
# Coloriuris Prestador de Servicios de Confianza

## Políticas y declaración de prácticas de la Autoridad de Sellado de Tiempo

| | |
|---|---|
| **Autor** | Coloriuris S.L. |
| **Versión** | 1.2 |
| **Estado del documento** | Aprobado |
| **Fecha de emisión** | 09-04-2018 |
| **OID (Object Identifier)** | 1.3.6.1.4.1.37799.20.5.0.1.2 |
| **Ubicación del documento** | https://cipsc.coloriuris.net/politicas/ |

# CONTENIDO

# Histórico de cambios del documento

| HISTÓRICO DEL DOCUMENTO | | | |
|---|---|---|---|
| Versión | Fecha | Descripción | Autor |
| 1.0 | 21/06/2017 | Políticas y declaración de prácticas de la Autoridad de Sellado de Tiempo de Coloriuris Prestador de Servicios de Confianza | Coloriuris SL |
| 1.0.1 | 02/07/2017 | • Corrección del perfil de certificado<br>• Actualización de los datos del Certificado de TSU<br>• Añadido anexo de Revisión de las Políticas | Coloriuris SL |
| 1.1 | 03/01/2018 | • Añadida nuevos CA v3.1 y Emisor v3.1 | Coloriuris SL |
| 1.2 | 09/04/2018 | • Corrección de términos<br>• Corrección de errores materiales<br>• Corrección del Certificado de Emisión de Sellos de la TSA v3.1 | Coloriuris SL |

# 1.- Declaración básica del servicio

La Declaración básica del servicio de sellado de tiempo de CIPSC (TSACI) recoge las condiciones y aspectos fundamentales de uso de los servicios de sellado de tiempo que, junto a otras condiciones y aspectos más específicos, se recogen en este documento. El contenido de esta declaración básica se corresponde con el del documento denominado *TSA Disclosure Statement* por el estándar ETSI EN 319 421, cuyas funciones el presente apartado cumple a todos los efectos.

Este documento se basa y amplía el documento de *Políticas y declaración de prácticas generales de CIPSC* con OID 1.3.6.1.4.1.37799.0.3.1.3.0, en adelante **DPPG**.

En consecuencia, mediante la presente declaración básica, TSACI afirma que:

**Titularidad**

La Autoridad de Sellado de Tiempo de Coloriuris (TSACI) es un servicio del Coloriuris S.L., empresa cuyos datos de contacto se encuentran en el apartado 1.6.4 del "DPPG".

**Disponibilidad del servicio**

El servicio de certificación de TSACI está disponible de forma ininterrumpida todos los días del año salvo la tramitación presencial de solicitudes, que únicamente estará disponible en el horario de oficina que establezca cada una de las Autoridades de Registro.

Podrán programarse interrupciones de los servicios cuando sea estrictamente necesario por razones técnicas, en cuyo caso estas deberán anunciarse con una antelación de al menos 24 horas en el directorio indicado en el epígrafe 1.6.3 del "DPPG".

**Publicación de la Política**

Todos y cada uno de los sellos de tiempo emitidos por TSACI contienen el identificador (OID) de este documento de Políticas y declaración de prácticas, el cual se incluye en la portada de este documento.

**Mecanismos criptográficos**

Los algoritmos criptográficos y la longitud de las claves utilizadas en la emisión de los sellos por TSACI cumplen con el estándar ETSI EN 319 422 *Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles* y son las siguientes:

- Para el cálculo del hash de las peticiones de sellos de tiempo se admiten los siguientes algoritmos: SHA-256.

- Para el cálculo del hash de los sellos de tiempo emitidos se utiliza SHA-256.
- La firma de los sellos de tiempo emitidos se realiza calculando el hash mediante SHA-256 y cifrándolo con algoritmos RSA, utilizando para ello una clave cuya longitud de al menos 2048 bits.

**Validez de los sellos de tiempo**

TSACI no establece otras limitaciones a la confianza que merecen sus servicios de sellado de tiempo que las que son inherentes a las tecnologías utilizadas. Si se determinara que los algoritmos criptográficos o la longitud de claves utilizados han dejado de aportar un nivel adecuado de seguridad, TSACI publicará inmediatamente dicha información en su página web.

**Precisión temporal**

TSACI asegura que el momento fijado en los sellos está dentro de los márgenes de error establecidos en el apartado 2.3 de este documento, con relación al tiempo establecido por las fuentes de tiempo UTC de confianza definidas en el apartado 3.4 y garantiza que no emitirá sellos de tiempo con una precisión menor que la antedicha.

