Coloriuris Prestador de Servicios de Confianza

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

Coloriuris, SL <cipsc@coloriuris.net>

Version 3.0.1 - 07/04/2026: O.I.D. 1.3.6.1.4.1.37799.20.5.0.3.0.1 - APROBADO

Índice

Histórico de cambios en el documento

Table 1. 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 • Actualización de los datos del Certificado de TSU • Añadido anexo de Revisión de las Políticas	Coloriuris, SL
1.1	03/01/2018	Añadidos nueva CA v3.1 y Emisor v3.1	Coloriuris, SL
1.2	09/04/2018	• Corrección de términos • Corrección de errores materiales • Corrección del Certificado de Emisión de Sellos de la TSA v3.1	Coloriuris, SL
2.0	30/06/2022	• Añadir referencia de la best practice ETSI 319 421. • Actualizar OID de la DPPG. • Actualizar en la política la identificación de la misma, con más detalle • Eliminación a toda referencia a Certificado de Emisión de Sellos de la TSA v3.0.	Coloriuris, SL
3.0	09/02/2026	• Adaptación a ETSI EN 319 421 v.1.3.1 • Nueva sección para definir el uso de CRL y 0CSP en el apartado 3. • Añadir nuevas CAs y nuevas TSUs • Corrección de términos	Coloriuris, SL
3.0.1	31/03/2026	• Añadir referencia a la ETSI EN 319 412-3 para la definición de perfiles de certificado de TSACI • Añadir fingerprints SHA1, SHA256 y SHA512 a la información completa de los certificados de CAs y TSUs	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, que corresponde específicamente con la *best practice: itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)*, cuyas funciones del 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 1.3.6.1.4.1.37799.0.3.1.4.0.0, en adelante DPPG.

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

1.1. Titularidad

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

1.2. Disponibilidad del servicio

El servicio de certificación de TSACI está disponible de forma ininterrumpida todos los días del año.

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”.

1.3. Identificación

El OID (object identifier) de las Políticas y declaración de prácticas de la Autoridad de Sellado de Tiempo de Coloriuris Prestador de Servicios de Confianza es: 1.3.6.1.4.1.37799.20.5.0.3.0.1.

1.4. Publicación de la política

Todos y cada uno de los sellos de tiempo emitidos por TSACI contienen un identificador (OID) que referencia a las Políticas y Declaración de Prácticas bajo las que han sido emitidos. Dicho identificador se corresponde al OID de la versión mayor de las Políticas y Declaración de Prácticas vigentes y se actualizará cada vez que dicho documento reciba una actualización mayor.

1.5. 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, SHA-384 y SHA-512.
- Para el cálculo del hash de los sellos de tiempo emitidos se utiliza SHA-256, SHA-382 y SHA-512.
- La firma de los sellos de tiempo emitidos se podrá realizar mediante el uso de claves de firma

RSA de al menos 2048 bits (*3072 bits a partir del 1 de enero de 2027*) o ECDSA de al menos 256 bits.

- Para el algoritmo de firma de los sellos se utilizará como mínimo SHA256withRSA (*vigente hasta el 31 de diciembre de 2026*), RSA-PSS MGF1withSHA256 o ECDSAwithSHA256 dependiendo de las claves utilizadas para la firma.

1.6. 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.

1.7. 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 3.5 y garantiza que no emitirá sellos de tiempo con una precisión menor que la antedicha.

1.8. 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.

1.9. Obligaciones

Las obligaciones de las partes usuarias están descritas en los apartados 2.6 del presente documento y en el apartado de las "DPPG" "2.3".

1.10. Registro de las operaciones

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

1.11. 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.

1.12. Responsabilidad

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

1.13. 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.

1.14. 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.

1.15. 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 20-01-2026 y con OID: 1.3.6.1.4.1.37799.20.5.0.3.0

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 2.1.2.2 y las partes usuarias, según se describen en el apartado 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.

2.6.1. 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.

2.6.2. 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 el apartado 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 3.5 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. Requisitos de comprobación de estado de certificados

Los certificados asociados al servicio de TSACI podrán ser validados utilizando las Listas de Revocación de Certificados (CRL) indicadas en los propios certificados. Adicionalmente, estas listas de revocación deberán ser publicadas en los repositorios indicados en el apartado 1.6.3 del "DPPG".

Opcionalmente se podrá ofrecer el servicio OCSP si así lo indican los propios certificados.

3.5. 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 es 1.3.6.1.4.1.37799.20.5.0.3.0.1.

- 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 las TSUs 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.

3.6. 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.

3.7. Certificados de TSACI

Los perfiles para los certificados de TSACI se establecerán de acuerdo a los definidos por la ETSI EN 319 412-3 para persona jurídica.

3.7.1. Certificados raíz

TSACI V 3.1.

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

Su contenido es el siguiente:

```
        Signature Algorithm: sha512WithRSAEncryption
        Subject: emailAddress = cipsc@coloriuris.net, CN = CIPSC - Ra\C3\ADz - Autoridad de Sellado de Tiempo
v3.1, organizationIdentifier = VATES-B99091696, OU = Prestador de Servicios de Confianza, O = Coloriuris S.L., L
= Zaragoza, C = ES
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            Authority Information Access:
                CA Issuers - URI:https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.1.crt
                OCSP - URI:https://ocspv3.coloriuris.net
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://cipsc.coloriuris.net/politicas/
            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://cipsc.coloriuris.net/crl/tsa/tsa-v3.1.crl                CRL Issuer:
                  DirName:emailAddress = cipsc@coloriuris.net, CN = CIPSC - Ra\C3\ADz - Autoridad de Sellado de
Tiempo v3.1, organizationIdentifier = VATES-B99091696, OU = Prestador de Servicios de Confianza, O = Coloriuris
S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                11:BC:35:3C:F5:EC:13:26:0E:60:43:B5:F8:86:A8:4E:1D:27:01:6A
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
```

TSACI CA01

El origen de la cadena de confianza de la TSACI CA01 es un certificado autofirmado emitido por CIPSC, con una clave RSA de 4096 Bits de longitud y un periodo de validez de 10 años.

Su contenido es el siguiente:

```
        Signature Algorithm: rsassaPss
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        Subject: CN = COLORIURIS CA01 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://cipsc.coloriuris.net/politicas/
            OCSP No Check:

            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2
```

```
            X509v3 Subject Key Identifier:
                61:61:40:A8:58:9C:7F:FC:9A:3C:A8:CC:9B:60:D2:F5:68:B2:9E:75
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
```

TSACI CA02

El origen de la cadena de confianza de la TSACI CA02 es un certificado autofirmado emitido por CIPSC, con una clave RSA de 4096 Bits de longitud y un periodo de validez de 20 años.

Su contenido es el siguiente:

```
        Signature Algorithm: rsassaPss
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        Subject: CN = COLORIURIS CA02 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://cipsc.coloriuris.net/politicas/
            OCSP No Check:

            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 Subject Key Identifier:
                BE:AC:4C:60:04:A3:4C:5F:FC:6A:41:E0:BD:A2:97:31:97:06:2F:FE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
```

TSACI CA03

El origen de la cadena de confianza de la TSACI CA03 es un certificado autofirmado emitido por CIPSC, con una clave ECDSA P-384 (secp384r1) y un periodo de validez de 20 años.

Su contenido es el siguiente:

```
        Signature Algorithm: ecdsa-with-SHA384
        Subject: CN = COLORIURIS CA03 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://cipsc.coloriuris.net/politicas/
            OCSP No Check:

            qcStatements:
```

```
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 Subject Key Identifier:
                0A:5B:B2:26:8C:21:5F:5E:3E:B7:D1:7A:D1:DC:C7:22:29:D5:37:E9
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
```

TSACI CA04

El origen de la cadena de confianza de la TSACI CA04 es un certificado autofirmado emitido por CIPSC, con una clave ECDSA P-384 (secp384r1) y un periodo de validez de 20 años.

Su contenido es el siguiente:

```
        Signature Algorithm: ecdsa-with-SHA384
        Subject: CN = COLORIURIS CA04 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://cipsc.coloriuris.net/politicas/
            OCSP No Check:

            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 Subject Key Identifier:
                03:BA:FE:15:05:26:FF:14:B1:1F:6E:98:08:19:64:AD:58:9F:1E:A2
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
```

3.7.2. Certificados para la emisión de sellos electrónicos cualificados de tiempo

Los perfiles de los certificados estarán identificados por el OID 1.3.6.1.4.1.37799.20.5.1.

TSACI dispondrá de varias TSUs para la emisión de los sellos electrónicos cualificados de tiempo, cada TSU tendrá su correspondiente certificado que podrá ser emitido por la propia TSACI de CIPSC utilizando sus propias CAs indicadas en el apartado 3.6.1 y cuyo periodo de validez será de al menos 10 años.

Certificado v3.1 (RSA 2048 bits)

Este certificado se podrá mantendrá en uso hasta el 31 de diciembre de 2026

```
        Signature Algorithm: sha512WithRSAEncryption
```

```
        Issuer: emailAddress = cipsc@coloriuris.net, CN = CIPSC - Ra\C3\ADz - Autoridad de Sellado de Tiempo
v3.1, organizationIdentifier = VATES-B99091696, OU = Prestador de Servicios de Confianza, O = Coloriuris S.L., L
= Zaragoza, C = ES
        Subject: CN = CIPSC - v3.1 - Emisor de sellos electronicos cualificados de tiempo de 2048,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                11:BC:35:3C:F5:EC:13:26:0E:60:43:B5:F8:86:A8:4E:1D:27:01:6A
            Authority Information Access:
                CA Issuers - URI:https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.1.crt
                OCSP - URI:https://ocspv3.coloriuris.net
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text:
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://cipsc.coloriuris.net/crl/tsa/tsa-v3.1.crl                CRL Issuer:
                  DirName:emailAddress = cipsc@coloriuris.net, CN = CIPSC - Ra\C3\ADz - Autoridad de Sellado de
Tiempo v3.1, organizationIdentifier = VATES-B99091696, OU = Prestador de Servicios de Confianza, O = Coloriuris
S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                7E:5A:DB:1E:ED:2E:13:B5:89:50:AC:5E:C2:3D:54:AA:7B:23:82:AC
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
```

Certificado TSU01 (RSA 3072 bits)

```
        Signature Algorithm: rsassaPss
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        Issuer: CN = COLORIURIS CA01 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject: CN = COLORIURIS QTSP TSU01 - Emisor de sellos electronicos cualificados de tiempo,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                61:61:40:A8:58:9C:7F:FC:9A:3C:A8:CC:9B:60:D2:F5:68:B2:9E:75
            Authority Information Access:
                CA Issuers - URI:http://ca01.coloriuris.net/certs/coloriuris-ca01-tsa.crt
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text: Certificado de emisión de sellos electrónicos cualificados de tiempo
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
```

```
    4:d=2  hl=2 l=   8 prim:   OBJECT           :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca01.coloriuris.net/crl/coloriuris-ca01-tsa.crl               CRL Issuer:
                  DirName:CN = COLORIURIS CA01 TSA, OU = Prestador de Servicios de Confianza,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                C9:DC:E7:8C:14:B1:EB:F1:7D:A6:D4:3F:3A:2A:25:C8:0F:66:7B:65
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
```

Certificado TSU02 (RSA 3072 bits)

```
        Signature Algorithm: rsassaPss
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        Issuer: CN = COLORIURIS CA02 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject: CN = COLORIURIS QTSP TSU02 - Emisor de sellos electronicos cualificados de tiempo,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                BE:AC:4C:60:04:A3:4C:5F:FC:6A:41:E0:BD:A2:97:31:97:06:2F:FE
            Authority Information Access:
                CA Issuers - URI:http://ca02.coloriuris.net/certs/coloriuris-ca02-tsa.crt
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text: Certificado de emisión de sellos electrónicos cualificados de tiempo
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT           :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca02.coloriuris.net/crl/coloriuris-ca02-tsa.crl               CRL Issuer:
                  DirName:CN = COLORIURIS CA02 TSA, OU = Prestador de Servicios de Confianza,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                77:AB:32:37:1C:68:98:84:E0:7E:37:02:4E:A3:12:7D:3A:27:24:D4
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
```

Certificado TSU03 (RSA 4096 bits)

```
        Signature Algorithm: rsassaPss
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
```

```
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        Issuer: CN = COLORIURIS CA01 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject: CN = COLORIURIS QTSP TSU03 - Emisor de sellos electronicos cualificados de tiempo,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                61:61:40:A8:58:9C:7F:FC:9A:3C:A8:CC:9B:60:D2:F5:68:B2:9E:75
            Authority Information Access:
                CA Issuers - URI:http://ca01.coloriuris.net/certs/coloriuris-ca01-tsa.crt
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text: Certificado de emisión de sellos electrónicos cualificados de tiempo
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca01.coloriuris.net/crl/coloriuris-ca01-tsa.crl                CRL Issuer:
                  DirName:CN = COLORIURIS CA01 TSA, OU = Prestador de Servicios de Confianza,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                CE:3B:A4:31:6F:59:F8:3C:E9:02:8E:48:22:9E:8F:21:74:75:72:BA
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
```

Certificado TSU04 (RSA 4096 bits)

```
        Signature Algorithm: rsassaPss
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        Issuer: CN = COLORIURIS CA02 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject: CN = COLORIURIS QTSP TSU04 - Emisor de sellos electronicos cualificados de tiempo,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                BE:AC:4C:60:04:A3:4C:5F:FC:6A:41:E0:BD:A2:97:31:97:06:2F:FE
            Authority Information Access:
                CA Issuers - URI:http://ca02.coloriuris.net/certs/coloriuris-ca02-tsa.crt
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text: Certificado de emisión de sellos electrónicos cualificados de tiempo
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
```

```
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca02.coloriuris.net/crl/coloriuris-ca02-tsa.crl               CRL Issuer:
                  DirName:CN = COLORIURIS CA02 TSA, OU = Prestador de Servicios de Confianza,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                C6:CF:22:35:02:B1:6D:F5:E2:F1:B0:AE:68:16:45:73:55:6B:1A:7C
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
```

