



AN INFOCERT COMPANY

# POLÍTICA DE CERTIFICACIÓN – ESTAMPA CRONOLÓGICA DE TIEMPO

*El Futuro Digital es Ahora*

## CONTENIDO

1.	INTRODUCCIÓN .....	6
1.1.	Consideraciones .....	6
1.2.	Estándares Generales.....	6
1.3.	Identificación.....	7
1.4.	Comunidad y Ámbito de Aplicación .....	8
1.4.1.	Autoridad de Estampa Cronológica de Tiempo (TSA) .....	8
1.4.2.	Autoridad de certificación (CA) emisora de certificados de TSU .....	8
1.4.3.	Autoridad de Registro (AR) .....	8
1.4.4.	Solicitante .....	8
1.4.5.	Suscriptor.....	8
1.4.6.	Parte usuaria que confía .....	9
1.4.7.	Ámbito de aplicación y usos.....	9
1.4.7.1.	Usos prohibidos y no autorizados .....	9
1.5.	Contacto.....	9
2.	CLAUSULAS GENERALES.....	9
2.1.	Obligaciones.....	9
2.1.1.	TSA y CA emisoras de certificados de TSU .....	9
2.1.2.	AR.....	10
2.1.3.	Solicitante del certificado de TSU .....	11
2.1.4.	Suscriptor.....	11
2.1.5.	Suscriptor del servicio de estampa cronológica de tiempo .....	12
2.1.6.	Tercero que confía o usuario .....	12
2.1.7.	Repositorio.....	12
2.2.	Responsabilidad .....	13
2.2.1.	Exoneración de responsabilidad .....	13
2.2.2.	Límite de responsabilidad en caso de pérdidas por transacciones.....	14
2.3.	Responsabilidad financiera .....	14
2.4.	Interpretación y ejecución .....	14
2.4.1.	Legislación.....	14
2.4.2.	Independencia .....	14
2.4.3.	Notificación.....	14

2.4.4.	Procedimiento de resolución de disputas.....	14
2.5.	Tarifas.....	14
2.5.1.	Tarifas de emisión de certificados y renovación .....	14
2.5.2.	Tarifas de acceso a los certificados .....	15
2.5.3.	Tarifas de acceso a la información relativa al estado de los certificados .....	15
2.5.4.	Tarifas por el acceso al contenido de estas Políticas de Certificación .....	15
3.	PUBLICACIÓN Y REPOSITARIOS.....	15
3.1.	Publicación de información de la TSA .....	15
3.1.1.	Distribución de la clave pública de las AC y de certificados de TSU .....	15
3.1.2.	Términos y condiciones .....	15
3.1.3.	Difusión de los certificados .....	16
3.1.4.	Frecuencia de publicación .....	16
3.2.	Controles de acceso .....	16
3.3.	Auditorías .....	17
3.3.1.	Frecuencia de las auditorías .....	17
3.3.2.	Identificación y cualificación del auditor.....	17
3.3.3.	Relación entre el auditor y la TSA .....	17
3.3.4.	Tópicos cubiertos por la auditoría .....	17
3.3.5.	Auditoría en las Autoridades de Registro.....	17
3.4.	Confidencialidad.....	17
3.4.1.	Tipo de información a mantener confidencial .....	17
3.4.2.	Tipo de información considerada no confidencial .....	18
3.4.3.	Divulgación de información de revocación/suspensión de certificados .....	18
3.4.4.	Envío a la Autoridad Competente.....	18
3.5.	Derechos de propiedad intelectual .....	18
4.	REQUERIMIENTOS OPERACIONALES.....	18
4.1.	Registro inicial .....	18
4.1.1.	Tipos de nombres .....	19
4.1.2.	Reglas utilizadas para interpretar varios formatos de nombres .....	19
4.1.3.	Unicidad de los nombres .....	19
4.1.4.	Procedimiento de resolución de disputas de nombres.....	19
4.1.5.	Reconocimiento, autenticación y función de las marcas registradas .....	19

4.1.6.	Métodos de prueba de la posesión de la clave privada .....	19
4.2.	Autenticación .....	19
4.2.1.	Autenticación de la identidad de una Entidad .....	19
4.2.2.	Autorización de la Entidad al Solicitante.....	19
	Identificación de la vinculación .....	20
4.3.	Emisión de certificados de TSU .....	20
4.4.	Renovación de la clave y del certificado.....	20
4.5.	Modificación de certificados .....	21
4.6.	Reemisión después de una revocación .....	21
4.7.	Aceptación de certificados de TSU .....	21
4.8.	Revocación de certificados.....	21
4.8.1.	Causas de revocación.....	21
4.8.2.	Quién puede solicitar la revocación.....	22
4.8.3.	Procedimiento de solicitud de revocación .....	22
4.9.	Validación del estado de un certificado .....	23
4.9.1.	Frecuencia de emisión de CRL .....	23
4.9.2.	Requisitos de comprobación de CRL.....	23
4.9.3.	Disponibilidad de comprobación on-line de la revocación .....	23
4.9.4.	Requisitos de la comprobación on-line de la revocación.....	23
5.	PROCEDIMIENTOS DE CONTROL DE SEGURIDAD .....	23
6.	PERFILES DE CERTIFICADO Y CRL.....	24
6.1.	Perfil de Certificado.....	24
6.1.1.	Número de versión .....	24
6.1.2.	Extensiones de los certificados .....	24
6.1.3.	Extensiones específicas.....	24
6.2.	Sello de tiempo .....	25
6.2.1.	Sincronización del reloj con UTC.....	25
6.3.	Identificadores de objeto (OID) de los algoritmos criptográficos.....	25
6.4.	Perfil de CRL .....	25
6.4.1.	Número de versión .....	25
6.4.2.	CRL y extensiones .....	25
6.5.	OCSP Profile .....	25

6.5.1.	Número de versión .....	25
6.5.2.	Extensiones OCSP .....	26
7.	ESPECIFICACIÓN DE LA ADMINISTRACIÓN.....	26
7.1.	Autoridad de las políticas .....	26
7.2.	Procedimientos de especificación de cambios.....	26
7.3.	Publicación y copia de la política.....	26
7.4.	Procedimientos de aprobación .....	26
7.5.	Modelo y condiciones contractuales.....	26
8.	ANEXO I – PROCESO DE ESTAMPA CRONOLÓGICA DE TIEMPO.....	27
8.1.	Recepción del sello.....	27
8.2.	Proceso de petición (TimeStamp Request) .....	28
8.3.	Proceso de sellado .....	28
8.4.	Proceso de verificación .....	28
9.	ANEXO II - DECLARACIÓN DE PRACTICAS DE LA TSA.....	30
9.1.	Declaración Informativa de la TSA-TSU .....	30
10.	ANEXO III - ACRONIMOS.....	31
11.	ANEXO IV – DEFINICIONES .....	32

## 1. INTRODUCCIÓN

### 1.1. Consideraciones

**Política de Certificación** es el conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad o en alguna aplicación, con requisitos de seguridad y utilización comunes, es decir, en general una Política de Certificación debe definir la aplicabilidad de tipos de certificado para determinadas aplicaciones que exigen los mismos requisitos de seguridad y formas de usos.

La **Declaración de Prácticas de Certificación** es definida como un conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados. En general contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, además sobre la relación de confianza entre el Suscriptor del Sello, la Parte Usuaría y la Autoridad de Certificación. Pueden ser documentos absolutamente comprensibles y robustos, que proporcionan una descripción exacta de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los certificados, etc.

Estos conceptos de Políticas de Certificación y Declaración de Prácticas de Certificación son distintos, pero aun así es muy importante su interrelación.

