Coloriuris Prestador de Servicios de Confianza

Políticas y declaración de prácticas generales

Autor	Coloriuris S.L.
Versión	3.1
Estado del documento	Aprobado
Fecha de emisión	09-04-2018
OID (Object Identifier)	1.3.6.1.4.1.37799.0.3.1.3.1
Ubicación del documento	https://cipsc.coloriuris.net/politicas/

CONTENIDO

Histórico de cambios del documento

HISTÓRICO DEL DOCUMENTO			
Versión	Fecha	Descripción	Autor
1.3	02/02/2015	Políticas y declaración de prácticas de Coloriuris Prestador de Servicios de Confianza	Coloriuris SL
2.0	14/07/2015	• Eliminación de las referencias a longitudes de clave y algoritmos no recomendados por la especificación TS 102 176-1 v2.1.1 (1024, SHA-1) • Corrección de referencias incorrectas a otros apartados en el punto 7.2.2. • Corrección del apartado 4.2.1.4 para ajustarse al artículo 18.a de la LFE en el tema de la posibilidad de almacenar temporalmente los datos de identificación o creación de firma. • Corrección de los plazos de publicación de CRL en el apartado 4.2.1.5 para ajustarse al artículo 10.1 de la LFE. • Actualización de los perfiles de certificado de los puntos 4.2.2.5 y 4.2.3.5 para incluir los campos correspondientes a los Qualified Certificate Statements. • Actualización de los apartados 4.2.3.2 y 4.2.3.5 con la información del contenido y los perfiles de Persona Jurídica para ajustarse al artículo 11 de la Ley 50/2003, de 19 de diciembre, de Firma Electrónica (LFE). • Cambio de los apartados 3.2, 3.3 y 3.4 para adaptarlos y ampliarlos en base a la especificación RF3647. • Nueva redacción del apartado 1.3. • Correcciones materiales • Actualización de datos de los perfiles de los certificados Raíz de la AC, SUB-AC, TSA y ASD. • Emisión de nuevos certificados raíz acordes con las actualizaciones que sustituyen a los anteriores. • Emisión de nuevos certificados de TSU.	Coloriuris SL
2.0.1	10/09/2015	• Actualización del perfil de sello electrónico para personas jurídicas, apartados 4.2.3.2 y 4.2.3.5. • Creación de la CAv3 para la emisión de certificados de sello electrónico según el estándar ETSI EN 319 412-3. 5 Servicios de sello electrónico • Se han añadido dos nuevos certificados en el ANEXO II: [AC] Certificado raíz de la Autoridad de Certificación v3 y [AC] Certificado de Emisión de certificados de sello electrónico para persona jurídica	Coloriuris SL
2.0.2	13/10/2015	• Desambiguación del termino “sello electrónico” entre los puntos 4 y 5 eliminando las referencias al mismo en el punto 4. • Inclusión de los nuevos OIDs identificativos de cada perfil de certificado final según el tipo de servicio, en los puntos 4.2.2.5, 4.2.3.5, 5.2.2.5, 6.3.6.2, 8.3.8.2. • Actualización de los perfiles de certificados finales. • Actualización de los certificados de emisión de sellos de tiempo. • Actualización de los certificados de firma de documentos de ASD. • Incluido nuevo Anexo III con la estructura de identificación de los OIDs de los perfiles de certificados finales.	Coloriuris SL

		• Corrección de errores tipográficos.	
3.0	21/06/2017	• Adaptación de las políticas al reglamento eIDAS • Retirada de la autoridad para los servicios relativos a documentos electrónicos. • Extracción de las políticas y prácticas particulares de los servicios activos a documentos externos	Coloriuris SL
3.0.1	02/07/2017	• Añadido Anexo de Revisión de las Políticas	Coloriuris SL
3.0.2	02/01/2018	• Ampliación plazos CRL	Coloriuris SL
3.1	09/04/2018	• Suprimir las referencias explicitas a las autoridades de certificación de servicios distintos al servicio de sellado de tiempo	Coloriuris SL

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* 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 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*
- ETSI EN 319 421 *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.*
- ETSI EN 319 422 *Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.*

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 sellos de tiempo 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 éstos 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.

Para cada uno de los servicios que presta CIPSC se proveen sus propios documentos externos que 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 y su respectivo documento particular 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 o las correspondientes al servicio 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: 1.3.6.1.4.1.37799.0.3.1.3.1.

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 una autoridad prestadora de servicios, que se sujeta a las políticas y prácticas establecidas en este documento y son las siguientes:

- Autoridad de sellado de tiempo (TSACI): encargada de la generación y emisión de sellos de tiempo.

Cada autoridad puede disponer de uno o varios certificados autofirmados y puede disponer también de certificados respaldados por estos certificados 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 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.

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.- 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, certificaciones de remisión y recepción de entrega electrónica certificada y diligencias de registro.

2.2.2.- 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.

Se incluirá en todas las evidencias que se generen y emitan en la prestación de los servicios del CIPSC el OID de estas políticas generales o, si procede, el OID de las políticas particulares de los servicios 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 el del servicio correspondiente) 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.

2.2.3.- 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 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 de sellos electrónicos, 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 pre-requisito 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 30 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 y que se indica en las condiciones particulares de cada servicio.

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.

El servicio de OCSP se facilita para todos los certificados emitidos por las autoridades de CIPSC. Las respuestas del mismo están autenticadas mediante certificados especiales emitidos por las correspondientes autoridades de CIPSC exclusivamente para ese propósito.

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 MINETAD y se procederá a su re-certificación.

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 Energía y Turismo y Agenda Digital 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 Energía, Turismo y Agenda Digital, 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 Energía, Turismo y Agenda Digital 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 Energía, Turismo y Agenda Digital, 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 119 312.

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.

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) mínimo 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 cualificada. 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/o 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 EN 319 411.

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.

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.

Anexo I

Acrónimos utilizados

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

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

Definiciones

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

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

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

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

Normativa

La normativa básica aplicable es la siguiente:

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

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

Estándares

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

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

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

Fdo.: Pedro Canut Zazurca

Responsable de Administración de Políticas de Coloriuris S.L.

Fecha: 09 de abril de 2018

Anexo II – Revisión de las Políticas

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

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

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

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

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

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

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