Coloriuris Prestador de Servicios de Confianza

Políticas y declaración de prácticas

Autor	Coloriuris S.L.
Versión	2.0.2
Estado del documento	Aprobado
Fecha de emisión	13-10-2015
OID (Object Identifier)	1.3.6.1.4.1.37799.0.3.1.2.0
Ubicación del documento	https://cipsc.coloriuris.net/politicas/

CONTENIDO

1 Las políticas y declaración de prácticas de Coloriuris Prestador de Servicios de Confianza...8
1.1.- Finalidad....8
1.2.- Estructura....9
1.3.- Alcance....11
1.4.- Ámbito de aplicación....11
1.5.- Identificación....11
1.6.- Administración y publicidad....11
1.6.1.- Validez....11
1.6.2.- Modificaciones....12
1.6.3.- Publicidad....12
1.6.4.- Datos de contacto....13
2 Políticas de los servicios de CIPSC....14
2.1.- Estructura de CIPSC....14
2.1.1.- Responsable de Administración de Políticas de Coloriuris....14
2.1.2.- Autoridades prestadoras de los servicios de confianza de CIPSC....14
2.1.2.1.- Aspectos comunes....14
2.1.2.2.- Autoridad de certificación (AC) y Autoridad de certificación v3 (ACv3)....15
2.1.2.3.- Autoridad de sellado de tiempo (TSACI)....15
2.1.2.4.- Autoridad para los servicios relativos a los documentos electrónicos (ASD)....16
2.1.3.- Autoridades de registro....16
2.2.- Firmantes y partes usuarias....17
2.2.1.- Firmantes y creadores de sellos....17
2.2.2.- Partes usuarias....17
2.2.3.- Aceptación de las Políticas y declaración de prácticas....17
2.2.4.- Verificación de las evidencias....18
2.3.- Obligaciones....18
2.3.1.- Coloriuris....18
2.3.2.- Obligaciones de los firmantes y creadores de sellos....19
2.3.3.- Obligaciones de las partes usuarias....19
2.4.- Responsabilidad de CIPSC....20
2.5.- Datos personales y confidencialidad....20
2.5.1.- Protección de datos de carácter personal....20
2.5.2.- Información confidencial....20
2.5.3.- Deber de secreto....21
2.6.- Auditorías....21
2.7.- Tarifas....21
2.8.- Reclamaciones y jurisdicción....22
2.8.1.- Comunicación de las reclamaciones....22
2.8.2.- Jurisdicción....22
3 Declaración de prácticas....23
3.1.- Introducción....23
3.2.- El ciclo de vida de los certificados....23

3.2.1.- Solicitud de certificados....24
3.2.2.- Tramitación de la solicitud de certificados....24
3.2.3.- Emisión de certificados....24
3.2.4.- Aceptación de certificados....25
3.2.5.- Uso del par de claves y del certificado....25
3.2.6. Renovación de certificados....25
3.2.7. Renovación de claves....25
3.2.8. Modificación de certificados....25
3.2.9. Revocación y suspensión de certificados....25
3.2.9.1. Circunstancias para la revocación....25
3.2.9.2. Entidad que puede solicitar la revocación....26
3.2.9.3. Procedimiento de solicitud de revocación....26
3.2.9.4. Periodo de gracia de la solicitud de revocación....27
3.2.9.5. Circunstancias para la suspensión....27
3.2.9.6. Entidad que puede solicitar la suspensión....27
3.2.9.7. Procedimiento para la solicitud de suspensión....27
3.2.9.8. Límites del período de suspensión....27
3.2.9.9. Frecuencia de emisión de CRLs....27
3.2.9.10. Requisitos de comprobación de estado de certificados....27
3.2.9.11. Otras formas de divulgación de información de revocación disponibles....27
3.2.9.12. Requisitos especiales de renovación de claves comprometidas....27
3.2.10. Servicios de comprobación de estado de certificados....28
3.2.10.1 Características operativas....28
3.2.10.2 Disponibilidad del servicio....28
3.2.11. Finalización de la suscripción....28
3.2.12. Depósito y recuperación de claves....28
3.3.- Controles de seguridad física, de procedimiento y de personal....28
3.3.1.- Controles de seguridad física....28
3.3.1.1.- Localización y construcción de las instalaciones....28
3.3.1.2.- Acceso físico....29
3.3.1.3.- Electricidad y aire acondicionado....29
3.3.1.4.- Exposición al agua....30
3.3.1.5.- Prevención y protección de incendios....30
3.3.1.6.- Almacenamiento de soportes....30
3.3.1.7.- Tratamiento de residuos....30
3.3.1.8.- Copia de respaldo fuera de las instalaciones....30
3.3.2.- Controles de procedimientos....30
3.3.2.1.- Funciones fiables....30
3.3.2.2.- Número de personas por tarea....31
3.3.2.3.- Identificación y autenticación para cada rol....32
3.3.2.4.- Separación de tareas en los diferentes roles....32
3.3.3.- Controles de personal....32
3.3.3.1.- Requisitos de historial, calificaciones, experiencia y autenticación....32
3.3.3.2.- Procedimientos de investigación de historial....32
3.3.3.3.- Requisitos de formación....32
3.3.3.4.- Requisitos y frecuencia de actualización formativa....33
3.3.3.5.- Secuencia y frecuencia de rotación laboral....33
3.3.3.6.- Sanciones para acciones no autorizadas....33
3.3.3.7.- Requisitos de contratación de personal....33
3.3.3.8.- Suministro de documentación al personal....34
3.3.4.- Procedimientos de log y auditoría....34
3.3.4.1.- Tipo de eventos registrados....34
3.3.4.2.- Frecuencia de procesamiento de logs....35
3.3.4.3.- Periodo de retención del log....35
3.3.4.4.- Protección del log....35
3.3.4.5.- Procedimiento de backup del log....35
3.3.4.6.- Recolección de logs....35
3.3.4.7.- Notificación de la acción causante de los logs....35
3.3.4.8.- Análisis de vulnerabilidades....36

3.3.5.- Archivado de registros....36
3.3.5.1.- Tipo de registros archivados....36
3.3.5.2.- Periodo de retención del archivo....36
3.3.5.3.- Protección del archivo....36
3.3.5.4.- Procedimientos de backup del archivo....36
3.3.5.5.- Requisitos para el sellado de tiempo de los registros....37
3.3.5.6.- Sistema de archivo....37
3.3.5.7.- Procedimientos para obtener y verificar la información del archivo....37
3.3.6.- Cambio de claves....37
3.3.7.- Plan de contingencias....37
3.3.7.1.- Procedimientos de gestión de incidencias....37
3.3.7.2.- Plan de actuación ante datos y software corruptos....39
3.3.7.3.- Procedimiento ante compromiso de la clave privada....39
3.3.7.4.- Continuidad de negocio después de un desastre....40
3.3.8.- Terminación de la AC o AR....40
3.3.8.1.- Entidad de Certificación....40
3.3.8.2.- Entidad de Registro....41
3.4.- Controles de seguridad técnica....41
3.4.1.- Generación e instalación del par de claves....41
3.4.1.1.- Generación del par de claves....41
3.4.1.2.- Distribución de la clave privada al firmante o creador de sello....42
3.4.1.3.- Distribución de la clave pública al emisor del certificado....42
3.4.1.4.- Distribución de las claves públicas de las autoridades prestadoras de servicios....43
3.4.1.5.- Tamaños de claves....43
3.4.1.6.- Algoritmos de firma de certificados....43
3.4.1.7.- Usos admitidos de las claves (KeyUsage field X.509v3)....44
3.4.2.- Protección de la clave privada....45
3.4.2.1.- Estándares de módulos criptográficos....45
3.4.2.2.- Control por más de una persona (n de m) sobre la clave privada....45
3.4.2.3.- Custodia de la clave privada....45
3.4.2.4.- Copia de respaldo de la clave privada....46
3.4.2.5.- Archivado de la clave privada....46
3.4.2.6.- Trasferencia de la clave privada a o desde el módulo criptográfico....46
3.4.2.7.- Almacenamiento de la clave privada en el módulo criptográfico....46
3.4.2.8.- Método de activación de la clave privada....47
3.4.2.9.- Método de desactivación de la clave privada....47
3.4.2.10.- Método de destrucción de la clave privada....47
3.4.2.11.- Calificación del módulo criptográfico....48
3.4.3.- Otros aspectos de gestión del par de claves....48
3.4.3.1.- Archivo de la clave pública....48
3.4.3.2.- Periodos de utilización de las claves pública y privada....48
3.4.4.- Datos de activación....48
3.4.4.1.- Generación e instalación de datos de activación....48
3.4.4.2.- Protección de datos de activación....49
3.4.4.3.- Otros aspectos de los datos de activación....49
3.4.5.- Controles de seguridad informática....49
3.4.5.1.- Requisitos técnicos específicos de seguridad informática....49
3.4.5.2.- Evaluación del nivel de seguridad informática....50
3.4.6.- Controles técnicos del ciclo de vida....51
3.4.6.1.- Controles de desarrollo de sistemas....51
3.4.6.2.- Controles de gestión de la seguridad....51
3.4.7.- Controles de seguridad de red....51
3.4.8.- Fuente de tiempo....52
4 Servicios de firma electrónica....53
4.1.- Declaración básica del servicio de confianza de CIPSC....53
4.2.- Política para la prestación de los servicios de certificación....55
4.2.1.- Aspectos generales....55

4.2.1.1.- Finalidad y alcance....55
4.2.1.2.- Clases de certificados....56
4.2.1.3.- Comunidad....56
4.2.1.4.- Obligaciones....57
4.2.1.5.- Publicación y conservación de los certificados....58
4.2.1.6.- Registro de información y conservación de firmas....59
4.2.2.- Certificados de firma electrónica para persona física....59
4.2.2.1.- Ámbito de aplicación y usos....59
4.2.2.2.- Contenido....59
4.2.2.3.- Periodo de validez....60
4.2.2.4.- Longitud de la clave....60
4.2.2.5.- Perfiles del certificado....60
4.2.2.6.- Perfil de CRL....64
4.2.3.- Certificados de firma electrónica para personas jurídicas....64
4.2.3.1.- Ámbito de aplicación y usos....64
4.2.3.2.- Contenido....64
4.2.3.3.- Periodo de validez....65
4.2.3.4.- Longitud de la clave....65
4.2.3.5.- Perfiles del certificado....65
4.2.3.6.- Perfil de CRL....68
4.3.- Declaración de prácticas....69
4.3.1.- Generación y emisión....69
4.3.2.- Renovación....72
4.3.3.- Revocación....73
4.3.4.- Certificado raíz y sellos de la AC....74
4.3.4.1.- Certificado raíz....74
4.3.4.2.- Certificado para la emisión de certificados de firma electrónica de persona física....75
4.3.4.4.- Certificado para la emisión de certificados de firma electrónica de persona jurídica....77
5 Servicios de sello electrónico....79
5.1.- Declaración básica del servicio de confianza de CIPSC....79
5.2.- Política para la prestación de los servicios de certificación....81
5.2.1.- Aspectos generales....81
5.2.1.1.- Finalidad y alcance....81
5.2.1.2.- Clases de certificados....82
5.2.1.3.- Comunidad....82
5.2.1.4.- Obligaciones....82
5.2.1.5.- Publicación y conservación de los certificados....84
5.2.1.6.- Registro de información y conservación de sellos electrónicos....85
5.2.2.- Certificado de sello electrónico....85
5.2.2.1.- Ámbito de aplicación y usos....85
5.2.2.2.- Contenido....85
5.2.2.3.- Periodo de validez....86
5.2.2.4.- Longitud de la clave....86
5.2.2.5.- Perfiles del certificado....86
5.2.2.6.- Perfil de CRL....90
5.3.- Declaración de prácticas....90
5.3.1.- Generación y emisión....90
5.3.2.- Renovación....93
5.3.3.- Revocación....94
5.3.4.- Certificado raíz y sellos de la AC....96
5.3.4.1.- Certificado raíz....96
5.3.4.2.- Certificado para la emisión de sellos electrónicos....97
6 Servicio de sellado de tiempo (Autoridad de Sellado de Tiempo de Coloriuris - TSACI)....99
6.1.- Declaración básica del servicio de sellado de tiempo de CIPSC....99

6.2.- Política para la prestación del servicio de sellado de tiempo....101
6.2.1.- Introducción....101
6.2.2.- Versiones....102
6.2.3.- Precisión....102
6.2.4.- Comunidad de usuarios....102
6.2.5.- Usos de los sellos de tiempo....102
6.2.6.- Obligaciones....103
6.2.7.- Registro de información referente a la operación de los servicios de sellado de tiempo....103
6.3.- Declaración de prácticas....104
6.3.1.- Acceso al servicio....104
6.3.2.- Disponibilidad del servicio....104
6.3.3.- Ciclo de vida de las claves....104
6.3.4.- Sello de tiempo....105
6.3.5.- Sincronización del reloj con UTC....105
6.3.6.- Certificado raíz y sellos de TSACI....106
6.3.6.1.- Certificado raíz....106
6.3.6.2.- Certificados para la emisión de sellos de tiempo....108
7 Política para la prestación del servicio de entrega electrónica certificada (EEC)....111
7.1.- Declaración básica del servicio de entrega electrónica certificada....111
7.2.- Aspectos generales....113
7.2.1.- Introducción....113
7.2.2.- Comunidad de usuarios....113
7.2.3.- Usos del servicio de entrega electrónica certificada....113
7.2.4.- Obligaciones....114
7.2.5.- Registro de información referente al servicio de entrega electrónica certificada....115
7.3.- Realización del servicio de entrega electrónica certificada....115
7.3.1.- Acceso al servicio....115
7.3.2.- Disponibilidad del servicio....115
7.3.3.- Entrega electrónica certificada....116
7.4.- El certificado de firma de EEC....117
7.4.1.- Formato....117
8 Autoridad para los servicios relativos a los documentos electrónicos (ASD)....118
8.1.- Declaración básica de los servicios relativos a los documentos electrónicos....118
8.2.- Política para la prestación de los servicios relativos a los documentos electrónicos....120
8.2.1.- Introducción....120
8.2.2.- Comunidad de usuarios....121
8.2.3.- Usos de los servicios relativos a los documentos electrónicos....121
8.2.4.- Obligaciones....122
8.2.5.- Registro de información referente a la operación de los servicios de autenticación de documentos....123
8.3.- Declaración de prácticas....124
8.3.1.- Acceso a los servicios....124
8.3.2.- Disponibilidad de los servicios....124
8.3.3.- Documentos electrónicos auténticos....124
8.3.4.- Registro de documentos electrónicos....125
8.3.5.- Archivo de documentos electrónicos....126
8.3.6.- Emisión de copias de los documentos electrónicos archivados....126
8.3.7.- Emisión de imágenes de los documentos electrónicos con código de verificación y acceso al punto de verificación....127

8.3.8.- Certificado raíz y sellos de la ASD....127
8.3.8.1.- Certificado raíz....127
8.3.8.2.- Certificados para la prestación de servicios relativos a los documentos electrónicos....128
Anexo I....133
Acrónimos utilizados....133
Definiciones....134
Normativa....136
Estándares....137
Anexo II – Certificados de CIPSC....139
[AC] Certificado raíz de la Autoridad de Certificación....139
[AC] Certificado Subautoridad de Emisión de certificados para persona física....139
[AC] Certificado Subautoridad de Emisión de certificados para persona jurídica....140
[AC] Certificado raíz de la Autoridad de Certificación v3....140
[AC] Certificado de Emisión de certificados de sello electrónico para persona jurídica....141
[ASD] Certificado raíz de la Autoridad de Certificación para servicios relativos a documentos electrónicos....141
[TSA] Certificado raíz de la Autoridad de Sellado de Tiempo....142
[TSA] Certificado de emisión de sellos de tiempo para servicios de Coloriuris....142
[TSA] Certificado de emisión de sellos de tiempo para las partes usuarias....142
Anexo III....143

1 Las políticas y declaración de prácticas de Coloriuris Prestador de Servicios de Confianza

1.1.- Finalidad

Coloriuris S. L. es una empresa especializada en prestar servicios para dotar de seguridad a la realización de actos jurídicos en Internet y a la utilización de documentos electrónicos. Con esta finalidad la empresa se constituye como prestador de servicios de confianza, bajo la denominación de "Coloriuris Prestador de Servicios de Confianza (en adelante, CIPSC)" y de acuerdo con lo dispuesto en la *Ley 59/2003, de 19 de diciembre, de firma electrónica*, en la *Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica* (vigente hasta el 30 de junio de 2016) y en el *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 el que se deroga la Directiva 1999/93/CE*.

La actividad de CIPSC se rige por lo establecido en el presente documento que cumple, en cuanto se refiere a la finalidad y contenidos, con lo establecido por las siguientes normas:

- ETSI TS 102 042, *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates*.
- ETSI TS 101 456, *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification Authorities issuing qualified certificates*.
- ETSI TS 102 023, *Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-stamping Authorities*.
- ETSI TS 102 573, *Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data objects*.
- ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

- ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- *ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*

En los servicios relativos a los documentos electrónicos CIPSC toma como referencia la normativa de interoperabilidad y, en particular, la Norma Técnica de Interoperabilidad (NTI) de Documento electrónico (Resolución de la Secretaría de Estado para la Función Pública, de 19 de julio de 2011), que define la estructura y otros aspectos básicos de los documentos electrónicos; con la NTI de Reutilización de recursos de información (Resolución de 19 de febrero de 2013), que especifica los metadatos de catálogos de recursos y está basada en el vocabulario RDF DCAT (*DCAT Application Profile for data portals in Europe, European Commission, 2013*); y la NTI de Política de gestión de documentos electrónicos (Resolución de 28 de junio de 2012), en la que se dan las directrices sobre el contenido de la política de gestión de documentos electrónicos y sobre los procedimientos para su elaboración y puesta en acción.

Lo aquí dispuesto se aplica a todos los intervinientes en los servicios de CIPSC, incluyendo a los firmantes, creadores de sellos electrónicos y partes usuarias. Todos ellos deben conocer el contenido del presente documento para que puedan establecer su confianza en los servicios proporcionados por CIPSC y adecuar su actuación a lo dispuesto en el mismo.

Este documento podrá ser utilizado también por terceras entidades y organismos independientes para comprobar y certificar que CIPSC actúa conforme a las políticas y prácticas recogidas en el mismo.

1.2.- Estructura

CIPSC presta los siguientes servicios de confianza:

- Creación, verificación y validación de firmas electrónicas
- Creación, verificación y validación de sellos electrónicos
- Creación, verificación y validación de sellos de tiempo electrónicos
- Servicio de entrega electrónica certificada
- Emisión de certificados relativos a la firma electrónica, los sellos electrónicos, los sellos de tiempo electrónicos y los servicios de entrega electrónica certificada
- Servicios relativos a los documentos electrónicos, que incluyen

- Autenticación de documentos
- Registro y archivo de documentos electrónicos

El presente documento regula en primer lugar los aspectos comunes a todos estos servicios, en los siguientes capítulos:

Régimen jurídico

Establece los derechos y obligaciones de las distintas partes intervinientes en la prestación de los servicios de confianza de CIPSC, así como el marco jurídico en el que estos se desarrollan y los mecanismos previstos para la resolución de conflictos.

Política para la prestación de los servicios de confianza

Tiene como objetivo definir los requisitos a cumplir por CIPSC para la prestación de los servicios de confianza, de acuerdo con los estándares que resulten de aplicación. Se definen los aspectos que son comunes al conjunto de los servicios.

Declaración de prácticas

Establece cómo CIPSC cumple los requerimientos técnicos, organizativos y procedimentales comunes a los distintos servicios y que se han establecido en la política para la prestación de los servicios de confianza.

Seguidamente, para cada uno de los servicios se incluyen los siguientes apartados:

Declaración básica

La declaración básica recoge las condiciones y aspectos fundamentales del servicio, que junto a otras condiciones y aspectos más específicos, se recogen en la Política correspondiente.

Política para la prestación del servicio

Tiene como objetivo definir los requisitos a cumplir por CIPSC para la prestación de un determinado servicio de confianza, de acuerdo con los estándares que resulten de aplicación. Se definen aspectos como los supuestos de utilización, los destinatarios, las condiciones para la prestación y acceso al servicio y los efectos del mismo.

Declaración de prácticas para la prestación del servicio

Establece cómo CIPSC cumple los requerimientos técnicos, organizativos y procedimentales establecidos en la Política del servicio y, en particular, las condiciones y las acciones de gestión y operación que se siguen en la prestación del mismo.

1.3.- Alcance

Este documento establece las reglas generales para la operación de CIPSC y la prestación de los distintos servicios, las obligaciones de CIPSC en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados, las medidas de seguridad técnicas y organizativas, los perfiles de los certificados y los mecanismos de información sobre la vigencia de los certificados.

1.4.- Ámbito de aplicación

Los servicios de CIPSC se prestan con sujeción a la versión de este documento que se encuentre vigente en el momento en el que se hacen efectivos, siendo ésta la que determinará su validez y efectos. Cuando el servicio consista en la generación y/o emisión de firmas electrónicas, sellos electrónicos, sellos de tiempo electrónicos, certificaciones de remisión y recepción de envíos electrónicos, de documentos auténticos y de diligencias de registro o de cualquier otra evidencia electrónica serán estas Políticas las que establecerán la validez y efecto de los mismos a lo largo de todo su ciclo de vida.

1.5.- Identificación

El OID (*object identifier*) de las Políticas y declaración de prácticas de Coloriuris Prestador de Servicios de Confianza es: 1.3.6.1.4.1.37799.0.3.1.2.0.

1.6.- Administración y publicidad

1.6.1.- Validez

Únicamente el Responsable de Administración de Políticas tiene la capacidad para aprobar las Políticas y declaración de prácticas de CIPSC. Esta aprobación deberá constar de forma expresa.

Sin perjuicio de lo dispuesto para la modificación de las Políticas y declaración de prácticas y para el caso de cese de la actividad de CIPSC, el presente documento tiene validez indefinida.

La invalidez de una o más de las previsiones de estas Políticas y declaración de prácticas no afectará al resto del documento. En este caso se tendrán dichas previsiones por no puestas.

1.6.2.- Modificaciones

Solo el Responsable de Administración de Políticas puede realizar y aprobar modificaciones de las Políticas y declaración de prácticas de CIPSC.

Se considerará que existe un cambio de versión cuando a juicio del Responsable de Administración de Políticas las modificaciones puedan afectar a la aceptabilidad de los servicios del CIPSC. En caso contrario se considerará que únicamente hay una nueva redacción de la misma versión.

En el primer supuesto se procederá al incremento del número mayor de versión del documento y la puesta a cero del número menor de la misma, modificándose también los campos correspondientes del Identificador de Objeto (OID), que son el penúltimo y el último, respectivamente. En el segundo supuesto se procederá al incremento del número menor de versión del documento, modificándose únicamente el último campo del Identificador de Objeto (OID).

1.6.3.- Publicidad

Las Políticas y declaración de prácticas de CIPSC se publicarán inmediatamente desde el momento de su aprobación inicial y, en su caso, de su modificación. La dirección web (URL) para la publicación será:

https://cipsc.coloriuris.net/politicas/

También se publicarán en la web los certificados raíz y sellos de las autoridades prestadoras de servicios de CIPSC. Esta publicación se hará en la dirección:

https://cipsc.coloriuris.net/certificados/

La dirección postal de CIPSC se publicará en:

https://cipsc.coloriuris.net/address/

La publicación de anuncios y comunicaciones sobre hechos relevantes que afecten a la prestación de los servicios de la CIPSC, se hará en la dirección de Internet:

https://cipsc.coloriuris.net/anuncios/

Por último, la publicación de las tarifas aplicables a la prestación de los distintos servicios de CIPSC se publicarán en la dirección:

https://cipsc.coloriuris.net/tarifas/

Estos contenidos se encontrarán disponibles de forma permanente, salvo causa de fuerza

mayor, y el acceso a los mismos será gratuito.

1.6.4.- Datos de contacto

Todos los firmantes, creadores de sellos , terceros aceptantes y cualquier entidad o persona que ostente un interés legítimo en relación con los servicios de CIPSC podrán ponerse en contacto con los miembros del mismo de las siguientes formas:

Correo electrónico: cipsc@coloriuris.net

Teléfono: +34976203670

Fax: +34976203671

Correo postal o personándose en la dirección: C/ Alfonso I nº 23, entlo. ctro., 50003 Zaragoza

2 Políticas de los servicios de CIPSC

2.1.- Estructura de CIPSC

2.1.1.- Responsable de Administración de Políticas de Coloriuris

El Responsable de Administración de Políticas es un miembro de Coloriuris que aprobará las presentes Políticas y declaración de prácticas, así como sus modificaciones. Todos los documentos de políticas y declaración de prácticas de CIPSC deben ser aprobados por el Responsable de Administración de Políticas.

El Responsable de Administración de Políticas es responsable de que la prestación de los servicios del CIPSC se ajuste a lo dispuesto en estas Políticas y declaración de prácticas y de asegurar la efectiva ejecución de los controles previstos. Asimismo se encarga de la dirección, supervisión y control de la prestación de los servicios de CIPSC, de las operatorias seguidas por cada una de sus autoridades prestadoras de servicios y de la correcta aplicación por las mismas de lo establecido en el presente documento.