Una DPC detallada no forma una base aceptable para la interoperabilidad de Autoridades de Certificación. Las Políticas de Certificación sirven mejor como medio en el cual basar estándares y criterios de seguridad comunes.

En definitiva, una política define “qué” requerimientos de seguridad son necesarios para la emisión de los certificados. La DPC nos dice “cómo” se cumplen los requerimientos de seguridad impuestos por la política.

### 1.2. Estándares Generales

El presente documento especifica la Política de Certificación (PC) de los siguientes servicios:

- Servicio de emisión de certificado de TSU
- Servicio de emisión de sellos de tiempo

Esta PC está basada en las especificaciones de:

- **IETF RFC 3628** – Policy Requirements for Time-Stamping Authorities (TSAs).
- **ETSI EN 319 421** - "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

Esta Política de Certificación está en conformidad con las disposiciones legales que rigen el asunto de Firma Electrónica en la Unión Europea y en España, cumpliendo todos los requisitos técnicos y de seguridad exigidos para emisión de certificados y la emisión de sellos de tiempo.

Esta política define las reglas y responsabilidades que deben seguir aquellas Autoridades de Certificación que deseen emitir los tipos de certificados definidos en el presente documento, imponiendo además ciertas obligaciones que deben ser tenidas en cuenta por los Firmantes y Partes Usuarias que confían en virtud de su especial relación con este tipo de certificados.

De esta forma, cualquier AC que emita este tipo de certificados, deberá ajustarse a los niveles de seguridad que se detallan en esta política de certificación y deberán informar a sus Suscriptores de su

existencia.

Los certificados emitidos bajo esta política requerirán la autenticación de la identidad de los Suscriptores. Esta identificación y autenticación se realizará según los términos de esta PC.

Respecto a los sellos de tiempo emitidos bajo esta política pueden ser usados, en particular, para proteger firmas electrónicas de larga duración, código ejecutable y transacciones realizadas en servicios electrónicos ofrecidos telemáticamente.

El certificado de Sello de tiempo es necesario para garantizar la existencia de un documento, o transacción electrónica, en un tiempo concreto, a través de:

- La firma digital de la autoridad de estampa cronológica de tiempo
- Identificador electrónico único del documento (HASH o resumen)
- Fecha y hora recogida de una fuente fiable de tiempo

La CA suspenderá y revocará sus certificados según lo dispuesto en esta política. La CA deberá conservar los registros de auditoría e incidencias de acuerdo con lo que se establece en esta política.

Las funciones críticas del servicio deberán ser realizadas al menos por dos personas. Los certificados de los Suscriptores tienen un periodo de validez determinado por esta PC y en ningún caso podrán realizarse copias de respaldo, ni almacenarse por la TSA, salvo por lo expresamente permitido por las normas aplicables.

La información personal recabada del Suscriptor se recogerá con el debido consentimiento del interesado y únicamente para los fines propios del servicio de certificación, el cual podrá ejercer en todo caso sus oportunos derechos de información, rectificación y cancelación. La CA deberá respetar así mismo la normativa aplicable en materia de protección de datos.

Los usuarios de servicios asociados a estos certificados como parte confiante deberá consultar estas políticas y las prácticas de certificación asociadas para obtener detalles de cómo se implementa esta política de certificación. Disponibles en <https://camerfirma.com.co/m.co/practicas-certificacion/>

La actividad de la AC podrá ser sometida a la inspección de la Autoridad de las Políticas (PA) o por personal delegado por la misma.

En lo que se refiere al contenido de esta PC, se considera que el lector conoce los conceptos básicos de PKI, certificación y firma digital, recomendando que, en caso de desconocimiento de dichos conceptos, el lector se informe a este respecto.

### 1.3. Identificación

La presente PC está identificada con los siguientes OID:

Certificado/Sello de tiempo	OID Políticas
TSU-2 Camerfirma	1.3.6.1.4.1.17326.10.13.1.3
Sello de tiempo TSU-2	1.3.6.1.4.1.17326.10.13.1.3.1

## 1.4. Comunidad y Ámbito de Aplicación

El servicio puede ser utilizado para la emisión de sellos de tiempo por los suscriptores que poseen un acuerdo comercial con Camerfirma Colombia y por receptores del servicio de emisión de sellos de tiempo de forma libre para confirmar la existencia de un documento electrónico en una fecha y hora determinada. La política de la autoridad de sellos de tiempo está basada en criptografía de clave pública, fuentes seguras de tiempo y certificados digitales.

### 1.4.1. Autoridad de Estampa Cronológica de Tiempo (TSA)

Una TSA (Autoridad de Estampa Cronológica de tiempo) es una entidad de confianza en el que el usuario (suscriptores y terceras partes receptoras de sellos) confían para la emisión de sellos de tiempo. La TSA tiene la responsabilidad última sobre todos los servicios relacionados con la emisión de los sellos de tiempo. La TSA tiene la responsabilidad sobre las TSU (Unidades de estampa cronológica de tiempo) las cuales emiten los sellos de tiempo en representación de la TSA. En lo que respecta a estas políticas la TSA corresponde a la AC CAMERFIRMA SAS - 002 - 2019

La TSA puede subcontratar todos o algunos de sus componentes, aunque en todo momento será la última responsable del servicio.

El servicio de estampa cronológica de tiempo se compone de una o varias AC emisoras de certificados para las Unidades de Estampa Cronológica de Tiempo (TSU). La TSU tiene asociada una clave privada que utiliza para la firmar de los sellos de tiempo. Esta estructura permite una mayor flexibilidad a la hora de implantar distintos servicios de estampa cronológica de tiempo con requerimientos diferenciados.

### 1.4.2. Autoridad de certificación (CA) emisora de certificados de TSU

Es la entidad responsable de la emisión, y gestión de los certificados digitales de TSU. La CA vincula una determinada clave pública con una Entidad, a través de la emisión de un Certificado de TSU. En estas políticas la Autoridad de certificación es “CAMERFIRMA SAS - 002 - 2019”.

### 1.4.3. Autoridad de Registro (AR)

Ente que actúa conforme esta Política de Certificación y, en su caso, mediante acuerdo suscrito con la TSA, cuyas funciones son la gestión de las solicitudes, identificación y registro de los solicitantes del Certificado y aquellas que se dispongan en las Prácticas de Certificación concretas.

### 1.4.4. Solicitante

A los efectos de esta Política, se entenderá por Solicitante a la persona física en su nombre o autorizada por una organización, y que solicita el Certificado TSU. Solicitante se considera igualmente a la persona física en su nombre o autorizada por una organización que mediante un acuerdo con la TSA para la obtención de sellos de tiempo.

### 1.4.5. Suscriptor

Bajo esta Política, el Suscriptor es una Entidad (empresa u organización de cualquier tipo), a la que se encuentra asociado el Certificado Camerfirma Colombia de TSU (Suscriptor del certificado).

También se considera suscriptor al poseedor de un acceso al servicio de estampa cronológica de tiempo ofrecido por una TSU bajo el control de Camerfirma Colombia (Suscriptor del Servicio).

#### 1.4.6. Parte usuaria que confía

En esta Política se entiende por Parte usuaria que confía la persona que voluntariamente confía en el certificado emitido a favor del Suscriptor, lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado/estampa cronológica y en consecuencia se sujeta a lo dispuesto en esta Política, por lo que no se requerirá acuerdo posterior alguno.

La Parte usuaria que confía también puede denominarse como “Tercero que confía”.

#### 1.4.7. Ámbito de aplicación y usos

El certificado de TSU emitido bajo esta política solo será utilizado para la emisión de sellos de tiempo.

##### 1.4.7.1. Usos prohibidos y no autorizados

Bajo la presente Política no se permite el uso que sea contrario a la normativa colombiana y comunitaria, a los convenios internacionales ratificados por el estado español, a las costumbres, a la moral y al orden público. Tampoco se permite la utilización distinta de lo establecido en esta Política y en la Declaración de Prácticas de Certificación.

