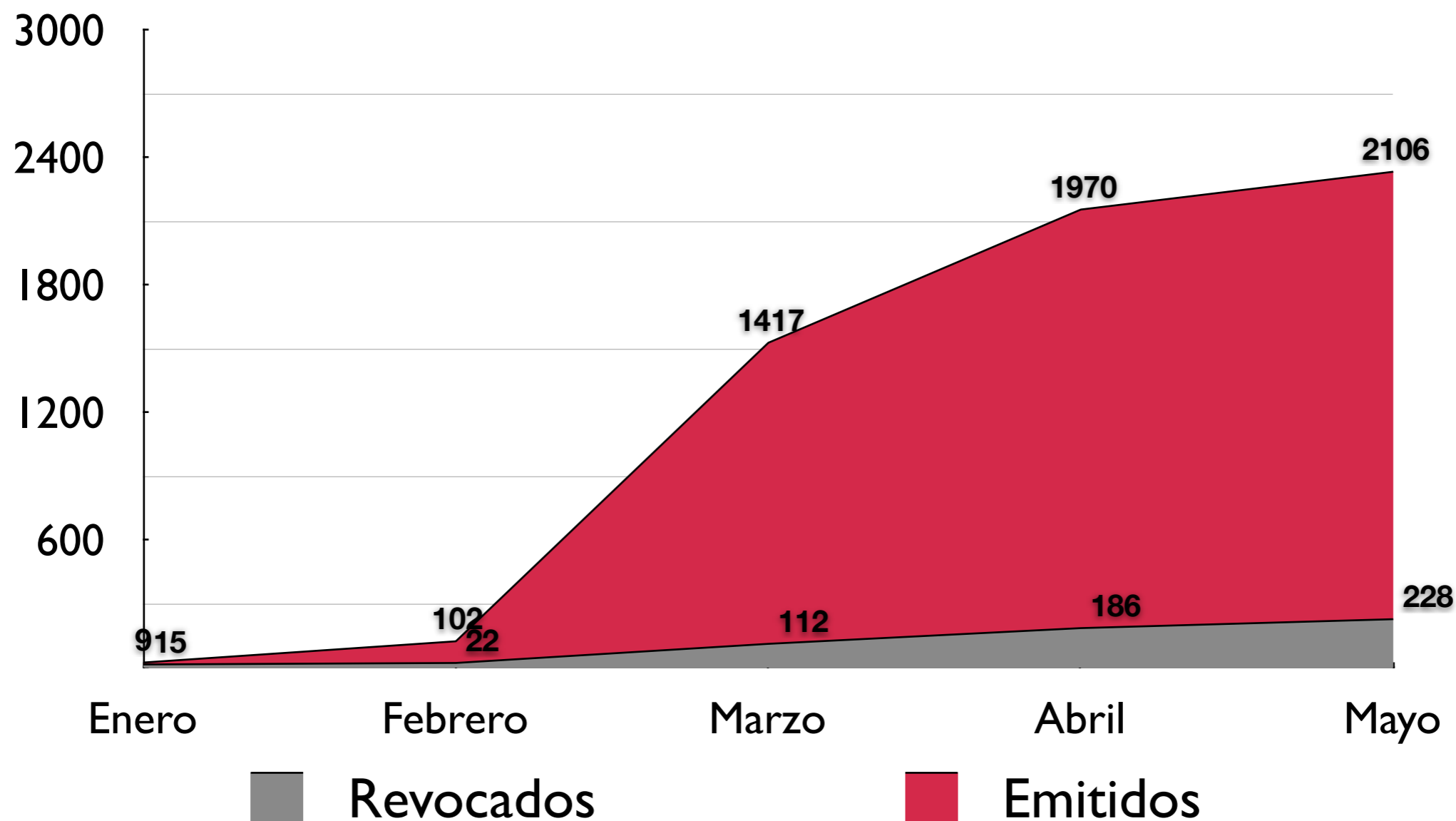


- Estadísticas IV
 - Distribución temporal de Certificados



- Estadísticas V

- Distribución temporal de SubjectAltNames



- Servicio de Certificados **Personales**
 - **Objetivo:** Identificar usuarios individuales y asegurar comunicaciones vía e-mail

Autenticación



Firma de eMail



- Servicio de Certificados **Personales**
 - **Usuarios potenciales:** Estos certificados van dirigidos al personal de todas las instituciones afiliadas a RedIRIS (alumnos también)
 - **Validez:** Tienen un periodo de validez de hasta 3 años

- Servicio de Certificados **Personales**

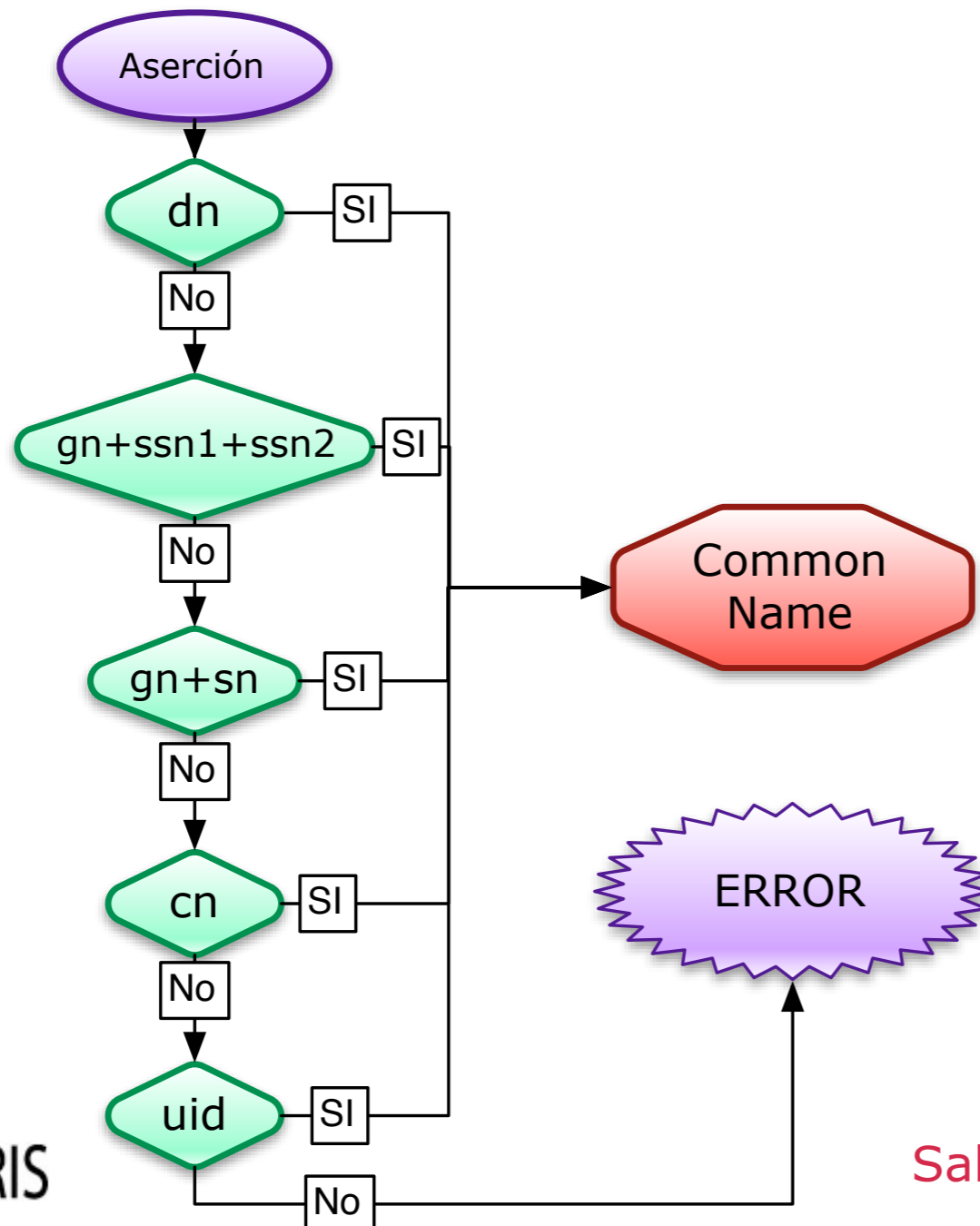
Características técnicas

- Subject DN
 - C=ES
 - O=RedIRIS
 - CN=Nombre Apellido1 Apellido2*
 - UN=email@dom.ain**
- Extensiones
 - **X509v3 Key Usage:** Digital Signature, Key Encipherment
 - **X509v3 Extended Key Usage:** E-mail Protection, TLS Web Client Authentication
 - **X509v3 Subject Alternative Name:** emailAddress1, ..., emailAddress10

• Servicio de Certificados **Personales**

Características técnicas

• Composición del Common Name



dn = Display name
gn = Given name
ssn1 = schacSn1
ssn2 = schacSn2
sn = Surname
cn = Common Name
uid = User identifier

- Servicio de Certificados **Personales**

Características técnicas

- Composición del Unstructured Name (UN)
 - Es un identificador **traceable, único y persistente** del dueño del certificado, en el ámbito del **IdP** (Proveedor de identidad)
 - Hemos decidido que sea el primer valor del atributo **mail** enviado en la aserción

- Servicio de Certificados **Personales**

Jerarquía de CAs

- AAA Certificate Services
 - UTN-USERFirst-Client Authentication and Email
 - TERENA Personal CA

- No existe Documento de Condiciones de Uso (CUSO)
- Se utilizará el CUSO enviado para SCS
 - Las instituciones actualmente dadas de alta en SCP no tendrán que enviar ningún papel nuevo
 - Los dominios habilitados para SCS serán los dominios permitidos para las direcciones de correo de los usuarios en SCP
 - Las direcciones de correo de una persona que no pertenezcan a los dominios habilitados para su institución serán ignoradas

- Condiciones de uso para SCP
 - RedIRIS se reserva el derecho a revocar el certificado unilateralmente
 - Siempre que observe que se incumple la CP/CPS
 - El solicitante declara la veracidad de los datos que van a ser certificados
 - El usuario acepta estas condiciones al solicitar un certificado en el interfaz
 - Al no haber documento de condiciones de uso

- Condiciones de uso para SCP
 - Vista preliminar del interfaz

The screenshot shows the RedIRIS web interface. On the left is a navigation menu with options like 'Sobre RedIRIS', 'La Red', 'Servicios', 'Proyectos', 'Actividades', and 'Difusión'. The main content area is titled 'ISC: Interfaz de Solicitud de Certificados' and 'Perfil de Certificado Personal'. It displays user information for 'Daniel Garcia Franco' from 'rediris.es' and lists email addresses 'daniel.garcia@rediris.es' and 'dani@rediris.es'. There is a dropdown menu for 'Duración del certificado' set to '2 Años' and a section for 'CSR (Certificate Submission Request)' with a large empty text box. At the bottom, there is a checkbox for 'Acepto' and an 'Enviar' button.

- Control de acceso al ISC
 - El control de acceso vía **ePA** (eduPersonAffiliation)
 - Valores aceptados:
 - **student**: Estudiantes
 - **faculty**: PDI
 - **staff**: PAS
 - **employee**: staff + faculty
 - **member**: staff + faculty + student
 - Usuarios con otros valores serán rechazados

- Inicio periodo de Beta finales de Junio
 - Con las mismas instituciones que SCS
 - ¿Deseas participar? mail a **scs-ra@rediris.es**
- Fin periodo de Beta finales Julio
- Inicio funcionamiento SCP Agosto 2010
 - En realidad será Septiembre por eso de las vacaciones ;-)

- Dos preguntas...
- Interesados en certificado para transacciones financieras/económicas
- Interesados en certificados de validación extendida