Certificado TSU05 (ECDSA P-256 bits)

```
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: CN = COLORIURIS CA03 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject: CN = COLORIURIS QTSP TSU05 - Emisor de sellos electronicos cualificados de tiempo,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                0A:5B:B2:26:8C:21:5F:5E:3E:B7:D1:7A:D1:DC:C7:22:29:D5:37:E9
            Authority Information Access:
                CA Issuers - URI:http://ca03.coloriuris.net/certs/coloriuris-ca03-tsa.crt
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text: Certificado de emisión de sellos electrónicos cualificados de tiempo
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  82 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2
   25:d=1  hl=2 l=  57 cons:  SEQUENCE
   27:d=2  hl=2 l=   6 prim:   OBJECT            :0.4.0.1862.1.5
   35:d=2  hl=2 l=  47 cons:   SEQUENCE
   37:d=3  hl=2 l=  45 cons:    SEQUENCE
   39:d=4  hl=2 l=  39 prim:     IA5STRING         :https://cipsc.coloriuris.net/pds/en.pdf
   80:d=4  hl=2 l=   2 prim:     PRINTABLESTRING   :en

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca03.coloriuris.net/crl/coloriuris-ca03-tsa.crl               CRL Issuer:
                  DirName:CN = COLORIURIS CA03 TSA, OU = Prestador de Servicios de Confianza,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                7F:41:44:25:68:8D:B2:56:B6:81:41:3D:F2:98:DF:39:DA:CE:C7:7E
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
```

Certificado TSU06 (ECDSA P-256 bits)

```
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: CN = COLORIURIS CA04 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
```

```
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject: CN = COLORIURIS QTSP TSU06 - Emisor de sellos electronicos cualificados de tiempo,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                03:BA:FE:15:05:26:FF:14:B1:1F:6E:98:08:19:64:AD:58:9F:1E:A2
            Authority Information Access:
                CA Issuers - URI:http://ca04.coloriuris.net/certs/coloriuris-ca04-tsa.crt
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text: Certificado de emisión de sellos electrónicos cualificados de tiempo
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca04.coloriuris.net/crl/coloriuris-ca04-tsa.crl               CRL Issuer:
                  DirName:CN = COLORIURIS CA04 TSA, OU = Prestador de Servicios de Confianza,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                32:93:2D:1C:67:69:08:7A:D5:AB:0C:90:E6:31:3F:94:1C:07:EB:02
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
```

Certificado TSU07 (ECDSA P-384 bits)

```
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: CN = COLORIURIS CA03 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject: CN = COLORIURIS QTSP TSU07 - Emisor de sellos electronicos cualificados de tiempo,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                0A:5B:B2:26:8C:21:5F:5E:3E:B7:D1:7A:D1:DC:C7:22:29:D5:37:E9
            Authority Information Access:
                CA Issuers - URI:http://ca03.coloriuris.net/certs/coloriuris-ca03-tsa.crt
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text: Certificado de emisión de sellos electrónicos cualificados de tiempo
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  82 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2
   25:d=1  hl=2 l=  57 cons:  SEQUENCE
   27:d=2  hl=2 l=   6 prim:   OBJECT            :0.4.0.1862.1.5
   35:d=2  hl=2 l=  47 cons:   SEQUENCE
   37:d=3  hl=2 l=  45 cons:    SEQUENCE
   39:d=4  hl=2 l=  39 prim:     IA5STRING         :https://cipsc.coloriuris.net/pds/en.pdf
```

```
   80:d=4  hl=2 l=   2 prim:     PRINTABLESTRING   :en

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca03.coloriuris.net/crl/coloriuris-ca03-tsa.crl               CRL Issuer:
                  DirName:CN = COLORIURIS CA03 TSA, OU = Prestador de Servicios de Confianza,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                2E:9E:B5:C4:9C:19:FD:65:7D:23:F9:25:01:7D:7C:80:DB:66:23:6B
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
```

Certificado TSU08 (ECDSA P-384 bits)

```
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: CN = COLORIURIS CA04 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject: CN = COLORIURIS QTSP TSU08 - Emisor de sellos electronicos cualificados de tiempo,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                03:BA:FE:15:05:26:FF:14:B1:1F:6E:98:08:19:64:AD:58:9F:1E:A2
            Authority Information Access:
                CA Issuers - URI:http://ca04.coloriuris.net/certs/coloriuris-ca04-tsa.crt
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text: Certificado de emisión de sellos electrónicos cualificados de tiempo
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca04.coloriuris.net/crl/coloriuris-ca04-tsa.crl               CRL Issuer:
                  DirName:CN = COLORIURIS CA04 TSA, OU = Prestador de Servicios de Confianza,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                11:82:89:A8:AC:39:0E:C5:3A:5D:90:AB:9A:7C:7E:FE:27:AC:CF:4C
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
```

Fdo.: Silvia Mª Canut Grávalos

Responsable de Administración de Políticas de Coloriuris S.L.

Zaragoza, Abril de 2026

Anexo A: Glosario

Acrónimos utilizados

AC
Autoridad de CIPSC para la prestación de servicios de confianza

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 6/ 2020, de 11 de noviembre.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y su normativa de desarrollo.
- 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 3039, Internet X.509 Public Key Infrastructure: Qualified Certificates Profile*
- *RFC 5280, Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL)*

Anexo B: Certificados de la TSACI

B.1. Certificado Raíz TSACI V 3.1.

```
        Version: 3 (0x2)
        Serial Number: 3661310668029754684 (0x32cf96a77442fd3c)
        Signature Algorithm: sha512WithRSAEncryption
        Issuer: emailAddress = cipsc@coloriuris.net, CN = CIPSC - Ra\C3\ADz - Autoridad de Sellado de Tiempo
v3.1, organizationIdentifier = VATES-B99091696, OU = Prestador de Servicios de Confianza, O = Coloriuris S.L., L
= Zaragoza, C = ES
        Validity
            Not Before: Dec 21 12:28:46 2017 GMT
            Not After : Dec 21 12:28:46 2037 GMT
        Subject: emailAddress = cipsc@coloriuris.net, CN = CIPSC - Ra\C3\ADz - Autoridad de Sellado de Tiempo
v3.1, organizationIdentifier = VATES-B99091696, OU = Prestador de Servicios de Confianza, O = Coloriuris S.L., L
= Zaragoza, C = ES
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:bd:99:fc:1b:55:1d:4e:ef:6b:df:a3:f4:10:b6:
                    3a:2f:08:88:b0:f3:a6:5f:3c:11:96:5f:76:fd:08:
                    4f:c4:db:e2:b9:08:c8:e7:11:60:d2:4e:9a:e1:b5:
                    d4:84:b9:c8:1d:04:8e:df:24:65:15:8f:6c:b2:00:
                    43:6f:dd:d2:58:04:88:bf:a1:50:00:50:6d:6c:5a:
                    9f:bb:9d:9a:ca:68:74:ac:bc:17:d1:d0:8a:fd:7f:
                    a7:15:78:8a:41:0d:1f:22:a5:b2:df:61:16:3e:09:
                    d6:5e:41:a5:aa:5e:57:ec:99:53:79:28:8e:08:d8:
                    26:10:8e:1a:86:61:bc:cd:d8:cc:04:b4:64:9e:a3:
                    04:17:2e:a4:c1:06:d8:6a:79:ec:1f:56:ec:0c:be:
                    6e:86:32:eb:ce:b4:21:67:4b:fd:22:7b:37:00:95:
                    06:8b:17:84:76:20:82:80:8b:86:66:ed:4e:92:62:
                    9a:a1:41:e7:8d:34:89:9b:1a:49:b7:2d:f4:23:37:
                    e7:cd:58:61:12:17:5c:4b:4e:ef:53:94:ff:e6:84:
                    e1:b2:3a:eb:16:b0:ea:dc:29:53:c3:49:36:5b:14:
                    71:d9:8c:85:c5:ed:ff:df:b8:1f:46:fe:bd:be:a7:
                    70:35:04:98:ab:74:78:a3:83:0a:5b:d5:38:8d:6c:
                    14:4c:cb:9c:c7:23:48:9f:ff:28:d8:04:f2:4f:9e:
                    55:34:cb:81:4b:a8:1a:df:24:07:f1:c4:e8:d1:24:
                    86:dd:ec:dc:ce:12:46:77:5a:b1:37:5a:a0:4e:df:
                    b9:73:e8:84:51:28:34:8b:b3:40:19:c3:a6:0a:92:
                    85:87:a6:ff:b1:8c:45:d8:7a:07:9f:40:64:9e:82:
                    93:d9:9e:43:3c:09:a3:bb:93:1d:27:c0:1a:9d:cc:
                    5f:b8:6c:f4:0e:ab:a5:30:15:6c:02:38:16:6b:2b:
                    05:eb:64:bd:1f:d0:e4:89:da:c4:6e:35:90:08:a7:
                    6c:c5:7b:02:0f:c7:70:e7:fd:e4:78:bc:42:95:a2:
                    c9:94:f0:9e:a8:e1:4a:12:ce:da:67:35:20:4b:9c:
                    3e:9f:bd:f4:86:ce:02:db:c6:34:51:fd:33:a2:c3:
                    25:0b:17:7d:cd:4f:83:5b:b2:11:eb:21:49:ee:1d:
                    2b:4c:8b:4d:70:c1:c8:c3:c3:03:a8:e0:56:e0:9b:
                    f4:6c:52:75:1c:1d:0f:40:1e:d2:4c:21:19:73:83:
                    98:d8:0d:66:1e:bc:34:74:e4:0f:5b:ae:ee:e5:99:
                    94:c9:e5:ef:72:5d:74:c5:d4:af:54:86:75:43:30:
                    95:86:75:1f:ff:4d:c6:bd:1b:ec:81:6e:3f:9b:22:
                    db:0c:0b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            Authority Information Access:
                CA Issuers - URI:https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.1.crt
```

```
                OCSP - URI:https://ocspv3.coloriuris.net
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://cipsc.coloriuris.net/politicas/
            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://cipsc.coloriuris.net/crl/tsa/tsa-v3.1.crl                CRL Issuer:
                  DirName:emailAddress = cipsc@coloriuris.net, CN = CIPSC - Ra\C3\ADz - Autoridad de Sellado de
Tiempo v3.1, organizationIdentifier = VATES-B99091696, OU = Prestador de Servicios de Confianza, O = Coloriuris
S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                11:BC:35:3C:F5:EC:13:26:0E:60:43:B5:F8:86:A8:4E:1D:27:01:6A
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
    Signature Algorithm: sha512WithRSAEncryption
    Signature Value:
        73:8a:77:85:3f:8e:ba:fe:d7:97:6d:ff:8a:70:51:f5:52:31:
        9e:7f:79:a6:c2:04:80:06:75:26:31:8e:50:3e:c1:0c:49:af:
        57:2b:95:75:0f:8f:a6:e0:d6:8c:9f:af:e9:21:e4:7f:f0:d9:
        c1:89:01:0d:8f:8f:11:da:82:2a:6f:d6:d4:40:87:e0:5f:bc:
        3b:c6:94:7e:cc:85:66:15:50:13:67:6c:b1:64:0b:8d:fd:5c:
        26:5a:c1:2b:4b:48:a1:f8:43:d7:91:4e:2c:e4:91:f8:02:1c:
        27:d2:5c:6e:57:d8:20:39:8e:3a:7e:ce:c1:5b:40:93:49:d2:
        00:63:9a:6a:05:82:18:14:cc:ad:3b:94:07:fe:b4:90:34:b6:
        fa:9f:4d:a3:84:8e:68:68:64:58:ed:74:e0:d4:1b:d7:83:08:
        95:d8:d4:9e:55:24:d0:53:19:af:65:8c:80:b8:7d:63:6f:75:
        8f:a9:fa:2d:a8:df:bc:8d:0a:84:68:a1:93:18:dd:39:f5:db:
        b8:fc:f7:58:a2:f8:72:15:db:79:9d:55:76:5a:78:e9:95:21:
        91:7d:cf:15:99:11:3d:0f:98:c3:58:21:c8:24:43:92:7f:54:
        32:b3:93:59:a8:e3:c2:26:32:0d:97:6d:03:05:3f:3f:9b:69:
        0a:99:6d:20:9b:1e:4c:39:75:fc:58:9d:55:02:3b:12:9d:7c:
        11:2f:e0:55:8c:5b:9d:d0:bf:f1:f7:99:29:9c:c9:dc:5d:88:
        5b:41:98:f6:f2:a2:3f:ea:c2:c7:04:57:4c:38:e0:6f:c0:25:
        7a:26:17:f4:fc:72:44:c5:c5:bc:f6:2c:18:ef:d1:c2:fd:e6:
        7b:84:c1:d1:f3:7b:4b:17:bc:44:65:73:45:37:84:05:71:6c:
        b1:6d:a5:07:05:ff:15:8e:e4:f5:cb:fd:f8:cc:d1:c2:62:23:
        c3:ba:4b:75:77:d4:39:aa:55:2c:b7:fb:e0:9a:0e:eb:6c:45:
        79:17:3f:ce:1f:60:f4:3e:8f:40:9f:2f:2f:85:dc:b1:3a:1f:
        92:31:9c:25:8c:b4:b5:e7:87:e7:dd:36:b9:23:b4:1c:d8:57:
        d7:46:e3:17:b5:20:9e:5e:21:56:c0:70:76:48:c8:2e:54:65:
        9e:91:48:9b:97:6c:d2:4a:d9:ff:43:71:49:ec:bf:42:91:44:
        10:2a:4a:f5:3c:91:e7:7e:de:68:b9:df:bb:61:ca:7e:81:32:
        53:ce:b9:67:bb:5a:a4:ac:e4:27:1d:59:75:fe:c6:b2:f9:c9:
        a1:50:3f:07:67:0a:29:ff:f4:81:52:18:86:49:ee:02:e3:d8:
        91:b4:8b:ea:27:ec:83:c9
SHA1 Fingerprint=F9:F0:87:AC:F2:65:2C:D0:CF:E1:0C:98:18:AC:A9:91:3D:BC:8F:28
sha256
Fingerprint=BA:2E:9B:F8:DA:C0:D4:AC:07:64:19:4B:34:30:59:FA:C9:C9:3A:DB:C0:10:A7:1A:E1:A9:AD:9B:81:48:C1:A3
sha512
Fingerprint=44:FF:B5:1C:03:1A:D9:D4:0C:9B:46:5C:18:5F:55:1F:14:E5:8F:36:E9:09:78:C0:95:34:DA:EF:FA:E4:B2:D5:BE:A2
:F1:C8:61:3D:60:57:2B:34:87:E7:A2:EB:FA:0C:95:D7:BB:21:98:B6:2E:D3:B7:1B:16:EA:8F:CE:2A:AB
```