No están autorizadas las alteraciones en los Certificados, que deberán utilizarse tal y como son suministrados por la TSA.

#### 1.5. Contacto

La presente política de certificación está administrada y gestionada por el Departamento Jurídico de AC Camerfirma SA, pudiendo ser contactado por los siguientes medios:

E-mail:	<a href="mailto:contacto@colombia.camerfirma.com">contacto@colombia.camerfirma.com</a>
Página web:	<a href="https://camerfirma.com.co/m.co/contacto-comercial/">https://camerfirma.com.co/m.co/contacto-comercial/</a>

## 2. CLAUSULAS GENERALES

### 2.1. Obligaciones

Este apartado incluye todas las obligaciones, garantías y responsabilidades de la TSA frente a los usuarios y terceras partes que voluntariamente confían en los servicios de estampa cronológica de tiempo, así como las obligaciones asumidas por las partes.

#### 2.1.1. TSA y CA emisoras de certificados de TSU

Las TSA que actúan bajo esta Política de Certificación estarán obligadas a cumplir con lo dispuesto por la normativa vigente y además a:

- Respetar lo dispuesto en esta Política

- Proteger sus claves privadas de forma segura
- Emitir certificados conforme a esta Política y a los estándares de aplicación
- Emitir certificados según la información que obra en su poder
- Publicar los certificados emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente
- Revocar los certificados según lo dispuesto en esta Política y publicar las mencionadas revocaciones en la CRL
- Informar a los suscriptores de la revocación de sus certificados, en tiempo y forma de acuerdo con la legislación española vigente
- Publicar esta Política y las Prácticas correspondientes en su página web
- Informar sobre las modificaciones de esta Política y de su Declaración Prácticas de Certificación a los Suscriptores/Creadores del Sello
- Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida o destrucción o falsificación
- La disponibilidad del servicio de estampa cronológica de tiempo tal como se describen el documento de SLA de Camerfirma Colombia
- La precisión de la fecha y hora incorporada en los sellos de tiempo basadas en el sistema UTC con una desviación máxima de **100ms**
- Suministrar una fuente fiable de tiempo a las TSU delegadas y establecer los mecanismos técnicos necesarios para detectar cualquier variación de los datos de tiempo utilizados por las TSU, notificando a los usuarios cualquier desviación o pérdida de fiabilidad del sistema
- Que los sellos de tiempo emitidos estarán libres de datos falsos y errores
- Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente

### 2.1.2. AR

Las AR que actúen bajo esta Política de Certificación estarán obligadas a cumplir con lo dispuesto por la normativa vigente y además a:

- Respetar lo dispuesto en esta Política
- Proteger sus claves privadas
- Comprobar la identidad de los solicitantes de Certificados de TSU
- Verificar la exactitud y autenticidad de la información suministrada por el solicitante acerca del Suscriptor del Sello de Tiempo
- Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el Solicitante acerca del Suscriptor del Sello de Tiempo

- Respetar lo dispuesto en los contratos firmados con la TSA y con el Solicitante en representación del Suscriptor del Sello de Tiempo
- Informar a la TSA de las causas de revocación, siempre y cuando tomen conocimiento

### 2.1.3. Solicitante del certificado de TSU

El Solicitante de un certificado de Camerfirma Colombia estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

- Suministrar a la TSA la información necesaria para realizar una correcta identificación
- Custodiar su clave privada de manera diligente
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez
- En el caso de tratarse de un certificado cualificado deberá identificarse ante la AR

### 2.1.4. Suscriptor

El Suscriptor de un Certificado Camerfirma Colombia de TSU estará obligado a cumplir con lo dispuesto por la normativa aplicable en cada momento y, además, a:

- Suministrar a la TSA la información necesaria para realizar una correcta identificación
- Realizar el pago del certificado conforme a la forma y medios establecidos por la TSA
- Realizar los esfuerzos que razonablemente estén a su alcance para confirmar la exactitud y veracidad de la información suministrada
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez
- Respetar lo dispuesto en esta política de certificación
- Proteger sus claves privadas de forma segura
- Asegurarse de que su certificado de TSU no ha caducado ni este revocado antes de ofrecer el servicio de estampa cronológica de tiempo
- Emitir sello de tiempo conforme a esta Política y a los estándares de aplicación
- Ofrecer el servicio con los requisitos de disponibilidad y precisión
- Informar inmediatamente a la TSA acerca de cualquier situación que pueda afectar a la validez del Certificado, o a la seguridad de las claves
- Utilizar el Certificado conforme a la Ley y a los límites fijados por las PC y el propio Certificado
- Sincronizarse con las fuentes de tiempo marcadas por el Prestador
- Someterse a la auditoría de sus sistemas por parte de la TSA o un tercero autorizado

- Facilitar el acceso de la TSA a su servicio de estampa cronológica de tiempo a los aplicativos con el objeto de establecer los controles correspondientes respecto a la corrección de la marca de hora
- Facilitar el acceso la TSA para recopilar información de los sellos emitidos o bien enviar un informe periódico sobre el número de sellos emitidos
- Presentar un acta de creación de las claves en un entorno seguro, tal como indican las CPS, y PC, firmado por una organización competente. Esta acta será valorada por personal técnico de la TSA
- En caso de utilizar recursos técnicos propios para la emisión de los certificadosLa utilización de la fuente de tiempo suministrada por la TSA y utilizar mecanismos técnicos que permitan detectar cualquier variación sobre esta.

#### **2.1.5. Suscriptor del servicio de estampa cronológica de tiempo**

En el proceso de obtención de un sello de tiempo, los subscriptores deben verificarla firma electrónica del sello de tiempo y comprobar el estado de los certificados certificado de la TSA-TSU.

#### **2.1.6. Tercero que confía o usuario**

Las terceras partes que voluntariamente confíen en los Sistemas de Certificación de esta TSA, asumen la obligación de:

- Verificar el estado de activación en que se encuentra el Certificado de la TSA-TSU al que se vincula el Sello Digital de Tiempo emitido, mediante consulta a la CRL u otro medio que se disponga para la verificación de estado del certificado
- En el supuesto de que el certificado haya expirado o haya perdido su validez por revocación deberá comprobar que:
  - a) La fecha de revocación o de caducidad es posterior a la fecha en que se emitió el sello de tiempo.
  - b) La función criptográfica que se empleó para obtener el sello siguesiendo segura
  - c) Que la longitud de la Clave criptográfica y el algoritmo de firmaelectrónica siguen siendo de práctica habitual.
- Tener en cuenta cualquier limitación en el uso del sello de tiempo indicado en lapolítica y prácticas de certificación correspondiente.
- Tomar en consideración cualquier limite prescrito en otros acuerdos de servicio.

#### **2.1.7. Repositorio**

La información relativa a la publicación y revocación/suspensión de los certificados se mantendrá accesible al público en los términos establecidos en la normativa vigente.

La AC deberá mantener un sistema seguro de almacén y recuperación de certificados y un repositorio de certificados revocados, pudiendo delegar estas funciones en una tercera entidad.

## 2.2. Responsabilidad

La TSA dispondrá en todo momento de un seguro de responsabilidad civil en los términos que marque la legislación vigente.

La TSA actuará en la cobertura de sus responsabilidades por sí o a través de la entidad aseguradora, satisfaciendo los requerimientos de los solicitantes de los certificados de TSU, de los Suscriptores/Creador del Sello de Tiempo y de los terceros que confíen en los certificados de TSU y sellos de tiempo.

Las responsabilidades de la TSA incluyen las establecidas por la presente Política de Certificación, así como las que resulten de aplicación como consecuencia de la normativa española e internacional.