El Responsable de Administración de Políticas se encarga también de analizar los informes de las auditorías, totales o parciales, que se hagan de CIPSC y de sus servicios, así como de establecer y supervisar, en su caso, las acciones correctoras a ejecutar.

El Responsable de Administración de Políticas será nombrado y cesado por la dirección de Coloriuris, mediante resolución expresa de la que deberá quedar constancia escrita.

2.1.2.- Autoridades prestadoras de los servicios de confianza de CIPSC

2.1.2.1.- Aspectos comunes

CIPSC dispone de cuatro autoridades prestadoras de servicios, que se sujetan a las políticas y prácticas establecidas en este documento y son las siguientes:

- Autoridad de certificación (AC): se encarga de la generación, emisión y revocación de certificados de firma electrónica y sello electrónico.
- Autoridad de Certificación v3 (ACv3): se encarga de la generación, emisión y revocación de certificados de sello electrónico.
- Autoridad de sellado de tiempo (TSACI): se encarga de la generación y emisión de sellos de tiempo y de certificados de entrega electrónica certificada.

- Autoridad para los servicios relativos a los documentos electrónicos (ASD): se encarga de la prestación de los servicios de creación, verificación, validación y autenticación de documentos electrónicos y del registro y archivo de documentos electrónicos.

Cada autoridad dispone de un certificado autofirmado y puede disponer también de sellos respaldados por este certificado raíz, que serán emitidos por la propia autoridad prestadora del servicio. Las claves asociadas a estos certificados se conservarán en un dispositivo criptográfico con los niveles de seguridad establecidos en estas Políticas.

En todo caso, CIPSC quedará identificado en los certificados electrónicos raíz de cada una de sus autoridades prestadoras de servicios, así como en los certificados emitidos para la prestación de cada uno de los servicios, tanto se trate de sellos electrónicos como de los certificados personales de los administradores y operadores, y en las evidencias que sean resultado de la prestación de uno de sus servicios.

Los administradores de cada una de las autoridades son las personas que dentro de Coloriuris tienen privilegios para generar y utilizar el certificado y claves raíz de dicha autoridad, así como los sellos derivados del mismo. En todo momento dichas personas estarán expresamente identificadas en la documentación interna de la CIPSC.

2.1.2.2.- Autoridad de certificación (AC) y Autoridad de certificación v3 (ACv3)

Los servicios que presta son los siguientes:

- Creación, verificación y validación de firmas electrónicas y sellos electrónicos: comprende los componentes técnicos y organizativos que emiten los certificados.
- Gestión del servicio de certificación: comprende los componentes técnicos y organizativos que supervisan y controlan que la operativa de la emisión de certificados se realice de forma adecuada.

2.1.2.3.- Autoridad de sellado de tiempo (TSACI)

Los servicios que presta son los siguientes:

- Creación, verificación y validación de sellos de tiempo: comprende los componentes técnicos y organizativos que emiten los sellos de tiempo.
- Gestión del servicio de sellado de tiempo: comprende los componentes técnicos y organizativos que supervisan y controlan que la operativa de la emisión de sellos de tiempo se realice de forma adecuada incluyendo, en particular, la sincronización temporal con la fuente fiable de referencia.

- Creación, verificación y validación de las evidencias asociadas a las certificaciones de remisión y recepción de entrega electrónica certificada y la gestión de emisión de entrega electrónica certificada y acreditación de ésta y de la recepción.

2.1.2.4.- Autoridad para los servicios relativos a los documentos electrónicos (ASD)

Los servicios que presta son los siguientes:

- Generación de las evidencias asociadas a los servicios relativos a los documentos electrónicos: comprende los componentes técnicos y organizativos que emiten los documentos electrónicos autenticados por CIPSC, las diligencias de registro y las demás evidencias resultantes de la prestación de los servicios relativos a los documentos electrónicos.

- Gestión de los servicios relativos a los documentos electrónicos: comprende los componentes técnicos y organizativos que supervisan y controlan que las operativas de autenticación de documentos electrónicos y la de registro y archivo de documentos electrónicos se realizan de forma adecuada.

La ASD opera el Archivo de documentos, que será un sistema adecuado para la preservación de los mismos, que se realizará en nombre y a cargo de CIPSC. Los administradores de la ASD, además de tener los privilegios de administración y configuración previstos en el apartado 2.1.2.1, los tendrán sobre el Archivo de documentos.

2.1.3.- Autoridades de registro

Las Autoridades de Registro (AR) reciben y procesan las solicitudes para la prestación de servicios de confianza por CIPSC y cumplen las demás funciones que, en su caso, se determinen en las correspondientes Políticas. En todo caso realizan las siguientes tareas:

- Recepción de los datos requeridos para la prestación de los servicios y, en su caso, comprobación de la identidad de los solicitantes, firmantes y creadores de sellos de los mismos así como de las demás circunstancias que sean requeridas para la prestación.

- Recepción y conservación de los documentos en soporte papel generados en el proceso de solicitud y prestación del servicio.

CIPSC dispondrá al menos de una AR incluida en su propia estructura. Opcionalmente podrán crearse otras AR, tanto dentro de CIPSC como a través de entidades externas, en cuyo caso será preciso que exista un contrato escrito, en el que la entidad externa deberá comprometerse expresamente a cumplir con lo dispuesto en este documento. Asimismo se establecerá la obligatoriedad de realizar auditorías, así como la periodicidad de las mismas. Las auditorías podrán

ser realizadas por Coloriuris o por una entidad externa.

Los operarios de las AR dispondrán de certificados emitidos por la Autoridad de certificación de CIPSC con los que firmaran electrónicamente las solicitudes de prestación de servicios que dirijan a las diferentes autoridades, cuando así lo establezca la correspondiente Política. La comunicación telemática entre las AR y las distintas autoridades se realizará a través de canales cifrados.

2.2.- Firmantes y partes usuarias

2.2.1.- Firmantes y creadores de sellos

Los firmantes y creadores de sellos son, respectivamente, las personas físicas y jurídicas que crean una firma electrónica o un sello electrónico utilizando los servicios de certificación prestados por CIPSC y que, por lo tanto, aceptan los términos y condiciones bajo los cuales éstos se prestan.

Los firmantes y creadores de sellos son responsables del uso que hagan de los servicios de CIPSC y, en la medida de sus posibilidades, han de contribuir a que las partes usuarias puedan valorarlos adecuadamente y conocer las condiciones que rigen su uso, especialmente en lo que se refiere a los efectos y validez de los certificados, sellos de tiempo, documentos autenticados y certificados de entrega.

Algunas de las Autoridades de CIPSC utilizan los servicios de las otras Autoridades para prestar sus servicios a los firmantes y creadores de sellos. Asimismo Coloriuris S.L. utiliza los servicios de CIPSC para la prestación de algunos de sus servicios, como *actaNavegacion*, *actaFirma* o *actaSMS*, entre otros. En estos casos Coloriuris actúa como creador de sellos electrónicos de los servicios y tiene las obligaciones establecidas para los mismos en este documento.

2.2.2.- Partes usuarias

Las partes usuarias son las personas físicas o jurídicas que confían en la identificación electrónica y los servicios de confianza de CIPSC y en las evidencias generadas por CIPSC como resultado de los mismos, especialmente firmas electrónicas, sellos electrónicos, sellos de tiempo electrónicos, documentos autenticados, certificaciones de remisión y recepción de entrega electrónica certificada y diligencias de registro.

2.2.3.- Aceptación de las Políticas y declaración de prácticas

Todos los firmantes y creadores de sellos de los servicios de CIPSC, por el mero hecho de utilizarlos, así como las partes usuarias, asumen en su totalidad lo dispuesto en la versión de las

Políticas y declaración de prácticas vigentes en el momento en el que se recibió el servicio solicitado o se aceptaron las evidencias resultantes del mismo, respectivamente.

El OID de estas Políticas y declaración de prácticas se incluirá en todas las evidencias que se generen y emitan en la prestación de los servicios del CIPSC como acreditación de su conformidad con la misma. Con este mismo fin, CIPSC sólo aceptará las peticiones de servicios que incluyan el OID de estas Políticas y declaración de prácticas o que, como mínimo exigible, no incluyan la mención a otra u otras políticas en forma tal que pudiera deducirse la conformidad con las mismas.

2.2.4.- Verificación de las evidencias

Los firmantes, creadores de sellos y partes usuarias deberán actuar con la debida diligencia para comprobar la autenticidad de las evidencias provenientes de los servicios de CIPSC, verificando que han sido firmadas correctamente y que la clave privada utilizada para su firma no estaba comprometida en el momento de la verificación. Durante el periodo de validez de los certificados utilizados por las autoridades prestadoras de los servicios de CIPSC, el estado de las claves privadas podrá verificarse en las direcciones indicadas en el apartado 1.6.3.

Una vez que caduquen los certificados utilizados por CIPSC las partes usuarias podrán confiar en las firmas respaldadas por los mismos si en el momento de la verificación se conoce que la clave privada correspondiente no ha sido comprometida en ningún momento y que tanto la función hash utilizada para la generación de la evidencia, así como el algoritmo criptográfico y el tamaño de la clave utilizados para firmarla electrónicamente se consideran todavía seguros.

2.3.- Obligaciones

2.3.1.- Coloriuris

Coloriuris asume la responsabilidad de que los servicios prestados por CIPSC se realizan de acuerdo con lo dispuesto en estas Políticas y declaración de prácticas, y del cumplimiento, tanto de los requisitos y controles establecidos en las mismas, como de las disposiciones legales que sean aplicables. En particular, asume las siguientes obligaciones:

1) Prestar los servicios de acuerdo con lo dispuesto en estas Políticas y declaración de prácticas.
2) Garantizar que las evidencias emitidas no contienen ningún dato erróneo o falso.
3) Utilizar tecnologías y equipos adecuados, y contar con personal con formación específica e informado de sus obligaciones.

4) Proporcionar acceso ininterrumpido a sus servicios, excepto en caso de interrupciones programadas o incidencias graves.

5) Llevar a cabo las revisiones y auditorías precisas para asegurar el cumplimiento de la legislación aplicable, de las Políticas y declaración de prácticas y de la normativa interna.

6) Publicar en su web información sobre las incidencias que hayan podido afectar a los servicios de forma que sea posible conocer cuáles han sido, en su caso, las evidencias afectadas.

2.3.2.- Obligaciones de los firmantes y creadores de sellos

Es obligación de los firmantes y creadores de sellos de los servicios de CIPSC:

1) Utilizar medios adecuados para la solicitud de los servicios y, en su caso, para la obtención de las evidencias resultantes del mismo.

2) Verificar la validez de las evidencias, según lo dispuesto en el apartado 2.2.4.

3) Conocer y aceptar las condiciones y limitaciones de utilización de las evidencias que se hayan establecido en la Política correspondiente.

4) Limitar y adecuar el uso de las evidencias resultantes del servicio a lo permitido por la Política que las regule.

5) No monitorizar la prestación de los servicios del CIPSC, ni manipularlos o alterar su correcto funcionamiento, ni realizar actos de ingeniería inversa sobre su implementación.

2.3.3.- Obligaciones de las partes usuarias

Es obligación de las partes usuarias que acepten y confíen en las evidencias emitidas por CIPSC:

1) Verificar la validez de las evidencias, según lo dispuesto en el apartado 2.2.4.

2) No confiar en las evidencias para usos distintos de los permitidos en la Política correspondiente.

3) Tener conocimiento de lo dispuesto en las presentes Políticas, aceptando y sujetándose a lo dispuesto en las mismas y, en particular, a las responsabilidades aplicables en la aceptación y uso de los servicios del CIPSC y de las evidencias resultantes de los mismos.

4) Notificar cualquier hecho o situación anómala relativa a los servicio del CIPSC y/o a las evidencias emitidas, y que pueda ser considerado como causa de revocación de las mismas.

2.4.- Responsabilidad de CIPSC

CIPSC sólo responderá en el caso de incumplimiento de las obligaciones contenidas en la legislación aplicable y en las presentes Políticas y declaración de prácticas.

CIPSC no asumirá responsabilidad alguna respecto a la utilización de las evidencias emitidas para cualquier uso no autorizado en las presentes Políticas y declaración de prácticas.

CIPSC no se responsabiliza del contenido de los documentos y datos a los que se apliquen sus servicios, y no responde de posibles daños y perjuicios en transacciones en las que se hayan utilizado.

CIPSC no representa en forma alguna a los firmantes, creadores de sellos ni partes usuarias de las evidencias que emite.

CIPSC no da ninguna garantía ni asume responsabilidad alguna, ante titulares de certificados o cualquier otra evidencia emitida ni ante las partes usuarias de las mismas, fuera de lo establecido en las presentes Políticas y declaración de prácticas.

CIPSC dispone de un seguro de responsabilidad civil, con una cobertura de tres millones de euros (3.000.000,00 €).

2.5.- Datos personales y confidencialidad

2.5.1.- Protección de datos de carácter personal

CIPSC aplica lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y su normativa de desarrollo, garantizando las normas y procedimientos internos de Coloriuris a la aplicación del nivel de seguridad exigido por esta normativa.

Cuando para la prestación de un determinado servicio sea necesario recabar datos personales del firmante, se verificará que éste es informado y presta su consentimiento al tratamiento de sus datos personales, a la finalidad de éste, y a su inclusión en el fichero declarado al efecto por Coloriuris.

Los datos de carácter personal no serán comunicados a terceros sin el consentimiento expreso del titular, salvo en el supuesto de que una Ley lo autorice expresamente.

2.5.2.- Información confidencial

Se considerará confidencial toda información que no sea declarada expresamente por CIPSC

como pública. En particular, tiene carácter confidencial la siguiente información:

- Las claves privadas utilizadas por CIPSC y por sus administradores y operarios.
- La información sobre las operaciones que lleve a cabo CIPSC.
- La información sobre seguridad, control y procedimientos de auditoría.
- La información de carácter personal de los firmantes.

Se considerará información pública y por lo tanto accesible por terceros la contenida en las presentes Políticas y declaración de prácticas, y aquella otra que así sea declarada por CIPSC.

2.5.3.- Deber de secreto

Todas las personas que tengan relación laboral o profesional con CIPSC están obligadas a guardar secreto de toda la información confidencial a la que tuvieran acceso en virtud de dicha relación. CIPSC les informará por escrito, al menos en el comienzo de la relación, guardando constancia de que dicha información ha sido recibida por el destinatario. Esta obligación persistirá una vez finalidad la vinculación con CIPSC.

2.6.- Auditorías

Coloriuris realizará auditorías del funcionamiento del CIPSC y de las autoridades encargadas de prestar los distintos servicios, al menos con periodicidad anual. Las auditorías deberán ser realizadas por un auditor independiente. Asimismo, y como se dispone en el apartado 2.1.3, se realizarán auditorías a las Autoridades de Registro, tanto a las integradas en la estructura de CIPSC como a las externas. Estas auditorías se realizarán como mínimo cada dos años y podrán ser realizadas por CIPSC o por una entidad externa.

En todas las auditorías se verificará, como mínimo, que las prácticas de CIPSC y sus autoridades prestadoras de servicios se ajustan a lo establecido en estas Políticas, a lo dispuesto por las autoridades administrativas y a lo establecido en la normativa vigente, así como que disponen de una metodología que garantiza la calidad de los servicios prestados.

2.7.- Tarifas

CIPSC publicará en el repositorio mencionado en el apartado 1.6.3 las tarifas que aplica para la prestación de cada uno de sus servicios.

CIPSC no aplicará ninguna tarifa por el acceso a la información necesaria para verificar la

validez las evidencias emitidas, ni a las presentes Políticas y declaración de prácticas, ni a la información que, en virtud de lo dispuesto en las mismas, deba hacerse pública.

2.8.- Reclamaciones y jurisdicción

2.8.1.- Comunicación de las reclamaciones

Cuando un firmante, creador de sellos o parte usuaria tengan una reclamación respecto a los servicios de CIPSC deberá comunicársela por cualquiera de los medios de contacto indicados en el apartado 1.6.4 de este documento. CIPSC contestará a la reclamación en el plazo máximo de una semana.

2.8.2.- Jurisdicción

Los firmantes, creadores de sellos y partes usuarias de los servicios de CIPSC aceptan la jurisdicción de los juzgados y tribunales de Zaragoza para cualquier controversia que pudiera suscitarse en relación con la prestación de servicios por parte de CIPSC, con expresa renuncia de cualquier otro fuero que pudiera corresponderles.

3 Declaración de prácticas

3.1.- Introducción

El funcionamiento de CIPSC se basa en las infraestructuras técnicas, los procedimientos y los mecanismos de control que se describen en esta Declaración de prácticas. Junto con el capítulo anterior, que se refiere a las Políticas, regulan la operación y requisitos que son comunes a los distintos servicios de confianza prestados por CIPSC.

Este documento y la demás información que resulte relevante para que los firmantes, creadores de sellos y partes usuarias valoren los servicios de CIPSC, se publican en los repositorios descritos en el apartado 1.6.3.

El Responsable de Administración de Políticas es responsable de mantener y aprobar todas las políticas y prácticas que rigen el funcionamiento de CIPSC, así como de la implementación y aplicación de las mismas. Entre otras medidas, CIPSC realiza evaluaciones y auditorías periódicas para determinar el estado de los controles y procedimientos de seguridad, efectuar el análisis de vulnerabilidades y aplicar las medidas que resulten pertinentes.

Coloriuris, a través del Responsable de Administración de Políticas, se responsabiliza de adoptar las medidas de seguridad necesarias para cumplir con los estándares y leyes que sean de aplicación, así como con las políticas y prácticas recogidas en el presente documento para la prestación de los servicios.

3.2.- El ciclo de vida de los certificados

Todos los certificados emitidos y utilizados por las Autoridades de CIPSC se ajustan al estándar X.509 versión 3 y al RFC 3039 "*Internet X.509 Public Key Infrastructure Qualified Certificates Profile*".

Los identificadores únicos (OID) de los algoritmos con cifrado RSA utilizados son los siguientes:

- SHA256RSA: 1.2.840.113549.1.1.11
- SHA512RSA: 1.2.840.113549.1.1.13

Las especificaciones contenidas en este apartado lo son sin perjuicio de las estipulaciones previstas en cada una de las políticas de certificación correspondientes a cada tipo de certificado.

3.2.1.- Solicitud de certificados

La Autoridad de Registro de CIPSC que reciba la solicitud le compete el determinar que el tipo de certificado solicitado se adecue a las características concretas del solicitante, de conformidad con el contenido de la Política de Certificación aplicable a dicho certificado y, de este modo, resolver la solicitud formulada.

En cada Política de Certificación se especifica la información que debe suministrarse con carácter previo, a quien solicite un certificado.

Sin perjuicio de lo cual se informa que:

a) La identificación de las personas físicas que soliciten un certificado reconocido exigirá su personación ante el operador de registro de la Autoridad de Registro de CIPSC (o de las A.R. externas que puedan crearse en el futuro) y se acreditará mediante el documento nacional de identidad, pasaporte u otros medios admitidos en derecho. Podrá prescindirse de la personación si su firma en la solicitud de expedición de un certificado reconocido ha sido legitimada en presencia notarial.

b) En el caso de certificados reconocidos de personas jurídicas (sellos electrónicos conforme a la denominación dada por R.U.E. 910/2014), el operador de registro de la A.R. de CIPSC (o de las A.R. externas que puedan crearse en el futuro) comprobará, además, los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público.

3.2.2.- Tramitación de la solicitud de certificados.

Compete a la Autoridad de Registro de CIPSC la comprobación de la identidad del solicitante, la verificación de la documentación y la constatación de que el solicitante ha firmado el documento de comparecencia. Una vez completa la solicitud, la Autoridad de Registro la remitirá a la AC correspondiente de CIPSC.

3.2.3.- Emisión de certificados

CIPSC no es responsable de la monitorización, investigación o confirmación de la exactitud de la información contenida en el certificado con posterioridad a su emisión. En el caso de recibir información sobre la inexactitud o la no aplicabilidad actual de la información contenida en el certificado, este puede ser revocado.

La emisión del certificado tendrá lugar una vez que CIPSC haya llevado a cabo las

verificaciones necesarias para validar la solicitud de certificación. El mecanismo por el que determina la naturaleza y la forma de realizar dichas comprobaciones es la Política para la prestación de los servicios de certificación.

3.2.4.- Aceptación de certificados

La aceptación de los certificados por parte de los firmantes y/o creadores de sellos se produce en el momento de la firma del contrato de certificación asociado a cada Política de Certificación. La aceptación del contrato implica el conocimiento y aceptación por parte del firmante y/o creador de sellos de la Política de Certificación asociada.

3.2.5.- Uso del par de claves y del certificado.

Los usos del par de claves y certificado quedan definidos por cada Política de Certificación asociada.

3.2.6. Renovación de certificados.

En cada una de las Políticas de Certificación asociadas a cada tipo de certificado se detalla la posibilidad o no de renovar los certificados, así como las condiciones para proceder a su renovación.

3.2.7. Renovación de claves

La renovación de claves implica necesariamente la renovación de certificado y no se pueden llevar a cabo como procesos separados.

3.2.8. Modificación de certificados.

No se pueden modificar los campos de los certificados. Cualquier modificación necesaria implicará un proceso de renovación del certificado.

3.2.9. Revocación y suspensión de certificados.

3.2.9.1. Circunstancias para la revocación

En general un certificado se revoca cuando:

- El firmante/creador de sellos o sus claves o las claves de sus certificados se han comprometido por:

- El robo, pérdida, revelación, modificación, u otro compromiso o sospecha de compromiso de la clave privada del usuario.
- El mal uso deliberado de claves y certificados, o la falta de observación de los requerimientos operacionales del acuerdo de suscripción, o de la presente DPC.

- Se produce la emisión defectuosa de un certificado debido a:
  - Que no se ha satisfecho un prerrequisito material para la emisión del certificado.
  - Que un factor fundamental en el certificado se sepa o crea razonablemente que puede ser falso.
  - Un error de entrada de datos u otro error de proceso.
- El par de claves generado por un usuario final se revela como "débil".
- La información contenida en un certificado o utilizada para realizar su solicitud se convierte en inexacta, por ejemplo cuando el dueño de un certificado cambia su nombre.
- Una solicitud de revocación válida se recibe de un usuario final.
- Una solicitud de revocación válida se recibe de una tercera parte autorizada, por ejemplo una orden judicial.
- El certificado de una AR o AC superior en la jerarquía de confianza del certificado es revocado.

Si bien las circunstancias para la revocación podrán ser especificadas en cada Política de Certificación correspondiente.

3.2.9.2. Entidad que puede solicitar la revocación

La revocación de un certificado se puede instar tanto por el firmante/creador de sellos como por parte de CIPSC, así como por cualquier persona que conozca fehacientemente que los datos asociados al certificado se convierten en inexactos o incorrectos.

Los firmantes y creadores de sellos pueden solicitar la revocación de su certificado por cualquier causa y deben solicitarla bajo las condiciones especificadas en el siguiente apartado.

3.2.9.3. Procedimiento de solicitud de revocación

El procedimiento para la solicitud de la revocación de cada tipo de certificado se definirá en la Política de Certificación correspondiente.

3.2.9.4. Periodo de gracia de la solicitud de revocación

La revocación se realizará de forma inmediata al procesamiento de cada solicitud verificada como válida. Por tanto no existe ningún periodo de gracia asociado a este proceso.

3.2.9.5. Circunstancias para la suspensión

La suspensión implica invalidez del certificado durante el tiempo que permanece suspendido. La suspensión únicamente se puede declarar si así lo dispone una autoridad judicial o administrativa, por el tiempo que la misma establezca. CIPSC no soporta la suspensión de certificados como operación independiente sobre sus certificados.

3.2.9.6. Entidad que puede solicitar la suspensión

La suspensión solo se podrá solicitar por parte de una autoridad judicial o administrativa.

3.2.9.7. Procedimiento para la solicitud de suspensión

La suspensión de un certificado deberá solicitarse por mandamiento judicial o administrativo.

3.2.9.8. Límites del período de suspensión

El que establezca la autoridad judicial o administrativa competente.

3.2.9.9. Frecuencia de emisión de CRLs

CIPSC publicará las CRL's de sus AACC en su repositorio cada 7 días siempre que no se hayan producido revocaciones, en caso de haber una revocación, la CRL correspondiente se publicará inmediatamente, sin perjuicio de que esta revocación pueda conocerse también mediante OCSP.

3.2.9.10. Requisitos de comprobación de estado de certificados

La verificación del estado de los certificados es obligatoria para cada uso de los certificados de entidades finales. Dicha comprobación puede hacerse a través del protocolo OCSP que proporciona CIPSC indicado en el apartado 4.2.1.5.

Adicionalmente CIPSC también contempla la publicación de CRLs.

3.2.9.11. Otras formas de divulgación de información de revocación disponibles

CIPSC se reserva la posibilidad de establecer en el futuro otras formas para informar de la revocación de los certificados.