B.1.1. Certificado de emisión de sellos electrónicos cualificados de tiempo v3.1 (RSA 2048 bits)

```
        Version: 3 (0x2)
        Serial Number: 7842311533657933281 (0x6cd57cca1da145e1)
        Signature Algorithm: sha512WithRSAEncryption
        Issuer: emailAddress = cipsc@coloriuris.net, CN = CIPSC - Ra\C3\ADz - Autoridad de Sellado de Tiempo
v3.1, organizationIdentifier = VATES-B99091696, OU = Prestador de Servicios de Confianza, O = Coloriuris S.L., L
= Zaragoza, C = ES
        Validity
            Not Before: Apr  6 11:35:35 2018 GMT
            Not After : Apr  5 11:35:35 2028 GMT
        Subject: CN = CIPSC - v3.1 - Emisor de sellos electronicos cualificados de tiempo de 2048,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c4:c0:9a:9f:a6:4a:77:eb:40:13:3b:1c:68:aa:
                    f2:8c:f7:a9:e9:3c:28:06:a6:8d:db:98:19:48:e0:
                    18:33:25:b2:e2:87:9c:dc:b4:3b:50:ec:3e:99:be:
                    89:f1:69:7b:f1:5d:7c:c2:d5:fd:97:07:46:e9:f2:
                    94:a3:a6:00:30:a6:eb:7e:2b:3d:4e:26:b8:45:f1:
                    31:bc:31:c8:55:83:4a:1d:08:f8:ed:d2:be:b1:c8:
                    3d:ae:ce:c4:fa:7e:3f:19:c2:a4:75:f4:1f:41:62:
                    9d:4b:f8:cd:26:65:d6:a3:2f:54:12:9d:31:8b:58:
                    48:70:5e:48:b3:06:98:1a:11:ad:22:1b:03:db:ce:
                    e9:f3:a5:a4:9a:f1:fb:47:59:b1:49:c4:ed:72:cd:
                    46:8b:41:85:23:ba:5e:66:1d:2d:c8:1e:0a:d3:b3:
                    80:19:4c:6d:a0:f7:b7:14:71:4e:95:7a:95:11:3c:
                    0c:af:65:45:e9:b5:a3:88:7b:f5:45:17:2a:7e:cd:
                    ae:a8:49:21:07:f0:ae:58:67:ab:f6:6a:65:ce:4d:
                    21:ff:d8:85:14:53:59:35:34:7b:53:b4:73:ff:6c:
                    d3:c5:46:c2:33:5a:55:08:5a:4d:59:1c:e9:be:ea:
                    1d:d1:cd:d1:62:ae:4e:4d:89:89:1c:5f:e7:37:de:
                    ff:01
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                11:BC:35:3C:F5:EC:13:26:0E:60:43:B5:F8:86:A8:4E:1D:27:01:6A
            Authority Information Access:
                CA Issuers - URI:https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.1.crt
                OCSP - URI:https://ocspv3.coloriuris.net
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text:
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://cipsc.coloriuris.net/crl/tsa/tsa-v3.1.crl                CRL Issuer:
                  DirName:emailAddress = cipsc@coloriuris.net, CN = CIPSC - Ra\C3\ADz - Autoridad de Sellado de
Tiempo v3.1, organizationIdentifier = VATES-B99091696, OU = Prestador de Servicios de Confianza, O = Coloriuris
S.L., L = Zaragoza, C = ES
```

```
            X509v3 Subject Key Identifier:
                7E:5A:DB:1E:ED:2E:13:B5:89:50:AC:5E:C2:3D:54:AA:7B:23:82:AC
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
    Signature Algorithm: sha512WithRSAEncryption
    Signature Value:
        1a:8f:49:91:d8:a6:97:0f:79:f4:cf:1c:28:8a:e5:88:98:1f:
        94:f1:02:3f:8e:9a:bd:8a:36:9a:a8:74:4b:c7:14:4e:ea:e5:
        6a:2b:c2:80:05:b4:dc:05:6f:c6:33:55:dc:f1:ee:76:fe:f3:
        bc:9f:fc:c2:60:95:cd:43:fe:53:55:26:84:0b:b5:cd:85:01:
        6d:c6:0c:62:b2:81:94:b7:a3:80:fc:5e:5e:3a:f2:3e:d4:11:
        23:2d:61:aa:f7:fe:7d:39:bd:ae:91:76:be:7e:12:ec:53:40:
        98:3d:6e:10:b1:c7:6d:2c:9a:d3:15:2f:c8:92:34:db:88:b4:
        1c:44:7b:76:08:0e:f9:08:8e:38:5c:57:4e:dd:b8:f4:e7:76:
        a7:28:0a:4f:c6:fa:18:52:b1:f4:bd:73:5f:2c:9c:1c:b5:e8:
        40:03:94:c1:88:69:4c:97:41:f7:e8:22:5b:e4:3f:74:73:bc:
        ec:14:e8:b9:8f:26:ac:96:ae:38:24:45:e9:b0:4b:bc:04:26:
        be:51:31:3f:f1:1f:e2:74:83:4d:f8:95:13:d9:45:9f:f7:c0:
        37:c9:fe:00:e9:43:0c:00:a7:70:54:d6:bd:bb:bd:a4:7d:38:
        22:2a:30:88:62:95:cc:4f:c2:12:1f:88:57:22:53:a4:0b:e4:
        ff:5c:84:81:ef:78:bd:39:6d:38:7c:d8:28:7e:52:50:f9:21:
        6d:2f:65:3a:a4:92:0c:eb:a9:7a:97:35:58:6d:18:7f:40:9e:
        df:b5:ee:8f:e1:2a:3b:a3:39:29:fb:24:05:19:ef:29:51:e3:
        ff:19:9e:87:0c:ef:2e:07:74:b6:91:8f:ef:b1:66:c4:49:88:
        ba:a8:78:dc:f3:59:80:3e:4f:e0:95:20:74:f4:a0:e2:85:ba:
        8c:0a:9c:d5:94:3f:41:4d:73:16:ad:62:ac:d8:b5:5d:ba:f0:
        42:3d:8e:fd:97:45:77:64:56:6e:e7:28:c7:bd:21:3b:31:af:
        c2:4b:b3:0e:b4:cf:a7:b6:ba:b1:01:24:20:91:34:fb:ca:eb:
        a1:3f:bd:f5:4b:45:4b:ba:fc:6c:ce:30:6b:7d:28:89:ee:6f:
        8c:fd:e1:92:64:f4:18:53:25:44:12:d3:59:86:77:fa:83:35:
        d4:8d:48:a8:43:99:9f:95:dc:1f:38:a9:d7:a9:7a:fd:6c:25:
        af:a5:e5:52:5b:db:9a:64:f1:78:0c:5e:05:f4:df:ea:0d:aa:
        c5:3a:9e:e8:65:38:1c:c4:53:77:48:a9:f8:84:2b:cb:75:1c:
        62:56:a9:85:8e:07:ac:da:9c:af:81:db:87:d9:5f:21:9e:09:
        ef:a5:d6:45:2c:af:d9:9a
SHA1 Fingerprint=78:F0:0B:B6:B0:59:45:31:DE:4D:54:72:2D:DE:3F:1E:D7:44:64:C7
sha256
Fingerprint=6C:17:A0:5F:0C:77:B9:6A:B0:39:A3:F8:50:58:73:1E:EB:02:F5:2F:B6:6D:87:D1:9B:93:D2:27:8D:82:64:99
sha512
Fingerprint=2C:01:B8:F9:DD:B3:7E:AD:3E:BD:33:D9:4A:D1:B1:B9:A5:38:A6:E9:2E:70:23:C3:A1:F2:49:32:F1:F8:B2:26:DB:03
:C2:F3:D9:08:86:47:AB:9A:F7:40:1E:0B:2E:AA:2D:89:2F:59:86:77:FF:B5:BA:77:11:E2:E0:C9:96:48
```

B.2. Certificado Raíz TSACI CA01

```
        Version: 3 (0x2)
        Serial Number:
            59:86:e3:50:e0:32:82:c1:a3:d7:fa:db:19:8b:81:1a:e1:3c:a7:27
        Signature Algorithm: rsassaPss
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        Issuer: CN = COLORIURIS CA01 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Validity
            Not Before: Jan 26 12:10:21 2026 GMT
            Not After : Jan 26 12:10:20 2046 GMT
        Subject: CN = COLORIURIS CA01 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
```

```
            Public-Key: (4096 bit)
            Modulus:
                00:9c:a5:d4:13:8c:0b:e1:29:ed:79:70:67:4f:ea:
                2b:be:48:86:c1:83:9b:33:97:36:e4:eb:0b:1e:3e:
                46:c4:17:4f:07:7b:0d:0b:6a:02:7e:44:18:02:2c:
                ba:99:89:c9:26:d5:3d:1a:6a:7e:7f:76:a3:dd:7c:
                98:7f:0e:68:e9:d2:59:01:b8:ad:81:a7:b1:56:5f:
                95:7e:f7:8d:93:9d:bf:5a:dc:38:06:13:63:df:6e:
                44:c2:d5:dd:45:41:ad:e3:46:e7:37:f5:57:11:a0:
                0c:37:4f:26:99:6e:f2:b8:0b:7e:32:63:6d:cf:b2:
                f9:15:97:c8:b4:47:f2:e0:7d:ab:e5:30:de:41:4c:
                f9:de:c6:b5:66:3b:78:f3:77:0c:88:6c:39:18:51:
                36:2d:70:bc:11:af:45:d3:38:34:55:24:35:c1:39:
                63:4a:8b:a5:b5:40:b7:95:d7:cb:42:37:d7:7c:0d:
                3f:84:88:5a:20:00:34:fd:31:56:9d:13:91:ec:0e:
                59:0e:4b:ca:53:33:dd:94:a7:45:26:36:96:3f:e3:
                1f:07:d8:fb:0b:03:aa:d3:21:58:e4:a7:1d:62:1d:
                6f:28:fd:0f:bb:6a:a8:63:d8:a2:84:b6:05:1a:00:
                98:e3:d1:da:c4:9a:82:43:83:98:04:cf:68:ab:82:
                5f:10:6c:be:9e:08:b7:18:44:13:50:3d:81:fb:3c:
                73:70:2f:d9:29:72:10:74:8b:d3:42:7f:4a:ba:5f:
                b8:a3:e2:7b:00:1f:41:0a:d6:6f:b4:9f:94:47:1d:
                d8:cb:48:ca:12:7c:83:fc:60:fd:4f:b1:9b:63:63:
                a5:1a:d4:68:ec:3a:12:9c:fe:65:54:e7:e4:fe:85:
                99:c2:a7:56:dc:ad:84:9c:61:80:38:2a:4f:7a:9f:
                6d:0d:55:0a:2c:f1:15:ce:2a:ed:ae:43:26:6a:28:
                1f:38:b7:36:04:b4:a6:9b:7f:3f:8b:3f:50:ef:89:
                80:5c:5d:13:e3:b0:92:71:05:ef:8f:d3:62:b7:1c:
                60:2d:02:54:1c:54:1e:b5:80:c3:69:63:73:56:f0:
                30:91:c5:bf:ec:11:c4:39:68:0f:b5:17:eb:07:8d:
                5b:60:58:fd:0e:0a:ba:08:91:c9:43:d7:7b:3f:a8:
                d5:23:86:b0:c2:93:5f:55:93:19:73:e0:9c:49:57:
                13:d2:cd:c1:69:92:26:9e:81:18:bb:c8:dd:4d:31:
                43:8b:60:66:9f:e9:66:c6:45:3c:87:3d:43:ab:eb:
                c6:4f:fc:e0:04:20:a0:be:c6:ea:8d:ba:8d:9f:84:
                80:f2:0c:3a:74:ce:92:e9:87:27:e8:21:c1:b2:31:
                59:1a:27
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://cipsc.coloriuris.net/politicas/
            OCSP No Check:

            qcStatements:
     0:d=0  hl=2 l=  23 cons: SEQUENCE
     2:d=1  hl=2 l=  21 cons:  SEQUENCE
     4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
    14:d=2  hl=2 l=   9 cons:   SEQUENCE
    16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 Subject Key Identifier:
                61:61:40:A8:58:9C:7F:FC:9A:3C:A8:CC:9B:60:D2:F5:68:B2:9E:75
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
    Signature Algorithm: rsassaPss
    Signature Value:
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        08:e6:08:74:13:4f:6e:e8:d1:55:eb:b9:9a:fe:da:88:b9:60:
        46:fc:fc:08:a4:5b:36:3c:3b:80:27:84:d0:d1:f1:21:4f:ec:
```

```
        d2:19:14:c9:e6:fb:22:57:36:d8:0d:39:62:f9:58:dc:bb:ba:
        8f:64:5a:95:34:4b:08:5e:f4:ef:ce:39:56:c9:44:ea:10:1a:
        ad:9f:7d:ff:63:34:7e:b0:7b:28:58:e1:59:5a:91:b9:e0:05:
        e2:cc:3d:0c:9d:39:f2:24:84:fc:da:99:58:7d:a8:7a:e0:d5:
        20:5e:bc:17:61:c1:94:1b:32:e7:31:04:4e:28:f5:ba:4c:b8:
        18:d0:a4:91:34:cd:9f:11:f4:60:99:17:8f:8e:ec:e5:54:0a:
        57:22:59:91:9e:c1:b4:e8:ce:44:0b:30:42:09:b6:81:9d:da:
        54:ae:42:09:5b:b5:86:7d:79:0c:66:79:5e:d2:f0:66:1a:5d:
        d2:b3:82:f7:a3:a4:7d:43:6e:be:38:98:f2:63:b7:75:1d:89:
        6a:cf:b8:89:f7:ad:34:aa:42:e1:11:0b:0e:08:76:b1:2a:48:
        1e:f8:44:0f:f2:c9:70:e9:58:f3:ac:0b:61:08:90:73:46:fa:
        dd:d4:43:97:7a:26:4c:71:02:df:02:92:eb:f0:83:bb:05:80:
        d1:ae:96:a7:d4:64:7d:ae:ee:86:8d:ad:b6:bf:6d:86:f1:99:
        85:f5:0c:fb:86:9a:c7:d1:54:5a:7a:58:fe:29:dc:cd:96:69:
        cb:47:4d:80:36:66:61:86:36:97:02:85:9e:dc:9b:dc:5c:d7:
        93:23:f9:f2:9e:8a:43:0b:f2:1e:19:ec:cc:57:23:41:ac:b8:
        fc:69:de:34:8c:bb:69:dc:c8:18:73:92:b2:36:5f:10:7b:0f:
        f6:63:30:be:11:03:ad:e2:cd:8a:21:7f:43:30:c7:85:28:d0:
        9b:08:6d:1d:74:9f:a8:ea:af:b9:92:de:b9:f5:1b:d5:4f:6f:
        b5:da:f4:e9:fe:94:33:c5:ad:39:5d:da:9d:86:f7:cc:6e:f1:
        93:a2:96:07:9e:ae:bc:c2:56:60:bf:52:c4:ee:b1:3a:23:61:
        45:0c:d5:f2:4b:ca:d9:9b:9f:50:ed:87:ca:1e:ff:36:79:9f:
        a8:93:8e:df:95:57:15:ab:e8:63:a8:84:4e:eb:a0:7d:41:48:
        e8:a3:cb:f3:08:fc:0f:f8:6e:dd:3b:45:34:64:51:38:40:ce:
        f2:f9:4a:95:70:71:5f:34:c4:e1:b5:1a:35:7c:6a:94:10:80:
        fe:28:58:ed:f5:dd:95:1d:86:0d:cf:46:15:7f:4c:ba:63:2b:
        78:67:6c:2e:11:ae:db:43
SHA1 Fingerprint=3E:F9:FB:A6:A1:22:AC:51:5B:6F:0A:40:45:9C:A6:BE:4E:41:EE:EF
sha256
Fingerprint=24:45:E9:BC:73:A7:2B:9C:17:FB:BA:A2:B4:81:89:0B:8C:C8:BD:2D:E2:71:78:EF:67:C9:89:61:BB:DF:AA:CF
sha512
Fingerprint=7A:6A:DE:CA:AF:67:8C:D6:19:46:7A:B6:77:22:AE:46:6A:F3:51:50:BB:F5:0D:EF:00:0F:03:95:B5:93:86:C5:E5:84
:79:0B:63:85:DB:52:D5:E9:AD:83:F8:10:D0:A5:E8:97:90:AA:4D:8E:9E:AD:CF:B4:90:2B:8C:24:B5:38
```