La TSA será responsable del daño causado ante el Suscriptor del sello tiempo o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

- La exactitud de toda la información contenida en sello de tiempo o en los certificados de TSU emitidos.
- La garantía de que, en el momento de la entrega del certificado, obra en poder del Suscriptor del Sello de Tiempo, la clave privada correspondiente a la clave pública dada o identificada en el certificado.
- La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
- La correspondencia entre el certificado solicitado y el certificado entregado.
- Cualquier responsabilidad que se establezca en cada momento por la legislación vigente.

### 2.2.1. Exoneración de responsabilidad

La TSA y las AR no serán responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.
- Por el uso de los certificados de TSU siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente Política de Certificación.
- Por el uso indebido o fraudulento de los certificados de TSU, sellos de tiempo o CRL emitidos por la TSA.
- Por el uso de la información contenida en el Certificado de TSU o en la CRL.
- Por el incumplimiento de las obligaciones establecidas para el Suscriptor del Sello de Tiempo o Parte Usaria en la normativa vigente, en la presente Política de Certificación, en las Prácticas Correspondientes o en los contratos establecidos por las partes.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación/suspensión.
- Por el contenido de los mensajes o documentos sellados en tiempo o cifrados digitalmente.
- Por la no recuperación de documentos cifrados con la clave pública del Suscriptor del Sello de tiempo.

- Fraude en la información presentada por el solicitante.

### 2.2.2. Límite de responsabilidad en caso de pérdidas por transacciones

Independientemente del importe de las transacciones, este tipo de certificados tienen un límite de responsabilidad igual a 0.

Esta garantía será de aplicación a efectos de lo dispuesto en la legislación vigente.

### 2.3. Responsabilidad financiera

La TSA no asume ningún tipo de responsabilidad financiera.

### 2.4. Interpretación y ejecución

#### 2.4.1. Legislación

La ejecución, interpretación, modificación o validez de las presentes Políticas se regirá por lo dispuesto en la legislación española y comunitaria vigentes en cada momento.

#### 2.4.2. Independencia

La invalidez de una de las cláusulas contenidas en esta Política de Certificación no afectará al resto del documento. En tal caso se tendrá la mencionada cláusula por no puesta.

#### 2.4.3. Notificación

Cualquier notificación referente a la presente Política de Certificación se realizará por correo electrónico o mediante correo certificado dirigido a cualquiera de las direcciones referidas en el apartado datos de contacto.

#### 2.4.4. Procedimiento de resolución de disputas

Toda controversia o conflicto que se derive del presente documento se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte.

### 2.5. Tarifas

#### 2.5.1. Tarifas de emisión de certificados y renovación

Los precios de los servicios de certificación o cualquiera de los otros servicios relacionados se definen en la Declaración de prácticas de certificación, publicado en la página web en la sección <https://camerfirma.com.co/practicas-certificacion/>

### 2.5.2. Tarifas de acceso a los certificados

El acceso a los certificados emitidos es gratuito, no obstante, la AC se reserva el derecho de imponer alguna tarifa para los casos de descarga masiva de CRL o cualquier otra circunstancia que a juicio de la AC deba ser gravada.

### 2.5.3. Tarifas de acceso a la información relativa al estado de los certificados

La TSA proveerá de un acceso a la información relativa al estado de los certificados o de los certificados revocados gratuito.

### 2.5.4. Tarifas por el acceso al contenido de estas Políticas de Certificación

El acceso al contenido de la presente Política de Certificación será gratuito.

## 3. PUBLICACIÓN Y REPOSITARIOS

### 3.1. Publicación de información de la TSA

La TSA estará obligada a publicar la información relativa a sus Políticas y Prácticade Certificación.

La presente Política de Certificación es pública y se encuentra disponible en el sitio de Internet <https://camerfirma.com.co/m.co/practicacertificacion/>

Las Prácticade Certificación de referencia serán así mismo públicas y se pondrán a disposición del público en la dirección de Internet <https://camerfirma.com.co/m.co/practicacertificacion/>

#### 3.1.1. Distribución de la clave pública de las AC y de certificados de TSU

LA TSA se asegura que en la distribución de las claves públicas se garantice su integridad y autenticidad. Esta distribución se realiza mediante un certificado digital emitido tanto para las AC emisoras de certificados de TSU como para los certificados de TSU.

Los certificados de AC emisoras de certificados de TSU y certificados de TSU se publican en la página web de Camerfirma Colombia.

AC Camerfirma Colombia no iniciará la emisión de sellos de tiempo antes de la publicación y distribución del certificado de la TSU bajo la cual los emite.

#### 3.1.2. Términos y condiciones

La TSA pondrá a disposición de los Suscriptores los términos y condiciones del servicio antes de proceder a la emisión del certificado o de entregar los datos de acceso a los servicios de estampa cronológica de tiempo. En concreto:

- La TSA pondrá a disposición de los Suscriptores/Creadores del Sello de Tiempo y Partes Usuarías los términos y condiciones relativos al uso de los certificados
- Las limitaciones de uso

- La información sobre cómo validar los certificados, incluyendo los requisitos para comprobar si un certificado ha sido revocado
- Los límites de responsabilidad
- El periodo de tiempo en que la información registrada será almacenada
- Los procedimientos para la resolución de disputas
- El ordenamiento jurídico aplicable
- Si la TSA ha sido acreditada conforme a la Política identificada en el certificado

La información referida en el apartado anterior estará disponible en el contrato suscrito con la TSA bien como emisora de un certificado de TSU o como suministradora directa del servicio de estampa cronológica de tiempo.

### 3.1.3. Difusión de los certificados

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los certificados son accesibles para los Suscriptores y las Partes Usuarías.

En concreto:

El certificado de la AC es público y se encontrará disponible en la página web de Camerfirma Colombia <https://camerfirma.com.co/>

La información de referencia estará disponible 24 horas al día, 7 días por semana. En caso de fallo del sistema u otros factores que no se encuentran bajo el control de la TSA, la TSA hará todos los esfuerzos para conseguir que este servicio informativo no esté inaccesible durante un período máximo de 24 horas.

### 3.1.4. Frecuencia de publicación

Las Políticas y Prácticas de Certificación se publicarán una vez hayan sido creadas o en el momento en que se apruebe una modificación de estas.

La AC publicará los certificados revocados/suspendidos en el momento en que reciba una petición autenticada y existan indicios de su necesidad.

La CRL que contiene la lista de los certificados revocados/suspendidos de Suscriptores/Creadores del Sello de tiempo se publicará con una frecuencia mínima diaria.

## 3.2. Controles de acceso

La AC podrá establecer sistemas de seguridad para controlar el acceso a la información contenida en el web, LDAP o CRL con el fin de evitar usos indebidos que afecten la protección de datos personales.

### 3.3. Auditorías

#### 3.3.1. Frecuencia de las auditorías

El servicio de TSA es evaluado en el alcance de la certificación ISO27001 que anualmente realiza AC Camerfirma. Adicionalmente en la evaluación de conformidad del reglamento europeo eIDAS sobre servicios cualificados de estampa cronológica de tiempo realizado anualmente:

ISO27001	AENOR	3 años con renovación de la certificación
EIDAS	CSQA	6 años con renovación de la acreditación

#### 3.3.2. Identificación y cualificación del auditor

El auditor debe poseer conocimientos y experiencia en sistemas de PKI y en seguridad de sistemas informáticos.

ISO27001	AENOR	<a href="http://www.aenor.es">www.aenor.es</a>
EIDAS	CSQA	<a href="http://www.csqa.it">www.csqa.it</a>

#### 3.3.3. Relación entre el auditor y la TSA

La auditoría deberá ser realizada por un auditor independiente y neutral. Lo anterior no impedirá la realización de auditorías internas periódicas.