3.2.9.12. Requisitos especiales de renovación de claves comprometidas

No hay ninguna variación en las cláusulas anteriores cuando la revocación sea debida al

compromiso de la clave privada.

3.2.10. Servicios de comprobación de estado de certificados.

3.2.10.1 Características operativas

CIPSC ofrece un servicio gratuito de publicación de Listas de Certificados Revocados (CRL) sin restricciones de acceso. Adicionalmente, ofrece servicios de validación de certificados mediante el protocolo OCSP,

3.2.10.2 Disponibilidad del servicio

Los sistemas CRLs y OCSP de consulta en línea del estado de los certificados están disponibles durante las 24 horas los 7 días de la semana.

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.

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

3.2.11. Finalización de la suscripción.

La suscripción finaliza con la expiración o revocación del certificado.

3.2.12. Depósito y recuperación de claves.

CIPSC no ofrece ese servicio.

3.3.- Controles de seguridad física, de procedimiento y de personal

3.3.1.- Controles de seguridad física

3.3.1.1.- Localización y construcción de las instalaciones

Las instalaciones en las que se procesa información cumplen los siguientes requisitos físicos:

- El edificio que contiene las instalaciones de procesamiento de información es físicamente

sólido, los muros externos del emplazamiento son de construcción sólida y está permanentemente vigilado por cámaras de seguridad, permitiendo únicamente el acceso a personas debidamente autorizadas.

- La sala de procesamiento tiene sus puertas cerradas y protegidas contra accesos no autorizados y no dispone de ventanas.

3.3.1.2.- Acceso físico

Las instalaciones disponen de un sistema de control de acceso físico:

- Únicamente está permitido el acceso a personal autorizado.
- Los derechos de acceso al área segura son revisados y actualizados periódicamente.
- Se requiere que todo el personal porte algún elemento de identificación visible y se fomenta que el personal requiera dicha identificación a cualquiera que no disponga de la misma.
- El personal ajeno a la operación de CIPSC que se encuentre trabajando en sus instalaciones es supervisado.
- Se mantiene de forma segura un fichero de los accesos conforme a la ISO 27001.
- Las puertas de entrada están dotadas con mecanismos de acceso.
- Un circuito cerrado de televisión que monitoriza la sala desde la que se presta el servicio de certificación.

3.3.1.3.- Electricidad y aire acondicionado

El Centro de Proceso de Datos cuenta con sistemas de energía y aire acondicionado adecuados para garantizar un entorno operativo fiable.

Así mismo las instalaciones disponen de una funcionalidad de alimentación ininterrumpida (SAI) que mantiene los equipos en funcionamiento durante el tiempo necesario para el cierre ordenado de los sistemas en el caso en que un fallo de energía o aire acondicionado provocara la caída de los mismos.

3.3.1.4.- Exposición al agua

Se han adoptado las medidas necesarias para minimizar los riesgos derivados de los daños por agua.

3.3.1.5.- Prevención y protección de incendios

El Centro de Procesos de Datos dispone de sistemas de detección automática de incendios con la finalidad de:

- Avisar del inicio de un incendio al servicio de vigilancia y al personal.
- Cumplir con las misiones de desconexión del sistema de ventilación, corte de la energía eléctrica y el disparo de la instalación automática de extinción.

3.3.1.6.- Almacenamiento de soportes

Los soportes de las copias de seguridad se almacenan de forma segura.

3.3.1.7.- Tratamiento de residuos

Los soportes que contengan información confidencial se destruyen de tal manera que la información no pueda recuperarse después de su destrucción.

3.3.1.8.- Copia de respaldo fuera de las instalaciones

CIPSC almacena los soportes de las copias de seguridad de forma que se encuentren protegidos frente a accidentes y a una distancia suficiente para evitar que resulten dañados en el caso de un desastre en el emplazamiento principal.

3.3.2.- Controles de procedimientos

3.3.2.1.- Funciones fiables

Se define “rol de confianza” como aquel al que se le asignan funciones que pueden dar lugar a problemas de seguridad si no se realizan adecuadamente, bien por accidente o de forma

malintencionada.

Con la finalidad de incrementar la probabilidad de que las funciones correspondientes a un "rol de confianza" se realicen correctamente, se contemplan dos enfoques:

- El primero es el diseño y configuración de la tecnología, de forma que se eviten errores y se prohíba un comportamiento inadecuado.
- El segundo es la distribución de las funciones entre varias personas de forma que la actividad malintencionada requiera la connivencia de varias de ellas.

Según lo especificado en la norma CEN CWA 14167-1, los roles mínimos establecidos son:

- **Responsable de Seguridad (Security Officer):** Mantiene la responsabilidad global sobre la administración y la implementación de las políticas y procedimientos de seguridad.
- **Administradores del sistema de Certificación (System Administrators):** Autorizado para realizar cambios en la configuración del sistema.
- **Operadores de Sistemas (System Operator):** Responsables de la gestión del día a día del sistema (Monitorización, backup, recovery,…)
- **Auditor interno (System Auditor):** Autorizado a acceder a los logs del sistema y verificar los procedimientos que se realizan sobre el mismo.
- **Operador de AC - Operador de Certificación :** Responsables de activar las claves de CA en el entorno Online.
- **Operador de AR (Registration Officer):** Responsables de aprobar, emitir, suspender y revocar los certificados de Entidad final.

Concretamente:

Las tareas de Auditor son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas.

Las personas implicadas en Administración de Sistemas no podrán ejercer ninguna actividad en las tareas de Auditoría o Certificación.

3.3.2.2.- Número de personas por tarea

Para reforzar la seguridad del sistema, se asignan personas diferentes para cada rol con la excepción del rol de operador que puede ser asumido por el administrador.

Además, se pueden asignar múltiples individuos a un mismo rol.

3.3.2.3.- Identificación y autenticación para cada rol

Los roles de confianza exigen la autenticación con un medio suficientemente seguro, y en cualquier caso siempre con usuarios personales.

3.3.2.4.- Separación de tareas en los diferentes roles

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurara que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

3.3.3.- Controles de personal

3.3.3.1.- Requisitos de historial, calificaciones, experiencia y autenticación

CIPSC emplea personal que posee la experiencia y calificación necesarias para los servicios que debe realizar.

Todo el personal con roles fiables está libre de intereses que puedan perjudicar la imparcialidad de las operaciones de CIPSC.

3.3.3.2.- Procedimientos de investigación de historial

No aplica según la legislación española.

3.3.3.3.- Requisitos de formación

El personal de CIPSC recibe la formación requerida para asegurar su competencia en la realización de sus funciones. Se incluye en la formación los siguientes puntos:

- Entrega de una copia de la Declaración de Prácticas de Certificación.
- Concienciación sobre la seguridad.
- Operación del software y hardware para cada rol específico.

- Procedimientos de seguridad para cada rol específico.
- Procedimiento de operación y administración para cada rol específico.
- Procedimientos para la recuperación de desastres.

3.3.3.4.- Requisitos y frecuencia de actualización formativa

Ante cambios tecnológicos del entorno, introducción de nuevas herramientas o modificación de procedimientos operativos, se llevará a cabo la formación adecuada para el personal afectado.

Ante cambios en la Declaración de Prácticas de Certificación, Políticas de Certificación u otros documentos relevantes, se llevarán a cabo sesiones formativas.

3.3.3.5.- Secuencia y frecuencia de rotación laboral

No aplicable.

3.3.3.6.- Sanciones para acciones no autorizadas

En el caso de comisión de una acción no autorizada con respecto a la operación de la Autoridad de Certificación se tomarán medidas disciplinarias. Se considerarán acciones no autorizadas las que contravengan la Declaración de Prácticas de Certificación o las Políticas de Certificación pertinentes tanto de forma negligente como malintencionada.

Si se produce alguna infracción, CIPSC suspenderá el acceso de las personas involucradas a todos los sistemas de información de CIPSC de forma inmediata al conocimiento del hecho.

Adicionalmente, en función de la gravedad de las infracciones, se aplicarán las sanciones previstas en el convenio colectivo de la empresa, o el Estatuto de los Trabajadores según corresponda a la situación laboral del infractor.

3.3.3.7.- Requisitos de contratación de personal

CIPSC manifiesta que cumple en su integridad la normativa vigente en materia de igualdad de oportunidades entre hombres y mujeres, y que además tiene una política activa al respecto.

CIPSC se compromete a que todo el personal adscrito a los Servicios conozca, asuma y

cumpla las obligaciones de esta Política y Declaración de Prácticas en cuanto a la forma y modo de su cumplimiento, seguridad y confidencialidad, que se harán extensivas a todos los intervinientes en los procesos, tratamientos y ejecución de las labores de certificación, constituyendo su código ético. A tal efecto CIPSC se compromete a obtener de cada uno de sus empleados y colaboradores un compromiso escrito en tal sentido.

CIPSC declara conocer los Principios del Pacto Mundial de las Naciones Unidas, asumiendo íntegramente su contenido y comprometiéndose a su estricto cumplimiento.

En relación a la asignación de roles y responsabilidades se estará a lo dispuesto en el apartado 3.3.2.1.

3.3.3.8.- Suministro de documentación al personal

Todo el personal relacionado con roles fiables recibe:

- Una copia de la Declaración de Prácticas de Certificación
- La documentación que define las obligaciones y procedimientos de cada rol.
- Tiene acceso a los manuales relativos a la operación de los diferentes componentes del sistema.

3.3.4.- Procedimientos de log y auditoría

Se utilizarán los ficheros de log para reconstruir los eventos significativos que han sido realizados por el software utilizado por CIPSC y las Entidades de Registro y el usuario o evento que los originó. Será también utilizado como un medio de arbitraje en posibles disputas mediante la comprobación de la validez de una firma en un momento determinado.

3.3.4.1.- Tipo de eventos registrados

Se almacenan en los logs:

- Todos los eventos relativos al ciclo de vida de las claves criptográficas.
- Todos los eventos relativos al ciclo de vida de los certificados.
- Todos los eventos relativos a la emisión de dispositivos criptográficos.

- Todos los eventos relativos a la administración de cuentas de operadores y administradores de CIPSC.

Se graba la fecha y hora de cada evento, utilizando una base de tiempos fiable.

3.3.4.2.- Frecuencia de procesamiento de logs

Los ficheros log son revisados periódicamente por el auditor de CIPSC.

3.3.4.3.- Periodo de retención del log

La información generada en el fichero log se mantiene en línea hasta el momento de ser archivada. Una vez archivados, los ficheros log son mantenidos durante 7 años.

3.3.4.4.- Protección del log

Se asigna a los Auditores el derecho de lectura del registro de log.

Está impedido el borrado no autorizado de los registros de log y la modificación de los mismos, mediante la escritura de los registros de log en un medio no modificable como un CD-ROM u otros.

3.3.4.5.- Procedimiento de backup del log

Se realizan copias de seguridad del log en línea con la misma planificación y controles que para el resto de elementos del sistema de CIPSC.

3.3.4.6.- Recolección de logs

Los archivos de log de AACC y AARR son almacenados en los sistemas internos de CIPSC.

3.3.4.7.- Notificación de la acción causante de los logs

No está contemplada la notificación de la acción de los ficheros log al origen del evento.

3.3.4.8.- Análisis de vulnerabilidades

Se realiza un análisis de vulnerabilidades periódico en los sistemas internos de CIPSC.

3.3.5.- Archivado de registros

3.3.5.1.- Tipo de registros archivados

Los tipos de datos o ficheros que son archivados, entre otros, son los siguientes:

- Datos relacionados con el procedimiento de registro y solicitud de certificados;
- Los registros de auditoría de la sección anterior;
- Histórico de claves

3.3.5.2.- Periodo de retención del archivo

Toda la información y documentación relativa a los certificados se conserva durante 15 años (a partir de la fecha de emisión).

3.3.5.3.- Protección del archivo

Se adoptarán las medidas de protección del archivo, para que no pueda ser manipulado ni destruido su contenido.

3.3.5.4.- Procedimientos de backup del archivo

Existe una política de copias de seguridad, Plan de Contingencias y plan de continuidad de negocio que definen los criterios y estrategias de actuación ante una incidencia. El diseño de toda la estrategia de actuación ante incidencias se basa en el correspondiente inventario de activos y análisis de riesgos.

3.3.5.5.- Requisitos para el sellado de tiempo de los registros

Los sistemas de información empleados por CIPSC garantizan el registro de los instantes de tiempo en los que se realizan. El instante de tiempo de los sistemas proviene de una fuente segura de fecha y hora. Todos los sistemas sincronizan su instante de tiempo con esta fuente.

3.3.5.6.- Sistema de archivo

El sistema de archivo se encuentra ubicado en las instalaciones de CIPSC y en las entidades que participan en la prestación del servicio.

3.3.5.7.- Procedimientos para obtener y verificar la información del archivo

El acceso a esta información está restringido al personal autorizado a tal efecto, protegiéndose frente a accesos físicos y lógicos según lo establecido en otras secciones del apartado 3.4 y el apartado 3.5 de la presente Declaración de Prácticas de Certificación.

3.3.6.- Cambio de claves

Para renovar un certificado de usuario, bien porque haya sido revocado o porque haya caducado, se deberá solicitar un nuevo certificado, siguiendo el proceso de emisión de certificados previsto en la Documentación específica para cada certificado.

La renovación de claves lleva aparejada la renovación del certificado.

3.3.7.- Plan de contingencias

3.3.7.1.- Procedimientos de gestión de incidencias

Existe un Plan de Contingencias que define las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación prestados por CIPSC.

Los principales objetivos del Plan de Contingencia son:

- Maximizar la efectividad de las operaciones de recuperación mediante el establecimiento de

tres fases:

- Fase de Notificación/Evaluación/Activación para detectar, evaluar los daños y activar el plan.
- Fase de Recuperación para restablecer temporal y parcialmente los servicios hasta la recuperación de los daños provocados en el sistema original.
- Fase de Reconstitución para restaurar el sistema y los procesos a su operativa habitual.

- Identificar las actividades, recursos y procedimientos necesarios para la prestación parcial de los servicios de certificación en un CPD alternativo durante interrupciones prolongadas de la operativa habitual.
- Asignar responsabilidades al personal designado de CIPSC y facilitar una guía para la recuperación de la operativa habitual durante largos periodos de interrupción.
- Asegurar la coordinación de todos los agentes (departamentos de la entidad, puntos de contacto externos y vendedores) que participen en la estrategia de contingencia planificada.

El Plan de Contingencias de CIPSC es de aplicación al conjunto de funciones, operaciones y recursos necesarios para restaurar la prestación de servicios de certificación. Dicho plan se aplica al personal de CIPSC asociado a la prestación de los servicios de certificación.

El Plan de Contingencias establece la participación de ciertos grupos en la recuperación de las operaciones de CIPSC.

La evaluación de los daños y el plan de acción se describen en el Plan de Contingencias.

En el caso de producirse la circunstancia de que el algoritmo, la combinación de los tamaños de clave utilizados o cualquier otra circunstancia técnica que mermara significativamente la seguridad técnica del sistema se aplicará dicho Plan de Contingencia. Se realizará un análisis de impacto. En ese análisis se estudiará la criticidad del problema de seguridad, su ámbito y la estrategia de recuperación ante la incidencia. Los puntos que se deben definir como mínimo en el informe de análisis de impacto son:

- Descripción detallada de la contingencia, ámbito temporal, etc
- Criticidad, ámbito
- Solución o soluciones propuestas
- Plan de despliegue de la solución elegida, que incluirá al menos:

- Notificación a los usuarios por el medio considerado más eficaz. Se incluirá tanto a los solicitantes como a los firmantes, creadores de sellos y verificadores (terceras partes confiables) de los certificados.
- Se informará en la web de la contingencia producida
- Revocación de los certificados afectados
- Estrategia de renovación

3.3.7.2.- Plan de actuación ante datos y software corruptos

Si los recursos hardware, software, y/o datos se alteran o son sospechosos de haber sido alterados se detendrá el funcionamiento de los servicios de CIPSC hasta el restablecimiento de un entorno seguro con la incorporación de nuevos componentes de eficiencia acreditable. De forma paralela se realizará una auditoría para identificar la causa de la alteración y asegurar la no reproducción de la misma.

En el caso de verse afectados certificados emitidos, se notificará del hecho a los firmantes , creadores de sellos de los mismos así como a MINETUR y se procederá a su recertificación.

3.3.7.3.- Procedimiento ante compromiso de la clave privada

La AC Raíz revocará el certificado de una AC subordinada en el caso que la clave privada de esa CA haya sido comprometida.

En el caso que la AC Raíz deba revocar el certificado de la AC subordinada, lo notificará inmediatamente a:

- La AC emisora
- Todas las AARR autorizadas para el registro de esa AC
- Todos los signatarios titulares de certificados emitidos por esa AA.
- Ministerio de Industria Energía y Turismo de España.

La AC Raíz, también publicará el certificado revocado en la CRL/ARL (Lista de Revocación de Autoridades de Certificación).

Después de resolver los factores que indujeron la revocación, la AC Raíz puede:

- Generar un nuevo certificado para la AC subordinada.
- Asegurar que todos los nuevos certificados y CRL emitidos por la AC son firmados utilizando la nueva clave.

La AC subordinada podrá emitir certificados a todas las entidades finales afectadas.

En caso de que la clave comprometida sea la de la AC raíz, se eliminará el certificado de todas las aplicaciones y se distribuirá uno nuevo.

3.3.7.4.- Continuidad de negocio después de un desastre

Se suspenderá la operación de la AC hasta el momento en que se haya completado el procedimiento de recuperación de desastre y se halle funcionando correctamente en el centro principal o alternativo.

Se activará el Plan de Contingencias y de Continuidad de Negocio de CIPSC.

3.3.8.- Terminación de la AC o AR

3.3.8.1.- Entidad de Certificación

En caso de cese de su actividad, CIPSC comunicará a los firmantes y creadores de sellos por cualquier medio que garantice el envío y la recepción de la notificación, con un plazo mínimo de antelación de 2 meses a su fecha de su extinción, su intención de cesar como prestador de servicios de certificación.

De la misma manera, se notificará a PSCs y cualquier entidad con la que CIPSC mantenga alguna relación contractual de uso de sus certificados.

Asimismo comunicará al Ministerio de Industria, Energía y Turismo, con la antelación indicada en el anterior apartado, el cese de su actividad y el destino que vaya a dar a los certificados, especificando, en su caso, si va a transferir la gestión y a quién o si extinguirá su vigencia.

La responsabilidad de esta notificación corresponde al Responsable de Seguridad de CIPSC, quien decidirá el mecanismo más adecuado.

En el supuesto de que CIPSC decidiera transferir la actividad a otro prestador de servicios de certificación, comunicará al Ministerio de Industria, Energía y Turismo y a los firmantes y creadores

de sellos de sus certificados los acuerdos de transferencia. A tal efecto CIPSC enviará el documento explicativo de las condiciones de transferencia así como de las condiciones de utilización que regularán las relaciones entre los firmantes y/o creadores de sellos y el PSC al cual se transfieren los certificados. Esta comunicación se realizará por cualquier medio que garantice el envío y la recepción de la notificación, con una antelación mínima de 2 meses al cese de su actividad.

Los firmantes y creadores de sellos deberán consentir de forma expresa la transferencia de los certificados, aceptando las condiciones del PSC al que se transfieren. Transcurrido el plazo de dos meses, sin que exista acuerdo de transferencia o sin que los firmantes y creadores de sellos acepten expresamente la misma, los certificados serán revocados.

En el supuesto de que no existieran acuerdos con otros PSC, finalizado el plazo de los 2 meses de antelación en la comunicación, todos los certificados serán revocados de manera automática.

CIPSC remitirá al Ministerio de Industria, Energía y Turismo, con carácter previo al cese definitivo de su actividad la información relativa a los certificados electrónicos cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a efectos de lo previsto en el artículo 20.1.f).

Se dará por finalizado cualquier autorización de terceros con los que CIPSC mantenga un contrato de prestación de servicios (identificación, emisión, albergue, etc.)

3.3.8.2.- Entidad de Registro

Una vez la Entidad de Registro cese en el ejercicio de las funciones que asuma transferirá los registros que mantenga a CIPSC, mientras exista obligación de mantener archivada la información dado que en otro caso, será cancelada y destruida.

3.4.- Controles de seguridad técnica

3.4.1.- Generación e instalación del par de claves

CIPSC adopta las medidas precisas para garantizar que las claves privadas de sus autoridades sean secretas y para mantener su integridad.

3.4.1.1.- Generación del par de claves

Elementos donde se genera el par de claves para cada una de las diferentes entidades que componen CIPSC:

- AC raíz: la máquina donde reside la AC raíz dispone de un dispositivo criptográfico (HSM) para la generación de claves de la AC raíz.
- AACC subordinadas: se deberán generar en un módulo criptográfico en cada máquina que albergue AACC.
- Certificados de usuario emitidos en tarjeta criptográfica o HSM: las claves son generadas por el dispositivo criptográfico.
- Certificado de usuario emitido en soporte software criptográfico: sus claves son generadas por el servidor donde reside el servicio
- Servidor de la Autoridad de Time Stamping (TSA) y Servidor de Validación OCSP: claves generadas en el módulo criptográfico asociado al sistema en el que residen ambos servidores.
- Para el caso de las claves generadas por el propio poseedor, éstas deberán ser generadas siguiendo las recomendaciones de algoritmo y longitud de clave mínimas definidas en ETSI TS 102 176

3.4.1.2.- Distribución de la clave privada al firmante o creador de sello

Método de entrega de la clave privada para las diferentes entidades que componen o colaboran con CIPSC:

- Certificados emitidos en tarjeta criptográfica: las claves privadas de autenticación y de firma se entregan con el dispositivo criptográfico.
- Certificados emitidos en HSM: las claves privadas de autenticación y de firma se albergan en el dispositivo criptográfico.
- Certificados emitidos en soporte software: la clave privada es generada en el propio servidor. No necesita ser entregada.

3.4.1.3.- Distribución de la clave pública al emisor del certificado

El método de entrega de la clave pública de las diferentes entidades que componen o colaboran con CIPSC al emisor de certificados correspondiente es el siguiente:

- AACC subordinadas: la clave pública es enviada a la AC raíz mediante formato X.509 o PKCS#10.

- Certificados emitidos en dispositivo criptográfico: se leen del dispositivo criptográfico.
- Certificado emitido en soporte software: la clave pública es enviada a la AC de CIPSC mediante formato X.509 o PKCS#10.

3.4.1.4.- Distribución de las claves públicas de las autoridades prestadoras de servicios

Las claves públicas de las Autoridades prestadoras de servicios se publicarán, así como su cadena de confianza, mediante los correspondientes certificados electrónicos en los repositorios descritos en el apartado 1.6.3 de este documento. El formato de los certificados será el definido por el estándar X509. v3, y su contenido y periodo de validez el que se determine en las Políticas correspondientes.

En la presente Declaración de Prácticas de Certificación, en el anexo II, se publican además las diferentes huellas de las AACC raíces y AACC subordinadas.

3.4.1.5.- Tamaños de claves

El tamaño de las claves dependiendo de los casos es:

- Al menos 2048 bits para claves de personas físicas y jurídicas, servidor OCSP, servidor TSA y certificados técnicos.
- Al menos 2048 bits para claves de AACC subordinadas.
- Al menos 4096 bits para claves raíz de AC.

Si se determinara que cualquiera de las longitudes de la clave han dejado de aportar un nivel suficiente de seguridad, CIPSC los sustituirá por otras cuyo nivel de seguridad se considere suficiente, y publicará la información sobre dichos cambios en el repositorio mencionado en el apartado 1.6.3.

3.4.1.6.- Algoritmos de firma de certificados

El identificador de algoritmo (AlgorithmIdentifier) que emplea CIPSC para firmar los certificados es SHA-256 (algoritmo de hash) con RSA (algoritmo de firma) que corresponde al identificador para "Secure Hash Algorithm 256 (SHA256) with Rivest, Shamir and Adleman (RSA) encryption".

Los certificados de usuario final están firmados con RSA con SHA-256. CIPSC recomienda a los usuarios finales que utilicen RSA con SHA-256 o superior a la hora de firmar con el certificado.

CIPSC utiliza un algoritmo cualificado por la industria y adecuado para el propósito de firma reconocida. Se tendrá en cuenta para ello el periodo de vigencia del certificado además sigue las recomendaciones indicadas por los diferentes estándares de ETSI.

En el caso de producirse la circunstancia de que el algoritmo, la combinación de los tamaños de clave utilizados o cualquier otra circunstancia técnica que mermara significativamente la seguridad técnica del sistema se aplicará el Plan de Contingencia. Se realizará un análisis de impacto. En ese análisis se estudiará la criticidad del problema de seguridad, su ámbito y la estrategia de recuperación ante la incidencia. Los puntos que se deben definir como mínimo en el informe de análisis de impacto son:

- Descripción detallada de la contingencia, ámbito temporal, etc
- Criticidad, ámbito
- Solución o soluciones propuestas
- Plan de despliegue de la solución elegida, que incluirá al menos:
    - Notificación a los usuarios por el medio considerado más eficaz. Se incluirá tanto a los solicitantes como a los firmantes, creadores de sellos y verificadores (terceras partes confiables) de los certificados.
    - Se informará en la web de la contingencia producida o Revocación de los certificados afectados
    - Estrategia de renovación

3.4.1.7.- Usos admitidos de las claves (KeyUsage field X.509v3)

Todos los certificados incluyen la extensión Key Usage y Extended Key Usage, indicando los usos habilitados de la claves.

