



Actualidad TCS

Sesión de Middleware

<https://www.rediris.es/tcs/>

Javi Masa – javier.masa@rediris.es

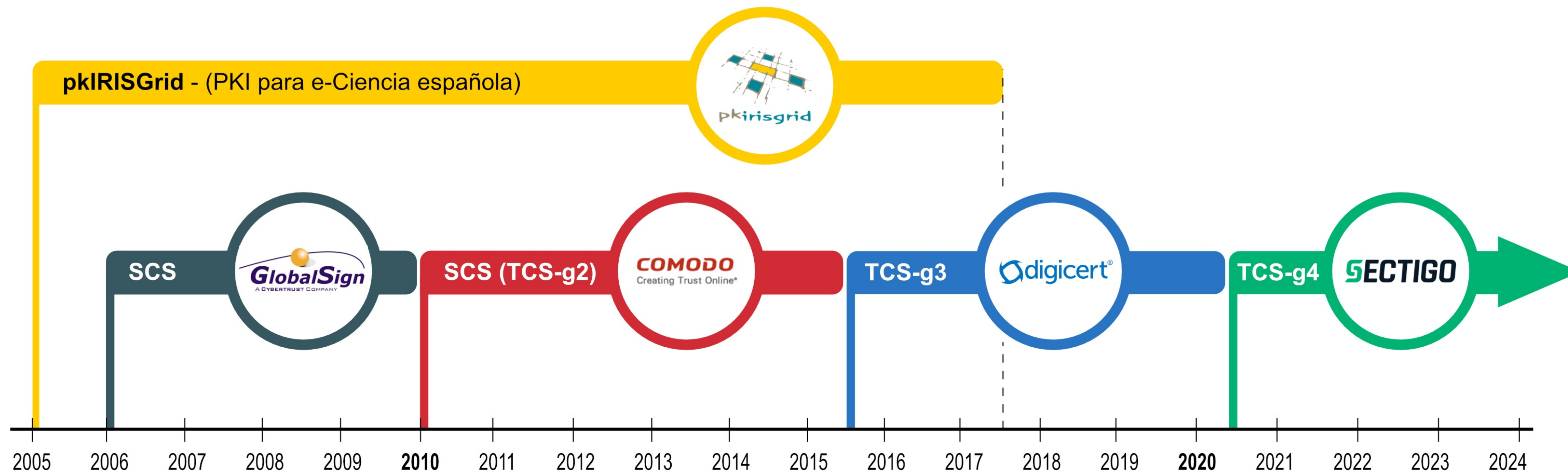
TCS: Certificados Digitales

Índice de contenido

1. Evolución histórica
2. TCS-g4
3. TCS en cifras
4. Incidentes
5. Futuro

TCS: Certificados Digitales

Evolución histórica



TCS: Certificados Digitales

TCS-g4 (generación 4)

- RedIRIS presta el servicio gracias a
 - Acuerdo con GÉANT
 - Contratación, por **10 años**, que ha hecho GÉANT con Sectigo tras un concurso público
- Alta en TCS
 - Requisitos
<https://www.rediris.es/tcs/alta/>
 - CUSO (documento de Condiciones de USO)
<https://www.rediris.es/tcs/doc/cuso/>
- Acceso
 - SCM (Sectigo Certificate Manager) portal
<https://cert-manager.com/customer/rediris>
 - Sectigo SAML portal
<https://cert-manager.com/customer/rediris/idp/clientgeant>