B.2.1. Certificado de emisión de sellos electrónicos cualificados de tiempo TSU01 (RSA 3072 bits)

```
        Version: 3 (0x2)
        Serial Number:
            1c:40:9e:1d:41:12:71:41:f2:f4:10:f3:29:c3:b7:9a:79:d6:97:f9
        Signature Algorithm: rsassaPss
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        Issuer: CN = COLORIURIS CA01 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Validity
            Not Before: Jan 26 17:42:10 2026 GMT
            Not After : Jan 26 17:42:09 2036 GMT
        Subject: CN = COLORIURIS QTSP TSU01 - Emisor de sellos electronicos cualificados de tiempo,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (3072 bit)
                Modulus:
                    00:97:ca:8f:13:46:bf:d5:97:8d:9c:23:2e:74:27:
                    e9:9a:cc:4c:a1:7d:51:76:2d:07:1f:64:a3:4c:89:
                    0a:e2:5b:ee:75:9e:a6:c0:a4:f8:d8:11:6e:4b:c0:
                    f8:eb:6f:dc:8d:7b:a0:c3:42:7a:cb:2b:10:e3:b4:
                    3c:f8:a1:64:f4:30:d0:82:9c:f0:b8:26:f7:9e:26:
```

```
                    1c:c2:3b:de:bf:ef:91:f3:c9:25:81:b7:7c:f2:4f:
                    76:6a:6a:b1:0f:01:52:1e:af:3c:03:a2:cb:26:bd:
                    b3:ed:88:66:c9:10:67:1e:af:eb:2f:12:f7:67:3b:
                    f3:5c:bc:6f:f6:d8:0f:7c:59:4d:b9:40:ae:6f:97:
                    52:9f:63:a1:e0:12:c0:44:71:c5:08:32:78:69:49:
                    39:36:a0:ba:a0:83:82:53:66:36:cc:46:d9:ec:9c:
                    97:cc:b3:62:d2:3e:a2:49:37:2a:9e:91:dc:14:13:
                    58:8d:fc:67:01:38:47:62:59:d3:38:7c:18:82:a7:
                    6e:40:0e:74:92:14:76:52:d2:4f:c9:88:a5:be:07:
                    7b:05:fb:a7:5c:64:30:55:6d:dc:3e:d1:20:fd:ce:
                    d3:24:80:bd:ee:3b:a1:52:61:32:98:a3:3c:69:e0:
                    5e:db:e2:cb:3b:9c:81:a3:a2:09:37:cd:50:78:4c:
                    21:12:1c:58:0c:05:42:b8:2d:6b:a5:ce:8d:7f:2f:
                    43:57:df:ad:e4:ef:f6:72:b2:93:4b:4a:63:30:45:
                    57:0c:1b:ec:e1:c8:19:c1:f7:d2:bf:75:51:9f:90:
                    60:fb:3b:ec:ec:4c:e9:3b:09:b0:f5:89:4b:44:63:
                    04:6f:cb:0c:2c:67:44:4d:a7:ac:37:16:e7:77:10:
                    2c:ac:56:bf:c5:8a:36:5e:c6:7b:00:3e:ef:cc:37:
                    0f:e5:9d:d5:97:ca:78:a4:ab:4b:e6:c6:71:6b:7b:
                    68:33:b0:be:b5:9d:f7:6a:6b:8b:68:db:5a:9c:62:
                    a4:b6:73:20:a8:10:6d:1a:08:95
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                61:61:40:A8:58:9C:7F:FC:9A:3C:A8:CC:9B:60:D2:F5:68:B2:9E:75
            Authority Information Access:
                CA Issuers - URI:http://ca01.coloriuris.net/certs/coloriuris-ca01-tsa.crt
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text: Certificado de emisión de sellos electrónicos cualificados de tiempo
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca01.coloriuris.net/crl/coloriuris-ca01-tsa.crl               CRL Issuer:
                  DirName:CN = COLORIURIS CA01 TSA, OU = Prestador de Servicios de Confianza,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                C9:DC:E7:8C:14:B1:EB:F1:7D:A6:D4:3F:3A:2A:25:C8:0F:66:7B:65
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
    Signature Algorithm: rsassaPss
    Signature Value:
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        53:57:79:7c:1a:4f:2a:63:5c:cf:ef:eb:2a:1a:66:9b:01:57:
        e9:ba:a4:f0:f5:15:5c:62:9a:62:d0:3f:03:99:5d:a5:3e:d2:
        04:0f:9e:ef:98:41:5a:8a:ab:5b:c7:52:cb:6b:7c:74:b3:e2:
        44:35:b3:a7:9c:9c:da:f9:18:ed:05:ad:e6:12:93:82:f8:9b:
        a8:46:3d:98:42:c3:ac:15:23:ec:99:49:dd:03:53:b8:17:2a:
        84:69:74:3f:65:02:24:b4:48:00:41:30:c6:04:f0:2c:55:ae:
        6b:38:90:fc:c1:a8:65:b3:b3:50:fd:08:17:f8:02:b1:40:29:
        1f:4a:57:fc:30:6d:60:81:6c:b9:f5:98:04:69:92:9d:d8:d8:
        6d:f3:5a:c5:96:9f:b3:87:a0:fd:d7:70:32:fd:6a:12:6e:25:
```

```
        b7:32:7b:fd:f5:d8:e5:06:76:cc:27:2b:b0:66:7d:39:c3:94:
        51:75:a0:26:5b:71:9b:22:be:67:ca:dc:88:5a:35:80:aa:7e:
        7d:ff:a8:d1:24:9d:3f:b4:f7:b0:95:a4:ed:d4:f4:12:96:24:
        c1:a1:40:02:5f:c3:d8:10:d3:a0:dd:7d:1e:ff:a4:b0:c7:e4:
        b5:88:01:27:71:5b:6f:b6:2f:e8:95:ea:51:1f:98:aa:bf:ea:
        31:17:05:a4:6e:db:82:ed:8f:a0:fa:13:cd:30:93:c2:98:26:
        37:98:70:04:b6:81:61:18:ed:1e:cf:96:5d:b3:6f:7e:c9:25:
        fa:8a:3a:8a:41:48:e2:90:8a:33:e8:1b:52:79:a6:b3:50:7c:
        56:55:75:4c:f4:74:ac:72:dc:1a:fa:6d:1b:d0:7a:e3:22:fb:
        cf:aa:ef:41:c7:4b:89:c4:fc:c2:5a:12:f5:ce:a0:cd:e9:bc:
        b8:ba:e3:87:7e:0d:42:71:bf:69:38:fb:e1:49:ca:59:ff:3b:
        24:05:13:92:e8:7a:f8:4f:e4:97:64:ea:f0:f3:d3:aa:54:3c:
        a8:c3:bb:c2:40:c7:e3:3c:63:14:d8:a5:a7:ab:ec:07:a3:85:
        e4:f7:fe:a8:18:4b:ec:d0:d4:95:1d:27:8e:7b:83:1f:92:8c:
        29:6a:2a:17:11:3d:25:01:e5:f1:9b:87:04:57:7b:8f:43:7c:
        c5:2c:01:6a:59:64:31:87:4c:1d:7e:02:0d:0a:a3:af:52:3b:
        2d:c2:e3:6b:b9:72:c6:21:8f:cb:73:d5:e1:f8:df:6b:53:69:
        4f:24:f5:af:08:a1:90:45:27:7e:2b:f8:5c:ba:22:8f:f3:a5:
        87:8c:68:a8:f5:95:82:37:cf:1e:0c:53:a7:0e:54:13:e5:14:
        33:a0:5f:e2:f6:7b:f4:86
SHA1 Fingerprint=9A:BF:64:92:64:FD:1E:09:51:39:37:5F:19:5B:27:AC:B9:B1:4B:DD
sha256
Fingerprint=6F:65:17:EE:94:6B:4B:6E:A2:D4:2F:56:EC:7A:72:57:1D:41:93:5A:AE:2D:BD:77:98:DE:B4:F1:29:BD:46:85
sha512
Fingerprint=89:A1:77:1C:22:E4:33:63:B5:05:54:39:BA:70:79:89:E9:CB:73:AF:64:F1:98:89:8C:39:2A:6D:FE:27:71:A9:35:F7
:46:94:1E:58:69:F8:CD:4B:C4:7B:6B:B0:C0:CF:C1:11:B3:4C:0F:6B:AA:A5:4C:0A:82:E6:22:EE:2E:AF
```

B.2.2. Certificado de emisión de sellos electrónicos cualificados de tiempo TSU03 (RSA 4096 bits)

```
        Version: 3 (0x2)
        Serial Number:
            15:a1:2a:06:60:8f:f9:90:02:58:09:fb:5b:a4:e8:83:74:91:25:2e
        Signature Algorithm: rsassaPss
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        Issuer: CN = COLORIURIS CA01 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Validity
            Not Before: Jan 26 17:44:28 2026 GMT
            Not After : Jan 26 17:44:27 2036 GMT
        Subject: CN = COLORIURIS QTSP TSU03 - Emisor de sellos electronicos cualificados de tiempo,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:cb:64:cb:c9:8d:bd:5b:70:a3:5e:88:0b:66:79:
                    78:6f:cc:2a:e5:24:68:fd:8b:b8:8a:30:dd:8c:e4:
                    54:7b:2c:57:ef:0e:5c:a5:fb:da:1e:70:af:56:0b:
                    ff:c4:9c:e3:d0:31:f7:b6:9e:e4:ec:c3:89:48:96:
                    25:7c:70:47:3a:18:0b:81:13:cb:3c:d0:20:4c:74:
                    a7:dd:75:b4:23:1f:74:98:b0:d1:b5:91:d2:c9:dc:
                    52:c6:f7:7e:2c:aa:cb:8b:0a:d7:16:70:a9:91:a9:
                    86:04:15:1c:7b:45:80:9c:86:c9:69:b7:da:89:3a:
                    c1:e8:27:8e:48:40:7e:47:4d:1c:e7:d3:b2:21:12:
                    fa:1a:03:2d:a9:3b:0c:80:06:4e:81:e1:61:d1:58:
                    03:79:03:4b:18:86:48:b9:d0:f6:29:82:15:66:f0:
                    25:2d:72:70:fd:10:41:1a:b9:c1:ab:fa:26:04:82:
```

```
                    c2:39:67:29:d5:23:65:8d:6a:58:70:c8:b4:80:e1:
                    78:ae:c9:19:09:89:80:c1:21:26:fa:65:cb:22:34:
                    bd:64:0d:fb:a3:26:83:81:00:74:69:cc:5e:dd:03:
                    f5:86:e3:4f:be:09:bb:c2:71:9d:68:5b:32:0e:df:
                    26:2a:3a:41:e6:8e:74:17:b3:26:80:25:f8:70:44:
                    68:bc:83:7f:d4:7c:8f:8f:65:93:39:c8:ca:51:82:
                    7e:b2:1e:e6:2e:b9:81:88:12:d6:82:5b:72:aa:9a:
                    7b:ef:f0:d3:d8:94:8d:2c:11:8a:2e:40:01:ec:bc:
                    b7:85:63:47:13:36:c1:fe:3a:42:5f:db:40:26:ba:
                    31:02:73:36:25:df:ea:cf:81:a5:1a:ad:d6:0e:9a:
                    a1:cd:7b:50:86:e2:19:3f:39:19:28:9e:a9:74:84:
                    32:7b:2b:3c:83:56:ac:ac:13:9c:ce:d9:ec:e5:62:
                    e1:d7:9f:4c:ec:31:65:9c:de:75:97:02:99:68:94:
                    ba:2e:8d:39:c5:c9:8d:04:91:08:22:8f:f2:1b:52:
                    bb:bc:70:2e:0d:d1:54:e2:c7:80:9c:7d:0e:e9:dc:
                    73:a5:c4:f8:a6:b8:21:c4:8f:bf:64:99:11:76:8f:
                    e9:04:34:f0:d0:6d:ad:05:ae:0b:1b:20:d6:e5:5f:
                    85:88:a8:92:18:dc:8a:f7:4c:ab:4e:bf:8e:5e:51:
                    80:1f:fa:f4:4c:68:39:a5:47:0d:89:29:67:7f:be:
                    7f:39:58:b6:09:e7:95:75:4f:ae:96:a5:3a:8d:09:
                    75:da:58:cc:24:be:71:ec:72:00:ae:c5:79:f5:5a:
                    0b:87:f0:ef:3f:7c:9b:59:2b:1f:90:e0:af:1f:02:
                    8c:c2:cf
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                61:61:40:A8:58:9C:7F:FC:9A:3C:A8:CC:9B:60:D2:F5:68:B2:9E:75
            Authority Information Access:
                CA Issuers - URI:http://ca01.coloriuris.net/certs/coloriuris-ca01-tsa.crt
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text: Certificado de emisión de sellos electrónicos cualificados de tiempo
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca01.coloriuris.net/crl/coloriuris-ca01-tsa.crl               CRL Issuer:
                  DirName:CN = COLORIURIS CA01 TSA, OU = Prestador de Servicios de Confianza,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                CE:3B:A4:31:6F:59:F8:3C:E9:02:8E:48:22:9E:8F:21:74:75:72:BA
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
    Signature Algorithm: rsassaPss
    Signature Value:
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        0c:b3:56:99:85:20:fa:8d:e8:d0:76:87:99:e8:d5:89:d2:08:
        10:dc:2e:b7:7a:7c:e3:bb:02:c5:db:ff:eb:e3:8a:53:54:83:
        b1:ef:6f:dd:87:57:b8:4b:bb:49:71:b8:4a:87:5d:dc:4c:ba:
        2a:cf:34:03:2c:e8:db:65:2d:19:3e:be:f3:90:39:29:95:d4:
        b3:85:44:5c:25:8f:8f:bb:e2:71:2e:3a:76:7a:19:b7:e0:d6:
        f9:4d:ef:10:21:62:77:5f:10:3e:90:46:3b:89:ae:d0:54:a8:
        67:cb:61:a3:16:71:d5:61:cb:10:34:db:59:d4:db:82:22:65:
```

```
        1e:bb:9b:d7:cd:a0:94:85:ca:cb:c6:c0:86:bf:9e:b9:8c:19:
        9d:b2:c5:17:3b:73:62:0f:80:71:2e:47:9d:9a:a3:61:6b:d5:
        98:a1:a8:d9:b2:dd:29:08:57:96:22:1d:2b:81:d6:05:f3:1c:
        44:b3:c7:14:2f:27:b0:db:1d:6c:a9:f5:f8:f2:ef:7d:e9:65:
        14:fd:27:69:fa:b0:d3:e8:36:52:ee:b7:33:16:04:2f:e2:c9:
        34:e4:af:11:ed:06:b7:2c:4f:2f:c1:f6:92:56:51:9b:ce:40:
        6c:48:35:d7:b6:73:ca:a0:e3:37:99:69:a8:e7:ff:68:26:cf:
        d3:05:64:d5:f3:09:33:7a:f8:69:ed:ae:b5:21:ae:f1:48:a2:
        00:78:59:5c:56:79:99:6c:5e:4a:8b:5b:dc:a2:93:55:9e:58:
        ce:a5:72:1b:09:eb:a9:6a:d3:33:24:97:fb:a8:19:68:d7:4c:
        c1:80:cf:5e:77:4c:1b:c6:32:5a:71:15:9c:ff:fa:63:b1:03:
        86:a3:43:19:32:be:9e:c5:e4:a8:8a:1f:46:ae:fb:96:b9:e3:
        c5:68:d8:0f:c0:74:1d:61:e9:db:80:5d:79:9d:b3:66:fe:9c:
        5a:35:b3:95:d0:06:23:ee:72:28:64:d1:e5:e7:31:00:8c:8f:
        0f:39:a0:57:d1:bd:c9:33:f0:ab:a1:55:39:78:62:15:71:58:
        2b:20:c7:5c:74:ec:38:42:e8:50:84:01:75:21:62:6b:53:a4:
        cc:4f:cd:f5:c8:ed:aa:9e:e6:04:9a:e6:bb:af:3b:44:41:11:
        43:47:17:a6:88:97:3e:78:9e:2e:80:a5:96:a7:7a:52:4d:20:
        12:8f:0d:20:ab:3d:d8:cb:25:84:ab:7f:94:92:4c:9c:a5:5a:
        59:76:b5:90:f2:ed:ea:69:c6:a3:78:36:8e:71:1d:8d:e1:07:
        15:53:22:5b:6e:f7:03:be:5a:37:09:ed:0b:64:fd:a0:37:32:
        f1:ab:37:eb:35:b8:37:d9
SHA1 Fingerprint=5A:AE:96:66:F0:2E:34:45:C0:F4:21:26:F9:9B:11:8A:34:75:D3:2F
sha256
Fingerprint=F8:7E:51:49:6F:C0:58:F6:D1:7C:8F:A3:9D:5D:C5:AD:C5:B7:F7:A2:E8:CE:71:A6:1D:72:B0:4D:0D:DD:28:8F
sha512
Fingerprint=FC:37:76:3C:BF:A5:DB:D4:8B:DE:69:32:E1:C5:E1:1C:FF:45:FA:16:DC:7F:08:C2:9C:A0:14:17:53:FB:CA:A2:DD:FF
:B6:A3:E4:FE:56:7B:0B:FA:2A:39:CE:29:2F:CA:0A:86:83:2B:F2:AB:F8:CE:CE:33:AE:E2:BD:33:83:A6
```

B.3. Certificado Raíz TSACI CA02

```
        Version: 3 (0x2)
        Serial Number:
            0e:10:3f:5a:90:ee:a8:9c:fc:96:bc:a3:0f:4e:cf:0e:f4:a1:c5:cb
        Signature Algorithm: rsassaPss
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        Issuer: CN = COLORIURIS CA02 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Validity
            Not Before: Jan 23 18:56:22 2026 GMT
            Not After : Jan 23 18:56:21 2046 GMT
        Subject: CN = COLORIURIS CA02 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:de:4a:1c:78:c5:36:b3:f6:22:26:c3:24:49:d5:
                    5d:b8:10:57:60:a2:02:00:08:0e:5c:c4:ff:4a:f9:
                    02:da:86:6f:3d:aa:47:7d:5d:8d:15:6d:fd:71:6d:
                    ae:4f:96:be:3b:9d:04:ae:e4:58:ca:58:c3:b0:db:
                    6d:64:63:04:8d:42:23:47:44:4f:5c:fd:68:20:05:
                    92:82:d6:f9:31:15:97:56:1f:d3:66:2c:d2:af:32:
                    83:6a:b3:63:ae:08:a7:ad:c6:90:42:13:bc:f3:22:
                    40:7f:d2:6f:c3:d2:eb:0b:a8:e4:13:4e:59:e0:ec:
                    ad:50:6e:87:47:76:37:90:53:41:1d:1f:66:08:6f:
                    7b:08:9d:8f:d3:89:fe:4a:0a:89:3d:67:d1:2c:3f:
                    77:eb:ea:de:95:01:c7:21:21:d7:3b:78:ba:0b:ec:
```

```
                75:71:2e:21:37:59:d2:77:ee:ab:af:8b:9a:c5:d7:
                11:7f:06:c9:78:4e:07:0e:55:bd:0d:3b:68:68:53:
                d7:7d:b6:75:e7:52:00:46:67:cb:77:f1:5b:a5:1c:
                16:0d:00:93:ac:ca:57:dc:0c:96:1d:d6:37:f8:e7:
                6a:8b:cd:ad:c6:b4:67:67:d7:66:ea:27:7e:bc:88:
                4e:61:a1:32:f8:6d:70:5f:6d:b6:56:9c:89:d2:64:
                53:16:da:cf:b5:bd:99:10:63:61:67:39:db:5d:01:
                21:24:c1:d2:20:78:2b:74:03:3f:6d:93:ce:a8:58:
                e1:53:1e:88:c5:92:83:fd:21:67:aa:6f:05:bb:93:
                e2:68:a2:38:fa:97:9c:2c:c4:34:01:61:b4:f8:de:
                4b:03:43:55:1a:21:9e:da:64:6f:c6:ea:be:41:cd:
                43:47:b6:39:a5:c3:38:5a:69:16:62:ac:5d:37:b1:
                9f:f8:7a:be:83:f5:3e:13:bc:db:3e:67:3e:66:ee:
                e4:bd:12:52:13:50:8e:53:cf:07:1c:c0:e0:f2:71:
                fd:15:df:3f:d7:7b:0b:a9:3d:8d:b5:a8:be:07:80:
                21:04:4a:a3:f0:9d:2e:d6:b2:5a:35:a3:32:bd:55:
                0f:16:d7:5a:ad:c0:a9:80:02:e3:57:39:0e:65:3a:
                1d:9e:8b:4e:9c:f0:b1:7d:a9:d1:c6:10:12:e9:5f:
                11:ce:ee:7f:b9:c9:00:f1:79:7d:53:80:7d:3e:2f:
                1a:a8:91:2b:e4:05:57:be:a2:2f:b3:12:41:84:d2:
                ad:33:b1:6f:c3:a3:dc:40:90:68:6f:39:0e:5e:da:
                07:2f:45:86:e9:95:1b:54:c2:eb:0d:c4:3d:a8:91:
                af:c1:20:df:a3:3c:9c:a9:93:51:f9:dc:44:17:6f:
                05:02:b1
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints: critical
            CA:TRUE
        X509v3 Certificate Policies:
            Policy: X509v3 Any Policy
              CPS: https://cipsc.coloriuris.net/politicas/
        OCSP No Check:

        qcStatements:
 0:d=0  hl=2 l=  23 cons: SEQUENCE
 2:d=1  hl=2 l=  21 cons:  SEQUENCE
 4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
14:d=2  hl=2 l=   9 cons:   SEQUENCE
16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

        X509v3 Subject Key Identifier:
            BE:AC:4C:60:04:A3:4C:5F:FC:6A:41:E0:BD:A2:97:31:97:06:2F:FE
        X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
 Signature Algorithm: rsassaPss
 Signature Value:
    Hash Algorithm: sha512
    Mask Algorithm: mgf1 with sha512
     Salt Length: 0x40
    Trailer Field: 0x01 (default)
    7d:8a:eb:61:66:17:f6:55:02:cc:e0:1a:a1:1d:6c:56:0f:40:
    90:bb:0b:27:9b:cc:56:d7:49:a7:a2:4c:5e:aa:34:fd:2d:c6:
    ee:b1:c2:bb:44:09:f4:15:1c:1f:74:b1:11:06:d8:75:ee:e0:
    32:84:b1:cd:d3:91:23:0d:c4:11:74:da:93:5b:23:f9:c9:54:
    a0:cc:0c:05:41:5a:90:95:63:91:ee:e0:a6:d2:fe:93:fc:69:
    2f:98:f5:2c:fd:1e:ff:81:e3:fe:31:db:cf:e1:87:81:53:4a:
    21:fb:e5:d6:ea:35:1f:bf:fb:1c:ca:00:fa:dc:02:75:c2:20:
    c4:92:38:4f:f2:73:30:35:b2:f9:9c:5b:f4:ae:f2:00:24:de:
    18:cb:ef:a8:a3:da:bf:e9:2c:6d:08:81:97:da:e2:2a:4d:d9:
    4c:f5:f8:b0:d6:28:b7:bf:aa:cb:07:0e:7d:61:10:24:aa:e3:
    31:d2:b7:42:b1:35:fb:45:18:02:41:e5:19:20:f2:26:73:86:
    5e:03:3e:d5:0a:86:ac:f5:5d:e4:9c:40:54:6e:27:46:8d:34:
    78:9b:ba:65:6e:67:5d:c8:0f:d5:bc:21:66:7b:fc:25:5b:12:
    74:a4:47:83:eb:e7:39:a0:97:1c:dc:28:57:dd:37:44:1e:5d:
    a8:88:04:a7:40:a2:12:76:48:61:36:e9:5e:21:35:2b:f6:8d:
```

```
        78:05:ca:ec:38:2f:c9:07:22:84:9e:e8:7a:c3:b2:fb:25:b8:
        a4:48:94:03:74:24:7c:87:42:75:9c:91:5d:17:4b:61:76:ef:
        79:00:b9:df:81:e3:4a:c6:9a:1d:88:44:bc:c5:fa:7d:0c:2f:
        3d:ce:65:70:09:b6:4d:fc:a5:84:b5:a1:1b:f0:08:27:ba:40:
        ae:c0:80:56:e1:21:9b:1b:94:a5:c4:fe:5c:1a:88:27:a6:2e:
        4c:80:c5:73:3f:a5:17:5a:93:5b:67:66:e0:61:f2:d5:14:e1:
        17:aa:63:9d:9a:50:01:35:f0:9e:d3:96:43:e5:66:88:ff:b3:
        5b:66:10:1c:3d:81:ad:ec:3d:4d:ab:2f:01:d0:c4:be:a7:56:
        d3:8d:f3:e1:9f:55:da:f0:d3:f6:43:61:c9:73:a0:38:f7:ed:
        b7:e9:39:c9:ac:b1:15:b8:f0:99:ed:5e:11:5f:cf:52:11:0b:
        94:7e:a3:18:1a:1c:4b:f4:73:dc:62:29:61:05:16:e8:9c:2b:
        83:41:84:13:9a:15:d6:da:d5:ee:6b:67:7b:93:b2:8b:33:f8:
        26:d2:ef:16:77:b4:44:ee:9d:2c:12:ab:e6:83:a2:7c:41:b1:
        da:a7:9d:ee:80:16:1d:2d
SHA1 Fingerprint=DE:F3:40:CA:F5:FA:B3:04:7A:79:84:C1:83:9B:77:72:B7:D2:B5:A3
sha256
Fingerprint=87:57:58:70:23:C2:F7:C4:52:85:0F:17:6E:F2:EE:CA:D7:49:1A:96:F4:A2:DD:D2:24:E1:49:CF:E0:EF:29:BC
sha512
Fingerprint=65:53:22:C3:39:7D:37:BD:C8:DF:4C:74:85:35:A6:3C:CD:95:80:6D:69:CD:11:DF:63:FB:D5:72:E2:C9:84:B1:36:15
:67:34:63:99:07:8A:AE:3C:74:4B:84:6A:30:55:46:3D:A9:05:A7:9E:5E:35:FA:F2:25:4B:17:7F:B3:13
```

B.3.1. Certificado de emisión de sellos electrónicos cualificados de tiempo TSU02 (RSA 3072 bits)

```
        Version: 3 (0x2)
        Serial Number:
            47:24:5c:39:a1:01:84:81:39:24:00:63:31:0e:07:86:53:82:27:92
        Signature Algorithm: rsassaPss
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        Issuer: CN = COLORIURIS CA02 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Validity
            Not Before: Jan 26 17:59:12 2026 GMT
            Not After : Jan 26 17:59:11 2036 GMT
        Subject: CN = COLORIURIS QTSP TSU02 - Emisor de sellos electronicos cualificados de tiempo,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (3072 bit)
                Modulus:
                    00:de:aa:eb:c8:19:e2:f2:ff:98:8e:37:11:53:e7:
                    e5:61:08:7a:e7:da:92:6b:14:2b:49:51:34:59:39:
                    14:f5:a1:6a:79:0d:2e:bb:d9:f2:b1:2d:0e:cf:10:
                    ab:1c:cf:84:5e:64:db:8a:f3:24:c1:7e:5b:87:4f:
                    4b:11:db:0a:d2:2b:5c:32:ad:3a:18:d1:c4:89:50:
                    c1:66:d4:fc:93:5e:71:b0:6f:d5:9d:f6:83:7c:01:
                    8b:ce:49:8f:7a:31:78:a9:d3:45:99:4c:89:95:9f:
                    9b:92:d9:19:e1:b0:29:40:c2:64:ed:76:d5:03:4f:
                    f4:95:62:0e:97:e4:30:48:60:dd:e4:1d:cf:cc:f6:
                    78:4b:e7:be:b9:a4:92:8b:90:f4:4d:63:18:d6:e2:
                    b6:62:1e:7b:6a:94:2c:97:7d:c1:f4:2e:bd:b6:84:
                    23:2c:cd:5d:af:8c:42:bc:3f:c6:34:57:74:ce:f4:
                    5e:07:1d:19:f3:88:72:26:2c:ed:ed:9a:63:45:83:
                    83:a5:7d:7c:fb:7e:df:a3:c2:f0:9d:9e:86:d2:74:
                    94:74:3b:58:9a:f8:75:cc:5a:ed:12:6c:f6:af:f2:
                    c2:a0:91:7b:20:b2:8b:4c:ef:a2:30:da:9d:6d:1c:
                    32:2a:9b:ea:3c:96:7b:a2:b5:43:1a:1b:de:57:7f:
                    15:3b:e8:0f:66:43:4a:37:71:cd:06:51:28:2f:04:
```

```
                    30:88:c1:31:7d:ac:60:07:3a:3b:d4:f2:0c:34:b0:
                    02:d8:5a:80:a6:25:3a:91:87:45:05:52:26:5d:c9:
                    d7:8b:2b:30:e2:7e:61:0f:84:d2:f9:ad:8b:44:01:
                    50:ad:ff:cb:c4:b1:0a:da:d3:2a:43:31:a2:3b:66:
                    d3:ce:cc:79:9f:7b:d1:8b:01:47:d5:54:6c:85:94:
                    c9:04:08:37:46:ce:b3:4a:b5:ba:9a:db:bb:c0:45:
                    a5:79:18:dd:13:68:5a:fb:bd:07:09:37:6f:b3:f3:
                    16:16:8d:92:8b:29:c3:7b:46:79
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                BE:AC:4C:60:04:A3:4C:5F:FC:6A:41:E0:BD:A2:97:31:97:06:2F:FE
            Authority Information Access:
                CA Issuers - URI:http://ca02.coloriuris.net/certs/coloriuris-ca02-tsa.crt
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text: Certificado de emisión de sellos electrónicos cualificados de tiempo
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca02.coloriuris.net/crl/coloriuris-ca02-tsa.crl                CRL Issuer:
                  DirName:CN = COLORIURIS CA02 TSA, OU = Prestador de Servicios de Confianza,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                77:AB:32:37:1C:68:98:84:E0:7E:37:02:4E:A3:12:7D:3A:27:24:D4
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
    Signature Algorithm: rsassaPss
    Signature Value:
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        29:8c:fb:9e:99:86:2e:03:af:41:f1:fd:23:eb:7b:47:e3:cc:
        a4:b8:68:e1:a3:54:2d:b7:06:92:3a:fb:81:eb:3e:54:58:aa:
        3d:45:32:f7:e9:8c:05:67:6d:b6:2b:4a:ba:f1:e2:dc:fe:c6:
        f9:13:ba:0e:b1:b7:37:7d:a9:65:3e:56:63:31:f6:20:50:03:
        fb:f1:3a:2a:e0:6c:c4:0e:28:03:2c:8d:0d:55:83:7c:10:f9:
        7d:f2:87:d5:ba:20:de:3b:cd:83:89:3e:fa:e9:08:ae:0a:a3:
        b4:33:77:57:0d:2f:d6:3b:c4:f4:9d:01:f3:b6:9f:7b:fe:aa:
        35:f9:35:5f:ad:3a:bd:2f:ce:b8:f9:0a:78:f4:6f:e1:26:e8:
        a3:7c:ca:2d:76:b3:a6:97:fb:c1:2b:70:b3:f1:55:ae:31:cb:
        3a:d7:3b:a6:66:c4:ec:0d:35:fa:6d:7d:1f:ed:c3:82:69:5b:
        e0:36:66:23:3c:bc:4e:cd:3a:4b:74:45:9c:16:cb:9d:45:b5:
        fa:f7:bf:1a:a0:c7:96:3b:ef:94:41:54:65:a7:b7:c2:c2:66:
        1a:f3:9b:23:2c:ea:9a:51:92:cf:92:50:a9:e3:01:60:56:84:
        1b:ab:91:4c:d7:1c:dc:0b:17:71:3b:d9:44:72:88:75:ee:d1:
        41:97:30:49:06:dc:37:e2:3b:82:24:2c:87:b0:3e:b4:3e:8b:
        e8:32:2a:23:d3:2e:1a:a1:67:0c:e6:df:b3:0c:ff:dc:b4:78:
        1e:ca:b1:73:db:d7:7e:d0:eb:d3:7f:13:0c:f3:4f:32:03:88:
        7f:aa:06:98:09:b6:2e:c2:c4:e9:1c:55:46:c2:6a:13:ce:7d:
        b2:40:20:9f:9a:f8:a5:51:cc:23:1a:45:c9:1f:18:85:f3:db:
        08:ee:79:cf:91:5d:35:fa:1a:52:a7:dc:80:88:c9:b4:c9:35:
        b3:38:41:dd:99:c8:e8:18:18:28:d9:2a:2f:83:be:e7:af:ae:
        14:d0:cf:82:e9:85:b8:6e:29:31:5e:db:0f:2c:47:ef:6f:dc:
```

```
        ae:36:69:38:9c:26:99:52:22:1d:e7:fe:c0:75:b3:c9:77:2f:
        1f:30:44:5c:4c:7e:ce:07:d9:a2:98:76:3d:e3:32:d1:e5:66:
        0c:16:cf:3c:e1:98:5f:cf:d1:fa:3f:39:5f:1d:e1:79:3e:8c:
        8f:94:30:32:a2:84:0a:81:a2:6c:b8:2a:28:45:9e:12:98:50:
        1d:7c:a7:26:b0:5f:8a:c2:ed:0d:12:8e:0b:23:19:4a:8f:c0:
        f5:51:c0:49:3f:68:60:a3:06:e3:8d:7b:8a:18:13:2f:40:59:
        b3:73:7f:b6:2b:20:19:a6
SHA1 Fingerprint=EB:3F:D6:46:3B:73:BC:65:85:12:F7:1F:5F:FE:B9:F2:44:67:0B:DE
sha256
Fingerprint=54:EF:3A:DB:D5:DB:91:60:5B:22:A2:F2:F9:6D:BB:43:55:F1:90:C7:A2:8B:61:58:44:13:41:4E:E9:24:C7:40
sha512
Fingerprint=27:CE:24:F0:F0:97:68:47:A9:74:9E:D1:55:E1:A6:F8:74:87:4B:3F:36:A7:0B:7B:FA:1F:0A:4B:21:C2:D1:0B:70:4B
:B5:40:78:C7:21:68:83:7E:E5:3D:2E:C9:CA:C5:0E:F4:B4:B6:C4:6D:CD:02:51:80:0F:DC:03:EB:F7:91
```