**Aplicabilidad**

TSACI considera que los usos más apropiados de los sellos de tiempo que emite son los relacionados con la prueba del momento en que ocurren hechos que tengan o puedan tener efectos jurídicos como son, por ejemplo, los descritos en el apartado 2.5 del presente documento. Los sellos emitidos por TSACI no pueden utilizarse en aplicaciones en las que del control del tiempo dependan actuaciones automatizadas que, en caso de fallo o error, puedan producir daños materiales o personales.

**Obligaciones**

Las obligaciones de las partes usuarias están descritas en los apartados 2.6 del presente documento y en el apartado 2.3.3.

**Registro de las operaciones**

TSACI registra sus operaciones y conserva esta información en adecuadas condiciones de seguridad, según lo previsto en los apartados 3.3.4 del “DPPG”.

**Normativa**

La prestación del servicio de sellado de tiempo por parte de TSACI se realiza de acuerdo con la legislación española y europea aplicable a la materia, con las presentes Políticas y declaración de prácticas y con la normativa interna de Coloriuris.

**Responsabilidad**

Las responsabilidades de TSACI y las limitaciones establecidas sobre la misma se describen en el apartado 2.4 del "DPPG".

**Reclamaciones**

Todas las reclamaciones de usuarios y terceros sobre la prestación de servicios de sellado de tiempo por TSACI deberán serle comunicadas según lo establecido en el apartado 2.8.1 del "DPPG". En el caso de que no se llegara a un acuerdo entre las partes estas se someterán a los juzgados y tribunales especificados en el apartado 2.8.2 del "DPPG", con renuncia a cualquier otro fuero que pudiera corresponderles.

**Garantía y auditorías**

TSACI garantiza que la prestación de los servicios de sellado de tiempo es conforme con lo establecido en estas Políticas y declaración de prácticas. De acuerdo con las mismas Coloriuris lleva a cabo auditorías periódicas del funcionamiento de la Autoridad de sellado de tiempo.

**Tarifas**

TSACI podrá pedir una contraprestación económica por la emisión de sus sellos de tiempo, de acuerdo con las tarifas que en cada momento se encuentren publicadas en su web.

# 2.- Política para la prestación del servicio

## 2.1.- Introducción

La presente Política regula la generación y emisión de sellos de tiempo por TSACI, de acuerdo con la especificación técnica ETSI EN 319 421. La clave privada utilizada y la unidad de sellado de tiempo (TSU) cumplen con las especificaciones técnicas de la normas: ETSI EN 319 422, *Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles*, RFC 3161, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*.

TSACI emplea una clave privada específica para la firma de los sellos de tiempo. Cada sello emitido contiene la identificación de la Políticas y declaración de prácticas que se le aplica.

## 2.2.- Versiones

Esta versión de las Políticas y declaración de prácticas de TSACI sustituye a todos los efectos y desde el momento de su publicación a las Políticas y prácticas de sellado de tiempo de la Autoridad de Sellado de Tiempo de Coloriuris S.L., de fecha 13-10-2015 y con OID: 1.3.6.1.4.1.37799.0.3.1.2.0.

## 2.3.- Precisión

Los Sellos de Tiempo (TST) se emiten con una precisión ±1 segundo UTC.

## 2.4.- Comunidad de usuarios

La comunidad para la generación, emisión y uso de estos certificados son la Autoridad de sellado de tiempo (TSACI), según se describe en el "DPPG" en sus apartados 2.1.2.1 y 2.1.2.3 y las partes usuarias, según se describen en el apartado 2.2.2 de dicho "DPPG".

TSACI es responsable de la emisión y gestión de los sellos de tiempo. Las partes usuarias son aquellas personas que confían en los sellos de tiempo emitidos por TSACI.

Todos ellos estarán sujeto a lo dispuesto en la presente Política.

## 2.5.- Usos de los sellos de tiempo

Los sellos de tiempo emitidos de acuerdo con esta política están diseñados para dar prueba del momento de los hechos y actos, con la finalidad principal de que puedan ser utilizados en

contextos jurídicos. Por ejemplo, son usos típicos de los sellos de TSACI los siguientes:

- Dotar de certeza temporal a las firmas electrónicas
- Preservar firmas electrónicas en archivos de larga duración
- Probar que determinados datos existían antes de un momento dado
- Acreditar el momento en que se realiza un acto y/o proceso jurídico, incluida la entrega electrónica certificada.
- Y, en general, su utilización en archivos de documentos electrónicos, bases de datos, sistemas de registro y logs.

Los sellos de tiempo de TSACI no pueden ser utilizados en aplicaciones críticas en las que un fallo o error del servicio pudiera suponer cualquier tipo de daño material o personal.