#### 3.3.4. Tópicos cubiertos por la auditoría

La auditoría deberá verificar en todo caso:

- Que la TSA tiene un sistema que garantice la calidad del servicio prestado
- Que la TSA cumple con los requerimientos de esta Política de Certificación
- Que las Prácticas de Certificación de la TSA se ajustan a lo establecido en esta Política, con lo acordado por la Autoridad aprobadora de la Política y con lo establecido en la normativa vigente

#### 3.3.5. Auditoría en las Autoridades de Registro

Solo AC Camerfirma Colombia opera como AR de la TSA.

### 3.4. Confidencialidad

#### 3.4.1. Tipo de información a mantener confidencial

Se determinará por la TSA la información que deba ser considerada confidencial, debiendo cumplir en todo caso con la totalidad de la normativa vigente en materia de protección de datos.

La TSA pondrá todos los medios a su alcance para garantizar la confidencialidad frente a terceros, durante el proceso de generación, de las claves privadas de firmadigital que proporciona. Asimismo, una vez generadas y entregadas las claves privadas, la AC se abstendrá de almacenar, copiar o conservar cualquier tipo de información que sea suficiente para reconstruir dichas claves, salvo expresa disposición legal en sentido contrario.

### **3.4.2. Tipo de información considerada no confidencial**

Se considerará como información no confidencial:

- La contenida en la presente Política y en las Prácticas de Certificación.
- La información contenida en los certificados siempre que el Suscriptor del sello tiempo haya otorgado su consentimiento.
- Cualquier información cuya publicidad sea impuesta normativamente.
- Las que así se determinen por las Prácticas de Certificación siempre que no contravengan ni la normativa vigente ni lo dispuesto en esta Política de Certificación.

### **3.4.3. Divulgación de información de revocación/suspensión de certificados**

La forma de difundir la información relativa a la revocación/suspensión de un certificado de TSU se realizará mediante la publicación de las correspondientes CRLy mediante protocolo de acceso en línea OCSP.

### **3.4.4. Envío a la Autoridad Competente**

Se proporcionará la información solicitada por la autoridad competente en los casos y forma establecidos legalmente.

## **3.5. Derechos de propiedad intelectual**

La TSA es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta Política de Certificación. Se prohíbe, por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva de la TSA sin la autorización expresa por su parte. No obstante, no necesitará autorización de la TSA para la reproducción del Certificado cuando la misma sea necesaria para su utilización por parte del Usuario legítimo y con arreglo a la finalidad del Certificado, de acuerdo con los términos de esta Política de Certificación.

## **4. REQUERIMIENTOS OPERACIONALES**

### **4.1. Registro inicial**

El registro de solicitud para la emisión de un certificado de TSU se realiza mediante oferta comercial, indicando en dicha oferta las condiciones de uso del certificado.

El registro para el acceso directo a los servicios de estampa cronológica de tiempo se realiza mediante oferta comercial, indicando en dicha oferta las condiciones de uso del servicio.

#### 4.1.1. Tipos de nombres

Todos los Suscriptores requieren un nombre distintivo (DN o distinguished name) conforme al estándar X.500 incorporado en el certificado de TSU.

#### 4.1.2. Reglas utilizadas para interpretar varios formatos de nombres

Se atenderá en todo caso a lo marcado por el estándar X.500 de referencia en la ISO/IEC 9594.

#### 4.1.3. Unicidad de los nombres

La AC se asegurará de que no existan dos certificados activos emitidos con igual titular teniendo estos titulares diferentes identidades.

#### 4.1.4. Procedimiento de resolución de disputas de nombres

Se atenderá a lo dispuesto en el apartado 2.4.4 de este documento.

#### 4.1.5. Reconocimiento, autenticación y función de las marcas registradas

Se admitirá la identificación de marcas o acrónimos de entidades siempre que en el propio certificado aparezca, además, la razón social y el número de identificación fiscal de la Entidad u otro elemento de identificación inequívoco, como el número de identificación fiscal, titular del signo distintivo registrado o no.

La AC no asumirá ninguna responsabilidad respecto del uso de marcas u otros signos distintivos, registrados o no, en la emisión de los Certificados expedidos bajo la presente Política de Certificación.

#### 4.1.6. Métodos de prueba de la posesión de la clave privada

El Suscriptor dispone de un mecanismo de generación de claves en dispositivo homologado. La prueba de posesión de la clave privada en estos casos es la petición recibida por Camerfirma en formato **PKCS#10** conjuntamente con el acta de la creación de las claves.

### 4.2. Autenticación

#### 4.2.1. Autenticación de la identidad de una Entidad

En el caso de los certificados emitidos bajo la presente Política donde se incorporan los datos de una Entidad, se exigirá, en todo caso, la acreditación de la existencia de la Entidad por un medio conforme a Derecho.

#### 4.2.2. Autorización de la Entidad al Solicitante

Para solicitar los certificados emitidos bajo esta Política, el Solicitante deberá acreditar su identidad conforme dispone la legislación vigente y que está debidamente autorizado por el Suscriptor (la Entidad) para solicitar el certificado desello electrónico.

Para la comprobación de la identidad del Solicitante se exigirá su presencia física y la entrega de la copia

y del original (para su cotejo) de su documento de identidad en los casos en que sea legalmente necesario.

Para comprobar que el Solicitante está autorizado por el Suscriptor para solicitar el certificado de TSU, se exigirá la entrega de una autorización específica firmada por alguien con poder de representación suficiente de la Entidad creadora del sello de tiempo, acompañada con una copia del documento de identidad del autorizante.

**En Administraciones públicas:** No se exige la documentación acreditativa de la existencia de la administración pública, organismo o entidad de derecho público, dado que dicha identidad forma parte del ámbito corporativo de la Administración General del Estado o de otras AAPP del Estado.

### Identificación de la vinculación

Certificado de TSU	Autorización para solicitar el certificado de por alguien con poder de representación suficiente de la entidad firmante. Certificado o consulta al Registro Mercantil para comprobar la constitución, personalidad jurídica de la entidad y el nombramiento y vigencia del cargo del autorizante.
--------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 4.3. Emisión de certificados de TSU

La AC utiliza todos los medios a su alcance para asegurar que la emisión y renovación de certificados se realiza de una forma segura. En particular:

- Cuando la AC genere las claves del Suscriptor del Sello, que el procedimiento de emisión del certificado está ligado de manera segura a la generación del par de claves por la AC.
- Que la clave privada ha sido generada de manera segura por el Suscriptor.
- La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la unicidad de los DN asignados a los Firmantes.
- La confidencialidad y la integridad de los datos registrados serán especialmente protegidos cuando estos datos sean intercambiados con el Suscriptor.
- La AC deberá verificar que el registro de los datos es intercambiado con proveedores de servicios reconocidos, cuya identidad es autenticada.
- La AC deberá notificar al solicitante la emisión de su certificado.
- El par de claves generado usado para la emisión del certificado de TSU no se empleará para ningún otro uso en cualquier otro certificado.

### 4.4. Renovación de la clave y del certificado

La TSA informará al Suscriptor antes de renovar de los términos y condiciones que hayan cambiado respecto de la anterior emisión.

La TSA en ningún caso emitirá un nuevo certificado conteniendo la anterior clave pública.

Los certificados NO CUALIFICADOS de TSU tendrán una duración mínima de 6 años. Los certificados

CUALIFICADOS serán de 5 años como máximo. El certificado de forma ordinaria se renueva anualmente de forma que los sellos emitidos tengan una

duración mínima. Esta situación no permite que un certificado de TSU y la clave asociada lleguen a término sin haber otro certificado y nueva clave ya distribuida que lo sustituya.