Las claves de AC raíz únicamente se utilizarán para firmar certificados de AACC subordinadas y ARLs, y que las claves de las AC subordinadas o emisoras únicamente se utilizarán para firmar certificados de usuario final y CRLs

Los usos admitidos de la clave para cada certificado están definidos en el apartado específico de cada certificado.

3.4.2.- Protección de la clave privada

3.4.2.1.- Estándares de módulos criptográficos

Un módulo de seguridad criptográfico (HSM) es un dispositivo de seguridad que genera y protege claves criptográficas. CIPSC utiliza módulos criptográficos hardware desarrollados por terceros y disponibles comercialmente. CIPSC únicamente utiliza módulos criptográficos con certificación FIPS 140-2 Nivel 3, CC EAL 4+ o superior.

CIPSC comprueba que los módulos de seguridad criptográficos no han sido manipulados durante su transporte y almacenamiento, y que conservan los embalajes originales de fábrica.

En cuanto a los dispositivos criptográficos con certificados para firma electrónica cualificada, aptas como dispositivos seguros de creación de firma (DSCF), cumplen el nivel de seguridad CC EAL4+, aunque también son admisibles las certificaciones equivalentes ITSEC E3 o FIPS 140-2 Nivel 2 como mínimo.

La norma europea de referencia para los dispositivos de firmantes o creadores de sellos utilizados es CEN CWA 14169.

CIPSC, en cualquier caso, mantiene el control sobre la preparación, almacenamiento y distribución de los dispositivos de los firmantes y creadores de sellos en los que CIPSC genera las claves.

3.4.2.2.- Control por más de una persona (n de m) sobre la clave privada

La utilización de las claves privadas de las AACC requiere la aprobación de al menos dos personas.

3.4.2.3.- Custodia de la clave privada

La clave privada de las AACC raíz están custodiadas por un dispositivo criptográfico hardware certificado con la norma FIPS 140-2 nivel 3 y/o CC EAL4+, garantizando que la clave privada nunca está fuera del dispositivo criptográfico. La activación y uso de la clave privada requiere el control multipersona detallado anteriormente.

Las claves privadas de las AC Subordinadas están custodiadas en dispositivos criptográficos seguros certificados con la norma FIPS 140-2 nivel 3 y CC EAL4+.

En los casos en los que el firmante o creador de sellos custodie la clave privada éste será el responsable de mantenerla bajo su exclusivo control.

3.4.2.4.- Copia de respaldo de la clave privada

A fin de garantizar la continuidad del servicio en caso de desastre total (destrucción del HSM que alberga las claves privadas de los certificados raíz) existe una copia de respaldo en un dispositivo seguro de creación de firma de las mismas características que el HSM en producción.

La copia de respaldo se ha llevado a cabo por el Administrador del Sistema de Certificación y el Operador de la Autoridad de Certificación, bajo supervisión del Responsable de Seguridad, conforme a lo dispuesto en el apartado 3.4.2.2, que conserva dicha copia de respaldo en una caja fuerte a una distancia suficiente del emplazamiento principal.

3.4.2.5.- Archivado de la clave privada

CIPSC no archivará la clave privada de firma de certificados después de la expiración del periodo de validez de la misma.

Las claves privadas de los certificados internos que usan los distintos componentes del sistema de la AC para comunicarse entre sí, firmar y cifrar la información podrán ser archivadas, después de la emisión del último certificado.

Las claves privadas de los firmantes y creadores de sellos pueden ser archivadas por ellos mismos, mediante la conservación del dispositivo de creación de firma u otros métodos, debido a que pueden ser necesarias para descifrar la información histórica cifrada con la clave pública, siempre que el dispositivo de custodia permita la operación.

3.4.2.6.- Trasferencia de la clave privada a o desde el módulo criptográfico

Sólo en caso de contingencia se utiliza el procedimiento a que se refiere el apartado 3.4.2.4, que se describe en el plan de contingencias, para recuperar las claves privadas en los módulos criptográficos.

3.4.2.7.- Almacenamiento de la clave privada en el módulo criptográfico

Las claves privadas, tanto de las AACC como AACC subordinadas se generan directamente

dentro del módulo criptográfico que las va a albergar. CIPSC sigue para la generación de las claves de las AACC las recomendaciones de ETSI TS 101 456, 7.2.1.

En los casos en los que se almacenen claves privadas fuera de los módulos criptográficos, éstas estarán protegidas de forma que se asegure el mismo nivel de protección que si estuviesen físicamente en el interior de los módulos criptográficos. Todos los HSMs utilizados por CIPSC para almacenar claves privadas de Autoridades de Certificación poseen la certificación Common Criteria 4+.

3.4.2.8.- Método de activación de la clave privada

Las claves de la AC Raíz y de las AACC subordinadas se activan por un proceso que requiere la utilización simultánea de n de m dispositivos criptográficos.

El acceso a la clave privada del firmante o creador de sellos se realiza por medio de un PIN. El dispositivo tiene un sistema de protección contra intentos de acceso que lo bloquean cuando se introducen más de tres veces un código de acceso erróneo. El firmante o creador de sellos dispone de un código de desbloqueo del dispositivo. Si se introduce tres veces erróneamente, el dispositivo se bloquea definitivamente, quedando inservible.

3.4.2.9.- Método de desactivación de la clave privada

Un administrador puede proceder a la desactivación de la clave de las Autoridades de CIPSC mediante el procedimiento proporcionado por el sistema del HSM.

En el caso del firmante o creador de sellos, la extracción del dispositivo criptográfico del lector supone la finalización de cualquier acción de operación en curso.

3.4.2.10.- Método de destrucción de la clave privada

El manual del HSM proporciona un método seguro de destrucción de claves de la AC.

En el caso de retirar el HSM que alberga las claves de la AC, éstas serán destruidas.

Este procedimiento no se aplica a las claves de firma o autenticación de usuario emitidas en tarjeta criptográfica salvo, en el caso de renovación de claves reutilizando el mismo dispositivo criptográfico, en el cual se destruirá la clave anterior y se generarán nuevas claves sobre el mismo soporte.

3.4.2.11.- Calificación del módulo criptográfico

Según indicado en el apartado 3.4.2.1 del presente documento

3.4.3.- Otros aspectos de gestión del par de claves

3.4.3.1.- Archivo de la clave pública

Los certificados generados por la AC, y por lo tanto las claves públicas, son almacenados por la AC durante el periodo de tiempo obligado por la legislación vigente.

3.4.3.2.- Periodos de utilización de las claves pública y privada

Es el periodo de validez de cada uno de los certificados.

3.4.4.- Datos de activación

3.4.4.1.- Generación e instalación de datos de activación

- Para los certificados de las AC, los datos de activación se generan en tokens criptográficos en posesión de personal autorizado,
- Certificados emitidos en dispositivo criptográfico: la utilización de la clave privada asociada a cada certificado requiere de un dato de activación (PIN) o contraseña.

  El dato de activación (PIN) o contraseña:

  - Se genera de forma aleatoria por el software de CIPSC y se graba en el dispositivo criptográfico que soporta el certificado.
  - Se genera e imprime en el momento de emitirse el certificado.
  - Se entrega al usuario por un sistema que permite mantener la confidencialidad.
  - CIPSC proporciona al firmante o creador de sellos una función para el cambio del PIN en la tarjeta.
  - El PIN nunca se almacena.

- Certificados emitidos en soporte software: la instalación y puesta en marcha de la clave privada asociada a los certificados requiere la utilización de los sistemas de seguridad que el propio usuario haya definido.

3.4.4.2.- Protección de datos de activación

En relación a los datos de activación de firma se requiere a los usuarios de los certificados:

- Memorizarlos.
- Emplear el máximo cuidado en protegerlos.
- No almacenarlos junto al dispositivo criptográfico ni compartirlos con otras personas.
- Cambiar el PIN y PUK antes de utilizarlo

3.4.4.3.- Otros aspectos de los datos de activación

No se estipula el tiempo de vida de los datos de activación. No obstante, se recomienda cambiarlos periódicamente para disminuir la posibilidad de que sean descubiertos.

3.4.5.- Controles de seguridad informática

3.4.5.1.- Requisitos técnicos específicos de seguridad informática

Existen una serie de controles en el emplazamiento de los diferentes elementos del sistema de prestación de servicio de certificación de CIPSC (AACC, BBDD de CIPSC, Servicios Internet de CIPSC, Operación AC y Gestión de Red):

- Controles operacionales.
    - Se documentan los procesos de operación a cargo del operador de la A.C. Y el administrador del sistema de seguridad conforme a los manuales del fabricante del HSM.

      Existe un Plan de Contingencias.
    - Están implantadas herramientas de protección contra virus y códigos malignos.
    - Se lleva a cabo un mantenimiento continuado del equipamiento, con el fin de asegurar su disponibilidad e integridad continuadas.

- La información de los soportes de información obsoletos y los medios removibles es borrada; los equipos son etiquetados y entregados al responsable de seguridad que los conserva en lugar seguro hasta su destrucción por parte de empresas especializadas.

- Intercambios de datos. Los siguientes intercambios de datos van cifrados para asegurar la debida confidencialidad.
  - Transmisión de datos de registro entre las AARR y la base de datos de registro.
  - Transmisión de datos de prerregistro.
  - La comunicación entre las AARR y las AACC.
- El servicio de publicación de revocaciones posee las funcionalidades necesarias para que se garantice un funcionamiento 24x7.
- Control de accesos.
  - Se utilizarán IDs de usuario únicos, de forma que los usuarios son relacionados con las acciones que realizan y se les puede responsabilizar de sus acciones.
  - La asignación de derechos se lleva a cabo siguiendo el principio de concesión mínima de privilegios.
  - Eliminación inmediata de los derechos de acceso de los usuarios que cambian de puesto de trabajo o abandonan la organización.
  - Revisión trimestral del nivel de acceso asignado a los usuarios.
  - La asignación de privilegios especiales se realiza “caso a caso” y se suprimen una vez terminada la causa que motivó su asignación.

3.4.5.2.- Evaluación del nivel de seguridad informática

La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad tal como se describe en el plan de contingencias y continuidad de negocio.

La seguridad física está garantizada por las instalaciones ya definidas anteriormente y la gestión de personal.

3.4.6.- Controles técnicos del ciclo de vida

3.4.6.1.- Controles de desarrollo de sistemas

Se realiza un análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente utilizado en las aplicaciones de Autoridad de certificación y de Autoridad de Registro, para garantizar que los sistemas son seguros. Se utilizan procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

3.4.6.2.- Controles de gestión de la seguridad

CIPSC mantiene un inventario de todos los activos informáticos y realizará una clasificación de los mismos de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración de los sistemas se audita de forma periódica, de acuerdo con lo establecido en la sección correspondiente de este documento.

Los sistemas de CIPSC se protegen contra virus y software no autorizado y malintencionado.

Se realiza un seguimiento de las necesidades de capacidad, y se planificarán procedimientos para garantizar suficiente disponibilidad electrónica y de almacenaje para los activos informativos.

3.4.7.- Controles de seguridad de red

Se garantiza que el acceso a las diferentes redes de CIPSC es limitado a individuos debidamente autorizados. En particular:

- Se implementan controles (como por ejemplo cortafuegos) para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos se configuran de forma que se impidan accesos y protocolos que no sean necesarios para la operación de la CIPSC.
- Los datos sensibles se protegen cuando se intercambian a través de redes no seguras (incluyendo los datos de registro del firmante/creador de sellos).
- Se garantiza que los componentes locales de red (como enrutadores) se encuentran ubicados en entornos seguros, así como la auditoría periódica de sus configuraciones.

3.4.8.- Fuente de tiempo

CIPSC obtiene el tiempo de sus sistemas de una conexión al Real Observatorio de la Armada siguiendo el protocolo NTP. La descripción del protocolo NTP se puede encontrar en el estándar de IETF RFC 5905.

4 Servicios de firma electrónica

4.1.- Declaración básica del servicio de confianza de CIPSC

La Declaración básica del servicio de confianza de CIPSC recoge las condiciones y aspectos fundamentales de uso de los servicios de certificación 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 *PKI Disclosure Statement* por los estándares ETSI TS 102 042 y ETSI TS 101 456, cuyas funciones el presente apartado cumple a todos los efectos.

Mediante la presente declaración básica, CIPSC afirma que:

Titularidad

CIPSC es un servicio del Coloriuris S.L., empresa cuyos datos de contacto se encuentran en el apartado 1.6.4 de este documento.

Disponibilidad del servicio

Los servicios de confianza de CIPSC están disponibles de forma ininterrumpida todos los días del año salvo la tramitación presencial de solicitudes de certificados, que únicamente estará disponible en el horario de oficina que establezca cada una de las Autoridades de Registro.

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

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.

Publicación de la Política

Todos y cada uno de los certificados emitidos por CIPSC contienen el enlace a esta declaración de política y prácticas, el cual se encuentra indicado en el apartado 1.6.3 de este documento.

Mecanismos criptográficos

Los algoritmos criptográficos y la longitud de las claves utilizadas en la emisión de los certificados por CIPSC cumplen con el estándar ETSI TS 102 042 V2.4.1 *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key*

certificates y son las siguientes:

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

Validez de los certificados

CIPSC no establece otras limitaciones a la confianza que merecen sus servicios de certificación 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, CIPSC publicará inmediatamente dicha información en su página web.

Aplicabilidad

CIPSC considera que los usos más apropiados de los certificados que emite son la identificación de los firmantes y creadores de sellos y la firma por los mismos de documentos electrónicos.

Obligaciones

Las obligaciones de los firmantes y creadores de sellos están descritas en los apartados 2.3.2 y 4.2.1.4 del presente documento y las de las partes usuarias en este último y en el apartado 2.3.3.

Registro de las operaciones

CIPSC registra sus operaciones y conserva esta información en adecuadas condiciones de seguridad, según lo previsto en los apartados 3.3.4 y 4.2.1.5 del presente documento.

Normativa

La prestación de los servicios de confianza por parte de CIPSC 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 CIPSC y de su Autoridad de certificación.

Responsabilidad

Las responsabilidades de CIPSC y las limitaciones establecidas sobre la misma se describen en el apartado 2.4 del presente documento.

Reclamaciones

Todas las reclamaciones de usuarios y terceros sobre la prestación de servicios de certificación

por CIPSC deberán serle comunicadas según lo establecido en el apartado 2.8.1 del presente documento. 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, con renuncia a cualquier otro fuero que pudiera corresponderles.

Garantía y auditorías

CIPSC garantiza que la prestación de los servicios de confianza 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 CIPSC y de las Autoridades de certificación.

Tarifas

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

4.2.- Política para la prestación de los servicios de certificación

4.2.1.- Aspectos generales

4.2.1.1.- Finalidad y alcance

La presente Política regula la generación y emisión de certificados por CIPSC. El servicio de confianza se presta por la Autoridad de certificación de CIPSC, en colaboración con las Autoridades de registro. Todos los certificados emitidos por CIPSC contienen un enlace a la Política que se les aplica. La prestación del servicio de confianza se realiza conforme a la legislación y estándares de aplicación, los cuales se detallan en el anexo Referencias de este documento, destacándose los siguientes:

- IETF
  - RCF 3647, *Internet X.509 Public Key Infrastructure Certificate Policy*
  - RFC 3739 y 3039, *Internet X.509 Public Key Infrastructure: Qualified Certificates Profile*
  - RFC 5280 y 3280, *Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL)*
- ETSI
  - ETSI TS 101 456 V1.2.1 *Policy requirements for certification authorities issuing qualified certificate*
  - ETSI TS 102 042 V1.1.1 *Policy requirements for certification authorities issuing public key certificate*

- ETSI TS 102 023 V1.2.1 *Policy requirements for time-stamping authorities*

- CA/Browser

  - *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*

4.2.1.2.- Clases de certificados

Todos los certificados emitidos por CIPSC vinculan unos datos de identificación y/o de creación de firma específicos y únicos con un firmante concreto y también único.

En base a esta Política, la Autoridad de certificación del CIPSC emite los siguientes tipos de certificados:

- **Certificados de firma electrónica de persona física:** Acreditan la vinculación de una clave pública y una persona física. Son válidos para la identificación y para la generación de firmas electrónicas. Podrán contener como atributos:

  - la vinculación de la persona física con una determinada organización y, opcionalmente, el cargo o puesto en la misma,

  - la cualificación académica y/o la profesión u oficio.

- **Certificados de firma electrónica de persona jurídica:** acreditan la vinculación de una clave pública y una persona jurídica. Son válidos para la identificación y para la generación de firmas electrónicas.

4.2.1.3.- Comunidad

La comunidad para la generación, emisión y uso de los certificados son la Autoridad de certificación (AC), según se describe en los apartados 2.1.2.1 y 2.1.2.2, las Autoridades de registro (AR), según se describen en el apartado 2.1.3, los firmantes, según se describen en el apartado 2.2.1, y las partes usuarias, según se describen en el apartado 2.2.2.

La AC es responsable de la emisión y gestión de los certificados, de la publicación de su estado y de la conservación de los certificados y de los registros sobre su actividad. Las AR recogen el compromiso del firmante con los datos de identificación y/o de creación de firma y conservan el documento acreditativo del mismo, así como la restante documentación que se establezca en su normativa interna. El firmante es la persona física o jurídica bajo cuyo control se encuentran los mencionados datos de identificación y/o de creación de firma y la única autorizada para su utilización. Las partes usuarias son aquellas personas que confían en la identificación electrónica y/o

los servicios de confianza de CIPSC.

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

4.2.1.4.- 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 firma electrónica y sello electrónico.

Autoridad de certificación

1) Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente para los certificados reconocidos.

2) Revocar los certificados cuando así proceda según lo dispuesto en esta Política, informando en todo caso a su titular.

3) Publicar en forma apropiada los certificados emitidos y, en su caso, la revocación de los mismos.

4) No almacenar ni copiar en ningún caso los datos de identificación o de creación de firma del firmante ni del creador de sellos.

5) Conservar la información sobre los certificados emitidos, al menos durante el período mínimo exigido por la normativa.

Autoridades de Registro

1) Comprobar mediante documentos apropiados la identidad del firmante o del creador de sellos y, en su caso, los atributos del mismo que vayan a incorporarse a los certificados.

2) Conservar los documentos que se indique en esta Política y, en particular, los acreditativos del compromiso del firmante o del creador de sello del certificado con los datos de identificación y/o de creación de firma asociados al mismo.

3) Comunicar a la AC, en cuanto tenga conocimiento de las mismas, la existencia de causas de revocación que afecten a uno o más certificados emitidos por CIPSC.

Firmante

1) Proporcionar a la AR la información que resulte precisa para la emisión del certificado, justificándola documentalmente cuando así proceda y respondiendo de su veracidad y exactitud.

2) Comunicar a la AR los cambios que puedan producirse en la información incluida en los

certificados, durante el periodo de validez de los mismos.

3) Custodiar los datos de identificación y/o de creación de firma o sello electrónico con la debida diligencia.

4) Informar a la AR de la existencia de causas de revocación que afecten a su certificado, en cuanto tenga conocimiento de las mismas.

5) Utilizar el certificado únicamente para los usos y con los fines permitidos en la presente Política.

Partes usuarias

Verificar la validez de los certificados de forma previa a la aceptación de cualquier identificación, firma o sello basada en los mismos, así como la vinculación entre éstos y los datos de identificación y/o creación de firma utilizados.

4.2.1.5.- Publicación y conservación de los certificados

CIPSC publicará en un directorio accesible a través de Internet y basado en el estándar *Online Certificate Status Protocol* (OCSP) todos los certificados emitidos que se encuentren vigentes en cada momento, informando de su estado, que podrá ser: valido o revocado. También publicará la lista de certificados revocados mediante listas de certificados revocados (*Certificate Revocation List*, CRL). El directorio dispondrá de un certificado de servidor, que garantizará su pertenencia a CIPSC, y las CRL estarán firmadas por CIPSC.

La AC dispondrá de una CRL diferenciada para cada una de las clases de certificados que emita. En caso de revocarse un certificado esta información se hará constar inmediatamente en el directorio y la AC creará una nueva CRL en el mismo instante en que se produzca la revocación quedando disponible inmediatamente en la url de la CRL correspondiente. Cuando no se haya realizado ninguna revocación la CRL se actualizará con frecuencia semanal.

Las direcciones web (URL) para la publicación serán:

- https://ocsp.coloriuris.net
- **https://cipsc.coloriuris.net/crl**

Estas direcciones estarán activas permanentemente, en los términos establecidos en el apartado 3.2.10.2.

Las partes usuarias deberán comprobar la validez de los certificados, preferiblemente consultando el directorio y si no comprobando que el certificado no se encuentra incluido en la última CRL publicada.

El acceso al directorio y a las listas de certificados revocados será libre y gratuito, si bien la AC podrá exigir que se aporte algún dato del certificado a verificar, al objeto de evitar descargas masivas y accesos indiscriminados a la información.

Por otra parte, CIPSC conservará todos los certificados emitidos, con las adecuadas condiciones de seguridad y durante un periodo mínimo de veinte años, a lo largo del cual proporcionará a los firmantes y creadores de sellos la posibilidad de recuperarlos.

4.2.1.6.- Registro de información y conservación de firmas

La AC y las AR mantienen registros de toda la información relevante referente a sus operaciones, según lo establecido en los apartados 3.3.4 y 4.2.1.5. Los registros referentes a un certificado se conservarán durante todo el periodo de vigencia del mismo y durante los 15 años posteriores a la finalización del mismo.

Además de los previstos en dicho apartado, la AC mantiene registros de los siguientes eventos:

- Solicitudes de emisión y revocación de certificados
- Autorizaciones recibidas de la AR para la emisión y revocación de certificados
- Emisión y revocación de certificados

Las AR son responsables de la conservación del documento acreditativo del compromiso de los firmantes y creadores de sellos con el certificado, así como la restante documentación que se establezca en estas Políticas y en su normativa interna.

4.2.2.- Certificados de firma electrónica para persona física

4.2.2.1.- Ámbito de aplicación y usos

Es una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el pseudónimo de esa persona y tendrá los efectos previstos en las leyes.

En esta Política no se establecen limitaciones respecto a los negocios jurídicos en los que estas firmas podrán ser utilizadas. Tampoco los certificados emitidos bajo la misma podrán contener ninguna restricción ni limitación.

4.2.2.2.- Contenido

El firmante quedará identificado por su nombre, apellido o apellidos, y número del

documento de identificación personal, que será el documento nacional de identidad, en el caso de los españoles, y el código de identificación del país, según la norma ISO 3166-1 alfa-2 y el número de pasaporte en el caso de quienes tengan otra nacionalidad. Los firmantes no podrán identificarse mediante apodos, alias o seudónimos.

Los certificados de firma electrónica podrán contener alternativa o simultáneamente los siguientes atributos:

Vinculación a una organización

La organización se identificará por su denominación o razón social, de acuerdo con el tenor literal que conste en la documentación aportada como prueba de la vinculación. También podrán utilizarse números de identificación oficiales de la misma, como el Número de Identificación Fiscal. La función o cargo del firmante en la organización sólo se hará constar cuando esté justificada documentalmente y, asimismo, con la denominación exacta que se utilice en los documentos.

Cualificación académica, profesión u oficio

La cualificación académica, profesión u oficio se identificarán por la denominación que conste en la documentación justificativa que se aporte.

Una misma persona sólo podrá ser firmante de un único certificado de persona física sin atributos, pero podrá disponer de varios certificados que contengan atributos, siempre que éstos sean distintos en cada certificado. En este caso se podrá añadir en el CN del certificado un acrónimo que permita diferenciar los distintos certificados, en la forma que se determine en la normativa interna para cada tipo de organización, cualificación profesional, profesión u oficio.

4.2.2.3.- Periodo de validez

Los certificados para las firmas electrónicas tienen un periodo de validez de cuatro años, que comenzará en todo caso en el mismo momento de su generación.

4.2.2.4.- Longitud de la clave

Las claves certificadas de acuerdo con la presente Política se ajustarán al estándar RSA y podrán tener una longitud de 2048 Bits.

4.2.2.5.- Perfiles del certificado

El contenido de los certificados será el indicado en este apartado, quedan marcados con letra cursiva los contenidos opcionales y se considera que existen dos tipos de perfiles disponibles:

- Certificado de persona física, identificado por el OID 1.3.6.1.4.1.37799.20.1.1.1 para

certificados emitidos en soporte software.

- Certificado de persona física en DSCF, identificado por el OID 1.3.6.1.4.1.37799.20.1.1.2 para certificados emitidos en un dispositivo seguro de creación de firma.

Perfil de certificado de persona física

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Subautoridad de emisión de certificados de persona física
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Asunto	
CN	nombre y apellido o apellidos del firmante - *acrónimo identificativo del certificado*
E	correo electrónico del firmante
SerialNumber	número identificativo del firmante (DNI o código país: nº pasaporte)
Apellidos (Surname)	apellido o apellidos del firmante
Nombre (Given Name)	nombre del firmante
O	*denominación o razón social de la organización* *número identificativo de la organización*
OU	*función o cargo en la organización*
T	*cualificación profesional, profesión u oficio*
Clave pública	RSA (2048 Bits)
Uso mejorado de clave	autenticación del cliente; correo seguro
AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/ac/subac/epf.crt aceso id-ad-ocsp https://ocsp.coloriuris.net
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/ac/subac/epf.crl
Bases del certificado	[1]Directiva de certificados:

	Identificador de directiva=1.3.6.1.4.1.37799.20.1.1.1 [1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado reconocido de persona física, antes de confiar en él compruebe la Política aplicable y la vigencia del mismo. [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
1.3.6.1.5.5.7.1.3 -IETF / 0.4.0.1862.1.1-ETSI	Qualified Certificate Statements
QcCompliance	
QcLimitValue	50€
QcRetentionPeriod	15 años
Uso de la clave	identificación, firma digital, no repudio, cifrado de clave, cifrado de datos

Perfil de certificado de persona física en DSCF

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Subautoridad de emisión de certificados de persona física
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Asunto	
CN	nombre y apellido o apellidos del firmante - *acrónimo identificativo del certificado*
E	correo electrónico del firmante
SerialNumber	número identificativo del firmante (DNI o código país: nº pasaporte)

Apellidos (Surname)	apellido o apellidos del firmante
Nombre (Given Name)	nombre del firmante
O	*denominación o razón social de la organización* *número identificativo de la organización*
OU	*función o cargo en la organización*
T	*cualificación profesional, profesión u oficio*
Clave pública	RSA (2048 Bits)
Uso mejorado de clave	autenticación del cliente; correo seguro
AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/ac/subac/epf.crt aceso id-ad-ocsp https://ocsp.coloriuris.net
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/ac/subac/epf.crl
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.37799.20.1.1.2 [1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado reconocido de persona física, antes de confiar en él compruebe la Política aplicable y la vigencia del mismo. [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
1.3.6.1.5.5.7.1.3 -IETF / 0.4.0.1862.1.1-ETSI	Qualified Certificate Statements
QcCompliance	
QcSSCD	
QcLimitValue	50€
QcRetentionPeriod	15 años
Uso de la clave	identificación, firma digital, no repudio, cifrado de clave, cifrado de datos

4.2.2.6.- Perfil de CRL

El contenido de la lista de certificados de firma electrónica revocados será el siguiente:

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Subautoridad de emisión de certificados de persona física
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Periodo máximo de validez	**7** días
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/ac/subac/epf.crl

4.2.3.- Certificados de firma electrónica para personas jurídicas

4.2.3.1.- Ámbito de aplicación y usos

Es una declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona con los efectos previstos en las leyes.

Los sellos podrán ser utilizados únicamente en actuaciones automatizadas, que serán las consistentes en la elaboración de documentos en base a información previamente obrante en el sistema como, por ejemplo, facturas o certificaciones, y aquellas otras cuyo contenido esté previamente determinado por la normativa o por la programación de los sistemas como, por ejemplo, la emisión de acuses de recibo.

4.2.3.2.- Contenido

El firmante quedará identificado por su denominación o razón social y su código de identificación fiscal. Dicha información quedará reflejada en el campo CN del certificado.

Asimismo, la misma información quedará reflejada por separado en los campos O para para la denominación o razón social y SerialNumber para el código de identificación fiscal.

Una misma persona jurídica podrá disponer de más de un certificado para distintas unidades organizacionales de la misma, que se harán constar en el campo OU, o para distintas funciones, que

se harán constar en el campo T. En este caso se podrá añadir en el CN del certificado un acrónimo que permita diferenciar los distintos certificados, en la forma que se determine en la normativa interna de la AC.

Además, de la información correspondiente a la persona jurídica, en el campo CN deberán incluirse el nombre y apellidos y el número de identificación fiscal del apoderado de la persona jurídica para el que se emite el certificado.

Además los certificados de persona jurídica podrán contener alternativa o simultáneamente los siguientes atributos:

Forma jurídica de la organización

La naturaleza o forma jurídica de la organización como, por ejemplo, sociedad limitada, sociedad anónima, asociación, etc., solo se hará constar cuando esté justificada documentalmente y se utilizará la denominación precisa que conste en los documentos.

Fines sociales

Los fines sociales se incorporarán tal y como consten en la documentación justificativa de los mismos, aunque podrán abreviarse siempre que no se cambien o desvirtúen de forma significativa.

4.2.3.3.- Periodo de validez

Los certificados de firma electrónica para personas jurídicas tendrán un periodo de validez de cuatro años, que comenzará en todo caso en el mismo momento de su generación.

4.2.3.4.- Longitud de la clave

Las claves certificadas de acuerdo con la presente Política se ajustarán al estándar RSA y tendrán una longitud de 2048 Bits.

4.2.3.5.- Perfiles del certificado

El contenido de los certificados será el indicado en este apartado, quedan marcados con letra cursiva los contenidos opcionales y se considera que existen dos tipos de perfiles disponibles:

- Certificado de persona jurídica, identificado por el OID 1.3.6.1.4.1.37799.20.1.2.1 para certificados emitidos en soporte software,
- Certificado de persona jurídica en DSCF, identificado por el OID 1.3.6.1.4.1.37799.20.1.2.2 para certificados emitidos en un dispositivo seguro de creación de firma.

Perfil del certificado de persona jurídica

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Subautoridad de emisión de certificados de persona jurídica
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Asunto	
CN	razón social o denominación legal, código de identificación fiscal de la persona jurídica, nombre y apellidos y número de identificación fiscal del apoderado.
E	correo electrónico del firmante
SerialNumber	código de identificación fiscal del firmante y forma jurídica
OU	*unidad organizacional*
O	razón social, denominación legal del firmante
GN	*fines*
T	*función a la que se destina el certificado*
Clave pública	RSA (2048 Bits)
Uso mejorado de clave	autenticación del cliente; correo seguro
AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/ac/subac/epj.crt aceso id-ad-ocsp https://ocsp.coloriuris.net
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/ac/subac/epj.crl
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.37799.20.1.2.1 [1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado cualificado de persona jurídica, antes de confiar en él compruebe la Política aplicable y la vigencia del mismo.

	[1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
1.3.6.1.5.5.7.1.3 -IETF / 0.4.0.1862.1.1-ETSI	Qualified Certificate Statements
QcCompliance	
QcLimitValue	50€
QcRetentionPeriod	15 años
Uso de la clave	identificación, firma digital, no repudio, cifrado de clave, cifrado de datos

Perfil del certificado de persona jurídica en DSCF

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Subautoridad de emisión de certificados de persona jurídica
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Asunto	
CN	razón social o denominación legal, código de identificación fiscal de la persona jurídica, nombre y apellidos y número de identificación fiscal del apoderado.
E	correo electrónico del firmante
SerialNumber	código de identificación fiscal del firmante y forma jurídica
OU	*unidad organizacional*
O	razón social, denominación legal del firmante
GN	*fines*
T	*función a la que se destina el certificado*

Clave pública	RSA (2048 Bits)
Uso mejorado de clave	autenticación del cliente; correo seguro
AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/ac/subac/epj.crt aceso id-ad-ocsp https://ocsp.coloriuris.net
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/ac/subac/epj.crl
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.37799.20.1.2.2 [1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado cualificado de persona jurídica, antes de confiar en él compruebe la Política aplicable y la vigencia del mismo. [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
1.3.6.1.5.5.7.1.3 -IETF / 0.4.0.1862.1.1-ETSI	Qualified Certificate Statements
QcCompliance	
QcSSCD	
QcLimitValue	50€
QcRetentionPeriod	15 años
Uso de la clave	identificación, firma digital, no repudio, cifrado de clave, cifrado de datos

4.2.3.6.- Perfil de CRL

El contenido de la lista de certificados de sellos electrónicos revocados será el siguiente:

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Subautoridad de emisión de certificados de persona jurídica
SerialNumber	B99091696

OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Periodo máximo de validez	**7** días
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/ac/subac/epj.crl

4.3.- Declaración de prácticas

4.3.1.- Generación y emisión

El trámite de registro se realizará en todo caso de forma presencial (salvo en el supuesto de generación de certificados a partir de otro certificado reconocido vigente del firmante). En este trámite el personal de la Autoridad de registro tomará las medidas necesarias a evitar la posible falsificación de un certificado reconocido, para ello comprobará la identidad del firmante, o de la persona que lo represente, verificando en este caso la vigencia y suficiencia de la representación, y examinará la documentación que acredite la información a incluir en el certificado, conservando copia de la misma. El operador de la AR informará al firmante de la existencia de estas Políticas y le entregará una copia de las mismas si éste así lo solicita.

La identificación de las personas físicas que soliciten un certificado reconocido exigirá su personación ante el operador de registro de la Autoridad de Registro de CIPSC (o de las A.R. externas que puedan crearse en el futuro) y se acreditará mediante el documento nacional de identidad, pasaporte u otros medios admitidos en derecho. Podrá prescindirse de la personación si su firma en la solicitud de expedición de un certificado reconocido ha sido legitimada en presencia notarial.

En el caso de certificados reconocidos de personas jurídicas, el operador de registro de la A.R. de CIPSC (o de las A.R. externas que puedan crearse en el futuro) comprobará, además, los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público.

Una vez realizadas estas comprobaciones la AR autorizará a la AC la generación del certificado, mediante una orden expresa en la que se incluirá el contenido del certificado y que

deberá estar firmada por el operador de la AR responsable de la misma. CIPSC conservará dicha orden al menos durante todo el periodo de validez del certificado y 15 años más.

Seguidamente, el firmante deberá firmar la licencia de uso del certificado, que contendrá necesariamente los siguientes extremos:

- El número de serie único del certificado.
- Los datos identificativos del firmante incluidos en el certificado.
- En su caso, los atributos del firmante contenidos en el certificado.
- El compromiso con los actos de identificación y/o las firmas realizados a partir de ese momento con los datos vinculados al certificado.
- La expresa aceptación del contenido de estas Políticas y, en particular con las obligaciones que se establecen para éste.
- El reconocimiento de que los datos aportados en este trámite y en especial los incorporados al certificado son ciertos y correctos.
- El consentimiento para el tratamiento de los datos personales aportados, para su comunicación en caso de cese de actividad de la AC, y para la publicación del certificado y de su estado.

Las Claves Privadas de los firmantes son de uso y control exclusivo de éstos y generadas por ellos mismos, bien a través de Dispositivos Seguros de Creación de Firma, bien en el equipo del propio usuario u otros medios equivalentes. Posteriormente se generan las Claves Pública y Privada (en un dispositivo criptográfico – Token o Tarjeta criptográfica - si el Solicitante dispone del mismo o en el navegador u otros medios equivalentes si no dispone de dicho dispositivo) que serán vinculadas al Certificado que se generará en una fase posterior. CIPSC asigna a la solicitud un código único.

La generación de los datos de identificación y/o creación de firma y de los correspondientes datos de validación, así como la posterior puesta a disposición podrá realizarse de tres modos:

Por el propio firmante

El firmante generará los datos de identificación y/o creación de firma de forma previa al trámite de registro, accediendo para ello a una operatoria que estará disponible en la web de CIPSC. Los datos serán generados dentro del equipo que el usuario utilice para el acceso y la solicitud para la generación del certificado conteniendo los datos de validación será remitida por un canal cifrado a la AC.

Una vez realizado íntegramente el trámite de registro, el certificado será puesto a su

disposición por medios telemáticos. Previamente a la entrega se comprobará que éste tiene el control efectivo sobre los datos de identificación y/o creación de firma certificados.

Si el firmante no comparece en el plazo de quince días, la solicitud se tendrá por abandonada y perderá su validez, sin que haya obligación de conservarla. Si el certificado no se entregara por resultar fallida la prueba mencionada en el párrafo anterior o por cualquier otro motivo, se tendrá por no emitido y no se publicará en la forma prevista en el apartado 4.2.1.5.

En el supuesto de generación del certificado a partir de otro certificado reconocido vigente no será precisa la comparecencia presencial a que se refiere el párrafo anterior.

En el trámite de registro

Se utilizará un *token* criptográfico, u otros medios equivalentes, que cumpla con los niveles de seguridad exigidos en la normativa interna de la AC y que será proporcionado al firmante por la AR, si este así lo solicita. Los datos de identificación y/o creación de firma se generarán dentro del mismo, de forma tal que no sea posible su conocimiento por la AR. El firmante deberá introducir personalmente la contraseña que proteja el contenido del *token*, y la AR no deberá tener en ningún momento acceso a la misma. Una vez realizado íntegramente el trámite de registro, se emitirá el certificado y se introducirá en el *token* criptográfico, que quedará en posesión de éste.

Por lotes

Se utilizará un *token* criptográfico, u otros medios equivalentes, que cumpla con los niveles de seguridad exigidos en la normativa interna de la AC y que será proporcionado al firmante por la AR o el propio equipo del usuario. Los datos de identificación y/o creación de firma se generarán dentro de éste y de forma tal que la AR no pueda conocerlos. Asimismo la AR generará la contraseña o contraseñas que protejan el contenido del *token*, incorporándolas a un sobre ciego o a un medio similar que garantice la total confidencialidad de las mismas y sin guardar ninguna copia. El certificado se emitirá y se introducirá en el *token* criptográfico. Una vez realizado íntegramente el trámite de registro, el *token* se entregará al firmante junto al sobre ciego o soporte que contenga las contraseñas.

Si el *token* no se entregara por no realizarse correctamente el acto de registro o por cualquier otro motivo, el certificado se tendrá por no emitido y no se publicará en la forma prevista en el apartado 4.2.1.5.

En el momento de la emisión del certificado, el firmante podrá solicitar a la AR que con antelación suficiente a su caducidad, proceda a la renovación sin necesidad de que medie una solicitud expresa.

4.3.2.- Renovación

La renovación implica la generación de unos nuevos datos de identificación y/o de generación de firma y los correspondientes datos de validación, así como la emisión de un nuevo certificado. En ningún caso se autorizará un nuevo certificado vinculado a datos previamente certificados.

Tanto el nombre común como, en su caso, los atributos del firmante del nuevo certificado serán los mismos que en el certificado renovado, no siendo necesaria la realización del trámite de registro.

Podrán realizarse renovaciones sucesivas de un certificado, siempre que no hayan transcurrido más de cinco años desde la realización del último trámite de registro.

El procedimiento para la renovación será el indicado a continuación, en función de la forma en la que se realizó la solicitud y generación del certificado:

Por el propio firmante

La solicitud de renovación deberá generarse dentro de los sesenta días anteriores a la caducidad del certificado a renovar. Para ello, el firmante accederá a una operatoria que estará disponible en la web de CIPSC. Los datos de identificación y/o de generación de firma serán generados dentro del equipo que el usuario utilice para el acceso y se generará una solicitud para la renovación del certificado, que deberá firmarse con el certificado a renovar y que será remitida por un canal cifrado a la AC. Una vez recibida la solicitud se generará el certificado y será puesto a disposición del firmante por medios telemáticos. Previamente a la entrega se comprobará que éste tiene el control efectivo sobre los datos de identificación y/o creación de firma certificados.

En el trámite de registro o por lotes

La renovación podrá realizarse de forma presencial, utilizando un *token* criptográfico, u otros medios equivalentes, que cumplan con los niveles de seguridad exigidos en esta Política y que podrá ser el mismo que contenía el certificado a renovar o en remoto a partir del propio equipo del usuario. Una vez firmada por el firmante la solicitud de renovación utilizando el certificado a renovar, se generarán los nuevos datos de identificación y/o creación de firma, de forma que la AR no pueda acceder a los mismos. El firmante deberá introducir personalmente la contraseña que proteja el contenido del *token*, y la AR no deberá tener en ningún momento conocimiento de la misma. Finalmente, se emitirá el certificado y se introducirá en el *token* criptográfico, que quedará en posesión del firmante.

La renovación también podrá realizarse por la AR, cuando el firmante así lo hubiera solicitado en el trámite de registro en los certificados emitidos por lotes o si así lo solicita

posteriormente a dicho trámite. En este caso se utilizará un *token* criptográfico, u otros medios equivalentes, que cumplan con los niveles de seguridad exigidos en esta Política y los datos de identificación y/o creación de firma se generarán en el mismo de forma que la AR no pueda acceder a los mismos. Asimismo, la AR generará la contraseña o contraseñas que protejan el contenido del *token*, incorporándolas a un sobre ciego o a un medio similar que garantice la total confidencialidad de las mismas y sin guardar ninguna copia. El nuevo certificado se emitirá y se introducirá en el *token* criptográfico, o medio equivalente, que se entregará al firmante o creador de sellos junto al sobre ciego o soporte que contenga las contraseñas. El firmante deberá acusar recibo de ambos elementos.

Si, por cualquier motivo, el certificado no fuera descargado con éxito por el firmante o el *token* no se le entregara, el certificado se tendrá por no emitido y no se publicará en la forma prevista en el apartado 4.2.1.5.

La AC o la AR deberán informar al firmante de las Políticas vigentes en el momento de la renovación. También deberán conservar las solicitudes de renovación y, en su caso, el acuse de recibo del *token* criptográfico durante el tiempo previsto en el apartado 4.2.1.6.

4.3.3.- Revocación

La revocación es la pérdida definitiva de validez de un certificado, por causa distinta de la caducidad. CIPSC no dispone de ningún mecanismo para la suspensión provisional de la validez de los certificados.

La AC procederá obligatoriamente a la revocación de los certificados cuando se de cualquiera de las siguientes causas:

- La solicitud del firmante, que deberá hacerse de forma que permita comprobar la identidad del mismo.
- El compromiso de los datos de identificación y/o de generación de firma, o la pérdida o avería del soporte en el que se conserven.
- El fallecimiento o declaración de incapacidad del firmante, en el caso de las personas físicas, o la extinción, en el de las jurídicas.
- La inexactitud del contenido del certificado, tanto cuando esta tenga carácter originario y se detecte con posterioridad a la emisión del certificado como cuando se deba a una variación de las circunstancias.
- El incumplimiento grave por parte por parte de CIPSC o del firmante de las obligaciones

establecidas en esta Política.

- El compromiso de las claves de la AC o cualquier otra causa por la que el certificado pierda su fiabilidad.
- Por resolución judicial expresa.
- El cese en la actividad de CIPSC, salvo cuando los certificados expedidos por aquel sean transferidos a otro prestador de servicios.

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las peticiones de revocación proceden del firmante o, en los demás supuestos, que están debidamente justificadas. Asimismo deberá proceder a la revocación con la máxima prontitud, publicándola por los medios previstos en el apartado 4.2.1.5.

Una vez revocado el certificado deberá informarse al firmante, aún cuando la solicitud de revocación hubiera procedido del mismo. En caso de error de la AC o si la revocación resultara injustificada por cualquier motivo se emitirá un nuevo certificado sin coste alguno para el firmante o creador de sellos, no aceptando CIPSC ninguna otra responsabilidad.

El servicio de gestión de las revocaciones estará disponible permanentemente en los términos previstos en el apartado 3.2.10.2.

4.3.4.- Certificado raíz y sellos de la AC

4.3.4.1.- Certificado raíz

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

Su contenido es el siguiente:

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la Autoridad de Certificación
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES

Asunto	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la Autoridad de Certificación
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Clave pública	RSA (4096 Bits)
AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/ac/raiz.crt aceso id-ad-ocsp https://ocsp.coloriuris.net
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/ac/ac.crl
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.37799.0.3.1.2.0 [1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado raíz de la Autoridad de Certificación de CIPSC. [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
Uso de la clave	firma de certificados, firma CRL sin conexión, firma de lista de revocación de certificados (CRL)

4.3.4.2.- Certificado para la emisión de certificados de firma electrónica de persona física

El certificado para la firma de certificados de persona física es emitido por la AC de CIPSC utilizando el certificado raíz, con una longitud de clave de 2048 Bits y un periodo de validez de 10 años.

Su contenido es el siguiente:

Emisor (Issuer)	

E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la Autoridad de Certificación
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Asunto	
E	cipsc@coloriuris.net
CN	CIPSC - Subautoridad de emisión de certificados de persona física
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Clave pública	RSA (2048 Bits)
AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/ac/raiz.crt aceso id-ad-ocsp https://ocsp.coloriuris.net
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/ac/ac.crl
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.37799.0.3.1.2.0 [1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=SubAutoridad CIPSC para emisión de certificados de firma electrónica para persona física [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
Uso de la clave	firma de certificados, firma CRL sin conexión, firma de lista de revocación de certificados (CRL)

4.3.4.4.- Certificado para la emisión de certificados de firma electrónica de persona jurídica

El certificado para la emisión de certificados de firma electrónica para personas jurídicas es emitido por la AC de CIPSC utilizando el certificado raíz, con una longitud de clave de 2048 Bits y un periodo de validez de 10 años.

Su contenido es el siguiente:

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la Autoridad de Certificación
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Asunto	
E	cipsc@coloriuris.net
CN	CIPSC - Subautoridad de emisión de certificados de persona jurídica
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Clave pública	RSA (2048 Bits)
AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/ac/raiz.crt aceso id-ad-ocsp https://ocsp.coloriuris.net
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/ac/ac.crl
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.37799.0.3.1.2.0 [1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador:

	Texto de aviso=SubAutoridad CIPSC para emisión de certificados para sello electrónico de persona jurídica [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
Uso de la clave	firma de certificados, firma CRL sin conexión, firma de lista de revocación de certificados (CRL)

5 Servicios de sello electrónico

5.1.- Declaración básica del servicio de confianza de CIPSC

La Declaración básica de este servicio de confianza de CIPSC recoge las condiciones y aspectos fundamentales de uso de los servicios de certificación 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 *PKI Disclosure Statement* por los estándares ETSI EN 319 411-1 cuyas funciones el presente apartado cumple a todos los efectos.

Mediante la presente declaración básica, CIPSC afirma que:

Titularidad

CIPSC es un servicio del Coloriuris S.L., empresa cuyos datos de contacto se encuentran en el apartado 1.6.4 de este documento.

Disponibilidad del servicio

Los servicios de confianza de CIPSC están disponibles de forma ininterrumpida todos los días del año salvo la tramitación presencial de solicitudes de certificados, que únicamente estará disponible en el horario de oficina que establezca cada una de las Autoridades de Registro.

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

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.

Publicación de la Política

Todos y cada uno de los certificados emitidos por CIPSC-v3 contienen el enlace del documento PKI Disclosure Statement, accesible desde la url: https://cipsc.coloriuris.net/pds/en.pdf

Mecanismos criptográficos

Los algoritmos criptográficos y la longitud de las claves utilizadas en la emisión de los certificados por CIPSC cumplen con el estándar ETSI TS 119 312 *Electronic Signatures and Infrastructures (ESI); Cryptographic Suites* y son las siguientes:

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

Validez de los certificados

CIPSC no establece otras limitaciones a la confianza que merecen sus servicios de certificación 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, CIPSC publicará inmediatamente dicha información en su página web.

Aplicabilidad

CIPSC considera que los usos más apropiados de los certificados que emite son la identificación de creadores de sellos y la firma por los mismos de documentos electrónicos (incluida factura electrónica).

Obligaciones

Las obligaciones de los creadores de sellos están descritas en el apartado 5.2.1.4 del presente documento y las de las partes usuarias en este último y en el apartado 2.3.3.

Registro de las operaciones

CIPSC registra sus operaciones y conserva esta información en adecuadas condiciones de seguridad, según lo previsto en los apartados 3.3.4 y 5.2.1.5 del presente documento.

Normativa

La prestación de los servicios de confianza por parte de CIPSC 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 CIPSC y de su Autoridad de Certificación.

Responsabilidad

Las responsabilidades de CIPSC y las limitaciones establecidas sobre la misma se describen en el apartado 2.4 del presente documento.

Reclamaciones

Todas las reclamaciones de usuarios y terceros sobre la prestación de servicios de certificación por CIPSC deberán serle comunicadas según lo establecido en el apartado 2.8.1 del presente documento. 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, con renuncia a cualquier otro fuero que pudiera corresponderles.

Garantía y auditorías

CIPSC garantiza que la prestación de los servicios de confianza 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 CIPSC y de las Autoridades de Certificación.

Tarifas

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

5.2.- Política para la prestación de los servicios de certificación

5.2.1.- Aspectos generales

5.2.1.1.- Finalidad y alcance

La presente Política regula la generación y emisión de certificados por CIPSC. El servicio de confianza se presta por la Autoridad de certificación de CIPSC, en colaboración con las Autoridades de registro. Todos los certificados emitidos por CIPSC contienen un enlace a la la Política que se les aplica. La prestación del servicio de confianza se realiza conforme a la legislación y estándares de aplicación, los cuales se detallan en el anexo Referencias de este documento, destacándose los siguientes:

- IETF
  - RCF 3647, *Internet X.509 Public Key Infrastructure Certificate Policy*
  - RFC 3739 y 3039, *Internet X.509 Public Key Infrastructure: Qualified Certificates Profile*
  - RFC 5280 y 3280, *Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL)*
- ETSI
  - ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
  - ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
  - ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5:

QCStatementss

- ETSI TS 102 042 V1.1.1 *Policy requirements for certification authorities issuing public key certificate*

- CA/Browser
  - *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*

5.2.1.2.- Clases de certificados

Todos los certificados emitidos por CIPSC vinculan unos datos de identificación y/o de creación de firma específicos y únicos con un creador de sellos concreto y también único.

En base a esta Política, la Autoridad de certificación del CIPSC emite los siguientes tipos de certificados:

- **Certificados de sello electrónico (persona jurídica):** acreditan la vinculación de una clave pública y una persona jurídica. Son válidos para la identificación y para la generación de sellos electrónicos.

5.2.1.3.- Comunidad

La comunidad para la generación, emisión y uso de los certificados son la Autoridad de Certificación v3 (ACv3), según se describe en los apartados 2.1.2.1 y 2.1.2.2, las Autoridades de registro (AR), según se describen en el apartado 2.1.3, los creadores de sellos, según se describen en el apartado 2.2.1, y las partes usuarias, según se describen en el apartado 2.2.2.

La AC es responsable de la emisión y gestión de los certificados, de la publicación de su estado y de la conservación de los certificados y de los registros sobre su actividad. Las AR recogen el compromiso del creador del sello con los datos de identificación y/o de creación de sellos y conservan el documento acreditativo del mismo, así como la restante documentación que se establezca en su normativa interna. El creador de sellos es la persona jurídica bajo cuyo control se encuentran los mencionados datos de identificación y/o de creación de firma y la única autorizada para su utilización. Las partes usuarias son aquellas personas que confían en la identificación electrónica y/o los servicios de confianza de CIPSC.

Todos ellos están sujetos a lo dispuesto en la presente Política.

5.2.1.4.- Obligaciones

Además de las obligaciones establecidas por ley y de las enumeradas en el apartado 2.3 de

este documento, se establecen las siguientes obligaciones específicas para la prestación del servicio de sello electrónico.

Autoridad de certificación

6) Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente para los certificados reconocidos.

7) Revocar los certificados cuando así proceda según lo dispuesto en esta Política, informando en todo caso a su titular.

8) Publicar en forma apropiada los certificados emitidos y, en su caso, la revocación de los mismos.

9) No almacenar ni copiar en ningún caso los datos de identificación o de creación de firma del firmante ni del creador de sellos.

10) Conservar la información sobre los certificados emitidos, al menos durante el período mínimo exigido por la normativa.

Autoridades de Registro

4) Comprobar mediante documentos apropiados la identidad del firmante o del creador de sellos y, en su caso, los atributos del mismo que vayan a incorporarse a los certificados.

5) Conservar los documentos que se indique en esta Política y, en particular, los acreditativos del compromiso del firmante o del creador de sello del certificado con los datos de identificación y/o de creación de firma asociados al mismo.

6) Comunicar a la AC, en cuanto tenga conocimiento de las mismas, la existencia de causas de revocación que afecten a uno o más certificados emitidos por CIPSC.

Creador de sello

6) Proporcionar a la AR la información que resulte precisa para la emisión del certificado, justificándola documentalmente cuando así proceda y respondiendo de su veracidad y exactitud.

7) Comunicar a la AR los cambios que puedan producirse en la información incluida en los certificados, durante el periodo de validez de los mismos.

8) Custodiar los datos de identificación y/o de creación de sello electrónico con la debida diligencia.

9) Informar a la AR de la existencia de causas de revocación que afecten a su certificado, en

cuanto tenga conocimiento de las mismas.

10) Utilizar el certificado únicamente para los usos y con los fines permitidos en la presente Política.

Partes usuarias

Verificar la validez de los certificados de forma previa a la aceptación de cualquier identificación, firma o sello basada en los mismos, así como la vinculación entre éstos y los datos de identificación y/o creación de firma utilizados.

5.2.1.5.- Publicación y conservación de los certificados

CIPSC publicará en un directorio accesible a través de Internet y basado en el estándar *Online Certificate Status Protocol* (OCSP) todos los certificados emitidos que se encuentren vigentes en cada momento, informando de su estado, que podrá ser: valido o revocado. También publicará la lista de certificados revocados mediante listas de certificados revocados (*Certificate Revocation List*, CRL). El directorio dispondrá de un certificado de servidor, que garantizará su pertenencia a CIPSC, y las CRL estarán firmadas por CIPSC.

La AC dispondrá de una CRL diferenciada para cada una de las clases de certificados que emita. En caso de revocarse un certificado esta información se hará constar inmediatamente en el directorio y la AC creará una nueva CRL en el mismo instante en que se produzca la revocación quedando disponible inmediatamente en la url de la CRL correspondiente. Cuando no se haya realizado ninguna revocación la CRL se actualizará con frecuencia semanal.

Las direcciones web (URL) para la publicación serán:

- https://ocsp.coloriuris.net
- **https://cipsc.coloriuris.net/crl**

Estas direcciones estarán activas permanentemente, en los términos establecidos en el apartado 3.2.10.2.

Las partes usuarias deberán comprobar la validez de los certificados, preferiblemente consultando el directorio y si no comprobando que el certificado no se encuentra incluido en la última CRL publicada.

El acceso al directorio y a las listas de certificados revocados será libre y gratuito, si bien la AC podrá exigir que se aporte algún dato del certificado a verificar, al objeto de evitar descargas masivas y accesos indiscriminados a la información.

Por otra parte, CIPSC conservará todos los certificados emitidos, con las adecuadas

condiciones de seguridad y durante un periodo mínimo de veinte años, a lo largo del cual proporcionará a los creadores de sellos la posibilidad de recuperarlos.

5.2.1.6.- Registro de información y conservación de sellos electrónicos

La AC y las AR mantienen registros de toda la información relevante referente a sus operaciones, según lo establecido en los apartados 3.3.4 y 5.2.1.5. Los registros referentes a un certificado se conservarán durante todo el periodo de vigencia del mismo y durante los 15 años posteriores a la finalización del mismo.

Además de los previstos en dicho apartado, la AC mantiene registros de los siguientes eventos:

- Solicitudes de emisión y revocación de certificados
- Autorizaciones recibidas de la AR para la emisión y revocación de certificados
- Emisión y revocación de certificados

Las AR son responsables de la conservación del documento acreditativo del compromiso de los creadores de sellos con el certificado, así como la restante documentación que se establezca en estas Políticas y en su normativa interna.

5.2.2.- Certificado de sello electrónico

5.2.2.1.- Ámbito de aplicación y usos

Es una declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa entidad con los efectos previstos en las leyes.

Los sellos podrán ser utilizados únicamente en actuaciones automatizadas, que serán las consistentes en la elaboración de documentos en base a información previamente obrante en el sistema como, por ejemplo, facturas o certificaciones, y aquellas otras cuyo contenido esté previamente determinado por la normativa o por la programación de los sistemas como, por ejemplo, la emisión de acuses de recibo.

5.2.2.2.- Contenido

El creador de sello electrónico quedará identificado por su denominación o razón social y su código de identificación fiscal. Dicha información quedará reflejada en el campo CN del certificado.

Asimismo, la misma información quedará reflejada por separado en los campos O para para la denominación o razón social y organizationIdentifier para el código de identificación fiscal, que

quedará reflejado en el certificado con la notación indicada por el estándar ETSI EN 319 412-1 para las personas jurídicas.

El certificado también deberá incluir obligatoriamente el país de residencia de la persona jurídica, éste quedará reflejado mediante el código ISO 3166 de dos letras en el campo C.

Una misma persona jurídica podrá disponer de más de un certificado para distintas unidades organizacionales de la misma, que se harán constar en el campo OU, o para distintas funciones, que se harán constar en el campo T. En este caso se podrá añadir en el CN del certificado un acrónimo que permita diferenciar los distintos certificados, en la forma que se determine en la normativa interna de la AC.

Además los certificados de sello electrónico podrán contener alternativa o simultáneamente los siguientes atributos:

Forma jurídica de la organización

La naturaleza o forma jurídica de la organización como, por ejemplo, sociedad limitada, sociedad anónima, asociación, etc., solo se hará constar cuando esté justificada documentalmente y se utilizará la denominación precisa que conste en los documentos.

Fines sociales

Los fines sociales se incorporarán tal y como consten en la documentación justificativa de los mismos, aunque podrán abreviarse siempre que no se cambien o desvirtúen de forma significativa.

5.2.2.3.- Periodo de validez

Los certificados de sello electrónico tendrán un periodo de validez de cuatro años, que comenzará en todo caso en el mismo momento de su generación.

5.2.2.4.- Longitud de la clave

Las claves certificadas de acuerdo con la presente Política se ajustarán al estándar RSA y tendrán una longitud de 2048 Bits.

5.2.2.5.- Perfiles del certificado

El contenido del certificado será el indicado en este apartado, quedan marcados con letra cursiva los contenidos opcionales y se considera que existen dos tipos de perfiles disponibles:

- Certificado de sello electrónico, identificado por el OID 1.3.6.1.4.1.37799.20.2.2.1, para aquellos certificados emitidos en soporte software.
- Certificado de sello electrónico en dispositivo seguro de creación de firma, identificado por el

OID 1.3.6.1.4.1.37799.20.2.2.2, que corresponde a aquellos certificados que se emitan para ser utilizados en un dispositivo SSCD.

Perfil de certificado de sello electrónico

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Emisión de certificados de persona jurídica
oganizationIdentifier (2.5.4.97)	VATES-B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Asunto	
CN	razón social o denominación legal y código de identificación fiscal de la persona jurídica
E	correo electrónico del creador de sellos
oganizationIdentifier (2.5.4.97)	código de identificación fiscal del creador de sello con la semántica indicada por ETSI 319 412-1
OU	*unidad organizacional*
O	razón social, denominación legal del creador de sellos
GN	*fines*
T	*función a la que se destina el certificado*
C	País de residencia de la persona jurídica
Clave pública	RSA (2048 Bits)
Uso mejorado de clave	autenticación del cliente; correo seguro
AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/ac/subac/epj-v3.crt aceso id-ad-ocsp https://ocsp.coloriuris.net
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/ac/subac/epj-v3.crl
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.37799.20.2.2.1

	[1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado cualificado de sello electrónico, antes de confiar en él compruebe la Política aplicable y la vigencia del mismo. [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
1.3.6.1.5.5.7.1.3 -IETF / 0.4.0.1862.1.1-ETSI	Qualified Certificate Statements
QCSyntax-v2	id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2)
QcCompliance	
QcLimitValue	50€
QcRetentionPeriod	15 años
QcPDS	{ https://cipsc.coloriuris.net/pds/en.pdf, en }
QcType	Id-etsi-qct-eseal (0.4.0.1862.1.6.2)
Uso de la clave	identificación, sello electrónico, no repudio, cifrado de clave, cifrado de datos

Perfil de certificado de sello electrónico en dispositivo seguro de creación de firma

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Emisión de certificados de persona jurídica
oganizationIdentifier (2.5.4.97)	VATES-B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES

Asunto	
CN	razón social o denominación legal y código de identificación fiscal de la persona jurídica
E	correo electrónico del creador de sellos
oganizationIdentifier (2.5.4.97)	código de identificación fiscal del creador de sello con la semántica indicada por ETSI 319 412-1
OU	*unidad organizacional*
O	razón social, denominación legal del creador de sellos
GN	*fines*
T	*función a la que se destina el certificado*
C	País de residencia de la persona jurídica
Clave pública	RSA (2048 Bits)
Uso mejorado de clave	autenticación del cliente; correo seguro
AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/ac/subac/epj-v3.crt aceso id-ad-ocsp https://ocsp.coloriuris.net
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/ac/subac/epj-v3.crl
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.37799.20.2.2.2 [1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado cualificado de sello electrónico con clave privada en DSCF, antes de confiar en él compruebe la Política aplicable y la vigencia del mismo. [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
1.3.6.1.5.5.7.1.3 -IETF / 0.4.0.1862.1.1-ETSI	Qualified Certificate Statements
QCSyntax-v2	id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2)
QcCompliance	
QcLimitValue	50€

QcRetentionPeriod	15 años
QcSSCD	
QcPDS	{ https://cipsc.coloriuris.net/pds/en.pdf, en }
QcType	Id-etsi-qct-eseal (0.4.0.1862.1.6.2)
Uso de la clave	identificación, sello electrónico, no repudio, cifrado de clave, cifrado de datos

5.2.2.6.- Perfil de CRL

El contenido de la lista de certificados de sellos electrónicos revocados será el siguiente:

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Emisión de certificados de persona jurídica
oganizationIdentifier (2.5.4.97)	VATES-B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Periodo máximo de validez	**7** días
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/ac/subac/epj-v3.crl

5.3.- Declaración de prácticas

5.3.1.- Generación y emisión

El trámite de registro se realizará en todo caso de forma presencial (salvo en el supuesto de generación de certificados a partir de otro certificado reconocido vigente del creador del sello). En este trámite el personal de la Autoridad de registro tomará las medidas necesarias a evitar la posible falsificación de un certificado reconocido, para ello comprobará la identidad del creador de sello electrónico y de la persona que lo represente, verificando en este caso la vigencia y suficiencia de la representación, y examinará la documentación que acredite la información a incluir en el

certificado, conservando copia de la misma. El operador de la AR informará al creador de sello electrónico de la existencia de estas Políticas y le entregará una copia de las mismas si éste así lo solicita.

En el caso de certificados reconocidos de personas jurídicas (sellos electrónicos conforme a la denominación dada por R.U.E. 910/2014), el operador de registro de la A.R. de CIPSC (o de las A.R. externas que puedan crearse en el futuro) comprobará, además, los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público.

Una vez realizadas estas comprobaciones la AR autorizará a la AC la generación del certificado, mediante una orden expresa en la que se incluirá el contenido del certificado y que deberá estar firmada por el operador de la AR responsable de la misma. CIPSC conservará dicha orden al menos durante todo el periodo de validez del certificado y 15 años más.

Seguidamente, el creador de sello electrónico deberá firmar la licencia de uso del certificado, que contendrá necesariamente los siguientes extremos:

- El número de serie único del certificado.
- Los datos identificativos del creador de sello incluidos en el certificado.
- En su caso, los atributos del creador de sello contenidos en el certificado.
- El compromiso con los actos de identificación y/o sellos electrónicos realizados a partir de ese momento con los datos vinculados al certificado.
- La expresa aceptación del contenido de estas Políticas y, en particular con las obligaciones que se establecen para éste.
- El reconocimiento de que los datos aportados en este trámite y en especial los incorporados al certificado son ciertos y correctos.
- El consentimiento – en su caso - para el tratamiento de los datos personales aportados, para su comunicación en caso de cese de actividad de la AC, y para la publicación del certificado y de su estado.

Las Claves Privadas de los creadores de sellos son de uso y control exclusivo de éstos y generadas por ellos mismos, bien a través de Dispositivos Seguros de Creación de Firma, bien en el equipo del propio usuario u otros medios equivalentes. Posteriormente se generan las Claves Pública y Privada (en un dispositivo criptográfico – Token o Tarjeta criptográfica - si el Solicitante dispone del mismo o en el navegador u otros medios equivalentes si no dispone de dicho dispositivo) que

serán vinculadas al Certificado que se generará en una fase posterior. CIPSC asigna a la solicitud un código único.

La generación de los datos de identificación y/o creación de sello electrónico y de los correspondientes datos de validación, así como la posterior puesta a disposición podrá realizarse de tres modos:

Por el propio creador de sello

El creador de sello generará los datos de identificación y/o creación de sello-e de forma previa al trámite de registro, accediendo para ello a una operatoria que estará disponible en la web de CIPSC. Los datos serán generados dentro del equipo que el usuario utilice para el acceso y la solicitud para la generación del certificado conteniendo los datos de validación será remitida por un canal cifrado a la AC.

Una vez realizado íntegramente el trámite de registro, el certificado será puesto a su disposición por medios telemáticos. Previamente a la entrega se comprobará que éste tiene el control efectivo sobre los datos de identificación y/o creación de sello electrónico.

Si el creador de sello-e no comparece en el plazo de quince días, la solicitud se tendrá por abandonada y perderá su validez, sin que haya obligación de conservarla. Si el certificado no se entregara por resultar fallida la prueba mencionada en el párrafo anterior o por cualquier otro motivo, se tendrá por no emitido y no se publicará en la forma prevista en el apartado 4.2.1.5.

En el supuesto de generación del certificado a partir de otro certificado reconocido vigente no será precisa la comparecencia presencial a que se refiere el párrafo anterior.

En el trámite de registro

Se utilizará un *token* criptográfico, u otros medios equivalentes, que cumpla con los niveles de seguridad exigidos en la normativa interna de la AC y que será proporcionado al creador de sello-e por la AR, si éste así lo solicita. Los datos de identificación y/o creación de sello-e se generarán dentro del mismo, de forma tal que no sea posible su conocimiento por la AR. El creador de sello-e deberá introducir personalmente la contraseña que proteja el contenido del *token*, y la AR no deberá tener en ningún momento acceso a la misma. Una vez realizado íntegramente el trámite de registro, se emitirá el certificado y se introducirá en el *token* criptográfico, que quedará en posesión de éste.

Por lotes

Se utilizará un *token* criptográfico, u otros medios equivalentes, que cumpla con los niveles de seguridad exigidos en la normativa interna de la AC y que será proporcionado al creador de

sello-e por la AR o el propio equipo del usuario. Los datos de identificación y/o creación de sello-e se generarán dentro de éste y de forma tal que la AR no pueda conocerlos. Asimismo la AR generará la contraseña o contraseñas que protejan el contenido del *token*, incorporándolas a un sobre ciego o a un medio similar que garantice la total confidencialidad de las mismas y sin guardar ninguna copia. El certificado se emitirá y se introducirá en el *token* criptográfico. Una vez realizado íntegramente el trámite de registro, el *token* se entregará al creador de sello-e junto al sobre ciego o soporte que contenga las contraseñas.

Si el *token* no se entregara por no realizarse correctamente el acto de registro o por cualquier otro motivo, el certificado se tendrá por no emitido y no se publicará en la forma prevista en el apartado 4.2.1.5.

En el momento de la emisión del certificado, el creador de sello-e podrá solicitar a la AR que con antelación suficiente a su caducidad, proceda a la renovación sin necesidad de que medie una solicitud expresa.

5.3.2.- Renovación

La renovación implica la generación de unos nuevos datos de identificación y/o de generación de sello-e y los correspondientes datos de validación, así como la emisión de un nuevo certificado. En ningún caso se autorizará un nuevo certificado vinculado a datos previamente certificados.

Tanto el nombre común como, en su caso, los atributos del creador de sello del nuevo certificado serán los mismos que en el certificado renovado, no siendo necesaria la realización del trámite de registro.

Podrán realizarse renovaciones sucesivas de un certificado, siempre que no hayan transcurrido más de cinco años desde la realización del último trámite de registro.

El procedimiento para la renovación será el indicado a continuación, en función de la forma en la que se realizó la solicitud y generación del certificado:

Por el propio creador de sello

La solicitud de renovación deberá generarse dentro de los sesenta días anteriores a la caducidad del certificado a renovar. Para ello, el creador de sello-e accederá a una operatoria que estará disponible en la web de CIPSC. Los datos de identificación y/o de generación de sello electrónico serán generados dentro del equipo que el usuario utilice para el acceso y se generará una solicitud para la renovación del certificado, que deberá firmarse con el certificado a renovar y que será remitida por un canal cifrado a la AC. Una vez recibida la solicitud se generará el

certificado y será puesto a disposición del creador de sello-e por medios telemáticos. Previamente a la entrega se comprobará que éste tiene el control efectivo sobre los datos de identificación y/o creación de firma certificados.

En el trámite de registro o por lotes

La renovación podrá realizarse de forma presencial, utilizando un *token* criptográfico, u otros medios equivalentes, que cumplan con los niveles de seguridad exigidos en esta Política y que podrá ser el mismo que contenía el certificado a renovar o en remoto a partir del propio equipo del usuario. Una vez firmada por el creador de sello-e la solicitud de renovación utilizando el certificado a renovar, se generarán los nuevos datos de identificación y/o creación de firma, de forma que la AR no pueda acceder a los mismos. El creador de sello-e deberá introducir personalmente la contraseña que proteja el contenido del *token*, y la AR no deberá tener en ningún momento conocimiento de la misma. Finalmente, se emitirá el certificado y se introducirá en el *token* criptográfico, que quedará en posesión del creador de sello-e.

La renovación también podrá realizarse por la AR, cuando el creador de sello-e así lo hubiera solicitado en el trámite de registro en los certificados emitidos por lotes o si así lo solicita posteriormente a dicho trámite. En este caso se utilizará un *token* criptográfico, u otros medios equivalentes, que cumplan con los niveles de seguridad exigidos en esta Política y los datos de identificación y/o creación de sello electrónico se generarán en el mismo de forma que la AR no pueda acceder a los mismos. Asimismo, la AR generará la contraseña o contraseñas que protejan el contenido del *token*, incorporándolas a un sobre ciego o a un medio similar que garantice la total confidencialidad de las mismas y sin guardar ninguna copia. El nuevo certificado se emitirá y se introducirá en el *token* criptográfico, o medio equivalente, que se entregará al creador de sellos junto al sobre ciego o soporte que contenga las contraseñas. El creador de sello-e deberá acusar recibo de ambos elementos.

Si, por cualquier motivo, el certificado no fuera descargado con éxito por el creador de sello-e o el *token* no se le entregara, el certificado se tendrá por no emitido y no se publicará en la forma prevista en el apartado 5.2.1.5.

La AC o la AR deberán informar al creador de sello-e de las Políticas vigentes en el momento de la renovación. También deberán conservar las solicitudes de renovación y, en su caso, el acuse de recibo del *token* criptográfico durante el tiempo previsto en el apartado 5.2.1.6.

5.3.3.- Revocación

La revocación es la pérdida definitiva de validez de un certificado, por causa distinta de la caducidad. CIPSC no dispone de ningún mecanismo para la suspensión provisional de la validez de los

certificados.

La AC procederá obligatoriamente a la revocación de los certificados cuando se de cualquiera de las siguientes causas:

- La solicitud del creador de sello-e, que deberá hacerse de forma que permita comprobar la identidad del mismo.
- El compromiso de los datos de identificación y/o de generación de sello-e, o la pérdida o avería del soporte en el que se conserven.
- La extinción del creador de sello electrónico.
- La inexactitud del contenido del certificado, tanto cuando esta tenga carácter originario y se detecte con posterioridad a la emisión del certificado como cuando se deba a una variación de las circunstancias.
- El incumplimiento grave por parte por parte de CIPSC o del creador de sello-e de las obligaciones establecidas en esta Política.
- El compromiso de las claves de la AC o cualquier otra causa por la que el certificado pierda su fiabilidad.
- Por resolución judicial expresa.
- El cese en la actividad de CIPSC, salvo cuando los certificados expedidos por aquel sean transferidos a otro prestador de servicios.

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las peticiones de revocación proceden del creador de sello-e o, en los demás supuestos, que están debidamente justificadas. Asimismo deberá proceder a la revocación con la máxima prontitud, publicándola por los medios previstos en el apartado 5.2.1.5.

Una vez revocado el certificado deberá informarse al creador de sello-e, aún cuando la solicitud de revocación hubiera procedido del mismo. En caso de error de la AC o si la revocación resultara injustificada por cualquier motivo se emitirá un nuevo certificado sin coste alguno para el creador de sellos, no aceptando CIPSC ninguna otra responsabilidad.

El servicio de gestión de las revocaciones estará disponible permanentemente en los términos previstos en el apartado 3.2.10.2.

5.3.4.- Certificado raíz y sellos de la AC

5.3.4.1.- Certificado raíz

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

Su contenido es el siguiente:

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz - Autoridad de Certificación
organizationIdentifier (2.5.4.97)	VATES-B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Asunto	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz - Autoridad de Certificación
organizationIdentifier (2.5.4.97)	VATES-B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Clave pública	RSA (4096 Bits)
AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/ac/raiz-v3.crt aceso id-ad-ocsp https://ocsp.coloriuris.net
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/ac/ac-v3.crl
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=2.5.29.32.0 [1,1]Información de certificador de directiva:

	Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
Uso de la clave	firma de certificados, firma CRL sin conexión, firma de lista de revocación de certificados (CRL)
1.3.6.1.5.5.7.1.3 -IETF / 0.4.0.1862.1.1-ETSI	Qualified Certificate Statements
QCSyntax-v2	id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2)

5.3.4.2.- Certificado para la emisión de sellos electrónicos

El certificado para la emisión de sellos electrónicos es emitido por la AC de CIPSC utilizando el certificado raíz, con una longitud de clave de 2048 Bits y un periodo de validez de 10 años.

Su contenido es el siguiente:

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz - Autoridad de Certificación
organizationIdentifier (2.5.4.97)	VATES-B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Asunto	
E	cipsc@coloriuris.net
CN	CIPSC - Emisión de certificados de persona jurídica
organizationIdentifier (2.5.4.97)	VATES-B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Clave pública	RSA (2048 Bits)

AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/ac/raiz-v3.crt aceso id-ad-ocsp https://ocsp.coloriuris.net
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/ac/ac-v3.crl
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=2.5.29.32.0 [1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
1.3.6.1.5.5.7.1.3 -IETF / 0.4.0.1862.1.1-ETSI	Qualified Certificate Statements
QCSyntax-v2	id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2)
Uso de la clave	firma de certificados, firma CRL sin conexión, firma de lista de revocación de certificados (CRL)

6 Servicio de sellado de tiempo (Autoridad de Sellado de Tiempo de Coloriuris - TSACI)

6.1.- Declaración básica del servicio de sellado de tiempo de CIPSC

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 TS 102 023, cuyas funciones el presente apartado cumple a todos los efectos.

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

Titularidad

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

Disponibilidad del servicio

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

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

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.

Publicación de la Política

Todos y cada uno de los sellos de tiempo emitidos por TSACI contienen el identificador (OID) de las Políticas y declaración de prácticas, el cual se incluye en el apartado 1.5 de este documento.

Mecanismos criptográficos

Los algoritmos criptográficos y la longitud de las claves utilizadas en la emisión de los sellos por TSACI cumplen con el estándar ETSI TS 101 861 *Time-Stamping Profile* y son las siguientes:

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

Validez de los sellos de tiempo

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

Precisión temporal

TSACI asegura que el momento fijado en los sellos está dentro de los márgenes de error establecidos en el apartado 6.2.3 de este documento, con relación al tiempo establecido por las fuentes de tiempo UTC de confianza definidas en el apartado 6.3.4 y garantiza que no emitirá sellos de tiempo con una precisión menor que la antedicha.

Aplicabilidad

TSACI considera que los usos más apropiados de los sellos de tiempo que emite son los relacionados con la prueba del momento en que ocurren hechos que tengan o puedan tener efectos jurídicos como son, por ejemplo, los descritos en el apartado 6.2.5 del presente documento. Los sellos emitidos por TSACI no pueden utilizarse en aplicaciones en las que del control del tiempo dependan actuaciones automatizadas que, en caso de fallo o error, puedan producir daños materiales o personales.

Obligaciones

Las obligaciones de las partes usuarias están descritas en los apartados 6.2.6 del presente documento y en el apartado 2.3.3.

Registro de las operaciones

TSACI registra sus operaciones y conserva esta información en adecuadas condiciones de seguridad, según lo previsto en los apartados 3.3.4 y 4.2.1.5 del presente documento.

Normativa

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

Responsabilidad

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

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 presente documento. 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 mencionado apartado 2.8.2, con renuncia a cualquier otro fuero que pudiera corresponderles.

Garantía y auditorías

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

Tarifas

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

6.2.- Política para la prestación del servicio de sellado de tiempo

6.2.1.- Introducción

La presente Política regula la generación y emisión de sellos de tiempo por TSACI, de acuerdo con la especificación técnica ETSI TS 102 023. La clave privada utilizada y la unidad de sellado de tiempo (TSU) cumplen con las especificaciones técnicas de la normas: ETSI TS 101 861, *Time-stamping Profile*, RFC 3161, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)* y OASIS *Digital Signature Services (DSS) Core 1.0* y *Timestamp Profile*.

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.

6.2.2.- 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 07-1-2014 y con OID: 1.3.6.1.4.1.37799.0.3.1.1.2.

6.2.3.- Precisión

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

6.2.4.- 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 los apartados 2.1.2.1 y 2.1.2.3, las Autoridades de registro (AR), según se describen en el apartado 2.1.3 y las partes usuarias, según se describen en el apartado 2.2.2.

TSACI es responsable de la emisión y gestión de los sellos de tiempo. Las AR tramitan las solicitudes externas, es decir no procedentes de otras autoridades de CIPSC, para la prestación de servicios de sellado 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.

6.2.5.- 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, especialmente a las avanzadas
- 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.

6.2.6.- Obligaciones

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

TSACI

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

Partes usuarias

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

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

TSACI mantiene registros de toda la información relevante referente a sus operaciones, según lo establecido en los apartados 3.3.4 y 4.2.1.5. Además de los previstos en dichos apartados, la AC mantiene registros de los siguientes eventos:

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

6.3.- Declaración de prácticas

6.3.1.- Acceso al servicio

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

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

6.3.2.- 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.

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.

6.3.3.- 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 TS 102 023 en sus puntos 7.2.1 y 7.2.2 en módulos criptográficos con las calificaciones indicadas en el epígrafe 3.4.2.1 de esta declaración.

No se realizarán copias de seguridad de las claves privadas de las TSU tal y como recomienda la norma ETSI TS 102 023 para reducir el riesgo de compromiso.

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.

6.3.4.- Sello de tiempo

TSACI adopta las medidas técnicas precisas para garantizar que sus sellos de tiempo son seguros e incluyen la fecha y hora correctas. Los sellos se emiten utilizando un dispositivo criptográfico (TSU).

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

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

Como anexo al sello se entrega a los usuarios el certificado electrónico que respalda la firma incorporada al sello. En el apartado 6.3.5 se describen los certificados utilizados por CIPSC con este fin, los cuales identifican plenamente a la TSU y a CIPSC.

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

6.3.5.- Sincronización del reloj con UTC

TSACI proporciona el instante de tiempo con la precisión declarada en el apartado 6.2.3 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.

6.3.6.- Certificado raíz y sellos de TSACI

6.3.6.1.- Certificado raíz

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

Su contenido es el siguiente:

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la Autoridad de Sellado de Tiempo
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Asunto	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la Autoridad de Sellado de Tiempo
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.

L	Zaragoza
C	ES
Clave pública	RSA (4096 Bits)
AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/tsa/raiz.crt aceso id-ad-ocsp https://ocsp.coloriuris.net
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/tsa/tsa.crl
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.37799.0.3.1.2.0 [1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado raíz de la Autoridad de Sellado de Tiempo de CIPSC. [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
Uso de la clave	firma de certificados, firma CRL sin conexión, firma de lista de revocación de certificados (CRL)

6.3.6.2.- Certificados para la emisión de sellos de tiempo

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

De acuerdo con lo recomendado por la norma ETSI TS 102 023, no se realizan copias de seguridad de las claves privadas de las Autoridades, con la finalidad de evitar el posible compromiso de las mismas.

Estos certificados serán los siguientes:

- un certificado de 2048 para la emisión de sellos de tiempo destinados a otros servicios de CIPSC o de Coloriuris identificado por el OID 1.3.6.1.4.1.37799.20.3.1
- un certificado de 2048 para la prestación del servicio de sellado de tiempo a las partes usuarias identificado por el OID 1.3.6.1.4.1.37799.20.3.2

Perfil del certificado para emisión de sellos de tiempo de CIPSC o Coloriuris

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la Autoridad de Sellado de Tiempo
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Asunto	
CN	CIPSC – Emisor de sellos de tiempo de 2048
OU	Emisión de sellos de tiempo para los servicios de Coloriuris
O	Coloriuris S.L.
L	Zaragoza
Clave pública	RSA (2048 Bits)
AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/tsa/raiz.crt aceso id-ad-ocsp https://ocsp.coloriuris.net

Punto de distribución CRL	https://cipsc.coloriuris.net/crl/tsa/tsa.crl
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.37799.20.3.1 [1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado para la emisión de sellos de tiempo [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
Uso de la clave	Firma digital, Cifrado de clave
Uso extendido de la clave	Time Stamping (Marca de Tiempo)

Perfil del certificado para emisión de sellos de tiempo a las partes usuarias

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

	Identificador de directiva=1.3.6.1.4.1.37799.20.3.2 [1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado para la emisión de sellos de tiempo [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
Uso de la clave	Firma digital, Cifrado de clave
Uso extendido de la clave	Time Stamping (Marca de Tiempo)

7 Política para la prestación del servicio de entrega electrónica certificada (EEC)

7.1.- Declaración básica del servicio de entrega electrónica certificada

La Declaración básica del servicio del servicio de entrega electrónica certificada de CIPSC recoge las condiciones y aspectos fundamentales del servicio 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 *PKI Disclosure Statement*, que los estándares ETSI TS 102 042 y ETSI TS 101 456 establecen para los servicios de certificación electrónica.

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

Titularidad

EEC es un servicio del Coloriuris S.L., empresa cuyos datos de contacto se encuentran en el apartado 1.3.4 de este documento.

Disponibilidad del servicio

La disponibilidad del servicio es la descrita en el apartado 3.3.1 del presente documento.

Publicación de la Política

Todas y cada una de las certificaciones de remisión y recepción de envíos electrónicos emitidas por EEC contiene el identificador (OID) de la Política, cuyo valor se incluye en el apartado 2.2 de este documento.

Mecanismos criptográficos

La firma de las certificaciones de remisión y recepción de envíos electrónicos se realiza calculando el hash mediante SHA 256, y cifrándolo con algoritmos RSA, utilizando para ello una firma emitida por ASD. Todas las firmas incorporan un sello de tiempo emitido por TSACI.

Validez de las certificaciones de remisión y recepción de envíos electrónicos

EEC no establece otras limitaciones a la confianza que merece su servicio de entrega electrónica certificada que las que son inherentes a las tecnologías utilizadas. Si se determinara que los algoritmos criptográficos o la longitud de claves utilizados para la firma de las certificaciones de remisión y recepción de envíos electrónicos han dejado de aportar un nivel adecuado de seguridad, CIPSC publicará inmediatamente dicha información en su página web.

Aplicabilidad

EEC considera que el uso más apropiado del servicio de entrega electrónica certificada es la generación de una prueba documental que acredite la remisión, por parte un remitente, la recepción y, en su caso, el acceso/ descarga a/de contenido adjunto, por parte de uno o más destinatarios, de un determinado envío electrónico, así como del momento en que ambas se produjeron.

Obligaciones

Las obligaciones de las partes usuarias están descritas en el apartado en el apartado 7.2.3.

Registro de las operaciones

EEC registra sus operaciones y conserva esta información en adecuadas condiciones de seguridad, según lo previsto en el apartado 3.5.3 del presente documento.

Normativa

La prestación del servicio de entrega electrónica certificada (EEC) por parte de CIPSC se realiza de acuerdo con la legislación española y europea aplicable a la materia, recogida en el apartado 7.2.1 del presente documento, con las presentes Políticas y declaración de prácticas y con la normativa interna de Coloriuris.

Responsabilidad

Las responsabilidades de CIPSC y las limitaciones establecidas sobre la misma se describen en el apartado 4.3 del presente documento.

Reclamaciones

Todas las reclamaciones de usuarios y terceros sobre la prestación del servicio de entrega electrónica certificada deberán serle comunicadas según lo establecido en el apartado 4.7.1 del presente documento. 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 mencionado apartado 4.7.2, con renuncia a cualquier otro fuero que pudiera corresponderles.

Garantía y auditorías

CIPSC garantiza que la prestación del servicio de entrega electrónica certificada es conforme con las estipulaciones incluidas en estas Políticas y declaración de prácticas. En este sentido, Coloriuris llevará a cabo auditorías periódicas del funcionamiento de CIPSC, de acuerdo con las directrices establecidas en el presente documento.

Tarifas

CIPSC podrá pedir una contraprestación económica por la prestación del servicio de entrega electrónica certificada, de acuerdo con las tarifas que en cada momento se encuentren publicadas en su web.

7.2.- Aspectos generales

7.2.1.- Introducción

La presente Política regula la prestación del servicio de entrega electrónica certificada por CIPSC. CIPSC emplea una clave privada generada por ASD para la firma de las certificaciones de emisión y recepción de los envíos electrónicos. Todas y cada una de estas firmas contienen la identificación de las Políticas y declaración de prácticas que se les aplican.

7.2.2.- Comunidad de usuarios

La comunidad para la entrega electrónica certificada son CIPSC según se describe en los apartados 2.1.2.1 y 2.1.2.3, las Autoridades de registro (AR), según se describen en el apartado 2.1.3, los firmantes y creadores de sellos, según se describen en el apartado 2.2.1, y las partes usuarias, según se describen en el apartado 2.2.2.

CIPSC es responsable de la remisión o puesta a disposición de los destinatarios de los envíos y del registro fehaciente de la recepción de los mismos, cuando ésta se produzca; y, en su caso, del acceso/ descarga a/de documentación adjunta. También es responsable de la generación y emisión de certificaciones firmadas acreditando estos hechos y el momento en el que se produjeron. Son partes usuarias quienes solicitan a CIPSC la realización de una entrega certificada, así como los destinatarios que aceptan recibirla. Asimismo aquellas personas que confían en las certificaciones de remisión y recepción generadas por CIPSC.

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

7.2.3.- Usos del servicio de entrega electrónica certificada

El uso más apropiado del servicio de entrega electrónica certificada es la generación de una prueba documental que acredite la remisión, por parte de CIPSC, y la recepción, por parte de uno o más destinatarios, de un determinado envío electrónico, así como del momento en que ambas se

produjeron y, en su caso, del acceso/ descarga a/de documentación adjunta con la finalidad principal de que pueda ser utilizada en contextos jurídicos.

7.2.4.- Obligaciones

Además de las obligaciones establecidas por la ley y de las enumeradas en el apartado 2.2 de este documento, se establecen las siguientes obligaciones específicas para la prestación del servicio de entrega electrónica certificada.

CIPSC

1) Remitir los envíos o ponerlos a disposición del destinatario o destinatarios en la forma dispuesta en esta Política, emitiendo la correspondiente certificación.

2) Disponer los medios apropiados para que el destinatario o destinatarios del envío puedan generar de forma segura el correspondiente acuse de recibo.

3) Validar, en su caso, la firma o firmas de los destinatarios en la forma exigida por las correspondientes Políticas de Certificación.

4) Recibir y conservar los certificados de estado de entrega, generando en base a los mismos la certificación de entrega y poniendo ésta a disposición del remitente.

5) Utilizar medios de firma y sellos de tiempo apropiados para la generación de las certificaciones.

6) Garantizar la confidencialidad de los envíos, utilizando para ello del cifrado de confidencialidad cuando así se solicite.

Partes usuarias

- Garantizar que los envíos remitidos obedecen a una relación jurídica con los destinatarios y que no son comunicaciones no deseadas por los mismos, salvo cuando el envío esté amparado por lo dispuesto en una ley.

- Proporcionar a CIPSC datos de contacto de los destinatarios que sean fiables y estén actualizados.

- Cuando la parte usuaria sea el aceptante de un envío, utilizar medios de firma apropiados para la generación del correspondiente acuse de recibo y, en su caso, para el acceso al contenido cifrado.

- Verificar la validez de las firmas y sellos de tiempo incorporados en las certificaciones de

remisión y recepción de envíos.

- Notificar cualquier hecho o situación anómala relativa al servicio de entrega electrónica certificada, y/o a las certificaciones emitidas, y que pueda ser considerado como causa de la perdida de fiabilidad de las mismas.

7.2.5.- Registro de información referente al servicio de entrega electrónica certificada

CIPSC mantiene registros de toda la información relevante referente a sus operaciones por un periodo de 15 años. Los registros se protegen para garantizar su integridad y confidencialidad.

Los registros están a disposición de quienes ostenten un interés legítimo para el acceso a los mismos y de las autoridades que los requieran de acuerdo con lo dispuesto en las leyes.

En particular se mantienen registros, que incluyen el momento en que se produjeron, sobre los siguientes eventos:

- Peticiones de entrega de envíos y resultado de las mismas
- Acuses de recibo emitidos por los destinatarios
- Certificaciones de remisión y recepción
- Certificados de acceso a documentos *online*

Los procedimientos para la generación y conservación de los mencionados registros se detalla en la documentación interna de gestión de EEC.

7.3.- Realización del servicio de entrega electrónica certificada

7.3.1.- Acceso al servicio

Los usuarios pueden solicitar la entrega electrónica certificada de uno o más envíos en las formas previstas en la documentación interna de gestión de EEC.

La dirección de acceso al servicio es https://www.coloriuris.net/envios-certificados/usuarios/coloriuris/login

7.3.2.- Disponibilidad del servicio

El servicio de entrega electrónica certificada está disponible de forma ininterrumpida,

según lo dispuesto en el apartado 3.3.1.

7.3.3.- Entrega electrónica certificada

El servicio de entrega certificada se prestará con todas o alguna de las siguientes modalidades:

- Con autenticación del destinatario mediante dirección de correo electrónico.
- Con autenticación del destinatario mediante número de teléfono móvil.
- Con autenticación del destinatario mediante un certificado electrónico concreto y cifrado del mensaje.

En todo caso el remitente deberá facilitar a CIPSC, bajo su responsabilidad, la dirección de correo electrónico y/o el número de teléfono móvil del destinatario o destinatarios del envío, así como el contenido de éste y una breve descripción del mismo (asunto). En la tercera modalidad deberá aportar asimismo el certificado o certificados electrónicos (clave pública) validos de los mismos. Los destinatarios únicamente podrán acceder al envío utilizando el certificado aportado para cada uno de ellos.

CIPSC pondrá el envío a disposición del destinatario o destinatarios en el servidor de correo entrante y/o en el terminal móvil del destinatario y/o en su sitio web, al que se accederá a través de una conexión segura, existiendo para cada envío y destinatario una URL única generada de forma aleatoria y con la longitud suficiente para aportar un grado razonable de seguridad.

En la tercera modalidad el envío se cifrará previamente con la clave pública del destinatario y éste deberá probar su identidad utilizando el certificado asociado al envío antes de acceder a la operatoria de entrega del envío. La operatoria de entrega del envío informará al destinatario del remitente, de la fecha del envío y del asunto. El destinatario deberá firmar el acuse de recibo y utilizar la clave asociada al certificado indicado por el remitente.

El acuse de recibo estará en formato y tendrá, como mínimo el siguiente contenido:

- Un número de serie único
- El identificador de las Políticas y declaración de prácticas aplicables.
- El resumen (*hash*) del envío
- Una diligencia expresiva de la naturaleza del certificado de estado de entrega y de su carácter probatorio de la recepción del envío cuyo resumen se incorpora

- La identidad del remitente
- La identidad del destinatario
- El asunto
- La fecha y hora de recepción

CIPSC, en la tercera modalidad, verificará que la firma electrónica generada por el destinatario tiene un formato válido y que el certificado utilizado está dentro de su plazo de validez. La consulta a las correspondientes CRL o directorios de certificados revocados estará en función del PSC que haya emitido el certificado y de la clase a la que este pertenezca. CIPSC indicará en su sitio web las clases de certificados para los que se realiza esta comprobación y, en su caso, entregará al remitente, junto al acuse de recibo firmado, las evidencias acreditativas de su resultado. CIPSC no realizará ninguna comprobación sobre la correspondencia entre los datos de los certificados y la identidad de los destinatarios.

CIPSC adopta las medidas técnicas precisas para garantizar que los acuses de recibo son seguros e incluyen una firma electrónica avanzada y un sello de tiempo que acredita el momento en el que se generó la misma, con la fecha y hora correctas. Para cada acuse de recibo se conservan los certificados que establecen la cadena de confianza de la firma incorporada y, en su caso, las evidencias acreditativas del resultado de la consulta o consultas realizadas para comprobar el estado de los certificados.

7.4.- El certificado de firma de EEC

7.4.1.- Formato

Los certificados utilizados por EEC de CIPSC son emitidos por ASD, que se ajustan al estándar X.509 versión 3 y al RFC 3039 "*Internet X.509 Public Key Infrastructure Qualified Certificates Profile*" y que incorporan un fechado de tiempo emitido por TSACI.

Los identificadores únicos (OID) de los algoritmos con cifrado RSA utilizados son los siguientes:

- SHA256RSA: 1.2.840.113549.1.1.11

La longitud de la clave del certificado es de 2048 bits, con un periodo de validez de 10 años según el perfil indicado en el apartado 7.3.8.2.

8 Autoridad para los servicios relativos a los documentos electrónicos (ASD)

8.1.- Declaración básica de los servicios relativos a los documentos electrónicos

La Declaración básica de los servicios relativos a los documentos electrónicos de CIPSC recoge las condiciones y aspectos fundamentales de estos servicios 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 *PKI Disclosure Statement*, que los estándares ETSI TS 102 042 y ETSI TS 101 456 establecen para los servicios de certificación electrónica.

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

Titularidad

ASD es un servicio del Coloriuris S.L., empresa cuyos datos de contacto se encuentran en el apartado 1.6.4 de este documento.

Disponibilidad del servicio

Los servicios relativos a los documentos electrónicos de ASD están disponibles de forma ininterrumpida todos los días del año salvo la tramitación presencial de solicitudes, que únicamente estará disponible en el horario de oficina que establezca cada una de las Autoridades de Registro.

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

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.

Publicación de la Política

Todos y cada una de las firmas de los documentos autenticados por ASD y de las diligencias de registro de documentos emitidas por CIPSC contienen el identificador (OID) de la Política, cuyo valor se incluye en el apartado 1.5 de este documento.

Mecanismos criptográficos

La firma de los documentos, de las diligencias de registro y de las demás evidencias asociadas a estos servicios se realiza calculando el hash mediante SHA-256 y cifrándolo con algoritmos RSA, utilizando para ello una clave cuya longitud es de 2048 bits. Todas las firmas incorporan un sello de tiempo emitido por TSACI.

Validez de los documentos autenticados y de las diligencias de registro

CIPSC establece como únicas limitaciones a la confianza que merecen sus servicios de autenticación de documentos y de registro y archivo de documentos aquellas que son inherentes a las tecnologías utilizadas. Si se determinara que los algoritmos criptográficos o la longitud de claves utilizados para la firma de las evidencias mencionadas han dejado de aportar un nivel adecuado de seguridad, CIPSC publicará inmediatamente dicha información en su página web.

Aplicabilidad

CIPSC considera que el uso más apropiado del servicio de autenticación de documentos es la generación de una prueba documental, con garantía de su origen e integridad. Normalmente se tratará de un servicio auxiliar a otros prestados por Coloriuris como, por ejemplo, Acta de Navegación o el archivo de firmas longevas, entre otros.

CIPSC considera que el uso más apropiado del servicio de registro y archivo de documentos electrónicos es la acreditación de su existencia y contenido exacto desde el momento del registro y su conservación en condiciones seguras a partir de éste. Asimismo se acredita la validez de las firmas y sellos incorporados a los mismos en el momento del registro, adoptándose las medidas apropiadas para que dicha garantía perdure durante el tiempo en el que los documentos obren en el archivo de CIPSC.

Obligaciones

Las obligaciones de las partes usuarias están descritas en los apartados 8.2.4 del presente documento y en el apartado 2.3.3.

Registro de las operaciones

CIPSC registra sus operaciones y conserva esta información en adecuadas condiciones de seguridad, según lo previsto en los apartados 3.3.4 y 8.2.5 del presente documento.

Normativa

La prestación de los servicios de autenticación de documentos y de registro y archivo de

documentos electrónicos por parte de CIPSC se realiza de acuerdo con la legislación española y europea aplicable a la materia, recogida en el anexo del presente documento, con las presentes Políticas y declaración de prácticas y con la normativa interna de Coloriuris.

Responsabilidad

Las responsabilidades de CIPSC y las limitaciones establecidas sobre la misma se describen en el apartado 2.4 del presente documento.

Reclamaciones

Todas las reclamaciones de usuarios y terceros sobre la prestación de los servicios relativos a los documentos electrónicos por CIPSC deberán serle comunicadas según lo establecido en el apartado 2.8.1 del presente documento. 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 mencionado apartado 2.8.2, con renuncia a cualquier otro fuero que pudiera corresponderles.

Garantía y auditorías

CIPSC garantiza que la prestación de los servicios relativos a los documentos electrónicos 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 CIPSC y de la Autoridad para la prestación de los servicios relativos a los documentos electrónicos (ASD).

Tarifas

CIPSC podrá pedir una contraprestación económica por la prestación de los servicios relativos a los documentos electrónicos, de acuerdo con las tarifas que en cada momento se encuentren publicadas en su web.

8.2.- Política para la prestación de los servicios relativos a los documentos electrónicos

8.2.1.- Introducción

La presente Política regula la generación y emisión de documentos electrónicos auténticos y el registro y archivo de documentos electrónicos por ASD. ASD emplea claves privadas específicas para la firma de los documentos electrónicos autenticados y de las diligencias de registro. Cada firma contiene la identificación de las Políticas y declaración de prácticas que se le aplican.

8.2.2.- Comunidad de usuarios

La comunidad para la prestación de los servicios relativos a los documentos electrónicos son la Autoridad para los servicios relativos a los documentos electrónicos (ASD), según se describe en los apartados 2.1.2.1 y 2.1.2.4, las Autoridades de registro (AR), según se describen en el apartado 2.1.3 y los partes usuarias, según se describen en el apartado 2.2.2.

En el servicio de autenticación de documentos, la ASD es responsable de la firma de los documentos autenticados. En el servicio de registro y archivo de documentos, la ASD es responsable del registro de los documentos, emitiendo la correspondiente diligencia de registro, y de su archivo y conservación.

Las AR tramitan las solicitudes externas, es decir no procedentes de otras autoridades de CIPSC, para la prestación de los servicios relativos a los documentos.

Las partes usuarias son quienes solicitan y obtienen un documento electrónico autenticado por CIPSC, quienes solicitan el registro y archivo de un documento electrónico por CIPSC y aquellas personas que confían en los documentos electrónicos auténticos, en las diligencias de registro y en las demás evidencias asociadas a los servicios relativos a los documentos electrónicos generadas por CIPSC.

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

8.2.3.- Usos de los servicios relativos a los documentos electrónicos

La generación de documentos electrónicos auténticos por CIPSC permite la generación de una prueba documental, con garantía de su origen e integridad, y normalmente se utilizará como un servicio auxiliar a otros prestados por Coloriuris como, por ejemplo, *actaNavegación*, *actaFirma* o *actaSMS*, o para el resellado de las evidencias archivadas, cuando sea preciso para el archivo de firmas longevas, entre otros.

El servicio del registro de documentos electrónicos permite acreditar de forma fehaciente la existencia y contenido de un documento en el momento del registro, así como la validez de las firmas y sellos incorporados al mismo. Por su parte el servicio de archivo permite preservar a lo largo del tiempo el documento y la fuerza probatoria de las firmas y sellos que lo acompañen, así como facilitar a las partes usuarias imágenes digitales de los documentos registrados, cuya fidelidad puede ser contrastada a través del correspondiente código de verificación en el punto de verificación de CIPSC.

8.2.4.- 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.

ASD

1) Utilizar medios de firma y sellos de tiempo apropiados para la autenticación de los documentos y para la firma de las diligencias de registro y demás evidencias asociadas a los servicios relativos a los documentos electrónicos, así como para el resellado de las firmas y sellos archivados a efectos de su preservación a lo largo del tiempo.

2) Validar las firmas y sellos incorporados a los documentos antes de proceder a su registro, dejando constancia autenticada del resultado de las validaciones y conservando durante todo el periodo de archivo del documento las evidencias resultantes de las mismas.

3) Registrar los documentos, asignándoles un número de identificación único y emitiendo y poniendo a disposición de la parte usuaria la correspondiente diligencia de registro.

4) Conservar los documentos durante el periodo acordado.

5) Garantizar la confidencialidad de los documentos archivados, facilitando únicamente copias e imágenes de los mismos a las personas – físicas o jurídicas – que ostenten un interés legítimo de acuerdo con las leyes.

6) Adoptar las medidas técnicas adecuadas para mantener la fuerza probatoria de las firmas y sellos incorporados a los documentos archivados durante todo el tiempo de conservación de los mismos.

7) Facilitar a las personas – físicas o jurídicas – que ostenten un interés legítimo de acuerdo con las leyes copia de los documentos archivados cuando sea requerido para ello, así como imágenes de los mismos acompañadas del correspondiente código de verificación.

8) Mantener accesible a través de Internet un punto de verificación en el que a través del correspondiente código de verificación pueda accederse a la copia auténtica de los documentos archivados.

9) Eliminar los documentos archivados cuando transcurra el plazo acordado o cuando así se lo solicite expresamente la persona física o jurídica legitimada, de forma que se haga imposible la posterior recuperación de su contenido.

Partes usuarias

1) Responder, cuando así se afirme expresamente en los mismos, de la veracidad del contenido de los documentos autenticados.

2) Conservar el identificador único asignado al documento en el momento del registro y facilitarlo a la ASD cuando solicite la realización de cualquier operación sobre el documento.

3) Difundir las imágenes de los documentos acompañadas del código de verificación únicamente para la finalidad prevista de probar la identidad entre la imagen y el documento registrado al que corresponda la misma.

4) Garantizar que a través del punto de verificación no se facilita el acceso a información reservada o de carácter personal por parte de quienes no tengan derecho al mismo.

5) Verificar la validez de las firmas y sellos de tiempo incorporados en los documentos electrónicos auténticos, en las diligencias de registro y en las demás evidencias emitidas por CIPSC y asociadas a los servicios relativos a los documentos electrónicos.

6) Notificar cualquier hecho o situación anómala relativa al servicio de autenticación de documentos, y/o a los documentos electrónicos auténticos emitidos, al servicio de registro y archivo de documento electrónicos y/o a los documentos registrados y archivados, y que pueda ser considerado como causa de la perdida de fiabilidad de los mismos.

7) Hacer un uso apropiado de las imágenes de los documentos acompañadas del código de verificación, utilizando este recurso únicamente con la finalidad prevista de comprobar la fidelidad de la imagen respecto al documento archivado al que corresponda la misma.

8.2.5.- Registro de información referente a la operación de los servicios de autenticación de documentos

ASD mantiene registros de toda la información relevante referente a sus operaciones por un periodo de 15 años, según se dispone en el apartado 3.3.4. Sin perjuicio de lo anterior, en el servicio de archivo este plazo se prolongará durante todo el periodo de archivo de los documentos a las que estas se refieran y los 5 años posteriores a la finalización de este. En caso de que no se hubiera acordado el archivo del documento, la ASD conservará copia de la diligencia de registro y, en su caso, de las evidencias adjuntas por un periodo de 15 años.

En particular se mantienen registros, que incluyen el momento en que se produjeron, sobre los siguientes eventos:

- Peticiones de emisión de documentos auténticos
- Emisión de documentos auténticos

- Peticiones de registro de documentos electrónicos
- Registro de documentos electrónicos, emisión de la correspondiente diligencia de registro e ingreso del documento en el archivo
- Emisión de copias de los documentos e imágenes de los mismos con código de verificación
- Operaciones de resellado de las firmas y sellos de los documentos archivados
- Eliminación de los documentos archivados

Los procedimientos para la generación y conservación de los mencionados registros se detalla en la documentación interna de gestión de ASD.

8.3.- Declaración de prácticas

8.3.1.- Acceso a los servicios

Los usuarios pueden solicitar la generación de documentos auténticos o el registro y archivo de documentos en las formas previstas en la documentación interna de gestión de ASD.

La dirección de acceso a los servicios es http://www.coloriuris.net/acta-registro/info/

El acceso al punto de verificación se realizará en la dirección: https://www.coloriuris.net/csv/

8.3.2.- Disponibilidad de los servicios

Los servicios relativos a los documentos están disponibles 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.

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.

8.3.3.- Documentos electrónicos auténticos

ASD adopta las medidas técnicas precisas para garantizar que los documentos electrónicos

auténticos son seguros e incluyen una firma electrónica avanzada y un sello de tiempo que acredita el momento en el que se generó la misma, con la fecha y hora correctas. Para cada documento se conservan los certificados que establecen la cadena de confianza de la firma incorporada y las evidencias acreditativas del resultado de la consulta o consultas realizadas para comprobar el estado de los certificados. Los documentos se firman utilizando un dispositivo criptográfico, y el certificado utilizado identifica plenamente a ASD.

Además de los contenidos exigidos por los estándares aplicables, todas las firmas incluyen el el identificador de las Políticas y declaración de prácticas aplicables, cuyo valor se indica en el apartado 1.5, y un número de serie único que identifica la firma incorporada por ASD.

8.3.4.- Registro de documentos electrónicos

El usuario del servicio entregará a la ASD el documento a registrar y le proporcionará los datos de identificación requeridos por la normativa interna de la ASD. En el caso de que el documento contenga firmas y/o sellos electrónicos la ASD procederá a validarlos, comprobando que las claves privadas utilizadas se corresponden con las públicas certificadas, que los certificados están dentro de su periodo de validez y, en caso de que se encuentren disponibles las CRL y/o los directorios OCSP del emisor de los certificados, su estado. CIPSC indicará en su sitio web las clases de certificados para los que se realiza esta comprobación. Para cada firma o sello se conservarán los certificados que establecen la cadena de confianza y, en su caso, las evidencias acreditativas del resultado de la consulta o consultas realizadas para comprobar el estado de los certificados.

La ASD generará una diligencia de registro que tendrá, como mínimo, el siguiente contenido:

- El número de registro único asignado al documento
- El identificador de las Políticas y declaración de prácticas aplicables, cuyo valor se indica en el apartado 1.5
- El resumen (*hash*) del documento registrado
- Una diligencia expresiva de la naturaleza del registro
- En su caso, una diligencia expresiva de las operaciones efectuadas para la validación de las firmas y/o sellos incorporadas al documento y del resultado de las mismas, incluyendo la referencia a las evidencias acreditativas de las mismas cuando estas hubieran sido facilitadas por los PSC consultados.
- La identidad del usuario

- Optativamente, el asunto
- La fecha y hora de registro
- En caso de que se haya acordado el archivo del documento, una diligencia expresiva de que el documento queda archivado por la ASD y el plazo inicial establecido para su conservación.

ASD firmará la diligencia de registro, incorporando a la firma un sello de tiempo acreditativo del momento del registro, y la pondrá a disposición del usuario junto con, en su caso, las evidencias acreditativas de las operaciones efectuadas para la validación de las firmas y/o sellos y el resultado de las mismas.

ASD adopta las medidas técnicas precisas para garantizar que las diligencias de registro son seguras e incluyen una firma electrónica avanzada y un sello de tiempo que acredita el momento en el que se generó la misma, con la fecha y hora correctas.

8.3.5.- Archivo de documentos electrónicos

ASD procederá al archivo de los documentos cuando así se haya acordado. El mecanismo utilizado para garantizar la perdurabilidad de las firmas y/o sellos incorporados a los documentos será el de las firmas longevas. Para ello se verificaran, validando la integridad de las firmas o sellos, el cumplimiento de los estándares y que contiene las referencias obligatorias. A continuación se completarán, obteniendo y anexándoles las referencias a certificados (incluyendo los certificados del firmante y todos los que formen la cadena de certificación), así como la información referente al estado de los certificados, obtenida mediante la consulta a las listas de certificados revocados (CRL) o a directorios OCSP. Una vez generadas las firmas longevas, la documentación interna de CIPSC definirá los procedimientos para mantener las evidencias y gestionar la actualización de las mismas.

Para la protección de la firma electrónica frente a la posible obsolescencia de los algoritmos, según se determine en la normativa interna de CIPSC, podrán utilizarse mecanismos de resellado, consistentes en añadir sucesivos sellos tiempo utilizando los algoritmos que en cada momento tengan un nivel de seguridad adecuado, o se garantizará la conservación de la firma en un depósito seguro, en forma tal que se asegure la protección contra falsificaciones y constando de forma fehaciente la fecha exacta en que las firmas o sellos se almacenaron en el mismo.

8.3.6.- Emisión de copias de los documentos electrónicos archivados

CIPSC facilitará copias de los documentos archivados al usuario o a quien pruebe que dispone de derecho suficiente para ello. CIPSC pondrá a disposición el documento, la diligencia de registro, las firmas o sellos que lo acompañaran, transformadas en firmas longevas y, en su caso,

incluyendo los sellos de preservación que les hubieran sido incorporados. Cuando la protección contra la obsolescencia de los algoritmos criptográficos se haya basado en la conservación en un depósito seguro acompañará también una certificación acreditativa de este hecho y del periodo de conservación, entregando una copia de las firmas o sellos resellándola de forma que se impida su modificación posterior a la entrega.

8.3.7.- Emisión de imágenes de los documentos electrónicos con código de verificación y acceso al punto de verificación

CIPSC facilitará imágenes digitales de los documentos archivados al usuario o a quien pruebe que dispone de derecho suficiente para ello. En dichas imágenes se incorporará un código de verificación con el que podrá accederse a la copia del documento en el punto de verificación de CIPSC. El código se generará mediante un mecanismo aleatorio, de forma que no pueda deducirse el mismo conociendo la información relativa al documento. También podrá incorporarse a la imagen una contraseña, que será necesario introducir junto al código de verificación para acceder al contenido del documento.

CIPSC informará en el punto de acceso de la fecha de registro del documento así como, en su caso, de las firmas y/o sellos incorporados al mismo, de su validez y de las medidas adoptadas para garantizar su preservación.

8.3.8.- Certificado raíz y sellos de la ASD

8.3.8.1.- Certificado raíz

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

Su contenido es el siguiente:

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la A.C. para servicios relativos a documentos electrónicos
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza

C	ES
Asunto	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la A.C. para servicios relativos a documentos electrónicos
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Clave pública	RSA (4096 Bits)
AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/asd/raiz.crt aceso id-ad-ocsp https://ocsp.coloriuris.net
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/asd/asd.crl
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.37799.0.3.1.2.0 [1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado raíz de la Autoridad de Autoridad de Servicios relativos a Documentos-e [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
Uso de la clave	firma de certificados, firma CRL sin conexión, firma de lista de revocación de certificados (CRL)

8.3.8.2.- Certificados para la prestación de servicios relativos a los documentos electrónicos

ASD dispondrá de certificados para la prestación de los servicios relativos a los documentos electrónicos, emitidos por la propia ASD de CIPSC utilizando su certificado raíz, y cuyo periodo de validez será de 10 años.

Estos certificados serán los siguientes:

- sellado de documentos creados por Coloriuris en la prestación de sus servicios, como

actaNavegación u otros. Este tipo de certificado estará identificado por el OID 1.3.6.1.4.1.37799.20.4.1.

- resellado de documentos, identificado por el OID 1.3.6.1.4.1.37799.20.4.2.
- sellado de las certificaciones de registro y demás evidencias asociadas al servicio de registro y archivo, identificado por el OID 1.3.6.1.4.1.37799.20.4.3.

La longitud de clave de todos ellos será de 2048 Bits. La función a la que se dedica el certificado se indicará en el campo CN.

El contenido del certificado para el sellado de documentos creados por Coloriuris en la prestación de sus servicios es el siguiente:

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la A.C. para servicios relativos a documentos electrónicos
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Asunto	
CN	CIPSC – Autenticación de documentos creados por Coloriuris
O	Coloriuris S.L.
OU	Prestador de servicios de Confianza
E	cipsc@coloriuris.net
SerialNumber	B99091696
Clave pública	RSA (2048 Bits)
AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/asd/raiz.crt aceso id-ad-ocsp https://ocsp.coloriuris.net
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/asd/asd.crl
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.37799.20.4.1

	[1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado de CIPSC para la autenticación de documentos generados por Coloriuris [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
Uso de la clave	firma digital, no repudio, cifrado de clave, cifrado de datos

El contenido del certificado para el resellado de documentos es el siguiente:

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la A.C. para servicios relativos a documentos electrónicos
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Asunto	
CN	CIPSC – Resellado de documentos
O	Coloriuris S.L.
OU	Prestador de servicios de Confianza
E	cipsc@coloriuris.net
SerialNumber	B99091696
Clave pública	RSA (2048 Bits)
AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/asd/raiz.crt aceso id-ad-ocsp https://ocsp.coloriuris.net
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/asd/asd.crl
Bases del certificado	[1]Directiva de certificados:

	Identificador de directiva=1.3.6.1.4.1.37799.20.4.2 [1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado de CIPSC para el resellado de documentos [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
Uso de la clave	firma digital, no repudio, cifrado de clave, cifrado de datos

El contenido del certificado para la prestación del servicio de registro y archivo es el siguiente:

Emisor (Issuer)	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la A.C. para servicios relativos a documentos electrónicos
SerialNumber	B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Asunto	
CN	CIPSC – Servicio de registro y archivo
O	Coloriuris S.L.
OU	Prestador de servicios de Confianza
E	cipsc@coloriuris.net
SerialNumber	B99091696
Clave pública	RSA (2048 Bits)
AIA Acceso Información del Emisor	acceso id-ad-http https://cipsc.coloriuris.net/certificados/asd/raiz.crt aceso id-ad-ocsp https://ocsp.coloriuris.net
Punto de distribución CRL	https://cipsc.coloriuris.net/crl/asd/asd.crl

Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.37799.20.4.3 [1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado de CIPSC para la prestación del servicio de registro y archivo [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://cipsc.coloriuris.net/politicas/
Uso de la clave	firma digital, no repudio, cifrado de clave, cifrado de datos

Anexo I

Acrónimos utilizados

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

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

Definiciones

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

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

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

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

Normativa

La normativa básica aplicable es la siguiente:

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

Secretaría de Estado para la Función Pública, de 19 de julio de 2011)

- NTI de Reutilización de recursos de información (Resolución de 19 de febrero de 2013)
- NTI de Política de gestión de documentos electrónicos (Resolución de 28 de junio de 2012)

Estándares

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

- *CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates V1*
- *CA/Browser Forum EV SSL Certificate Guidelines V 1.3*
- ETSI EN 319 401, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures.
- ETSI TS 101 456, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification Authorities issuing qualified certificates.
- ETSI TS 101 733, Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)
- ETSI TS 101 861, Time-stamping Profile.
- ETSI TS 101 903, XML Advanced Electronic Signatures (XAdES)
- ETSI TS 102 023, Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-stamping Authorities.
- ETSI TS 102 042, Policy Requirements for certification authorities issuing public key certificates.
- ETSI TS 102 176.1, Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash Functions and Asymmetric Algorithms.
- ETSI TS 102 573, Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data objects.
- ISO/IEC 18014-1, Time-stamping services — Part 1: Framework
- RCF 3647, *Internet X.509 Public Key Infrastructure Certificate Policy*

- RFC 3161, Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP).
- RFC 3628, Policy Requirements for Time-Stamping Authorities (TSAs)
- RFC 3739 y 3039, *Internet X.509 Public Key Infrastructure: Qualified Certificates Profile*
- RFC 5280 y 3280, *Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL)*

Fdo.: Pedro Canut Zazurca

Responsable de Administración de Políticas de Coloriuris S.L.

Fecha: 13 de octubre de 2015

Anexo II – Certificados de CIPSC

[AC] Certificado raíz de la Autoridad de Certificación

Asunto	C = ES L = Zaragoza O = Coloriuris S.L. OU = Prestador de Servicios de Confianza SERIALNUMBER = B99091696 CN = CIPSC – Raíz de la Autoridad de Certificación E = cipsc@coloriuris.net
Validez	De 14/07/2015 a 14/07/2035
Huella digital (SHA1)	DC 4E 4C 1F 0A E6 7B DD 18 B3 91 E4 A7 EA 36 E0 4F E8 7D 06
URLs descarga	DER https://cipsc.coloriuris.net/certificados/ac/raiz.crt PEM https://cipsc.coloriuris.net/certificados/ac/raiz.pem

[AC] Certificado Subautoridad de Emisión de certificados para persona física

Asunto	C = ES L = Zaragoza O = Coloriuris S.L. OU = Prestador de Servicios de Confianza SERIALNUMBER = B99091696 CN = CIPSC – Subautoridad de emisión de certificados de persona física E = cipsc@coloriuris.net
Validez	De 14/07/2015 a 14/07/2025
Huella digital (SHA1)	2A D6 80 C8 6F 3F 72 ED 9C A7 0B 10 6B 6D 44 F8 56 47 4A 23
URLs descarga	DER https://cipsc.coloriuris.net/certificados/ac/subac/epf.crt PEM https://cipsc.coloriuris.net/certificados/ac/subac/epf.pem

[AC] Certificado Subautoridad de Emisión de certificados para persona jurídica

Asunto	C = ES L = Zaragoza O = Coloriuris S.L. OU = Prestador de Servicios de Confianza SERIALNUMBER = B99091696 CN = CIPSC - Subautoridad de emisión de certificados de persona jurídica E = cipsc@coloriuris.net
Validez	De 14/07/2015 a 14/07/2025
Huella digital (SHA1)	DC 4E 4C 1F 0A E6 7B DD 18 B3 91 E4 A7 EA 36 E0 4F E8 7D 06
URLs descarga	DER https://cipsc.coloriuris.net/certificados/ac/subac/epj.crt PEM https://cipsc.coloriuris.net/certificados/ac/subac/epj.pem

[AC] Certificado raíz de la Autoridad de Certificación v3

Asunto	C = ES L = Zaragoza O = Coloriuris S.L. OU = Prestador de Servicios de Confianza ORGANIZATIONIDENTIFIER (2.5.4.97) = VATES-B99091696 CN = CIPSC - Raíz - Autoridad de Certificación E = cipsc@coloriuris.net
Validez	De 10/09/2015 a 10/09/2035
Huella digital (SHA1)	E3 97 E9 2E D5 D6 90 F9 00 80 53 13 23 1C 55 3F 86 C1 E9 AC
URLs descarga	DER https://cipsc.coloriuris.net/certificados/ac/raiz-v3.crt PEM https://cipsc.coloriuris.net/certificados/ac/raiz-v3.pem

[AC] Certificado de Emisión de certificados de sello electrónico para persona jurídica

Asunto	C = ES L = Zaragoza O = Coloriuris S.L. OU = Prestador de Servicios de Confianza ORGANIZATIONIDENTIFIER (2.5.4.97) = VATES-B99091696 CN = CIPSC - Emisión de certificados de persona jurídica E = cipsc@coloriuris.net
Validez	De 10/09/2015 a 10/09/2025
Huella digital (SHA1)	3E B7 0D 19 94 60 86 9D 0F A2 82 5B F8 5D 94 F4 A5 2A 47 A5
URLs descarga	DER https://cipsc.coloriuris.net/certificados/ac/subac/epj-v3.crt PEM https://cipsc.coloriuris.net/certificados/ac/subac/epj-v3.pem

[ASD] Certificado raíz de la Autoridad de Certificación para servicios relativos a documentos electrónicos.

Asunto	C = ES L = Zaragoza O = Coloriuris S.L. OU = Prestador de Servicios de Confianza SERIALNUMBER = B99091696 CN = CIPSC - Raíz de la Autoridad de Certificación E = cipsc@coloriuris.net
Validez	De 14/07/2015 a 14/07/2035
Huella digital (SHA1)	20 99 4A 8E DF 70 6F E5 60 1A 73 44 F1 54 20 62 01 C5 2F 66
URLs descarga	DER https://cipsc.coloriuris.net/certificados/asd/raiz.crt PEM https://cipsc.coloriuris.net/certificados/asd/raiz.pem

[TSA] Certificado raíz de la Autoridad de Sellado de Tiempo.

Asunto	C = ES L = Zaragoza O = Coloriuris S.L. OU = Prestador de Servicios de Confianza SERIALNUMBER = B99091696 CN = CIPSC - Raíz de la Autoridad de Sellado de Tiempo E = cipsc@coloriuris.net
Validez	De 14/07/2015 a 14/07/2035
Huella digital (SHA1)	6C EC B5 0B F0 96 A0 2A E8 A6 F7 0C 20 2B FD D6 1C 6B E6 9B
URLs descarga	DER https://cipsc.coloriuris.net/certificados/tsa/raiz.crt PEM https://cipsc.coloriuris.net/certificados/tsa/raiz.pem

[TSA] Certificado de emisión de sellos de tiempo para servicios de Coloriuris

Asunto	L = Zaragoza O = Coloriuris S.L. NIF B99091696 OU = Emisión de sellos de tiempo para los servicios de Coloriuris CN = CIPSC – Emisor de sellos de tiempo de 2048
Validez	De 13/10/2015 a 13/10/2025
Huella digital (SHA1)	0A BC C5 2E 02 C0 50 36 61 F0 D3 6F 80 B4 5D 35 F0 D9 36 E2
URL descarga	https://cipsc.coloriuris.net/certificados/tsa/tsu/coloriuris-2048.crt

[TSA] Certificado de emisión de sellos de tiempo para las partes usuarias

Asunto	L = Zaragoza O = Coloriuris S.L. NIF B99091696 CN = CIPSC – Emisor de sellos de tiempo de 2048
Validez	De 13/10/2015 a 13/10/2025
Huella digital (SHA1)	4E 8A A2 A0 94 91 D3 6E FA 7C A1 2F C8 AF D2 56 29 D9 18 1F
URL descarga	https://cipsc.coloriuris.net/certificados/tsa/tsu/terceros-2048.crt

Anexo III

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

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

1.3.6.1.4.1.37799	.20	Perfiles de certificados finales de los servicios de CIPSC			
		.1	Servicios de firma electrónica		
			.1	Certificados de Persona Física	
				.1	Certificado de Persona Física
				.2	Certificado de Persona Física en DSCF
			.2	Certificados Cualificados de Persona Jurídica	
				.1	Certificado de Persona Jurídica
				.2	Certificado de Persona Jurídica en DSCF
		.2	Servicios de sello electrónico		
			.2	Certificados de sello electrónico	
				.1	Certificado de Sello Electrónico
				.2	Certificado de Sello Electrónico en DSCF
		.3	Servicio de sellado de tiempo		
			.1	Certificado de sello de tiempo para servicios de CIPSC o Coloriuris	
			.2	Certificado de sello de tiempo para partes usuarias	
		.4	Servicios relativos a documentos electrónicos		
			.1	Certificado de autenticación de documentos creados por Coloriuris	
			.2	Certificado para resellado de documentos	
			.3	Certificado de Servicio de Registro y Archivo	