TCS: Certificados Digitales

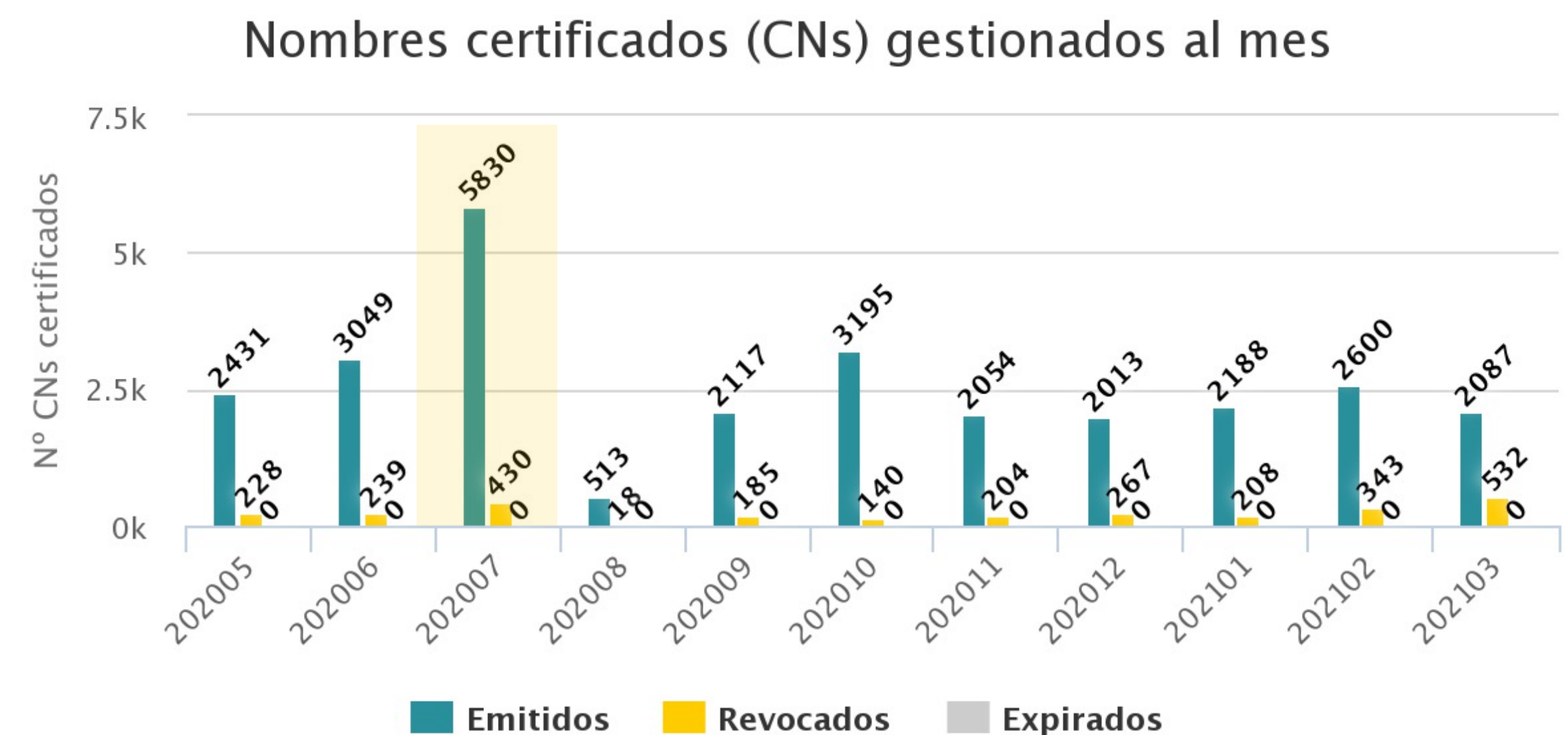
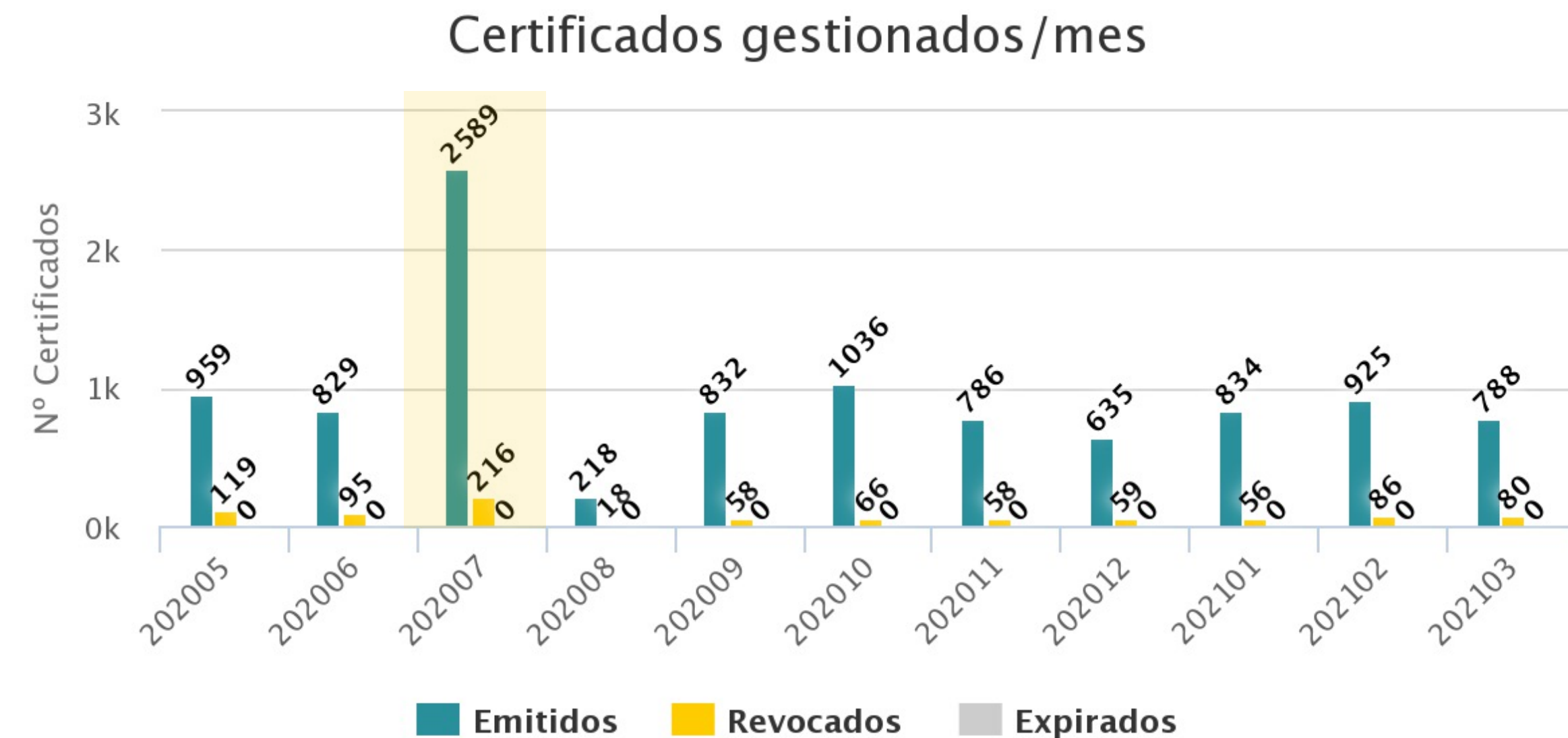
TCS en cifras (desde mayo 2020)