#### 4.5. Modificación de certificados

Ante cualquier necesidad de modificación de certificados, la TSA realizará una revocación del certificado y una nueva emisión con los datos corregidos.

#### 4.6. Reemisión después de una revocación

La AC no realizará reemisiones.

#### 4.7. Aceptación de certificados de TSU

Aceptando el certificado, el Suscriptor del Sello de tiempo confirma y asume la exactitud del contenido de este, con las consiguientes obligaciones que de ello se deriven frente a la TSA o cualquier tercero que de buena fe confíe en el contenido del Certificado de TSU.

#### 4.8. Revocación de certificados

Se entenderá por revocación aquel cambio en el estado de un certificado motivado por la pérdida de validez de un certificado en función de alguna circunstancia distinta a la caducidad de este. Al hablar de revocación nos referiremos siempre a la pérdida de validez definitiva.

##### 4.8.1. Causas de revocación

Los Certificados deberán ser revocados cuando concurra alguna de las circunstancias siguientes:

- Solicitud voluntaria del Suscriptor del sello de tiempo
- Pérdida o inutilización por daños del soporte del certificado
- Fallecimiento del Suscriptor del sello de tiempo (si es persona física) o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos.
- Terminación o extinción de la entidad.
- Cese en su actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.
- Inexactitudes graves en los datos aportados por el Solicitante para la obtención del certificado, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el Certificado, no se adecuen a la realidad.
- Resolución de la TSA indicando que el certificado no se ha emitido siguiendo los términos y condiciones marcadas por las políticas de certificación correspondientes.
- Pérdida de los derechos de la TSA para emitir certificados bajo esta política.
- La TSA es consciente de que el Suscriptor del sello ha sido añadido a una lista de personas no autorizadas o insolventes, o está operando desde un lugar donde la política de la AC impida la

emisión de certificados.

- Que se detecte que las claves privadas del Suscriptor del Sello de tiempo o de la TSA han sido comprometidas, bien porque concurren las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, bien por cualesquiera otras circunstancias, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al Suscriptor del Sello.
- Por incumplimiento por parte de la TSA, del Solicitante o el Suscriptor del Sello de tiempo de las obligaciones establecidas en esta política.
- Por la resolución del contrato con el Suscriptor del Sello de tiempo.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto de que se ponga en duda la fiabilidad del Certificado.
- Por resolución judicial o administrativa que lo ordene.
- Por la concurrencia de cualquier otra causa especificada en la presente política.

#### 4.8.2. Quién puede solicitar la revocación

El representante de la Entidad EL suscriptor del Sello de tiempoLa TSA.

#### 4.8.3. Procedimiento de solicitud de revocación

La revocación de un certificado podrá solicitarse únicamente por el representante de la Entidad, por el Suscriptor del Sello de tiempo mediante solicitud a la TSA.

Todas las solicitudes deberán ser en todo caso autenticadas.

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los certificados son revocados basándose en peticiones de revocación autorizadas y validadas.

La información relativa al retraso máximo entre la recepción de una petición de revocación y su publicación estará disponible como máximo en un periodo de 3 horas.

El Suscriptor del Sello de tiempo cuyo certificado haya sido revocado deberá ser informado del cambio de estado de su certificado. Así mismo, el Suscriptor del Sello de tiempo deberá ser informado del levantamiento de la suspensión. La TSA utilizará todos los medios a su alcance para conseguir este objetivo, pudiendo intentar la mencionada comunicación por e-mail, teléfono, correo ordinario o cualquier otra forma adecuada al supuesto concreto.

Una vez que un certificado es revocado, este no podrá volver a su estado activo. La revocación de un certificado es una acción, por tanto, definitiva.

La CRL, en su caso, será firmada por una AC emisora de certificados de TSU o por una autoridad de confianza de la TSA.

El servicio de gestión de las revocaciones estará disponible las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control de la TSA, la TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

La información relativa al estado de la revocación estará disponible las 24 horas del día, los 7 días de la

semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control de la TSA, la TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información se encuentre disponible.

Se deberán realizar los esfuerzos que razonablemente estén a su alcance para confirmar la autenticidad y la confidencialidad de la información relativa al estado de los certificados.

La información relativa al estado de los certificados deberá estar disponible públicamente.

#### **4.9. Validación del estado de un certificado**

##### **4.9.1. Frecuencia de emisión de CRL**

La TSA proporcionará la información relativa a la revocación de los certificados a través de una CRL. La CRL se emite cada 24 horas desde la última emisión con una validez de 48 horas y cada vez que se produzca una revocación.

La TSA actualizará y publicará la CRL dentro de las 3 horas siguientes a la recepción de una solicitud de suspensión que haya sido previamente validada.

##### **4.9.2. Requisitos de comprobación de CRL**

Las Partes Usuarias podrán comprobar el estado de los certificados en los cuales va a confiar, debiendo comprobar en todo caso la última CRL emitida. No obstante, la TSA podrá imponer una tarifa por el acceso a la CRL.

##### **4.9.3. Disponibilidad de comprobación on-line de la revocación**

Se proporcionará un servicio on-line de comprobación de revocaciones OCSP, el cual estará disponible las 24 horas del día los 7 días de la semana. En caso de fallo del sistema, del servicio o de cualquier otro factor que no esté bajo el control de la TSA, la TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

##### **4.9.4. Requisitos de la comprobación on-line de la revocación**

La Parte Usuaria que desee comprobar la revocación de un certificado, podrá hacerlo de forma on-line a través del servicio [ocsp.camerfirma](https://ocsp.camerfirma.com) utilizando el certificado de OCSP emitido por la AC que emitió el certificado de TSA. Estos certificados están publicados en la página web de AC Camerfirma Colombia <https://camerfirma.com.co/m.co/>

## **5. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD**

El prestador de los servicios deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que toda la información relevante concerniente a los servicios descritos en este documento es gestionada y protegida de forma segura durante el periodo de tiempo que pueda ser necesario a efectos probatorios en los procedimientos legales utilizando los medios ajustados al estado del arte en seguridad de la información.

Al ser procedimientos comunes a otros servicios de emisión, se desarrollará en la DPC correspondiente,

los aspectos relativos a los procedimientos de Control de seguridad, cubriendo los siguientes aspectos:

- Archivo de registros
- Análisis de vulnerabilidades
- Gestión de contingencias
- Controles de Seguridad física
- Controles procedimentales
- Controles de seguridad de personal
- Controles de Seguridad Técnica de las claves.
- Controles de seguridad informática
- Controles de gestión de la seguridad
- Controles de seguridad de la red
- Controles de ingeniería de los módulos criptográficos

## 6. PERFILES DE CERTIFICADO Y CRL

### 6.1. Perfil de Certificado

Todos los certificados emitidos bajo esta política serán conformes a:

- Estándar X.509 versión 3
- RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and CRL profile”.

Y aquellos que son cualificados con:

- ETSI EN 319 412-3 v1.1.1 “Certificate Profiles-Part 3 Certificate profile forcertificates issued to legal persons”.

#### 6.1.1. Número de versión

Deberá indicarse en el campo versión que se trata de la v.3.

#### 6.1.2. Extensiones de los certificados

Los perfiles de certificados están redactados en documentos independientes. Dichos documentos deben estar a disposición de cualquier tercero que lo solicite.

#### 6.1.3. Extensiones específicas

El certificado, emitido bajo la presente Política, podrá incluir por petición delSuscriptor del sello de tiempo extensiones adicionales con información específica de su propiedad. Esta información estará bajo la exclusiva responsabilidad del suscriptor. Dichas extensiones no se marcarán como críticas y sean reconocibles como tales.

## 6.2. Sello de tiempo

El sello de tiempo tendrá seguirá las especificaciones de la RFC3161 *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*.