B.3.2. Certificado de emisión de sellos electrónicos cualificados de tiempo TSU04 (RSA 4096 bits)

```
        Version: 3 (0x2)
        Serial Number:
            2a:88:aa:5b:0a:51:bc:95:e5:c4:3e:70:16:f7:d2:62:9f:e5:6c:c4
        Signature Algorithm: rsassaPss
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        Issuer: CN = COLORIURIS CA02 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Validity
            Not Before: Jan 26 18:01:13 2026 GMT
            Not After : Jan 26 18:01:12 2036 GMT
        Subject: CN = COLORIURIS QTSP TSU04 - Emisor de sellos electronicos cualificados de tiempo,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:dd:6f:7a:7e:47:1a:7d:fa:39:0c:86:aa:00:d1:
                    21:69:e2:86:ce:c0:f3:4e:f1:d3:d8:ab:40:4e:4c:
                    04:86:3a:ab:73:6a:9e:05:43:67:8e:34:e2:e0:75:
                    30:b4:d4:42:48:09:ae:78:09:a2:7c:39:6d:f2:df:
                    1c:92:c3:8b:75:9c:73:eb:be:a2:03:ef:1f:e3:71:
                    9c:d4:05:48:27:66:5f:59:82:21:26:bc:a3:c3:f7:
                    8a:ea:d3:ba:15:6e:d9:e7:06:45:7f:57:37:1c:4b:
                    5d:34:9b:b4:23:b0:09:7e:ec:3a:c5:d3:23:82:4e:
                    10:63:3a:a4:45:ae:54:68:49:35:3d:7b:f3:a4:72:
                    58:a3:4a:a7:d4:1e:8a:f6:d1:1d:3b:4b:b8:f5:81:
                    33:6e:2a:1a:8b:9b:d0:a4:5b:41:2c:c4:74:5e:62:
                    a6:20:3d:34:50:d1:02:ce:d6:ea:51:ba:fe:ae:43:
                    59:7c:4c:82:50:ad:25:d2:2d:84:a4:69:54:9f:8d:
                    ec:53:f4:66:a6:cd:68:fd:c9:9f:0b:85:2b:d5:70:
                    10:ec:39:40:7a:5a:17:c8:63:ca:bf:46:a7:8c:6b:
                    cf:49:7d:2d:87:05:e7:f0:65:3b:53:3f:0b:8b:07:
                    87:a5:48:3a:65:90:6b:71:d8:44:de:ed:7c:df:62:
                    1e:19:d8:f1:00:15:5c:08:a6:33:18:33:6d:dd:0a:
                    c9:f0:14:b3:9b:0c:c2:70:d3:e6:e4:9b:37:be:f7:
                    0e:bb:9f:77:b2:22:1a:c9:81:4a:19:3c:6c:90:58:
                    b0:0f:3b:8b:67:7d:93:88:20:b1:22:f6:be:36:51:
                    bf:90:6a:21:a2:65:47:06:86:66:62:8f:08:25:95:
                    da:6b:8f:79:51:39:0d:b7:33:30:d1:15:48:e2:66:
                    a5:19:f1:97:e0:f6:04:90:a9:c4:d0:fd:ae:60:a7:
                    3e:35:9a:80:9f:fc:b8:a6:e3:d3:df:2d:46:bc:74:
```

```
                    74:55:0c:db:44:b0:8a:10:e4:fd:eb:2a:10:57:53:
                    a6:c2:87:27:9d:ae:57:b4:8a:43:ed:b7:bf:e7:4c:
                    3c:90:ff:e5:95:e8:a6:8b:87:70:6d:ac:49:38:42:
                    ef:de:4c:d4:84:c6:a1:3a:36:73:c4:a6:e7:18:77:
                    79:cb:4e:81:71:da:a7:24:db:c4:bd:cb:d9:e2:50:
                    ba:cd:c8:2b:6e:4d:21:57:7a:97:14:3d:2e:6c:a7:
                    55:f9:fa:b6:e4:20:43:8e:0d:19:f7:f4:ac:79:90:
                    8c:3b:08:74:5e:c9:7d:3f:0c:d2:2f:c2:d9:c0:76:
                    39:90:e8:0a:70:f4:53:86:15:cc:10:c2:e7:33:5d:
                    7a:22:a3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                BE:AC:4C:60:04:A3:4C:5F:FC:6A:41:E0:BD:A2:97:31:97:06:2F:FE
            Authority Information Access:
                CA Issuers - URI:http://ca02.coloriuris.net/certs/coloriuris-ca02-tsa.crt
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text: Certificado de emisión de sellos electrónicos cualificados de tiempo
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca02.coloriuris.net/crl/coloriuris-ca02-tsa.crl                CRL Issuer:
                  DirName:CN = COLORIURIS CA02 TSA, OU = Prestador de Servicios de Confianza,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                C6:CF:22:35:02:B1:6D:F5:E2:F1:B0:AE:68:16:45:73:55:6B:1A:7C
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
    Signature Algorithm: rsassaPss
    Signature Value:
        Hash Algorithm: sha512
        Mask Algorithm: mgf1 with sha512
         Salt Length: 0x40
        Trailer Field: 0x01 (default)
        3c:02:1e:ab:e6:d0:c4:82:70:d5:52:f5:4d:f9:58:23:7f:82:
        e1:ea:84:ca:9e:84:82:69:05:d3:c3:79:3f:3a:b1:e3:a7:88:
        4f:a6:fb:a9:27:27:b2:ff:19:eb:f8:b0:77:b7:93:aa:4b:af:
        58:73:f1:ab:07:c6:25:ac:2d:7b:43:c1:3e:99:33:6f:67:cf:
        f1:8c:64:04:f3:43:c6:6b:72:55:42:9f:8b:f4:4f:e7:7b:3b:
        cd:b0:68:77:63:0f:c0:3a:aa:ea:55:0c:d9:e0:0d:c8:bc:c1:
        1e:58:2b:aa:76:dc:14:3c:c8:a1:1e:d2:95:04:5e:89:0b:8c:
        9f:c3:bd:9e:c1:00:57:f3:10:26:98:5e:36:c3:d5:96:c9:c6:
        2f:e3:34:db:5f:1b:a7:cb:81:90:a4:56:70:2e:5e:2b:b8:67:
        ff:58:af:b8:8e:a6:59:36:21:f0:97:3d:f0:a6:0d:5c:d7:ec:
        27:a3:ee:4c:d8:d7:b5:f4:79:85:2a:81:e0:9a:dc:ab:94:11:
        be:49:da:d4:62:eb:d2:85:e2:aa:56:bd:6e:e1:25:12:08:2a:
        73:61:07:3b:79:8f:82:c6:c7:d2:73:dd:76:f7:de:3c:6c:16:
        66:72:f0:0b:5e:5c:18:f7:a8:c8:3d:2a:d1:7b:e1:ba:b4:b8:
        d7:3d:1b:ad:ce:68:e2:00:86:c0:68:83:4e:29:dd:ae:89:5a:
        b5:49:c8:b5:df:a5:54:31:65:a4:d5:df:d5:24:83:66:fa:26:
        84:7c:57:7b:1e:10:98:7f:90:5b:2d:50:fe:a7:0a:0e:cc:7c:
        45:5f:3f:96:cf:2e:45:d4:7f:95:b6:69:3b:f1:dc:f3:28:77:
        85:1f:18:f9:45:4d:ef:0d:a1:e9:a1:ae:76:13:6d:1b:5d:b7:
        9b:a6:a5:37:43:30:78:2a:d9:aa:1c:52:eb:9a:2c:b6:47:bc:
```

```
        93:5b:d1:a2:18:dc:e8:fe:3c:45:77:9b:93:53:40:28:c0:6d:
        1a:7f:82:56:d6:41:d7:db:09:a2:a3:97:4e:7b:45:b2:eb:ba:
        a5:1e:c2:e2:75:eb:b0:5a:16:27:df:9f:95:66:70:7d:c6:db:
        63:5b:61:97:67:b0:af:fc:05:7f:2f:3b:8c:3b:d1:4d:96:47:
        0a:27:0e:e2:87:f8:dc:cf:cf:0f:52:e3:8c:6b:e9:95:d3:76:
        c9:a2:7d:6a:0c:90:37:f5:1d:0a:43:41:f0:ac:a8:dd:60:32:
        14:f7:1b:cd:7b:11:c2:ee:f6:77:34:81:02:fd:93:2f:7d:f5:
        49:0f:31:1b:73:ff:b5:00:e5:58:24:03:87:64:78:c2:c2:fa:
        13:a3:66:86:ea:3b:5a:0e
SHA1 Fingerprint=97:C9:30:D3:EC:D6:93:34:A0:4A:2E:E1:20:22:EF:0D:BE:72:F7:F8
sha256
Fingerprint=8E:A8:3C:2E:B2:52:FC:9D:D6:9A:B8:D6:A3:2C:6D:01:B3:20:64:AE:B7:91:DC:E6:00:2C:26:3B:8D:A3:60:CE
sha512
Fingerprint=C8:17:57:D2:8C:C3:3C:2E:6A:CB:78:0D:BB:92:67:F1:85:60:35:90:0C:E7:C3:26:1F:94:D6:B5:F8:5E:5F:E4:A0:75
:45:27:7F:5D:28:71:4C:03:43:B2:59:DC:91:F5:1F:EF:F1:76:AD:6E:9C:D7:52:9B:32:9F:2A:60:84:E3
```

B.4. Certificado Raíz TSACI CA03

```
        Version: 3 (0x2)
        Serial Number:
            57:34:6e:56:32:12:da:2e:53:41:37:97:7e:32:f3:d4:9c:bd:8d:b2
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: CN = COLORIURIS CA03 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Validity
            Not Before: Jan 26 12:13:15 2026 GMT
            Not After : Jan 26 12:13:14 2046 GMT
        Subject: CN = COLORIURIS CA03 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:ad:0e:75:30:27:f3:40:8b:5c:74:f2:6e:6f:11:
                    66:80:9f:ae:4f:68:5b:34:c0:00:0a:7c:d1:34:15:
                    e0:db:91:97:26:11:3a:8f:90:19:ee:db:2e:36:bf:
                    67:dd:5d:9b:bc:12:13:7e:c5:4c:a8:37:78:71:d6:
                    f1:ec:c5:7a:dd:cb:02:10:5a:85:bb:30:d8:a4:f1:
                    27:96:78:82:eb:68:27:47:de:c7:44:fa:3e:42:a7:
                    bc:ab:12:6c:45:ff:14
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://cipsc.coloriuris.net/politicas/
            OCSP No Check:

            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 Subject Key Identifier:
                0A:5B:B2:26:8C:21:5F:5E:3E:B7:D1:7A:D1:DC:C7:22:29:D5:37:E9
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
```

```
    Signature Algorithm: ecdsa-with-SHA384
    Signature Value:
        30:65:02:31:00:9b:e4:7b:4c:a8:10:f5:98:d3:fd:27:aa:b1:
        6d:0d:d0:bf:f5:cf:a1:6e:ef:85:dd:35:37:e9:ef:db:58:c3:
        8e:f3:fe:30:0c:a1:80:56:f3:a4:9f:82:94:16:61:3a:31:02:
        30:43:3c:d4:3e:73:99:58:3c:68:31:4f:a6:af:d5:66:ad:13:
        1f:f9:5f:09:b8:07:f6:06:9d:7c:be:2e:42:a8:25:1a:e2:15:
        22:43:ca:bc:fb:7e:3b:df:ac:a0:aa:82:61
SHA1 Fingerprint=67:31:ED:C3:63:0F:03:35:6D:8C:A0:BE:E0:55:76:65:DB:28:70:9C
sha256
Fingerprint=3C:D8:BC:E8:AD:23:80:15:29:30:12:33:C7:2D:C1:8C:75:17:9B:B5:E1:E2:A5:17:96:DB:B1:BE:E4:5B:FC:65
sha512
Fingerprint=46:B5:49:C4:74:DD:3F:9E:54:BA:B5:D4:0E:CB:B6:D3:00:E2:4B:11:6B:17:98:1E:25:3B:F5:1E:F5:CB:DF:BF:8E:1A
:77:D4:2D:D6:BD:3B:2A:D3:75:BA:90:95:41:ED:BA:D2:83:56:E4:4A:4D:53:7C:1A:63:5C:BA:4E:6A:A3
```

B.4.1. Certificado de emisión de sellos electrónicos cualificados de tiempo TSU05 (ECDSA P-256 bits)

```
        Version: 3 (0x2)
        Serial Number:
            10:b6:e4:3f:bb:8b:6b:82:0d:51:da:f9:04:c1:ba:77:c7:8f:a8:05
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: CN = COLORIURIS CA03 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Validity
            Not Before: Jan 26 17:46:36 2026 GMT
            Not After : Jan 26 17:46:35 2036 GMT
        Subject: CN = COLORIURIS QTSP TSU05 - Emisor de sellos electronicos cualificados de tiempo,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:25:f3:84:e1:48:b4:b9:8c:c9:ba:25:d7:f6:15:
                    0b:04:c4:e8:1e:ad:02:37:93:d4:ae:8e:b3:0a:bf:
                    c5:2d:00:d6:93:9b:5f:78:00:80:76:14:97:bf:0a:
                    4e:97:8f:b5:1a:c8:6f:e9:4e:9f:fe:5c:cc:10:a2:
                    64:2e:bd:8b:5e
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                0A:5B:B2:26:8C:21:5F:5E:3E:B7:D1:7A:D1:DC:C7:22:29:D5:37:E9
            Authority Information Access:
                CA Issuers - URI:http://ca03.coloriuris.net/certs/coloriuris-ca03-tsa.crt
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text: Certificado de emisión de sellos electrónicos cualificados de tiempo
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  82 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2
   25:d=1  hl=2 l=  57 cons:  SEQUENCE
   27:d=2  hl=2 l=   6 prim:   OBJECT            :0.4.0.1862.1.5
   35:d=2  hl=2 l=  47 cons:   SEQUENCE
```

```
   37:d=3  hl=2 l=  45 cons:    SEQUENCE
   39:d=4  hl=2 l=  39 prim:     IA5STRING         :https://cipsc.coloriuris.net/pds/en.pdf
   80:d=4  hl=2 l=   2 prim:     PRINTABLESTRING   :en

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca03.coloriuris.net/crl/coloriuris-ca03-tsa.crl               CRL Issuer:
                  DirName:CN = COLORIURIS CA03 TSA, OU = Prestador de Servicios de Confianza,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                7F:41:44:25:68:8D:B2:56:B6:81:41:3D:F2:98:DF:39:DA:CE:C7:7E
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
    Signature Algorithm: ecdsa-with-SHA384
    Signature Value:
        30:65:02:30:60:85:af:e7:38:45:48:44:25:58:92:64:b0:a3:
        33:54:23:92:6f:1e:dc:4e:29:db:5c:44:a2:ea:cb:85:23:e4:
        a9:e5:1c:72:11:b2:fa:1d:44:7b:02:a0:09:9e:cb:c8:02:31:
        00:ef:b9:73:90:f8:2f:11:4d:9a:18:2a:cb:71:7e:f9:99:5f:
        81:d9:87:c8:b2:8a:8b:08:22:ca:57:45:3c:76:aa:0f:54:c4:
        df:cd:6e:63:e7:24:08:8f:8e:3e:e3:bc:31
SHA1 Fingerprint=8C:3A:AC:39:F7:5E:8E:26:3D:A6:82:0B:E2:0E:21:77:35:A8:C0:2E
sha256
Fingerprint=F8:35:40:CD:65:5B:FA:67:FE:5F:0D:08:F4:AB:13:42:68:59:9C:A0:B9:60:8D:AD:F4:8F:9C:72:1C:0B:29:BF
sha512
Fingerprint=36:FF:5D:79:05:D9:2F:30:F2:AD:DC:E7:F3:EE:9C:60:52:E1:F7:6A:07:5E:D4:C3:68:E4:76:34:35:24:2D:A0:FD:FF
:3F:EC:BE:0B:D4:7A:C0:2D:EB:4E:D3:25:01:C1:D0:F6:4F:40:37:ED:D6:0A:AC:35:A5:05:B0:4B:CD:E1
```

B.4.2. Certificado de emisión de sellos electrónicos cualificados de tiempo TSU07 (ECDSA P-384 bits)

```
        Version: 3 (0x2)
        Serial Number:
            59:34:1d:46:51:f1:28:24:fd:84:2a:9c:1e:73:2c:1d:b7:d8:fd:2c
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: CN = COLORIURIS CA03 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Validity
            Not Before: Jan 26 17:48:34 2026 GMT
            Not After : Jan 26 17:48:33 2036 GMT
        Subject: CN = COLORIURIS QTSP TSU07 - Emisor de sellos electronicos cualificados de tiempo,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:a1:27:ce:73:c4:12:f8:b7:df:77:4f:24:81:ee:
                    a6:2a:94:5d:be:e7:1a:cf:fc:e2:14:0c:cf:ba:bd:
                    d5:68:4f:f1:c7:27:fe:44:20:be:38:b6:71:44:5d:
                    5b:d3:f4:74:7c:56:3b:42:27:2b:c3:2e:16:04:a0:
                    66:81:80:ec:e9:b5:af:28:5b:72:dc:77:86:f8:3e:
                    76:a7:12:3e:33:83:38:17:9d:75:67:00:83:83:15:
                    2e:45:ef:05:fc:3b:d8
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                0A:5B:B2:26:8C:21:5F:5E:3E:B7:D1:7A:D1:DC:C7:22:29:D5:37:E9
            Authority Information Access:
                CA Issuers - URI:http://ca03.coloriuris.net/certs/coloriuris-ca03-tsa.crt
            X509v3 Certificate Policies:
```

```
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text: Certificado de emisión de sellos electrónicos cualificados de tiempo
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  82 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2
   25:d=1  hl=2 l=  57 cons:  SEQUENCE
   27:d=2  hl=2 l=   6 prim:   OBJECT            :0.4.0.1862.1.5
   35:d=2  hl=2 l=  47 cons:   SEQUENCE
   37:d=3  hl=2 l=  45 cons:    SEQUENCE
   39:d=4  hl=2 l=  39 prim:     IA5STRING         :https://cipsc.coloriuris.net/pds/en.pdf
   80:d=4  hl=2 l=   2 prim:     PRINTABLESTRING   :en

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca03.coloriuris.net/crl/coloriuris-ca03-tsa.crl               CRL Issuer:
                  DirName:CN = COLORIURIS CA03 TSA, OU = Prestador de Servicios de Confianza,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                2E:9E:B5:C4:9C:19:FD:65:7D:23:F9:25:01:7D:7C:80:DB:66:23:6B
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
    Signature Algorithm: ecdsa-with-SHA384
    Signature Value:
        30:65:02:30:76:bb:4d:57:7e:18:48:58:7f:92:f0:9e:b3:3f:
        71:ca:5a:48:f3:77:a2:2b:1b:82:ae:50:57:84:f8:fc:05:6a:
        f3:bd:6f:88:80:6e:8c:53:76:1a:60:a1:6c:dc:35:f0:02:31:
        00:a5:29:19:52:19:d4:58:eb:1b:2a:c3:84:40:48:fb:92:29:
        0c:e7:b0:78:8f:cc:a8:e8:1e:bc:5a:33:4c:f7:49:81:7d:71:
        63:f8:23:d7:37:54:9b:2e:62:00:e8:74:bd
SHA1 Fingerprint=76:E7:18:C7:53:01:3C:E1:CF:B0:D8:9A:9E:DC:C6:24:3A:E8:EE:02
sha256
Fingerprint=B9:2D:D9:DA:E0:8D:1A:8B:21:6A:FE:28:8B:4F:6E:B5:F6:B5:D2:A1:C2:C5:7C:B3:AA:6D:C0:FA:E0:0E:95:B7
sha512
Fingerprint=04:DA:2A:C4:83:46:E2:EE:1C:79:D2:62:10:FB:0C:56:CC:6C:4A:48:AF:B3:47:08:91:A8:17:03:7C:77:DD:DF:44:0B
:9F:B5:5D:EA:A7:E8:D3:91:C0:16:12:2C:A1:B5:9A:EF:3B:17:B7:DF:54:6F:44:92:9F:55:02:55:C7:4E
```

B.5. Certificado Raíz TSACI CA04

```
        Version: 3 (0x2)
        Serial Number:
            33:03:ca:59:87:11:b1:39:78:9a:44:ed:09:f1:44:53:f9:2a:83:f7
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: CN = COLORIURIS CA04 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Validity
            Not Before: Jan 23 18:59:02 2026 GMT
            Not After : Jan 23 18:59:01 2046 GMT
        Subject: CN = COLORIURIS CA04 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:ea:25:2b:b9:e9:73:e6:0d:7a:2c:bf:6c:f0:f0:
```

```
                    ff:69:61:cd:aa:c2:9b:e7:bc:fb:79:90:7a:38:17:
                    c1:35:8f:6e:75:2a:5c:09:0d:47:03:82:c6:d0:a5:
                    c8:71:f7:90:d5:ea:d8:b0:18:8b:12:43:1e:5e:97:
                    71:cd:e7:4d:70:20:48:bc:10:c2:48:99:5e:f9:02:
                    a6:11:95:23:ef:83:ac:a9:b0:02:36:dd:64:cf:11:
                    c9:02:b7:a8:47:b3:34
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://cipsc.coloriuris.net/politicas/
            OCSP No Check:

            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 Subject Key Identifier:
                03:BA:FE:15:05:26:FF:14:B1:1F:6E:98:08:19:64:AD:58:9F:1E:A2
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
    Signature Algorithm: ecdsa-with-SHA384
    Signature Value:
        30:64:02:30:3a:74:1c:90:78:5d:7e:b2:52:f0:d7:e5:2c:a3:
        0d:6b:d7:8d:51:c3:82:aa:0a:bb:44:c2:6c:f8:e9:cd:3e:30:
        c1:8c:af:bf:e3:5a:fa:88:1f:71:af:a5:96:d7:cf:11:02:30:
        64:72:6a:62:86:62:e6:99:24:f3:2a:ff:64:03:04:e6:eb:4a:
        e3:13:32:d0:2b:6c:1a:9e:48:22:df:bd:d0:d0:d2:89:68:37:
        a9:8d:9a:79:3f:3b:31:00:32:2f:96:80
SHA1 Fingerprint=85:35:4F:DA:BC:B0:AE:D6:3B:6E:F7:35:35:07:ED:40:2A:43:ED:1B
sha256
Fingerprint=18:96:66:EE:5B:28:78:CF:60:4A:FD:70:C5:69:CA:B0:B4:73:EC:1B:88:AE:80:13:E2:5A:54:86:78:98:E1:4D
sha512
Fingerprint=39:E8:EE:28:E0:5F:D8:F1:4C:0B:D8:11:75:68:6D:86:8E:6E:8A:F3:89:0E:57:71:6C:88:80:48:63:ED:14:2B:C9:96
:37:DC:FB:52:7E:50:35:FC:09:DB:DC:96:96:D4:40:25:6B:20:01:C1:FA:DF:E8:5B:4A:91:EC:D0:DD:62
```

B.5.1. Certificado de emisión de sellos electrónicos cualificados de tiempo TSU06 (ECDSA P-256 bits)

```
        Version: 3 (0x2)
        Serial Number:
            54:69:9d:a9:b1:4e:8f:03:a3:44:0d:24:a9:ad:59:71:c1:e4:e4:d0
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: CN = COLORIURIS CA04 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Validity
            Not Before: Jan 26 18:03:17 2026 GMT
            Not After : Jan 26 18:03:16 2036 GMT
        Subject: CN = COLORIURIS QTSP TSU06 - Emisor de sellos electronicos cualificados de tiempo,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:6b:9d:5c:28:5a:ec:c9:59:d2:86:fd:39:b4:da:
```

```
                    3c:a3:bd:2b:d5:e9:23:35:1f:e5:6b:f7:2b:11:1e:
                    7d:86:42:ec:93:ae:f8:1f:17:10:a2:f4:2b:2a:1e:
                    c4:25:be:dd:65:96:76:d0:d5:26:df:58:8f:f8:6a:
                    a2:ef:aa:10:4c
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                03:BA:FE:15:05:26:FF:14:B1:1F:6E:98:08:19:64:AD:58:9F:1E:A2
            Authority Information Access:
                CA Issuers - URI:http://ca04.coloriuris.net/certs/coloriuris-ca04-tsa.crt
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text: Certificado de emisión de sellos electrónicos cualificados de tiempo
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca04.coloriuris.net/crl/coloriuris-ca04-tsa.crl                CRL Issuer:
                  DirName:CN = COLORIURIS CA04 TSA, OU = Prestador de Servicios de Confianza,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                32:93:2D:1C:67:69:08:7A:D5:AB:0C:90:E6:31:3F:94:1C:07:EB:02
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
    Signature Algorithm: ecdsa-with-SHA384
    Signature Value:
        30:65:02:31:00:fb:b0:79:2b:a0:54:06:1f:ba:97:3b:25:0d:
        73:fc:ce:e7:d9:a3:1d:e2:5c:ea:35:6e:a0:d9:77:7e:86:06:
        20:5c:9f:c2:2e:92:59:e0:df:10:38:ba:3d:da:58:cf:10:02:
        30:7c:84:f2:11:de:f6:c8:6a:ec:8d:e5:1f:9b:8b:d2:bd:a4:
        fe:86:7d:1a:3f:2d:cd:ef:98:62:89:13:c7:58:18:20:b3:98:
        9b:cf:8d:29:4f:b9:fc:3e:2d:13:b9:6a:96
SHA1 Fingerprint=2C:11:D8:E8:D5:DA:E2:3A:B9:61:00:17:B1:9F:4A:26:8F:3C:BC:96
sha256
Fingerprint=3B:20:17:60:A6:FA:3B:E4:EB:56:97:FE:B9:29:7F:9F:E8:6D:A5:B5:FF:57:18:39:F5:8F:67:C4:F6:5E:0D:A2
sha512
Fingerprint=61:14:3E:C4:B1:B7:D7:FD:BA:88:CF:7A:94:4B:95:3E:73:0A:66:C9:B0:B5:E2:FF:FF:95:81:69:2D:42:E7:DC:A8:8B
:4F:08:EC:DB:C2:96:8F:E7:6F:51:25:02:52:61:2A:BC:A3:A8:96:7D:5B:9A:2A:58:AB:84:61:4B:06:C6
```

B.5.2. Certificado de emisión de sellos electrónicos cualificados de tiempo TSU08 (ECDSA P-384 bits)

```
        Version: 3 (0x2)
        Serial Number:
            64:25:64:c7:60:0e:9d:30:07:e2:76:fd:85:03:43:3f:cb:6b:64:45
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: CN = COLORIURIS CA04 TSA, OU = Prestador de Servicios de Confianza, organizationIdentifier =
VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Validity
            Not Before: Jan 26 18:05:02 2026 GMT
            Not After : Jan 26 18:05:01 2036 GMT
```

```
        Subject: CN = COLORIURIS QTSP TSU08 - Emisor de sellos electronicos cualificados de tiempo,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:60:00:3d:a8:60:75:8e:c8:96:9f:a1:39:60:6f:
                    6f:d3:31:57:3a:cc:7a:e9:c2:3d:2c:5e:a3:af:c5:
                    2c:96:3b:f5:57:24:62:f9:18:00:29:78:99:14:cb:
                    12:2d:f8:89:6d:98:22:b4:53:ca:d7:e1:37:fc:b3:
                    09:95:32:58:23:da:a2:87:df:e9:1d:fb:27:02:04:
                    83:1b:f3:a0:ef:d6:d2:0c:d2:b5:e7:7c:30:e6:c9:
                    b0:d0:78:b6:34:2b:56
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                03:BA:FE:15:05:26:FF:14:B1:1F:6E:98:08:19:64:AD:58:9F:1E:A2
            Authority Information Access:
                CA Issuers - URI:http://ca04.coloriuris.net/certs/coloriuris-ca04-tsa.crt
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.37799.20.5.1
                  CPS: https://cipsc.coloriuris.net/politicas/
                  User Notice:
                    Explicit Text: Certificado de emisión de sellos electrónicos cualificados de tiempo
            X509v3 Extended Key Usage: critical
                Time Stamping
            qcStatements:
    0:d=0  hl=2 l=  23 cons: SEQUENCE
    2:d=1  hl=2 l=  21 cons:  SEQUENCE
    4:d=2  hl=2 l=   8 prim:   OBJECT            :1.3.6.1.5.5.7.11.2
   14:d=2  hl=2 l=   9 cons:   SEQUENCE
   16:d=3  hl=2 l=   7 prim:    OBJECT            :0.4.0.194121.1.2

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca04.coloriuris.net/crl/coloriuris-ca04-tsa.crl               CRL Issuer:
                  DirName:CN = COLORIURIS CA04 TSA, OU = Prestador de Servicios de Confianza,
organizationIdentifier = VATES-B99091696, O = Coloriuris S.L., L = Zaragoza, C = ES
            X509v3 Subject Key Identifier:
                11:82:89:A8:AC:39:0E:C5:3A:5D:90:AB:9A:7C:7E:FE:27:AC:CF:4C
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
    Signature Algorithm: ecdsa-with-SHA384
    Signature Value:
        30:66:02:31:00:db:f5:58:79:3c:b0:7a:4d:12:3c:d6:26:76:
        4b:82:7a:d6:63:30:18:8a:c5:5f:09:86:59:66:94:31:c7:4a:
        94:74:dc:d5:e8:f6:c9:e6:42:63:0b:42:54:a3:ba:b9:fd:02:
        31:00:80:d3:9c:ff:5f:00:90:b9:d3:f2:3c:ed:dd:20:ef:be:
        d4:27:c0:c3:59:b4:3b:4d:93:75:15:38:65:d9:47:83:66:92:
        52:a6:f6:19:48:03:12:d5:e2:e1:db:5f:09:84
SHA1 Fingerprint=6F:13:2E:6E:E2:98:C5:EC:68:1F:9B:2D:87:AB:C0:C9:02:CC:42:0D
sha256
Fingerprint=85:14:13:B5:6F:63:39:97:5D:4B:B3:20:09:31:F0:99:E6:A3:63:F1:73:DE:39:CE:4E:15:57:0C:E6:21:D8:B4
sha512
Fingerprint=F1:19:05:29:A0:C3:F0:65:42:57:84:A3:9D:73:26:81:CD:B4:7C:8D:FF:44:F5:80:38:9C:8F:08:12:25:0D:3B:08:29
:CC:0B:9E:06:03:36:9E:0A:85:2E:7F:BA:BB:31:E9:A4:60:B6:83:51:F5:0D:24:D8:3A:CF:80:1E:89:ED
```

Anexo C: Revisión de las Políticas

Las presentes políticas se revisarán cada 12 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 anual 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.

Coloriuris, S.L.
CIF B99091696
R.M. Zaragoza - T - 3330, L - 0, F - 107, H – Z40193
c/ Alfonso I, no 23 (50003 – Zaragoza)

telf: +34 976 203 670
info@coloriuris.net

web: https://www.coloriuris.net
blog: https://www.coloriuris.net/blog
wikipedia: https://es.wikipedia.org/wiki/Coloriuris
twitter: https://twitter.com/coloriuris