MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

Servicio de Certificados Personales de RedIRIS

SCP

Daniel García - daniel.garcia@rediris.es

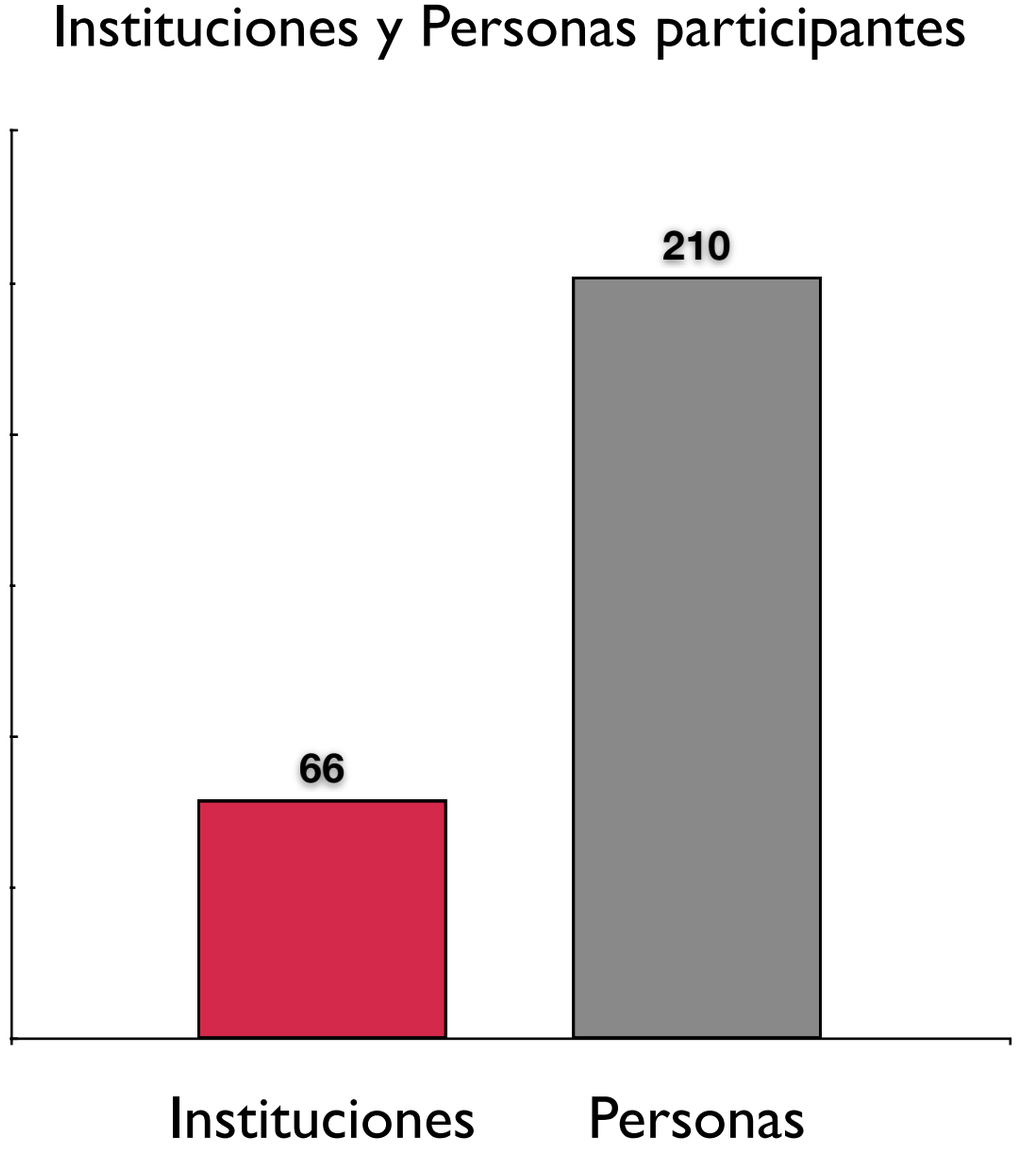
RedIRIS

Córdoba, 15/11/2010

Índice

- Nueva estructura de la web de SCS
  - Una sección por cada perfil de certificación
    - Certificado SSL de servidor.
    - Certificado personal.
    - Certificado de firma de código.
    - Certificado SSL de servidor para e-Ciencia.
    - Certificado personal para e-Ciencia.
  - En cada sección se detalla como solicitarlos

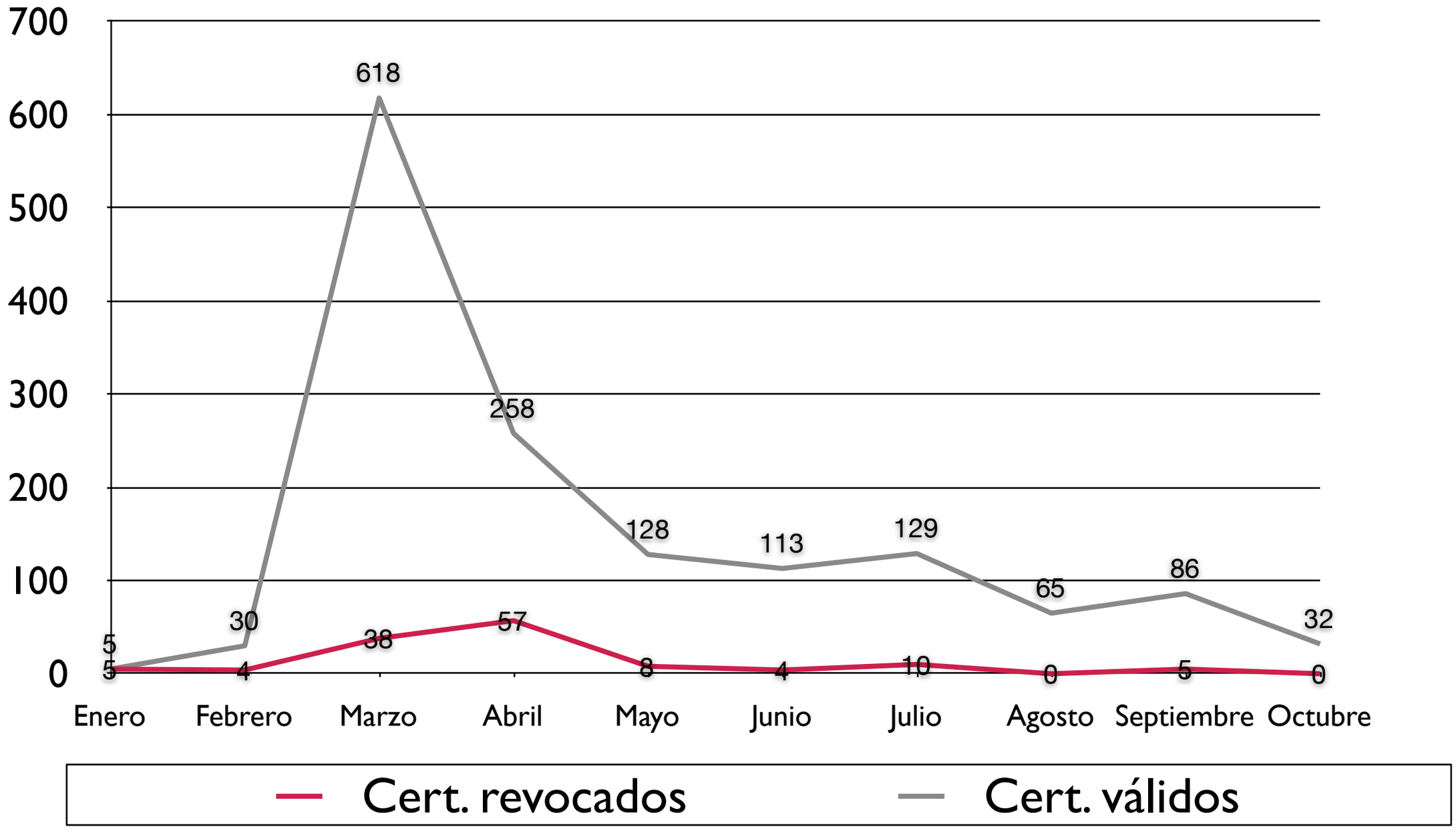
- Instituciones y Personas



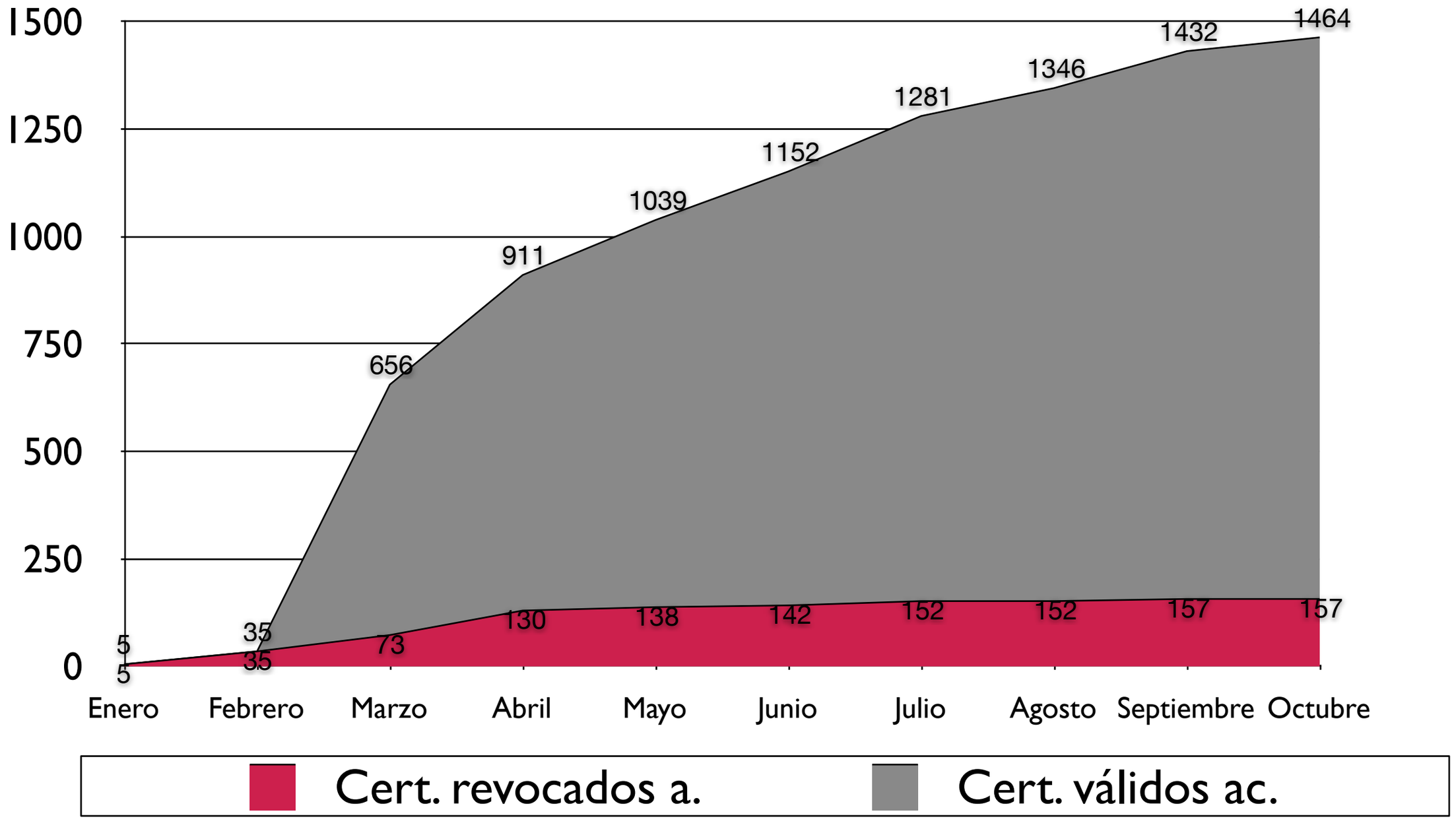
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Certificados validos y revocados



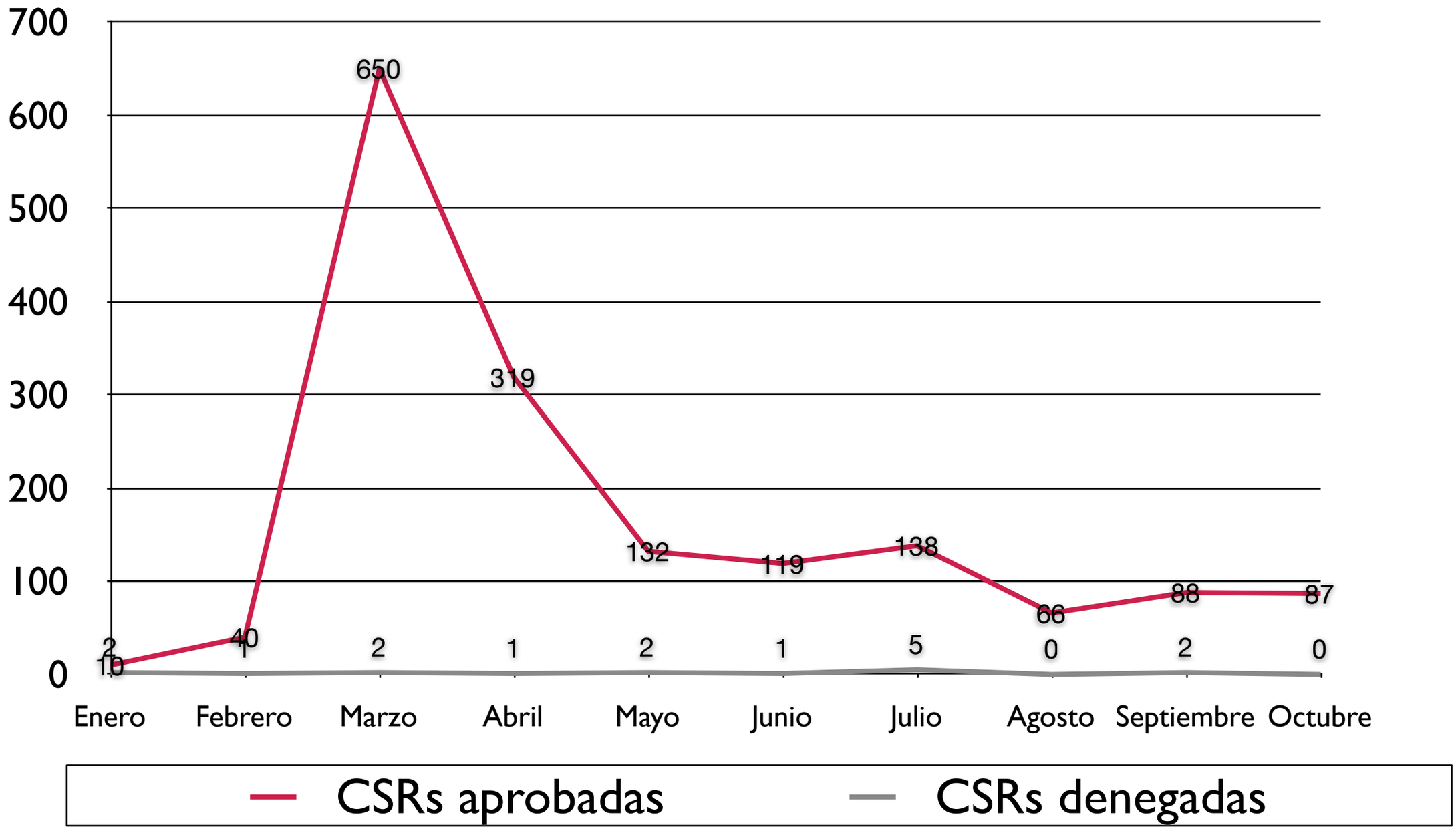
- Certificados validos y revocados acumulado



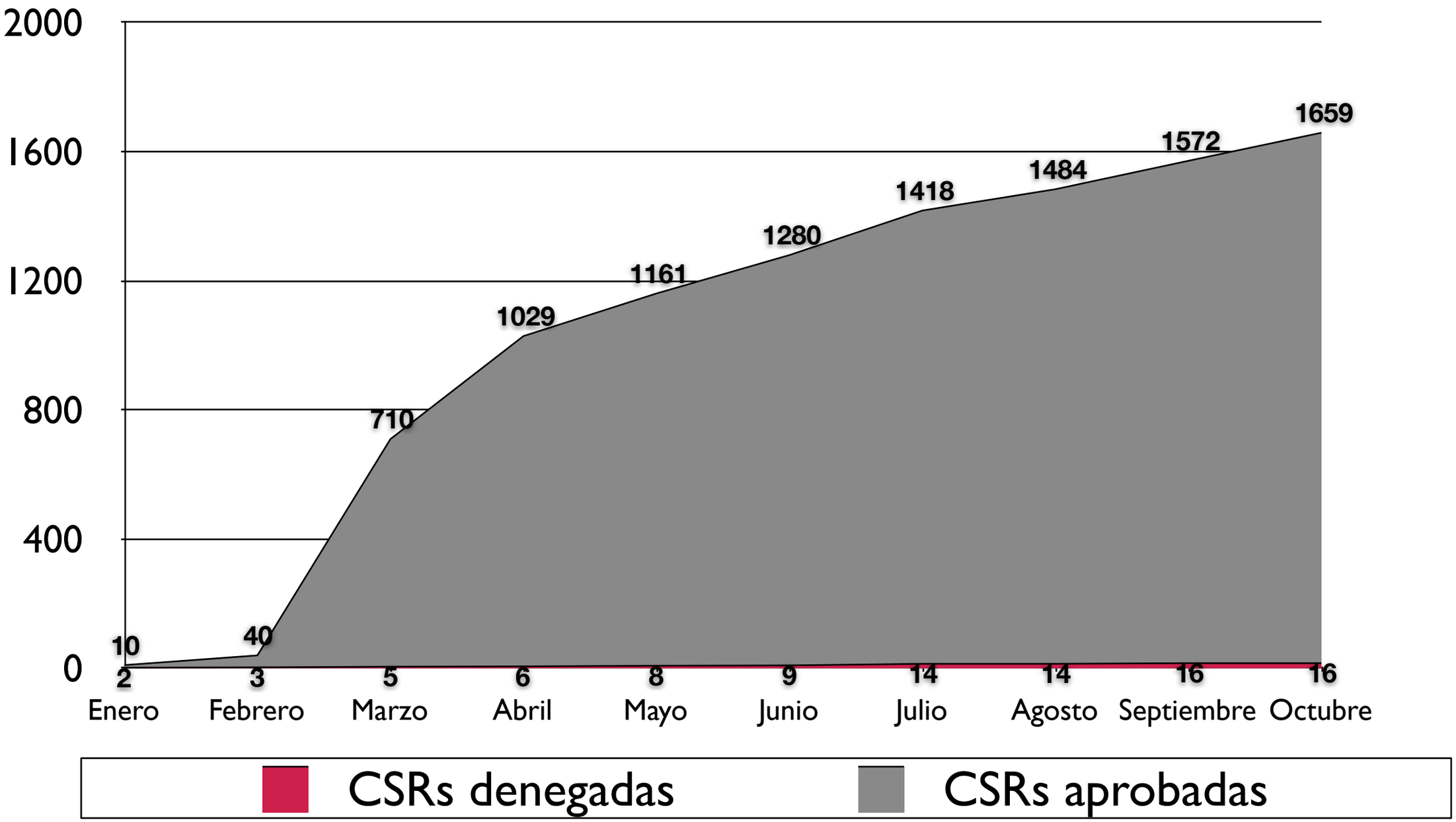
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- CSRs aprobadas y denegadas



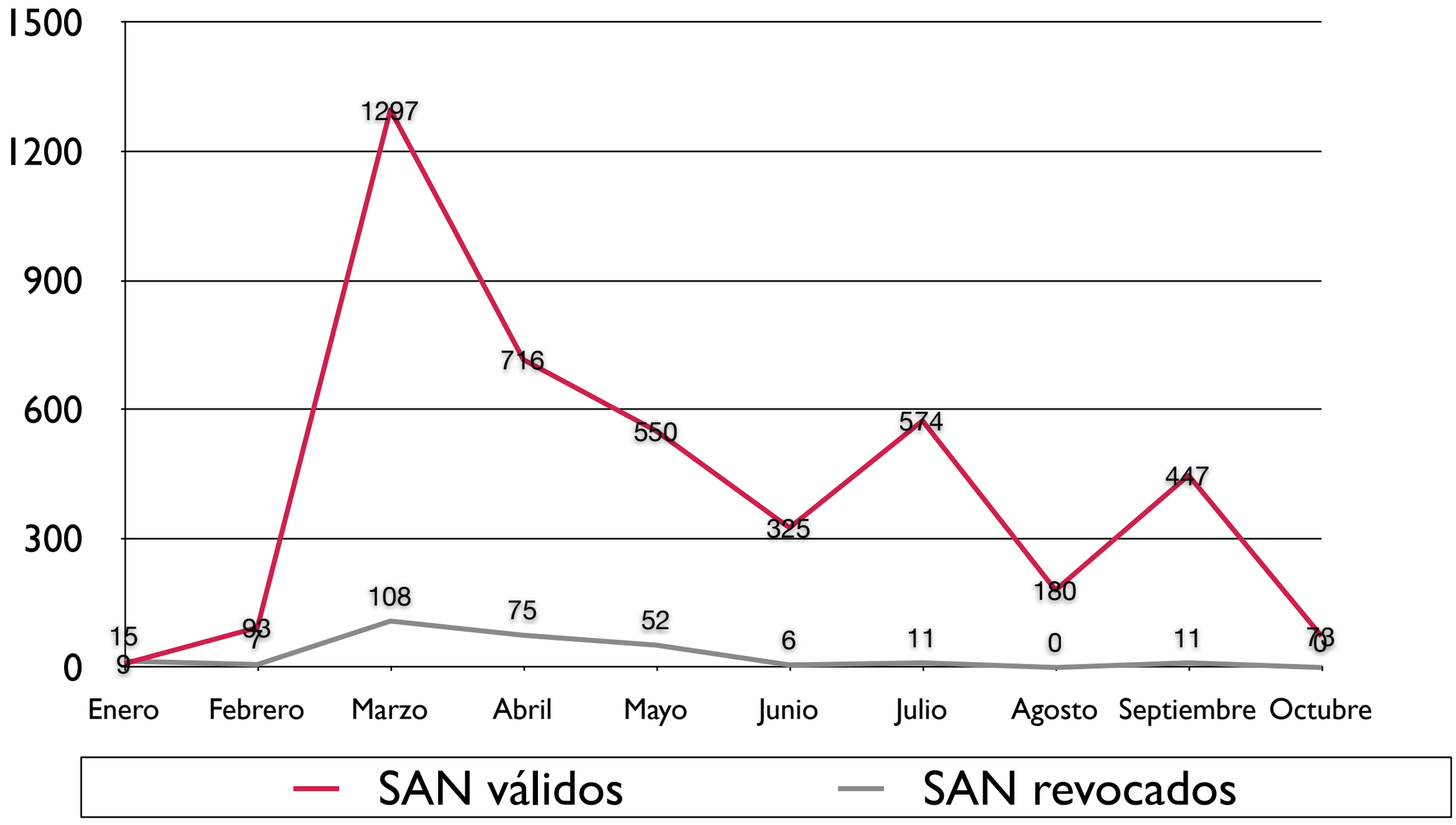
- CSRs aprobadas y denegadas acumulado



MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

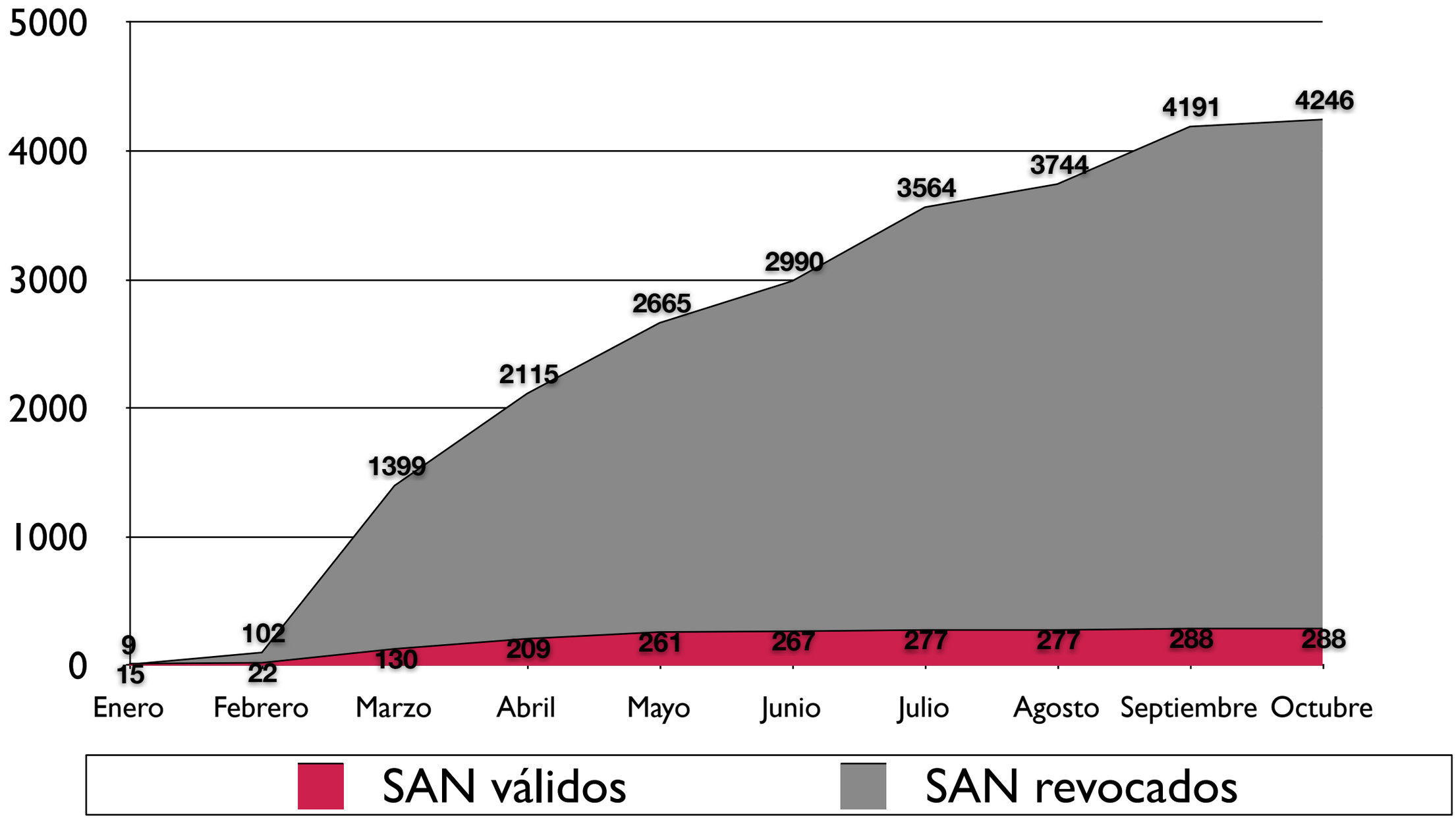
- SubjectAltNames válidos y revocados



MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

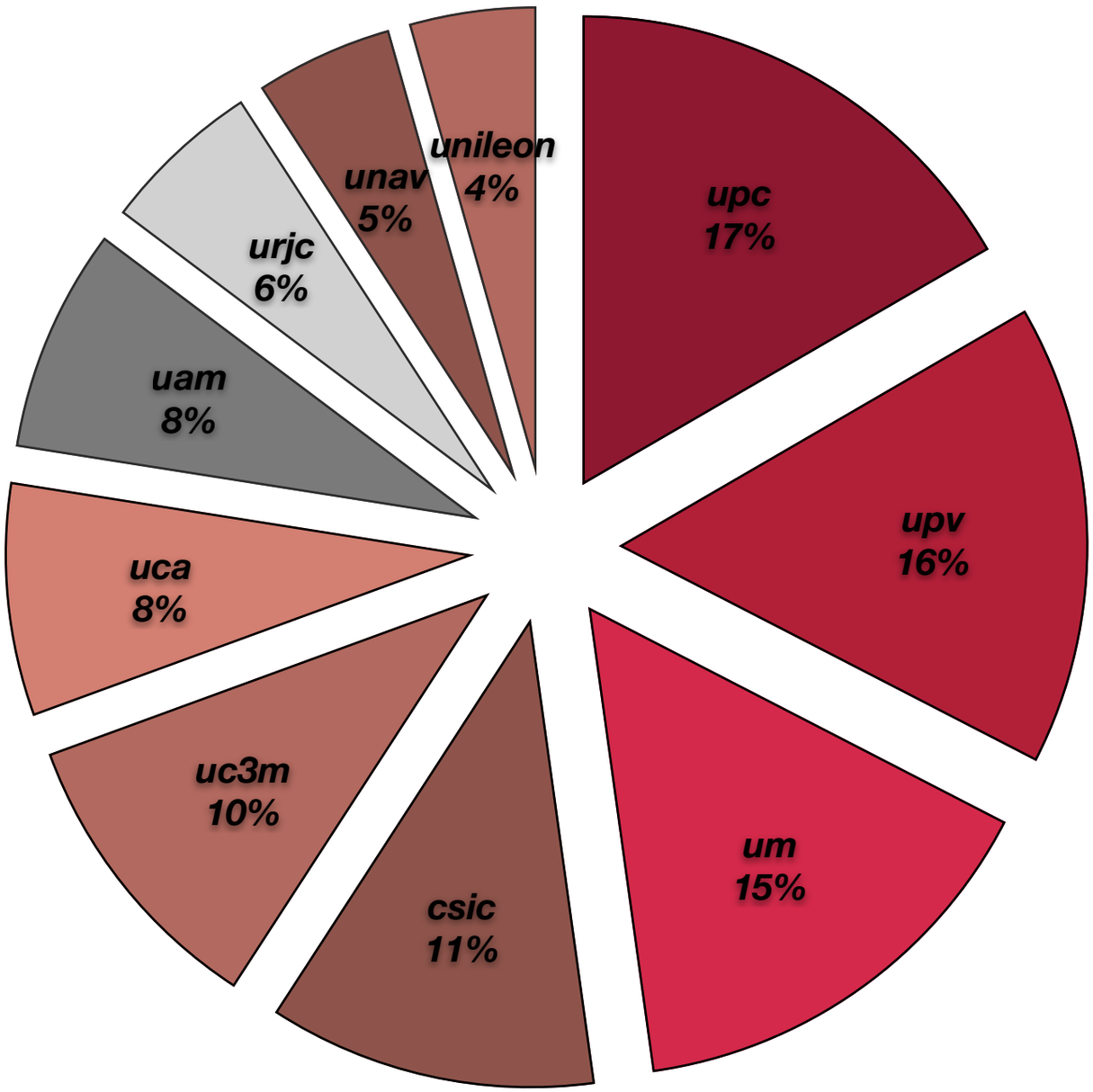
- SubjectAltName válidos y revocados acumulado

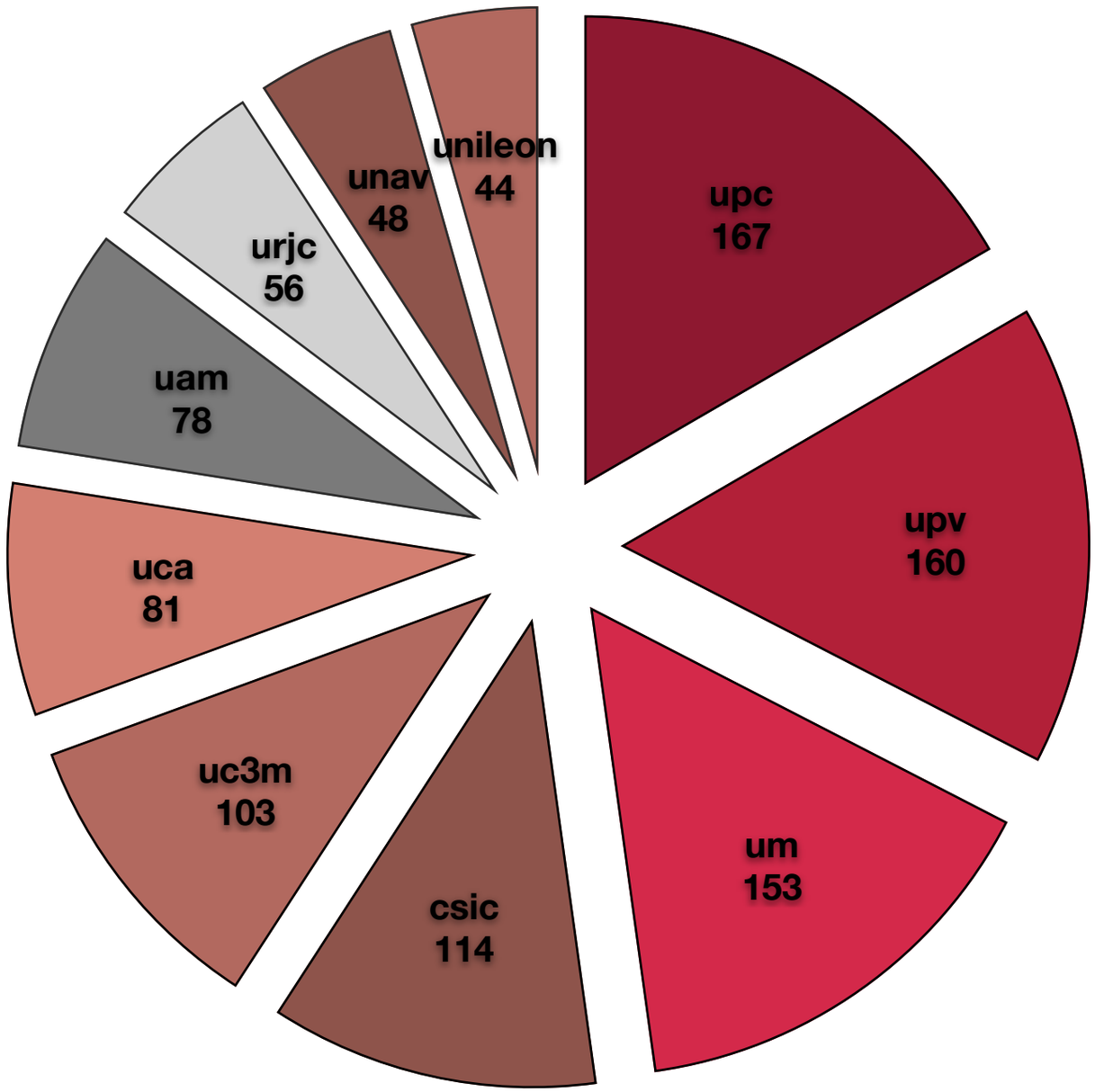


MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Distribución de certificados por instituciones





RedIRIS

- 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 1, 2 y 3 años

- Servicio de Certificados **Personales**

Características técnicas

- Subject DN
  - C=ES
  - O=RedIRIS
  - CN=Nombre Apellido1 Apellido2
  - UN=Identificador OpenID
    - http://yo.rediris.es/soy/uid@rediris.es/
    - http://eu.rediris.es/con/uid@rediris.es/
    - http://jo.rediris.es/soc/uid@rediris.es/
    - http://ni.rediris.es/uid@rediris.es/naiz/

- Servicio de Certificados **Personales**

Características técnicas

- Extensiones
  - **X509v3 Key Usage**:
    - Digital Signature: Firma digital
    - Key Encipherment: Cifrado de secretos compartidos/claves
  - **X509v3 Extended Key Usage**:
    - E-mail Protection: Firma/cifrado correo electrónico usando S/MIME
    - TLS Web Client Authentication: Autenticación de cliente
  - **X509v3 Subject Alternative Name**:
    - emailAddress1
    - ...
    - emailAddress10

- Servicio de Certificados **Personales**

Características técnicas

- Composición del Common Name
  - Se genera a partir de los atributos
    - displayName
    - givenName
    - schacSn1
    - schacSn2
    - surname
    - commonName
    - uid
  - Como se detalla en

www.rediris.es/scs/perfiles/personal/guia.html#subjectdn

- 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)
  - Será el identificador largo OpenID que ofrece RedIRIS a traves del SIR

www.rediris.es/sir/howto-openid.html

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Servicio de Certificados **Personales**

Jerarquía de CAs

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

www.rediris.es/scs/perfiles/personal/guia.html#cas

- **No existe Documento Condiciones Uso**
- 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

- **Requisitos** para el alta de una institución en SCP
  - Identificador del conector SIR
  - Dirección de correo electrónico para el servicio
  - URL explicativa del servicio para los usuarios finales de la institución
- Se **debe** enviar por correo electrónico a:

scs-ra@rediris.es

- **Si no está actualmente dado de alta en SCS**
- Dar de alta a la institución

www.rediris.es/scs/perfiles/ssl/

- Y seguir los pasos detallados anteriormente

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Condiciones del servicio SCP
  - 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
  - RedIRIS se reserva el derecho a revocar el certificado unilateralmente
  - Siempre que observe que se incumple la CP/CPS

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

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

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Control de acceso al ISC
  - Como siempre os recomendamos comprobar las aserciones

◂ Servicios ◂ SCS ◂ Beta

ISC: Interfaz de Solicitud de Certificados

Sus credenciales SIR son correctas para acceder al ISC

Los datos de su aserción son:

- sPUC: urn:mace:terena.org:schac:personalUniqueCode:es:rediris:sir:mbid:{md5}749302e9ede903cf76a809cadb90b7b6
- cn: Daniel Garcia Franco
- mail: daniel.garcia@rediris.es
- uid: dani
- 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:scs:personal:435654
  - urn:mace:dir:entitlement:common-lib-terms

http://www.rediris.es/scs/isc/testassertion.php

Demo del Interfaz SCP

Uso SCP con interfaz web gmail

- Instituciones han migrado/están migrando su correo a Google
- Para usar SCPs en el interfaz web de gmail
  - Existen plugin para Firefox
  - addons.mozilla.org/en-US/firefox/addon/592/
- De momento no hemos encontrado soporte para Google-aps

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Muchas gracias a:
  - Dolores de la Guia (CSIC)
  - Miguel Macias (UPV)
  - Juan C. Sanchez (BSC)
  - Pedro Pérez (UPCOMILLAS)
  - Rafael Calzada y Juanma Canelada (UC3M)
- Por ayudarnos con la beta

- Cuando empieza todo esto... ¡YA!
- Tras los grupos pasamos a producción el interfaz
- Podéis enviar ya los emails con
  - Identificador conector SIR, email contacto y URL.
- En cuanto estén registrados vuestros datos os avisaremos.

- Hasta 30 de Junio de 2011 se pueden solicitar sin costes.
- Los detalles para solicitarlos los pondremos en la web **en breve**

http://www.rediris.es/scs/ev/

- Para los que no puedan/quieran esperar

https://secure.comodo.net/products/!PlaceOrder?ap=TERENASCS&product=337

PREGUNTAS

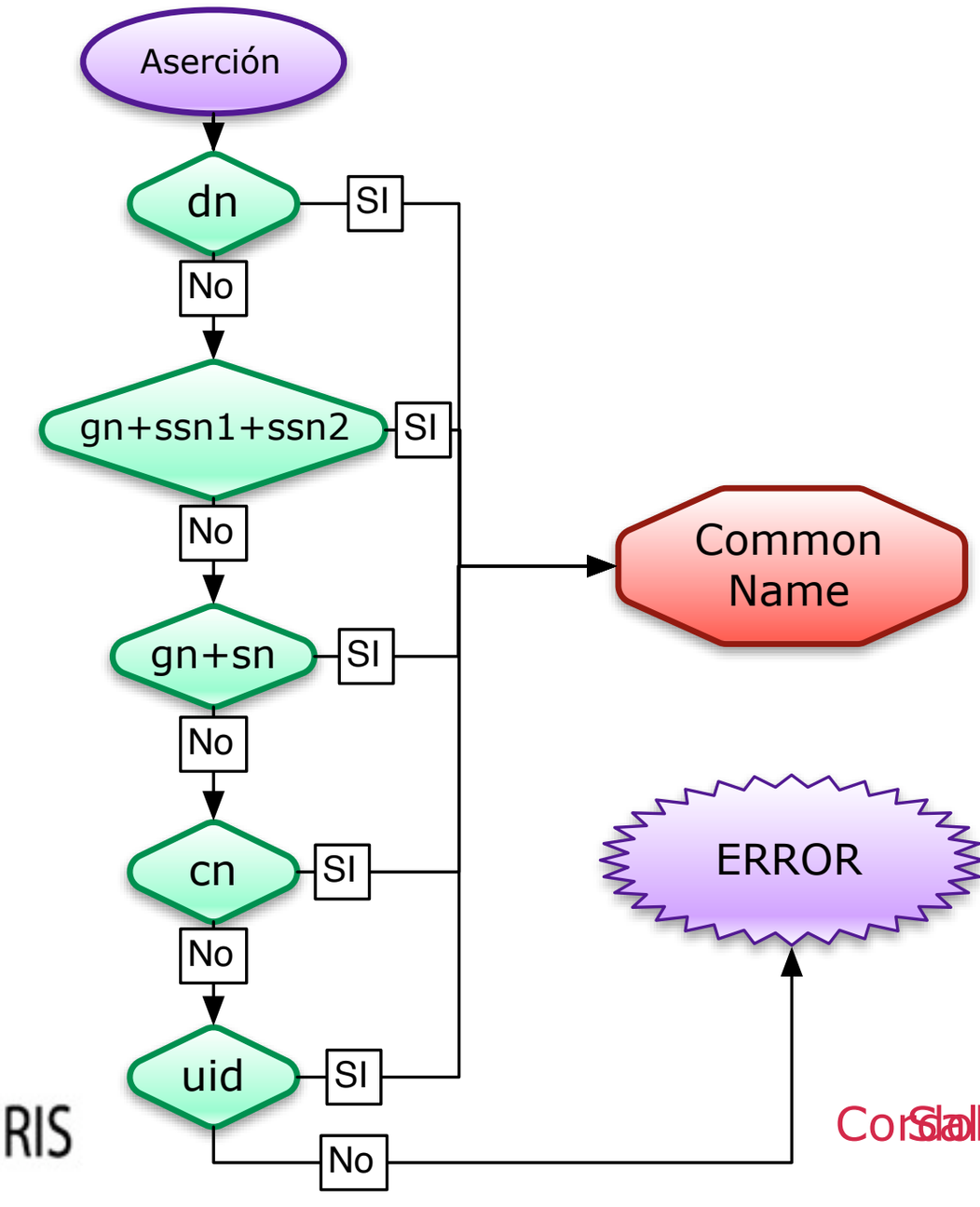
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- 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