### 6.2.1. Sincronización del reloj con UTC

El servicio de sincronización de tiempos estará compuesto por tres fuentes distintas:

- **NTP** del ROA (Real Observatorio de la Armada) que establece el tiempo dereferencia en España vía RedIris.
- **GPS** sincronizado con 3 satélites. Precisión **30 ms**.
- Sincronización de tiempos vía **Radio DCF77** con la estación transmisora en Mainflingen (Frankfurt). La precisión 10 mseg.

El sistema calculará el tiempo en base a estas tres fuentes. El reloj del ordenador se controlará de acuerdo con los algoritmos de selección y sincronización de la RFC1305 (NTP v3).

Los sistemas de mantendrán en todo momento sincronizados con una desviaciónmáxima de 100ms

## 6.3. Identificadores de objeto (OID) de los algoritmos criptográficos

SHA-256 With RSA Encryption (1.2.840.113549.1.1.11)

## 6.4. Perfil de CRL

El perfil del certificado de CRL está redactado en un documento independiente. Dicho documento debe estar a disposición de cualquier tercero que lo solicite.

### 6.4.1. Número de versión

El formato de las CRL utilizadas es el especificado en la versión 2 (X509 v2).

### 6.4.2. CRL y extensiones

Se soporta y se utilizan CRL conformes al estándar X.509.

## 6.5. OCSP Profile

### 6.5.1. Número de versión

Los certificados de respondedor OCSP son emitidos por cada AC gestionada porAC Camerfirma según el estándar RFC 6960.

### 6.5.2. Extensiones OCSP

El perfil del certificado de OCSP está redactado en un documento independiente. Dicho documento debe estar a disposición de cualquier tercero que lo solicite.

## 7. ESPECIFICACIÓN DE LA ADMINISTRACIÓN

### 7.1. Autoridad de las políticas

El departamento jurídico constituye la autoridad de las políticas (PA) y es responsable de la administración de las políticas.

La PA pondrá a disposición estas políticas a los empleados afectados en el repositorio documental de la empresa.

### 7.2. Procedimientos de especificación de cambios

Cualquier elemento de esta política es susceptible de ser modificado.

Todos los cambios realizados sobre las políticas serán inmediatamente publicados en la web de Camerfirma Colombia <https://camerfirma.com.co/m.co/>

Camerfirma Colombia mantendrá un histórico con las versiones anteriores de las políticas.

Los terceros que confían afectados pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la publicación.

Cualquier acción tomada como resultado de unos comentarios queda a la discreción de la PA.

Si un cambio en la política afecta de manera relevante a un número significativo de terceros que confían de la política, la PA puede discrecionalmente asignar un nuevo OID a la política modificada.

### 7.3. Publicación y copia de la política

Una copia de esta política estará disponible en formato electrónico en la página web de AC Camerfirma SA <https://camerfirma.com.co/practicas-certificacion/>

### 7.4. Procedimientos de aprobación

Para la aprobación y autorización de una TSA se deberán respetar los procedimientos especificados por la PA.

Las partes de la DPC de una AC que contenga información relevante en relación con su seguridad, toda o parte de esa DPC no estarán disponible públicamente.

### 7.5. Modelo y condiciones contractuales

Las condiciones contractuales se exponen mediante los “Términos y condiciones generales del servicio de certificación digital”, dichas disposiciones se elaboran con base en la normatividad aplicable a las actividades de certificación digital y los lineamientos propios de las mismas, expuestas en el desarrollo del presente documento y la Declaración de Prácticas de Certificación expuesta en la web de Camerfirma. Los términos y condiciones se encuentran publicados en nuestra página web de <https://camerfirma.com.co/>

## 8. ANEXO I – PROCESO DE ESTAMPA CRONOLÓGICA DE TIEMPO

El procedimiento de estampa cronológica de tiempo implica:

- **Usuario peticionario:**

El proceso de petición, en el cual el solicitante debe realizar la preparación del objeto a sellar (RFC3161 y RFC5816 Timestamp Request).

- **Unidad de estampa cronológica de tiempo:**

- Revisión de la corrección de la petición

Este componente está diseñado para revisar que la petición es completa y correcta. Si el resultado es positivo, los datos se envían como entrada a la Generación de Sello de Tiempo.

- Generación del parámetro tiempo

Este componente usa una fuente de confianza para la distribución de parámetros de tiempo. Estos parámetros serán usados como entrada al proceso de Generación de estampa Cronológica de Tiempo.

- Generación de la Estampa Cronológica de Tiempo

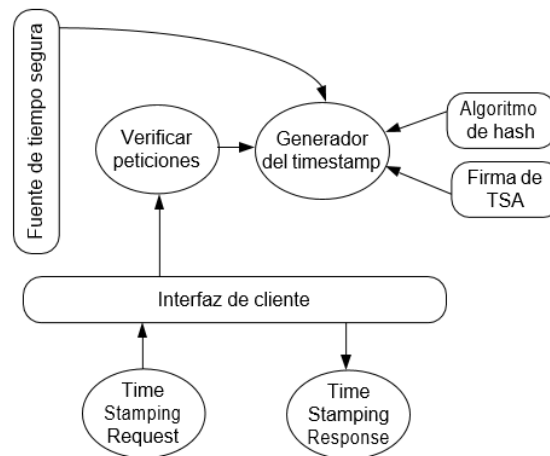
Esta función es la responsable de crear un sello de tiempo que asocie el instante de tiempo actual, un número de serie único, los datos proporcionados para el sellado de tiempo y garantizar los requerimientos de política a la que se adhiere.

- Estampa cronológica de tiempo -Time Stamp Token (TST)

Este componente calcula el indicador del sello de tiempo que se devolverá al cliente.

### 8.1. Recepción del sello

El proceso de verificación del sello, en el que se evalúa la autenticidad del sello de tiempo recibido.



## 8.2. Proceso de petición (TimeStamp Request)

El proceso comienza con la petición por parte de un tercero de un sello de tiempo a aplicar a un determinado documento.

Para ello el peticionario debe generar una petición *TimeStamp Request* según la RFC3161.

Los parámetros que el peticionario deberá enviar son:

- Hash del documento a sellar
- Nombre del algoritmo de hash a utilizar
- OID de política bajo la cual se proporcionará el sello

## 8.3. Proceso de sellado

En el proceso de sellado, el sistema realiza diferentes acciones, primero realiza una revisión de la petición, verificando la correcta estructuración del objeto “TimeStampRequest” y el origen de la misma. Durante esta verificación se comprueba que se han introducido los parámetros esperados como el algoritmo de hash y la política de sellado y que son correctos. Anteriormente se ha mencionado los posibles valores del algoritmo de hash soportados por el servicio, **SHA256, aunque se permiten por compatibilidad servicios con SHA1.**

Posteriormente se obtiene de la fuente segura y se genera el token de tiempo que es firmado electrónicamente con las claves privadas de sellado de Camerfirma Colombia.

En caso de que sea imposible la obtención de la exactitud requerida por parte de la fuente de tiempos por cualquiera de los caminos establecidos, el token de sello de tiempo no será emitido.

Finalmente se genera la respuesta TimeStamp Response, siguiendo las especificaciones de la RFC3161 y RFC5816.

El método de comunicación entre las entidades y el servicio de estampa cronológica de tiempo de Camerfirma Colombia se realizará:

- Mediante protocolo HTTP/HTTPS con autenticación en cliente, con el fin de poder validar las peticiones realizadas
- Mediante usuario y contraseña

## 8.4. Proceso de verificación

Los certificados de las AC emisoras de certificados de TSU y los certificados de TSU están disponibles en la página web de Camerfirma Colombia.