- Participantes**

- 180 instituciones con Sectigo
- Quedan instituciones con DigiCert que deberían solicitar el alta con Sectigo
- 490 administradores RAO en SCM
- 175 administradores DRAO en SCM
- 648 administradores entre Sectigo y DigiCert en la lista TCS-USER

- Certificados**

- Más de 10.000 certificados emitidos
- Más de 28.000 nombres certificados
- Quedan certificados válidos con DigiCert



TCS: Certificados Digitales

Incidentes: revocaciones masivas

| Certs. afectados | CAs | Fecha aviso | Fecha revocación | Descripción |
|------------------|-------------------|---------------------------|-------------------------|---|
| 2.492 | DigiCert | 08/07/2020 (miércoles) | 11/07/2020 (sábado) | Certs EV por problemas en una auditoría (TERENA SSL High Assurance CA 3) |
| 39 | DigiCert, Sectigo | 16/10/2020 (viernes) | 20/10/2020 (martes) | Problemas menores no relacionados con la seguridad. <ul style="list-style-type: none">• "Locality spelled incorrectly, should be Logroño", y tenía "Logron"• "stateOrProvinceName should be Santa Cruz de Tenerife as per ISO/ Wiki", y tenía "Tenerife".• "City is incorrect", por tener el valor "Valladolid1". |
| 30 | Sectigo | 09/11/2020 (lunes) | 13/11/2020 (viernes) | Problemas menores no relacionados con la seguridad. <ul style="list-style-type: none">• "State or Province Name is not valid for country",<ul style="list-style-type: none">• Aparecía "Guip??Zcoa" en vez de "Gipuzkoa"• Aparecía "Vizcaya" en lugar de "Bizkaia" |

TCS: Certificados Digitales

Futuro de la gestión de los certificados

- Decisiones del CA/Browser Forum
 - Reducción de la validez de los certificados de servidor a 1 año, y posible reducción a menos tiempo en el futuro
 - Nos obliga a solicitar e instalar todos los certificados cada año
 - Revocaciones masivas forzadas por motivos no relacionados con la seguridad
 - Nos obliga a solicitar e instalar muchísimos certificados en pocos días
- Uso de ACME (*Automatic Certificate Management Environment*)
 - Más de 500 certificados solicitados con ACME
 - TCS Webinar: ACME - <https://wiki.geant.org/display/TCSNT/TCS+Training/>
 - SCM doc - https://www.rediris.es/tcs/doc/scm/#scm_cert_ssl_acme

tcs@rediris.es