## 2.6.- Obligaciones

Además de las obligaciones establecidas por la ley y de las enumeradas en el apartado 2.3 de este documento, se establecen las siguientes obligaciones específicas para la prestación de los servicios de sellado de tiempo.

TSACI

1) Mantener sincronizado el reloj de la TSU con la precisión declarada con respecto al tiempo UTC.
2) Proporcionar acceso ininterrumpido a los servicios de sellado de tiempo excepto en caso de interrupciones programadas, pérdidas de la sincronización temporal o incidencias graves.

Partes usuarias

1) Emplear medios adecuados para la solicitud y obtención de sellos de tiempo.
2) Utilizar los sellos de tiempo únicamente para los usos y con los fines permitidos en la presente Política.
3) Verificar la validez de los sellos de tiempo.
4) No confiar en los sellos de tiempo para usos distintos de los permitidos en esta Política.
5) Notificar cualquier hecho o situación anómala relativa al servicio de sellado, y/o a los sellos de tiempo emitidos, y que pueda ser considerado como causa de revocación de los mismos.

## 2.7.- Registro de información referente a la operación de los servicios de sellado de tiempo

TSACI mantiene registros de toda la información relevante referente a sus operaciones, según lo establecido en los apartados 3.3.4 del "DPPG". Además de los previstos en dicho apartado, la AC mantiene registros de los siguientes eventos:

- Peticiones para la emisión de sello de tiempo
- Emisión de sellos de tiempo

# 3.- Declaración de prácticas

## 3.1.- Acceso al servicio

Los usuarios pueden solicitar los sellos de tiempo de la forma prevista en los protocolos TSP *Time-Stamp Protocol* (RFC 3161).

La dirección de acceso al servicio es https://cipsc.coloriuris.net/tsa/

## 3.2.- Disponibilidad del servicio

El servicio de sellado de tiempo de TSACI está disponible de forma ininterrumpida.

Podrán programarse interrupciones de los servicios cuando sea estrictamente necesario por razones técnicas, en cuyo caso estas deberán anunciarse con una antelación de al menos 24 horas en el directorio indicado en el epígrafe 1.6.3 del "DPPG".

Cuando la interrupción se deba a causas de fuerza mayor o incidencias graves, CIPSC actuará con la máxima diligencia para conseguir la puesta en marcha de los servicios, así como para minimizar los posibles perjuicios que se hayan causado a los firmantes, creadores de sellos y/o partes usuarias.

## 3.3.- Ciclo de vida de las claves

La generación y protección de las claves privadas en uso por las TSU de TSACI se lleva a cabo siguiendo las recomendaciones de la norma ETSI EN 319 421 en sus puntos 7.6.2 y 7.6.3 en módulos criptográficos con las calificaciones indicadas en el epígrafe 3.4.2.1 de esta declaración.

Las claves públicas asociadas a las claves privadas y sus respectivos certificados se encontrarán disponibles en los repositorios indicados en el epígrafe 1.6.3 del "DPPG".

## 3.4.- Sello de tiempo

TSACI adopta las medidas técnicas precisas para garantizar que sus sellos de tiempo son

seguros e incluyen la fecha y hora correctas. Los sellos se emiten utilizando un dispositivo criptográfico (TSU).

Los sellos de tiempo generados son conformes con los estándares referenciados en el anexo de este documento, y su formato y contenido es el especificado en el RFC 3161 *Time-stamp Protocol (TSP)*. Todos los sellos incluyen, como mínimo el siguiente contenido:

- El identificador de la Política aplicable, cuyo valor se indica en el apartado 1.5.
- El resumen (*hash*) del conjunto de datos cuya existencia en ese momento se acredita.
- Un número de serie único que identifica el sello de tiempo.
- El tiempo, expresado en el formato Tiempo Universal Coordinado (Hora Zulu).
- La firma electrónica del sello, generada por la TSU.

Como anexo al sello se entrega a los usuarios el certificado electrónico que respalda la firma incorporada al sello. En el apartado 3.6 se describen los certificados utilizados por CIPSC con este fin, los cuales identifican plenamente a la TSU y a CIPSC.

TSACI audita la exactitud de la fuente de tiempo y no emitirá sellos de tiempo si su precisión se encuentra fuera del margen establecido.

## 3.5.- Sincronización del reloj con UTC

TSACI proporciona el instante de tiempo con la precisión declarada en el apartado 2.3 de la Política, tomando como referencia una fuente segura de tiempo de entre las siguientes:

- Fuente de tiempo stratum 1 a través del protocolo NTP. Esta fuente de tiempo provee precisión al nivel del microsegundo utilizando sincronización con el sistema de satélites Navstar.
- Real Instituto y Observatorio de la Armada (ROA), el cual según lo dispuesto en el R.D. 1308/1992, de 23 de octubre, es el encargado del mantenimiento y difusión oficial de la escala "Tiempo Universal Coordinado" (UTC-ROA), que constituye la base de la hora legal en todo el territorio nacional. Esta señal se recibe mediante el protocolo NTP a través de Internet.
- Del reloj atómico de Braunschweig, Alemania, (Physikalisch Technische Bundesanstalt), que representa la hora oficial dentro del Eurosistema. Es codificada y transmitida vía radio.

El reloj utilizado por la TSU se recalibra periódicamente y de forma automática respecto a

la fuente de tiempo segura. También es capaz de detectar las desviaciones respecto a la precisión establecida y activar una nueva calibración si ésta es necesaria.

El reloj y la TSU están permanentemente ubicadas en un entorno físico seguro y están protegidas frente a accesos no autorizados, tanto físicos como remotos.

Los eventos relativos a la sincronización y modificación de la hora del reloj respecto a la fuente de tiempo segura se registran al objeto de detectar las desviaciones producidas, sea de forma accidental o intencionada.

## 3.6.- Certificado raíz y sellos de TSACI

### 3.6.1.- Certificados raíz

El origen de la cadena de confianza de la TSACI v3.0 es un certificado autofirmado emitido por CIPSC, con una longitud de clave de 4096 Bits y un periodo de validez de 20 años.

Su contenido es el siguiente:

| | |
|---|---|
| **Emisor (Issuer)** | |
| **E** | cipsc@coloriuris.net |
| **CN** | CIPSC - Autoridad de Sellado de Tiempo v3 |
| **organizationIdentifier (2.5.4.97)** | VATES-B99091696 |
| **OU** | Prestador de servicios de Confianza |
| **O** | Coloriuris S.L. |
| **L** | Zaragoza |
| **C** | ES |
| **Asunto** | |
| **E** | cipsc@coloriuris.net |
| **CN** | CIPSC - Autoridad de Sellado de Tiempo v3 |
| **organizationIdentifier (2.5.4.97)** | VATES-B99091696 |
| **OU** | Prestador de servicios de Confianza |
| **O** | Coloriuris S.L. |

| | |
|---|---|
| **L** | Zaragoza |
| **C** | ES |
| **Clave pública** | RSA (4096 Bits) |
| **AIA Acceso Información del Emisor** | acceso id-ad-http https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.crt<br>aceso id-ad-ocsp https://ocsp.coloriuris.net |
| **Punto de distribución CRL** | https://cipsc.coloriuris.net/crl/tsa/tsa-v3.crl |
| **Bases del certificado** | [1]Directiva de certificados:<br>Identificador de directiva=2.5.29.32.0<br>[1,1]Información de certificador de directiva:<br>Id. de certificador de directiva=CPS<br>Certificador:<br>https://cipsc.coloriuris.net/politicas/ |
| **Uso de la clave** | firma de certificados, firma CRL sin conexión, firma de lista de revocación de certificados (CRL) |
| **1.3.6.1.5.5.7.1.3 -IETF / 0.4.0.1862.1.1-ETSI** | QCStatements |
| **QCSyntax-v2** | id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2) |

El origen de la cadena de confianza de la TSACI v3.1 es un certificado autofirmado emitido por CIPSC, con una longitud de clave de 4096 Bits y un periodo de validez de 20 años.

Su contenido es el siguiente:

| | |
|---|---|
| **Emisor (Issuer)** | |
| **E** | cipsc@coloriuris.net |
| **CN** | CIPSC - Autoridad de Sellado de Tiempo v3.1 |
| **organizationIdentifier (2.5.4.97)** | VATES-B99091696 |
| **OU** | Prestador de servicios de Confianza |
| **O** | Coloriuris S.L. |
| **L** | Zaragoza |
| **C** | ES |
| **Asunto** | |

| | |
|---|---|
| **E** | cipsc@coloriuris.net |
| **CN** | CIPSC - Autoridad de Sellado de Tiempo v3.1 |
| **organizationIdentifier (2.5.4.97)** | VATES-B99091696 |
| **OU** | Prestador de servicios de Confianza |
| **O** | Coloriuris S.L. |
| **L** | Zaragoza |
| **C** | ES |
| **Clave pública** | RSA (4096 Bits) |
| **AIA Acceso Información del Emisor** | acceso id-ad-http https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.1.crt<br>aceso id-ad-ocsp https://ocspv3.coloriuris.net |
| **Punto de distribución CRL** | http://cipsc.coloriuris.net/crl/tsa/tsa-v3.1.crl |
| **Bases del certificado** | [1]Directiva de certificados:<br>Identificador de directiva=2.5.29.32.0<br>[1,1]Información de certificador de directiva:<br>Id. de certificador de directiva=CPS<br>Certificador:<br>https://cipsc.coloriuris.net/politicas/ |
| **Uso de la clave** | firma de certificados, firma CRL sin conexión, firma de lista de revocación de certificados (CRL) |
| **1.3.6.1.5.5.7.1.3 -IETF / 0.4.0.1862.1.1-ETSI** | QCStatements |
| **QCSyntax-v2** | id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2) |

## 3.6.2.- Certificados para la emisión de sellos electrónicos cualificados de tiempo

TSACI dispondrá de dos certificados para la emisión de los sellos electrónicos cualificados de tiempo, emitidos por la propia TSACI de CIPSC utilizando su certificado raíz, y cuyo periodo de validez será de 10 años.

El perfil de estos certificados estarán basados en claves de 2048 para la emisión de sellos de tiempo e identificados por el OID 1.3.6.1.4.1.37799.20.5.1

**Perfil del certificado v3.0**

| | |
|---|---|
| **Emisor (Issuer)** | |
| **E** | cipsc@coloriuris.net |
| **CN** | CIPSC - Raíz de la Autoridad de Sellado de Tiempo v3 |
| **organizationIdentifier (2.5.4.97)** | VATES-B99091696 |
| **OU** | Prestador de servicios de Confianza |
| **O** | Coloriuris S.L. |
| **L** | Zaragoza |
| **C** | ES |
| **Asunto** | |
| **CN** | CIPSC - v3 – Emisor de sellos de tiempo de 2048 |
| **organizationIdentifier (2.5.4.97)** | VATES-B99091696 |
| **O** | Coloriuris S.L. |
| **L** | Zaragoza |
| **C** | ES |
| **Clave pública** | RSA (2048 Bits) |
| **AIA Acceso Información del Emisor** | acceso id-ad-http https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.crt<br>aceso id-ad-ocsp https://ocsp.coloriuris.net |
| **Punto de distribución CRL** | http://cipsc.coloriuris.net/crl/tsa/tsa-v3.crl |
| **Bases del certificado** | [1]Directiva de certificados:<br>Identificador de directiva=1.3.6.1.4.1.37799.20.5.1 |

| | |
|---|---|
| | [1,1]Información de certificador de directiva:<br>Id. de certificador de directiva=Aviso de usuario<br>Certificador:<br>Texto de aviso=Certificado cualificado de emisión de sellos de tiempo electrónicos<br>[1,2]Información de certificador de directiva:<br>Id. de certificador de directiva=CPS<br>Certificador:<br>https://cipsc.coloriuris.net/politicas/ |
| **Uso de la clave** | Firma digital, No repudio |
| **Uso extendido de la clave** | Time Stamping (Marca de Tiempo) |
| **1.3.6.1.5.5.7.1.3 -IETF / 0.4.0.1862.1.1-ETSI** | QCStatements |
| **QCSyntax-v2** | id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2) |
| ***EuQCompliance*** | Id-etsi-tsts-EuQCompliance (0.4.0.19422.1.1) |
| **Uso de la clave** | Sello de tiempo, no repudio |

## Perfil del certificado v3.1

| | |
|---|---|
| **Emisor (Issuer)** | |
| **E** | cipsc@coloriuris.net |
| **CN** | CIPSC - Raíz de la Autoridad de Sellado de Tiempo v3.1 |
| **organizationIdentifier (2.5.4.97)** | VATES-B99091696 |
| **OU** | Prestador de servicios de Confianza |
| **O** | Coloriuris S.L. |
| **L** | Zaragoza |
| **C** | ES |
| **Asunto** | |
| **CN** | CIPSC - v3.1 - Emisor de sellos electronicos cualificados de tiempo de 2048 |
| **organizationIdentifier (2.5.4.97)** | VATES-B99091696 |
| **O** | Coloriuris S.L. |
| **L** | Zaragoza |
| **C** | ES |

| | |
|---|---|
| **Clave pública** | RSA (2048 Bits) |
| **AIA Acceso Información del Emisor** | acceso id-ad-http https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.1.crt<br>aceso id-ad-ocsp https://ocspv3.coloriuris.net |
| **Punto de distribución CRL** | http://cipsc.coloriuris.net/crl/tsa/tsa-v3.1.crl |
| **Bases del certificado** | [1]Directiva de certificados:<br>Identificador de directiva=1.3.6.1.4.1.37799.20.5.1<br>[1,1]Información de certificador de directiva:<br>Id. de certificador de directiva=Aviso de usuario<br>Certificador:<br>Texto de aviso=Certificado de emisión de sellos electrónicos cualificados de tiempo<br>[1,2]Información de certificador de directiva:<br>Id. de certificador de directiva=CPS<br>Certificador:<br>https://cipsc.coloriuris.net/politicas/ |
| **Uso de la clave** | Firma digital, No repudio |
| **Uso extendido de la clave** | Time Stamping (Marca de Tiempo) |
| **1.3.6.1.5.5.7.1.3 -IETF / 0.4.0.1862.1.1-ETSI** | QCStatements |
| **QCSyntax-v2** | id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2) |
| **Uso de la clave** | Sello de tiempo, no repudio |

# Anexo I

## Acrónimos utilizados

- **AC:** Autoridad de CIPSC para la prestación de servicios de confianza
- **AR:** Autoridad de registro
- **ASD:** Autoridad de CIPSC para la prestación de servicios relativos a los documentos electrónicos
- **CEN-CWA:** Committee Européen de Normalisation- CEN Workshop Agreement
- **CIPSC:** Coloriuris Prestador de Servicios de Confianza
- **CN:** Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500
- **CRL:** Certificate Revocation List (Lista de Certificados Revocados)
- **DSCF**: Dispositivo Seguro de Creación de Firma
- **EAL:** Evaluation Assurance Level
- **ETSI:** European Telecommunications Standard Institute
- **FIPS:** Federal Information Processing Standard (Estándar USA de procesado de información)
- **HSM**: Hardware Security Module. Módulo de seguridad criptográfico empleado para almacenar claves y realizar operaciones criptográficas de modo seguro.
- **IETF**: Internet Engineering Task Force (Organismo de estandarización de Internet)
- **OASIS:** Organization for the Advancement of Structured Information Standard
- **OCSP**: Online Certificate Status Protocol. Este protocolo permite comprobar en línea la vigencia de un certificado electrónico.
- **OID**: Object identifier (Identificador de objeto único)
- **PKI**: Public Key Infrastructure (Infraestructura de Clave Pública)
- **PSC**: Prestador de Servicios de Confianza
- **RFC**: Request For Comments (Estándar emitido por la IETF)

- **SSCD**: Secure Signtature Creation Device (Dispositivo Seguro de Creación de Firma)
- **TSA**: Time-stamping Authority (Autoridad de Sellado de Tiempo)
- **TSACI:** Autoridad de CIPSC para la prestación del servicio de sellado de tiempo
- **TST**: Time-stamping Token (Sello de Tiempo)
- **TSU**: Time-stamping Unit (Unidad de Sellado de Tiempo)
- **UTC**: Coordinated Universal Time (Tiempo Universal Coordinado)
- **XAdES:** XML Advanced Electronic Signatures

## Definiciones

- **Autoridades prestadoras de servicios de CIPSC:** son las autoridades que prestan cada uno de los servicios de confianza del CIPSC
- **Certificado de firma electrónica:** una declaración electrónica que vincula los datos de validación de una firma con una persona física o jurídica y confirma, al menos, el nombre o el seudónimo de esa persona;
- **Certificado de sello electrónico:** una declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona.
- **Clave de sesión**: clave que se genera de forma específica para una comunicación o sesión, terminando su utilidad una vez finalizada ésta.
- **Clave pública y clave privada**: la criptografía asimétrica emplea un par de claves en la que lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa, a una de esas claves se la denomina pública (coincide con los datos de creación de la firma electrónica) y se la incluye en el certificado electrónico, mientras que a la otra se la denomina privada y únicamente es conocida por el titular del certificado.
- **Datos de identificación de la persona:** un conjunto de datos que permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica;
- **Datos de validación:** los datos utilizados para validar una firma electrónica o un sello electrónico.
- **Declaración de prácticas**: declaración de las prácticas que una Autoridad emplea para la prestación de sus servicios.

- **Documento electrónico:** todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual.
- **Evidencia:** Son los elementos auténticos emitidos por el CIPSC. Comprenden, en particular, los certificados electrónicos, los sellos de tiempo y los certificados de emisión y recepción de envíos electrónicos certificados y, en general, cualquier documento electrónico autentico emitido como resultado de la prestación de un servicio de confianza del CIPSC y contemplado expresamente en estas Políticas y declaración del prácticas.
- **Identificación electrónica:** el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica;
- **Política de sellado de tiempo**: conjunto de reglas que establecen la aplicabilidad del sello de tiempo y sus características de emisión.
- **Prestador de servicios de certificación:** persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
- **Prestador de servicios de confianza:** una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianzas.
- **Sello de tiempo electrónico:** datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante.
- **Sello de tiempo**: estructura de datos que ligan unos datos determinados a un instante de tiempo particular, proporcionando evidencia de su existencia con anterioridad a ese instante.
- **Sello electrónico:** datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos.
- **Servicio de confianza:** el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en: la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o la creación, verificación y validación de certificados para la autenticación de sitios web, o la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.
- **Servicio de entrega electrónica certificada:** un servicio que permite transmitir datos entre

partes terceras por medios electrónicos y aporta pruebas relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que protege los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizada.

- **Firmante:** persona física que crea una firma electrónica.
- **Creador de sello:** persona jurídica que crea un sello electrónico.
- **Parte usuaria**: persona física o jurídica que confía en la identificación electrónica o el servicio de confianza.
- **Tiempo universal coordinado (UTC):** escala de tiempo, basada en el segundo, definida por el Comité de Radio de la Unión Internacional de Telecomunicaciones (ITU-T) TF.460-5.
- **Unidad de sellado de tiempo (Time-Stamp Unit ó TSU):** conjunto de hardware y software que se gestiona como una unidad y que tiene una única clave privada de firma activa en cada momento.
- **Validación:** el proceso de verificar y confirmar la validez de una firma o sello electrónicos.

## Normativa

La normativa básica aplicable es la siguiente:

- Reglamento (UE) 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
- Ley 59/2003, de 19 de diciembre, de firma electrónica
- Ley Orgánica 15/1999, de 13 de diciembre, de protección de los datos de carácter personal
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
- Ley 34/2002, de 11 de julio de Servicios de la Sociedad de Información y Comercio Electrónico.
- Norma Técnica de Interoperabilidad (NTI) de Documento electrónico (Resolución de la Secretaría de Estado para la Función Pública, de 19 de julio de 2011)
- NTI de Reutilización de recursos de información (Resolución de 19 de febrero de 2013)

- NTI de Política de gestión de documentos electrónicos (Resolución de 28 de junio de 2012)

## Estándares

El contenido de los siguientes documentos es relevante para el desarrollo y/o aplicación de las presentes Políticas y declaración de prácticas de Coloriuris Prestador de Servicios de Confianza:

- *CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates V1*
- *CA/Browser Forum EV SSL Certificate Guidelines V 1.3*
- ETSI EN 319 401, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures.
- ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy requirements for Trust Service Providers issuing qualified certificates; Part 1: General requirements.
- ETSI EN 319 411-2, Electronic Signatures and Infrastructures (ESI); Policy requirements for Trust Service Providers issuing qualified certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI EN 319 421, Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 122, Electronic Signatures and Infrastructures (ESI); CAdES digital signatures;
- ETSI EN 319 132, Electronic Signatures and Infrastructures (ESI); XAdES digital signatures;
- ETSI EN 319 412, Electronic Signatures and Infrastructures (ESI); Certificate Profiles;
- ETSI EN 319 422, Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- ETSI TS 119 312, Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- ISO/IEC 18014-1, Time-stamping services — Part 1: Framework
- RCF 3647, *Internet X.509 Public Key Infrastructure Certificate Policy*
- RFC 3161, Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP).
- RFC 3628, Policy Requirements for Time-Stamping Authorities (TSAs)
- RFC 3739 y 3039, *Internet X.509 Public Key Infrastructure: Qualified Certificates Profile*

- *RFC 5280 y 3280, Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL)*

Fdo.: Pedro Canut Zazurca

Responsable de Administración de Políticas de Coloriuris S.L.

Fecha: 09 de abril de 2018

# Anexo II – Certificados de la TSACI

## [TSA] Certificado raíz v3.0

| | |
|---|---|
| Asunto | C = ES<br>L = Zaragoza<br>O = Coloriuris S.L.<br>OU = Prestador de Servicios de Confianza<br>organizationIdentifier = VATES-B99091696<br>CN = CIPSC - Raíz - Autoridad de Sellado de Tiempo v3<br>E = cipsc@coloriuris.net |
| Validez | De 21/06/2017 a 21/06/2037 |
| Huella digital (SHA1) | 01 C4 76 53 40 6D 53 F3 61 51 01 06 51 40 3C 47 BB 46 37 8B |
| URLs descarga | DER https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.crt<br>PEM https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.pem |

## [TSA] Certificado de emisión de sellos electrónicos cualificados de tiempo v3.0

| | |
|---|---|
| Asunto | C = ES<br>L = Zaragoza<br>O = Coloriuris S.L.<br>organizationIdentifier= VATES-B99091696<br>CN = CIPSC – v3 - Emisor de sellos de tiempo de 2048 |
| Validez | De 04/07/2017 a 04/07/2027 |
| Huella digital (SHA1) | B5 F9 09 C0 21 F2 F6 2B B4 72 23 9D 84 5C B6 4E 06 B9 B1 01 |
| Huella digital (SHA256) | D89C1C4E9477B4768B1C46F7E16129541CCDE19951A4912AF65743E7BD5513BE |
| URL descarga | https://cipsc.coloriuris.net/certificados/tsa-v3/tsu/2048.crt |

## [TSA] Certificado raíz v3.1

| | |
|---|---|
| Asunto | C = ES<br>L = Zaragoza<br>O = Coloriuris S.L.<br>OU = Prestador de Servicios de Confianza<br>organizationIdentifier = VATES-B99091696<br>CN = CIPSC – Raíz – Autoridad de Sellado de Tiempo v3.1<br>E = cipsc@coloriuris.net |
| Validez | De 21/12/2017 a 21/12/2037 |
| Huella digital (SHA1) | F9 F0 87 AC F2 65 2C D0 CF E1 0C 98 18 AC A9 91 3D BC 8F 28 |
| URLs descarga | DER https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.1.crt<br>PEM https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.1.pem |

## [TSA] Certificado de emisión de sellos electrónicos cualificados de tiempo v3.1

| | |
|---|---|
| Asunto | C = ES<br>L = Zaragoza<br>O = Coloriuris S.L.<br>organizationIdentifier= VATES-B99091696<br>CN = CIPSC – v3.1 – Emisor de sellos electronicos cualificados de tiempo de 2048 |
| Validez | De 06/04/2018 a 05/04/2028 |
| Huella digital (SHA1) | 78 F0 0B B6 B0 59 45 31 DE 4D 54 72 2D DE 3F 1E D7 44 64 C7 |
| Huella digital (SHA256) | 6C17A05F0C77B96AB039A3F85058731EEB02F52FB66D87D19B93D2278D826499 |
| URL descarga | https://cipsc.coloriuris.net/certificados/tsa-v3.1/tsu/2048.crt |

# Anexo III

Tabla descriptiva de los OIDS identificadores de los perfiles de certificados finales en uso por los servicios de TSACI

Base OID asignada por IANA a Coloriuris: **1.3.6.1.4.1.37799**

| **1.3.6.1.4.1.37799** | **.20** | **Perfiles de certificados finales de los servicios de CIPSC** | | |
|---|---|---|---|---|
| | | **.5** | Autoridad de Sellado de Tiempo | |
| | | | **.1** | Certificado de emisión de sellos electrónicos cualificados de tiempo |

# Anexo IV – Revisión de las Políticas

Las presentes políticas se revisarán cada 6 meses (revisión ordinaria) y cada vez que se produzca algún cambio legislativo y/o en las normas ETSI que sean de aplicación. Asimismo, las políticas se revisarán cada vez que se active un nuevo servicio de confianza o se produzca un cese en alguno de los servicios de confianza prestados por CIPSC.

La revisión ordinaria de las políticas correrá a cargo del responsable de administración de políticas, que examinará las páginas oficiales del Ministerio de Energía, Turismo y Agenda Digital, del ETSI y de la Unión Europea (o de los organismos que pudieran sustituirlos en el futuro) con cadencia semestral a fin de comprobar si ha habido cambios que precisen una modificación de las mismas.

En el supuesto de que no existieran cambios que apliquen a las políticas de Coloriuris se levantará acta que se trasladará a la Dirección para su visto bueno.

En el supuesto de que si existieran cambios que apliquen a las políticas de Coloriuris se levantará igualmente acta que se trasladará a la Dirección para su visto bueno. Asimismo se comunicará la nueva versión de las políticas, con los cambios en el documento, al Regulador nacional solicitando de éste que se pronuncie acerca de la necesidad de someter los cambios al organismo evaluador de la conformidad.

Los cambios producidos se publicaran en la sede electrónica de CIPSC tanto en la url propia de estas políticas como en la sección /anuncios.

De igual modo se procederá en el supuesto de notificaciones de cambios legislativos y/o en las normas ETSI que aplican a las presentes políticas por parte del Regulador y/ o de las partes usuarias.

Las modificaciones necesarias en las políticas se llevarán a cabo de forma inmediata.