Verificar el estado de activación en que se encuentra el certificado de las AC emisoras de certificados de TSU al que se vincula el Sello Digital de Tiempo emitido, mediante consulta a la CRL u otro medio que se disponga para la verificación de estado del certificado.

Validar que la firma del sello de tiempo está realizada con la clave privada del certificado de TSU utilizando el certificado de clave pública del certificado de TSU una vez validado su origen y su validez temporal y su no revocación.

En el supuesto de que el certificado haya expirado o haya perdido su validez por revocación deberá comprobar que:

- La fecha de caducidad del certificado que emitió la estampa cronológica de tiempo es posterior a la fecha en que se emitió este.
- Comprobar que el certificado emisor de la estampa cronológica de tiempo no ha sido revocado por compromiso de la clave. En este caso todos los sellos de tiempo emitidos por este certificado dejarían de ser válidos y se deberían resellar todos los documentos afectados.
- La función criptográfica que se empleó para obtener el sello sigue siendo segura.
- Que la longitud de la clave criptográfica y el algoritmo de firma electrónica siguen siendo de práctica habitual.
- Tener en cuenta cualquier limitación en el uso del sello de tiempo indicado en la política y prácticas de certificación correspondiente.
- Tomar en consideración cualquier límite prescrito en la Declaración de Prácticas de Certificación de Camerfirma Colombia o en cualquier otro aspecto descrito en las condiciones de uso del servicio.

## 9. ANEXO II - DECLARACIÓN DE PRACTICAS DE LA TSA

- Camerfirma Colombia dispone de un análisis de riesgos realizado en el marco de su certificación ISO27001 en cuyo alcance se encuentran los servicios de TSA
- Este documento junto con la DPC de Camerfirma Colombia identifican las obligaciones de todos los agentes (internos y externos) implicados en el soporte al servicio de sellado de tiempos
- Camerfirma Colombia publica sus prácticas y políticas de certificación de forma libre y gratuita en su página web
- La TSA pone a disposición en su página web a todos los suscriptores y usuarios los términos y condiciones de uso de los servicios de sellado de tiempo y emisión de certificados de TSU
- La TSA dispone de un responsable de alto nivel con autoridad para aprobar la Declaración de Prácticas
- La autoridad responsable de la declaración de prácticas se asegura que estas están implantadas de forma correcta
- La TSA comunica mediante su página web los cambios que se realicen en esta política y en las prácticas de certificación

### 9.1. Declaración Informativa de la TSA-TSU

Esta información no reemplaza a la Política de Sellado de Tiempo ni a las Prácticas de estampa cronológica de tiempo, sino que proporciona información suplementaria y simplificada, destinada a los suscriptores del servicio.

Esta información se puede encontrar en <https://camerfirma.com.co/estampa-tiempo/>

## 10. ANEXO III - ACRONIMOS

AC	Autoridad de Certificación
AR	Autoridad de Registro
CPS	<i>Certification Practice Statement</i> . Declaración de Prácticas de Certificación
CRL	<i>Certificate Revocation List</i> . Lista de certificados revocados
CSR	<i>Certificate Signing Request</i> . Petición de firma de certificado
DCCF	Dispositivo cualificado de creación de firma
DES	<i>Data Encryption Standard</i> . Estándar de cifrado de datos
DN	<i>Distinguished Name</i> . Nombre distintivo dentro del certificado digital
DSA	<i>Digital Signature Algorithm</i> . Estándar de algoritmo de firma
DSCF	Dispositivo seguro de creación de firma
DSADCF	Dispositivo seguro de almacén de datos de creación de firma
FIPS	<i>Federal Information Processing Standard Publication</i>
IETF	<i>Internet Engineering Task Force</i>
ISO	<i>International Organization for Standardization</i> . Organismo Internacional de Estandarización
ITU	<i>International Telecommunications Union</i> . Unión Internacional de Telecomunicaciones
LDAP	<i>Lightweight Directory Access Protocol</i> . Protocolo de acceso adirectorios
OCSP	<i>On-line Certificate Status Protocol</i> . Protocolo de acceso alestado de los certificados
OID	<i>Object Identifier</i> . Identificador de objeto
PA	<i>Policy Authority</i> . Autoridad de Políticas
PC	Política de Certificación
PIN	<i>Personal Identification Number</i> . Número de identificación personal
PKI	<i>Public Key Infrastructure</i> . Infraestructura de clave pública
RSA	Rivest-Shamir-Adleman. Tipo de algoritmo de cifrado
SHA	<i>Secure Hash Algorithm</i> . Algoritmo seguro de Hash
SSL	<i>Secure Sockets Layer</i> . Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor
TCP/IP	<i>Transmission Control Protocol/Internet Protocol</i> . Sistema de protocolos, definidos en el marco de la IETF. El protocolo TCP se usa para dividir en origen la información en paquetes, para luego recomponerla en destino. El protocolo IP se encarga de direccionar adecuadamente la información hacia su destinatario.
TSA	<i>Time-Stamping Authority</i>
TSU	<i>Time-Stamping Unit</i>
TST	<i>Time-Stamp Token</i>
UTC	<i>Coordinated Universal Time</i>

11. ANEXO IV – DEFINICIONES

<b>Autoridad de Certificación (AC)</b>	Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Suscriptor y el Tercero que confía, vinculando una determinada clave pública con una persona
<b>Autoridad de Políticas (AP)</b>	Persona o conjunto de personas responsables de todas las decisiones relativas a la creación, administración, mantenimiento y supresión de las políticas de certificación y DPC
<b>Autoridad de Registro (AR)</b>	Entidad responsable de la gestión de las solicitudes e identificación y registro de los solicitantes de un certificado
<b>Certificación cruzada</b>	El establecimiento de una relación de confianza entre dos AC, mediante el intercambio de certificados entre las dos en virtud de niveles de seguridad semejantes
<b>Certificado</b>	Archivo que asocia la clave pública con algunos datos identificativos del suscriptor y es firmada por la AC
<b>Clave pública</b>	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos. También llamada datos de verificación de firma
<b>Clave privada</b>	Valor matemático conocido únicamente por el suscriptor y usado para la creación de una firma digital o el descifrado de datos. También llamada datos de creación de firma. La clave privada de la AC será usada para firma de certificados y firma de CRL
<b>CPS</b>	Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta (también referida como DPC o Declaración de Prácticas de Certificación)
<b>CRL</b>	Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la AC
<b>Datos de Activación</b>	Datos privados, como PIN o contraseñas empleados para la activación de la clave privada
<b>DCCF</b>	<i>Dispositivo cualificado de creación de firma.</i> dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II del Reglamento (UE) 910/2014
<b>DSADCF</b>	<i>Dispositivo seguro de almacén de los datos de creación de firma.</i> Elemento software o hardware empleado para custodiar la clave privada del suscriptor de forma que solo él tenga el control sobre la misma.

<b>DSCF</b>	<i>Dispositivo Seguro de creación de firma.</i> Elemento software o hardware empleado por el suscriptor para la generación de firmas electrónicas, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el suscriptor.
<b>Entidad</b>	Dentro del contexto de las políticas de certificación de Camerfirma, aquella empresa u organización de cualquier tipo a la cual pertenece o se encuentra estrechamente vinculado el suscriptor.
<b>Firma digital</b>	El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera: que los datos no han sido modificados (integridad) que la persona que firma los datos es quien dice ser (identificación) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)
<b>OID</b>	Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.
<b>Par de claves</b>	Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.
<b>PKI</b>	Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública.
<b>Política de certificación (PC)</b>	Conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y de utilización comunes.
<b>Suscriptor</b>	Dentro del contexto de las políticas de certificación de Camerfirma, persona cuya clave pública es certificada por la AC y dispone de una privada válida para generar firmas digitales.
<b>Tercero que confía</b>	Dentro del contexto de las políticas de certificación de Camerfirma, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado.