POLÍTICA DE CERTIFICACIÓN

Certificado Digital

AC CAMERFIRMA TSA

Versión 2.2.0

SELLO JURIDICO

Firmado digitalmente por SELLO JURIDICO
Fecha: 2022.08.23 13:14:06 +02'00'

Autor: Juan Ángel Martín (Consultor de Cumplimiento)

Revisión: Andrés Vázquez (Dirección de Departamento de Cumplimiento)

Aprobación (PA): Departamento Jurídico de Camerfirma

Este documento se puede obtener en la dirección https://policy.camerfirma.com

Información sobre el documento

Nombre:	Política de Certificación Camerfirma para Sello de Tiempo
Código	PC-SELLO-TSA
Versión:	2.2.0
Elaborado por:	TSA Camerfirma SA
Idioma:	Español
Descripción:	Define los criterios básicos a seguir por el prestador de servicios de certificación que ofrezca servicios de sellado de tiempo.
Estado del documento:	Activo
Referencia:	1.3.6.1.4.1.17326.10.13.1 TSA 1.3.6.1.4.1.17326.10.13.1.3 TSU-3 1.3.6.1.4.1.17326.10.13.1.2.1 Sello TSU-2 1.3.6.1.4.1.17326.10.13.1.3.1 Sello TSU-3
Localización:	https://policy.camerfirma.com

Control de versiones

VERSIÓN	MOTIVACIÓN DEL CAMBIO	PUBLICACIÓN
V1.1	Revisión para la emisión de certificados de TSU gestionadas por terceras partes.	Septiembre 2.009
V1.2	Revisión OIDs.	Noviembre 2.010
V1.2.1	Revisión general y corrección de referencias erróneas entre apartados. Actualización del contenido de todos los apartados.	Junio 2.015
V2.0	Revisión general.	Marzo 2.017
V2.0.1	Incorporación comentarios acreditación Perú.	Abril 2.017
V2.0.2	2.1.1 Incorporamos notificación por perdida de fiabilidad Título del 3.3 añadiendo especificación de TSU. 5.2.1 Declaración de máxima desviación de 100ms. 6.1 Incorporamos procedimiento de notificación de políticas. 7.4 incorporación de comprobación de la validez del certificado de TSU.	Abril 2017
V2.0.3	Incorporamos obligaciones de terceras partes 2.1.8 Limitación del uso del par de claves de TSU 3.3	Mayo 2017
v.2.0.4	No emisión de sellos antes de publicar el certificado de TSU 2.6.1.1 Detalle de renovación de certificado TSU 3.4	Junio 2018
v2.1.0	Refundición con PC Camerfirma Sellado Tiempo Perú	Junio 2022

v2.2.0	Corrección en el ‘Control de versiones’ de este documento. Se incorpora la fecha correcta de la versión anterior a esta y que se corresponde con la de la fecha de la firma de la Autoridad de Políticas. Incorporación de la Sección ‘3 Gestión de claves de la TSA’ 5.4. Renovación de la clave y el certificado, sustitución de ‘El certificado de forma ordinaria se renueva anualmente’ por ‘El certificado se renueva a más tardar 1 año antes de su caducidad’. 7.3. Identificadores de objeto (OID) de los algoritmos criptográficos, incorporación del algoritmo sha512WithRSAEncryption	Agosto 2022

Identificación de políticas

La forma de identificar distintos tipos de certificados digitales se realiza mediante identificadores de objeto (OIDs). Un OID concreto permite a las aplicaciones distinguir claramente el certificado que se presenta.

El identificador de política está compuesto por una serie de números separados entre sí por puntos que conforman un identificador único.

Ver 1.3 Identificación.

Índice de Contenido.

1. Introducción

AC Camerfirma S.A. (Camerfirma España) es una empresa que fue creada en el año 1999 con domicilio en España, donde se establece como prestador de servicios de certificación al amparo de la LEY 59/2003, de 19 de diciembre, de firma electrónica en España.

Camerfirma España, como entidad líder española en la emisión de certificados empresariales en el sector privado tiene mucho que ofrecer en cuanto a conocimiento de esta tecnología a nivel europeo e incluso mundial. Camerfirma España desde el comienzo de su trayectoria como sociedad anónima en el año 2000, mantiene una estrecha relación con los mercados de Sudamérica y cuenta en su labor con numerosos proyectos de consultoría y de implantación de PKI con las Cámaras de Comercio sudamericanas.

En el año 2014, Camerfirma logró acreditarse como Entidad de Certificación en Perú y en 2017 a través de su participada de Camerfirma Perú S.A.C. (Camerfirma Perú). En el año 2016, se acreditó como prestador de servicios de intermediación digital y servicios de emisión de Sellos de Tiempo (Timestamp), para brindar dichos servicios en Perú y dar cumplimiento a la regulación peruana establecida por la Autoridad Administrativa Competente (AAC), INDECOPI. En 2017, fue su participada Camerfirma Perú la entidad jurídica que consiguió obtener dicha acreditación de Servicio de Valor Añadido.

Como entidad de Sellado de Tiempo – TSA, Camerfirma Perú asume las responsabilidades de representación de los servicios de sello de tiempo brindados por Camerfirma España.

La infraestructura tecnológica y operativa de la TSA Camerfirma Perú es provista por Camerfirma España. Dicha infraestructura ha obtenido la certificación WebTrust for Certification Authorities, y es verificada anualmente por auditores autorizados.

1.1. Consideración Inicial

Por no haber una definición taxativa de los conceptos de Declaración de Prácticas de Certificación (DPC o CPS) y Políticas de Certificación (PC) y debido a algunas confusiones formadas, entendemos que es necesario aclarar dichos conceptos.

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 Usuaria 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. Vista General

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, en España y en Perú, 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 generales que debe seguir la Autoridad de Sellado de tiempo TSA para la emisión de sellos de tiempo. Este documento define los participantes del proceso sus responsabilidades y derechos, así como el margen de aplicabilidad. Información más detallada de estos procedimientos puede ser encontrada en las Prácticas de certificación de AC Camerfirma SA.

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 servicio de sellado de tiempo se compone de dos componentes diferenciados:

- Suministro de Sellos de Tiempo.

- Gestión del servicio de sellado de tiempo.

La división de estos componentes solamente se toma por motivos de clarificación de los requerimientos especificados en estas políticas.

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 sellado de tiempo.
- Identificador electrónico único del documento (HASH o resumen).
- Fecha y hora recogida de una fuente fiable de tiempo.

Tanto los usuarios del servicio como la Parte Usuaria deberán consultar estas políticas y las prácticas de certificación de la TSA para obtener detalles de cómo se implementa esta política de certificación.

En lo que se refiere al contenido de esta Política de Certificación, 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. En la página Web de Camerfirma (www.camerfirma.com) hay algunas informaciones útiles. Se ha utilizado el estándar RFC 3647 "*Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framewortk*" del Internet Engineering Task Force (IETF) como guía de asistencia en la redacción de este documento.

1.3. Identificación

La presente PC está identificada con los siguientes OID:

Certificado/Sello de tiempo	OID Políticas
TSU-3 Camerfirma	[Camerfirma] 1.3.6.1.4.1.17326.10.13.1.3
Sello de tiempo TSU-3	[Camerfirma] 1.3.6.1.4.1.17326.10.13.1.3.1
Sellos de tiempo bajo - eIDAS	
Certificado Cualificado de TSU en QSCD	[Camerfirma] 1.3.6.1.4.1.17326.10.16.5.1.1 [ETSI EN 319 411 2 - QCP-l-qscd] 0.4.0.194112.1.3
Sello de tiempo Cualificado de TSU en QSCD	[Camerfirma] 1.3.6.1.4.1.17326.10.16.5.1.1.1
Certificado de TSU	[Camerfirma] 1.3.6.1.4.1.17326.10.16.5.1.2
Sello de tiempo Certificado de TSU	[Camerfirma] 1.3.6.1.4.1.17326.10.16.5.1.2.1

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 AC Camerfirma 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 Sellado de Tiempo (TSA)

Una TSA (Autoridad de Sellado 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 sellado de tiempo) las cuales emiten los sellos de tiempo en representación de la TSA. En los que respecta a estas políticas la TSA corresponde a AC Camerfirma SA.

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

El servicio de sellado de tiempo se compone de una o varias AC emisoras de certificados para las Unidades de Sellado 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 sellado con requerimientos diferenciados.

Existe una autoridad de Sellado de tiempo TSA que emite certificados a TSU. Las TSU (Unidades de Sellado de Tiempo) pueden emitir sellos de tiempo en nombre de la TSA bajo condiciones distintas en lugares distintos y con recursos independientes. Estas a su vez podrán emitir sellos de tiempo.

Los sellos de tiempo se distinguirán por las TSU emisora y por el OID de política descrito en él.

1.4.2 Autoridad de certificación (AC) emisora de certificados de TSU

Es la entidad responsable de la emisión, y gestión de los certificados digitales de TSU. La AC 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 “AC Camerfirma SA”.

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 de TSU. (Suscriptor del certificado).

También se considera suscriptor al poseedor de un acceso al servicio de sellado de tiempo ofrecido por una TSU bajo el control de Camerfirma. (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/sellado 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.

1.4.8 Usos Prohibidos y no Autorizados

Bajo la presente Política no se permite el uso que sea contrario a la normativa española, peruana 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:	compliance@camerfirma.com
Localización:	https://www.camerfirma.com

2. Cláusulas 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 sellado de tiempo, así como las obligaciones asumidas por las partes.

2.1.1 TSA y AC 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 sellado de tiempo tal como se describen el documento de SLA de AC Camerfirma SA.
- 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 perdida 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 Camerfirma 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 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 sellado.
- 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 auditoria de sus sistemas por parte de la TSA o un tercero autorizado.
- Facilitar el acceso de la TSA a su servicio de sellado 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 certificados La 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 sellado de tiempo

En el proceso de obtención de un sello de tiempo, los subscriptores deben verificar la 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:
    - La fecha de revocación o de caducidad es posterior a la fecha en que se emitió el sello de tiempo.
    - 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 cuanta cualquier limitación en el uso del sello de tiempo indicado en la política 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 Sellos 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 Usuaria 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

La TSA no se responsabilizará por las pérdidas por transacciones.

2.3. Responsabilidad financiera

La TSA no asume ningún tipo de responsabilidad financiera.

Podrán establecerse garantías particulares a través de seguros específicos que se negociarán individualmente.

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 cualesquiera otros servicios relacionados estarán disponibles para las Partes Usuarias en la página web de Camerfirma www.camerfirma.com y / o en la de cada AR concreta.

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.

2.5.5 Política de reintegros

Sin estipular.

2.6. Políticas y Prácticas de Certificación

2.6.1 Declaración de Prácticas de la TSA

La TSA demostrara que cuanta con la fiabilidad necesaria para la provisión del servicio de sellado de tiempos

En particular:

- Dispondrá de un análisis de riesgos para evaluar los activos de empresa y las amenazas de tal forma que determine si son necesarios controles de seguridad u operativos para protegerlos.

- Dispondrá de una Declaración de Prácticas y procedimientos usados para dar respuesta a todos los requerimientos expuestos en estas políticas.

- Las Declaración de Practicas identificara las obligaciones de todos los agentes (internos y externos) implicados en el soporte al servicio de sellado de tiempos.

- La TSA pondrá a disposición de suscriptores y usuarios la Declaración de Prácticas y cualquier documentación relevante que garantice la conformidad con esta política. La TSA no tiene que publicar la documentación que considere de uso confidencial.

- La TSA distribuirá a todos los suscriptores y usuarios los términos y condiciones de uso.

- La TSA dispondrá de un responsable de alto nivel con autoridad para aprobar la Declaración de Practicas.

- La autoridad responsable de la declaración de prácticas se asegurará que estas están implantadas de forma correcta.

- La TSA comunicara los cambios que valla a realizar en la Declaración de Practicas, estas deberán ser aprobadas y puestas a disposición de suscriptores y usuarios.

2.6.2 Declaración Informativa de la TSA-TSU.

La TSA o la TSU de forma delegada informará a todos los suscriptores y potenciales usuarios, los términos y condiciones sobre el uso del servicio de sellado de tiempo.

Esta Declaración al menos especificará por cada política distinta utilizada por la TSA:

- Contacto de la TSA

- Política de sello de tiempo aplicada

- Al menos, un algoritmo resumen que se utilizara para representar a los datos a sellar en tiempo.

- Tiempo estimado de validez de la firma usada para firmar el token de tiempo. (Depende del algoritmo resumen usado el algoritmo de firma usado y la longitud de la clave).

- La exactitud de la fuente de tiempo empleada respecto a UTC.

- Cualquier limitación en el uso del servicio.

- Las obligaciones del suscriptor.

- Las obligaciones de los usuarios.

- Información de cómo verificar los sellos de tiempo de forma que un usuario puede considerar razonable confiar en un sello de tiempo y cualquier posible limitación en la validez de este.

- El periodo de tiempo de retención de los ficheros de auditoría.
- El marco jurídico aplicable, incluido cualquier declaración de cumplimiento de las regulaciones jurídicas nacionales.
- Limitaciones de responsabilidad.
- Proceso de resolución de disputas.
- Si la TSA ha sido auditada por un organismo independiente respecto a la conformidad con estas políticas de sellado de tiempo.
- Disponibilidad del servicio y expectativas de resolución ante incidentes que afecten a la provisión del servicio de sellado de tiempo.

2.7. Publicación y repositorios

2.7.1 Publicación de información de la TSA

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

La presente Política de Certificación es pública y se encuentra disponible en el sitio de Internet https://policy.camerfirma.com

Las Prácticas de Certificación de referencia serán así mismo públicas y se pondrán a disposición del público en la dirección de Internet https://policy.camerfirma.com

2.7.1.1 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.

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

2.7.1.2 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 sellado de tiempo. En concreto:

- La TSA pondrá a disposición de los Suscriptores/Creadores del Sello de Tiempo y Partes Usuarias 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 sellado de tiempo.

2.7.1.3 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 Usuarias.

En concreto:

- El certificado de la AC es público y se encontrara disponible en la página web de Camerfirma www.camerfirma.com.
- 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.

2.7.2 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 las mismas.

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.

2.7.3 Controles de acceso

El acceso a la información catalogada como pública será gratuito y estará a disposición de los suscriptores y usuarios.

2.8. Auditorias

2.8.1 Frecuencia de las auditorias

El servicio de TSA es evaluado en el alcance de la certificación ISO27001 que anualmente realiza AC Camerfirma SA. Adicionalmente en el alcance de las auditorias WEBTRUST anual y finalmente en la evaluación de conformidad del reglamento europeo eIDAS sobre servicios cualificados de sellado de tiempo realizado anualmente.

ISO27001 e ISO20000	AENOR	3 AÑOS CON REVISION ANUAL
EIDAS	CSQA	2 AÑOS CON REVISION ANUAL
WEBTRUST	AUREN	ANUAL

2.8.2 Identificación y cualificación del auditor

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

ISO27001 e ISO20000	AENOR	www.aenor.es
EIDAS	CSQA	www.csqa.it
WEBTRUST	AUREN	www.auren.com

2.8.3 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.

2.8.4 Tópicos cubiertos por la auditoria

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.

2.9. Confidencialidad

2.9.1 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 firma digital 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.

2.9.2 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.

2.9.3 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 CRL y mediante protocolo de acceso en línea OCSP.

2.9.4 Envío a la Autoridad Competente

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

2.10. 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.

3. Gestión de claves de la TSA

3.1. Generación de claves de la TSA

La TSA se asegurará que sus claves criptográficas son generadas bajo un estricto control.

En particular:

- Las claves de TSA se generan en un ambiente de seguridad, directamente controlado por personal confiable de AC Camerfirma.
- La generación de las claves de TSA se generan dentro de un módulo criptográfico que reúna los requisitos FIPS 140-1 nivel 3.
- La generación de las claves de TSU pueden ser realizadas entornos diferentes, tanto en dispositivos hardware como software, estando este hecho descrito dentro del certificado asociado a las claves. Cuando las claves se generen en un dispositivo hardware este deberá cumplir los requerimientos identificados en FIPS 140-1 [FIPS 140-1] level 3 o superior, o Cumpla los requerimientos identificados en CEN Workshop Agreement CWA14167-2, o Es un sistema confiable certificado EAL 4 o superior.
- Los Algoritmos criptográficos usados para la creación de la clave la firma y la longitud de la clave estarán reconocidos por un organismo de supervisión nacional o de acuerdo con las prácticas comunes en la gestión de sellos de tiempo.

3.1.1 Protección de la clave privada de la TSA-TSU

La TSA se asegurará que la clave privada de la TSU y de la TSA permanecen confidenciales y mantienen su integridad.

En particular:

- La clave privada de la TSA se mantendrá en un dispositivo criptográfico que cumpla los requerimientos identificados en FIPS 140-1 [FIPS 140-1] level 3 o superior, o Cumpla los requerimientos identificados en CEN Workshop Agreement CWA14167-2, o en un sistema confiable certificado EAL 4 o superior.
- La clave privada de la TSU se mantendrá en un dispositivo criptográfico que cumpla los requerimientos identificados en FIPS 140-1 [FIPS 140-1] level 3 o superior, o Cumpla los requerimientos identificados en CEN Workshop Agreement CWA14167-2, o en un sistema confiable certificado EAL 4 o superior.
- Bajo esta política se permitirá la opción de almacenar las claves de la TSU en un almacén software, aunque esta situación será reflejada en el contenido del certificado asignando uno de los OIDs que identifican esta política.
- No se recomienda la copia de las claves privadas para minimizar el riesgo de compromiso de clave. Si se realiza la copia, se utilizará tanto para la copia como la restauración de la clave un entorno seguro, así como al menos el concurso de dos personas cualificadas y confiables, encargadas expresamente en la declaración de prácticas para realizar estas operaciones.

- Cualquier copia de la clave privada, será debidamente protegida para garantizar su confidencialidad.

3.1.2 Distribución de la clave pública de la TSA-TSU

La TSA se asegurará que en la distribución de las claves públicas se garantice su integridad y autenticidad.

La clave pública de verificación se pondrá a disposición de las partes confiantes a través de un certificado de identidad.

3.1.3 Cambio de claves de TSA-TSU

El periodo de validez de las claves de TSU y TSA no será superior al periodo de tiempo que los algoritmos criptográficos elegidos sean adecuados para este uso.

Se requiere en esta política que los registros de actividad del servicio sean mantenidos al menos un año más de la duración del certificado asociado a la clave de la TSA-TSU.

Si la clave de la TSA-TSU está comprometida, habrá un número mayor de sellos de tiempo afectados cuanta más duración tenga el certificado asociado.

El compromiso de la clave de la TSA-TSU no solo depende de las características del módulo criptográfico sino de los procedimientos usados en la inicialización y exportación (cuando esta esté implementada).

3.1.4 Fin del ciclo de vida de la clave de TSA-TSU

La TSA garantizará que la clave privada de la TSA-TSU no será usada después del final de su ciclo de vida.

En particular:

- Que se utilizaran procedimientos técnicos y operacionales para generar nuevas claves cuando la actual caduca.

- La clave privada de la TSA-TSU o cualquier parte de ella, es destruida completamente de tal forma que no pueda ser recuperada.

- El sistema no permitirá la emisión de un sello de tiempo firmado con una clave privada de TSU caducada, ni que se firme un certificado de TSU con una clave privada de TSA caducada.

3.1.5 Gestión del ciclo de vida del dispositivo criptográfico usado para firmar sello de tiempo

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la seguridad del hardware criptográfico a lo largo de su ciclo de vida. En particular, que:

- El hardware criptográfico usado para la firma de sellos de tiempo no se manipula durante su transporte.
- El hardware criptográfico usado para la firma de sellos de tiempo no se manipula mientras está almacenado.
- El uso del hardware criptográfico usado para la firma de sellos de tiempo requiere el uso de al menos dos empleados de confianza.
- El hardware criptográfico usado para la firma de sellos de tiempo está funcionando correctamente.
- La clave privada de firma de la TSU almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

Antes de que el uso de la clave privada de la TSA caduque se deberá realizar un cambio de claves. La vieja TSA y su clave privada se desactivarán y se generará una nueva TSA con una clave privada nueva y un nuevo DN.

Los siguientes certificados serán puestos a disposición pública en el directorio:

- Clave pública de la nueva TSA firmada por la clave privada de la vieja TSA.
- Clave pública de la vieja TSA firmada con la clave privada de la nueva TSA.

3.2. Recuperación en caso de compromiso de la clave o desastre

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar en caso de desastre o compromiso de la clave privada de la TSA que éstas serán restablecidas tan pronto como sea posible. En particular:

3.2.1 La clave de la TSA se compromete

El plan de la continuidad de negocio de la TSA (o el plan de contingencia) tratará el compromiso o el compromiso sospechado de la clave privada de la TSA como un desastre.

En caso de compromiso, la TSA tomará como mínimo las siguientes medidas:

- Informar a todos los suscriptores, usuarios y otras TSA s con los cuales tenga acuerdos u otro tipo de relación del compromiso.

- Indicar que los certificados e información relativa al estado de la revocación firmados usando esta clave pueden no ser válidos.

3.2.2 Instalación de seguridad después de un desastre natural u otro tipo de desastre

La TSA debe tener un plan apropiado de contingencias para la recuperación en caso de desastres.

La TSA debe reestablecer los servicios de acuerdo con esta política dentro de las 48 horas posteriores a un desastre o emergencia imprevista. Tal plan incluirá una prueba completa y periódica de la preparación para tal restablecimiento.

3.3. Cese de la TSA

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que se minimizan los posibles perjuicios que se puedan crear a los suscriptores o usuarios como consecuencia del cese de su actividad y en particular del mantenimiento de los registros necesarios a efectos probatorios en los procedimientos legales. En particular:

a) Antes del cese de su actividad deberá realizar, como mínimo, las siguientes actuaciones:

- Informar a todos los suscriptores, usuarios y otras TSA s con los cuales tenga acuerdos u otro tipo de relación del cese.

- La TSA revocará toda autorización a entidades subcontratadas para actuar en nombre de la TSA en el procedimiento de emisión de certificados.

- La TSA realizará las acciones necesarias para transferir sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios que confían.

- Las claves privadas de la TSA serán destruidas o deshabilitadas para su uso.

b) La TSA tendrá contratado un seguro que cubra hasta el límite contratado los costes necesarios para satisfacer estos requisitos mínimos en caso de quiebra o por cualquier otro motivo por el que no pueda hacer frente a estos costes por sí mismo.

c) Se establecerán en la DPC las previsiones hechas para el caso de cese de actividad. Estas incluirán:

- Informar a las entidades afectadas.

- Transferencia de las obligaciones de la TSA a otras partes.

- Cómo debe ser tratada la revocación de certificados emitidos cuyo periodo de validez aún no ha expirado.

En particular, la TSA deberá:

- Informar puntualmente a todos los suscriptores, empleados y usuarios con una anticipación mínima de 6 meses antes del cese.

- Transferir todas las bases de datos importantes, archivos, registros y documentos a la entidad designada durante las 24 horas siguientes a su terminación.

4. Controles de Seguridad Física, Procedimental y de Personal

4.1. Controles de Seguridad física

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el acceso físico a los servicios críticos y que los riesgos físicos de estos elementos sean minimizados. En particular:

TSA General

- El acceso físico a las instalaciones vinculadas a la generación de certificados y servicios de gestión de revocaciones deberá ser limitado a las personas autorizadas y las instalaciones en las que se firman los certificados deberán ser protegidas de las amenazas físicas.

- Se establecerán controles para impedir la perdida, daño o compromiso de los activos de la empresa y la interrupción de la actividad

- Se establecerán controles para evitar el compromiso o robo de información

Emisión de certificados sellos de tiempo y gestión de revocaciones.

- Las actividades relativas a la emisión de certificados, sellos de tiempo y gestión de revocaciones serán realizadas en un espacio protegido físicamente de accesos no autorizados al sistema o a los datos.

- La protección física se conseguirá por medio de la creación de unos anillos de seguridad claramente definidos (p.ej. barreras físicas) alrededor de la emisión de certificados y gestión de revocaciones. Aquellas partes de esta tarea compartidas con otras organizaciones quedarán fuera de este perímetro.

- Los controles de seguridad física y medioambiental serán implementados para proteger las instalaciones que albergan los recursos del sistema, los recursos del sistema en sí mismos y las instalaciones usadas para soportar sus operaciones. Los programas de seguridad física y medioambiental de la TSA relativos a la generación de certificados y servicios de gestión de revocaciones estarán provistos de controles de acceso físico, protección ante desastres naturales, sistemas antincendios, fallos eléctricos y de telecomunicaciones, humedad y protección antirrobo.

Se implementarán controles para evitar que los equipos, la información, soportes y software relativos a los servicios de la TSA sean sacados de las instalaciones sin autorización.

4.1.1 Ubicación y construcción

Las instalaciones de la TSA deben estar ubicadas en una zona de bajo riesgo de desastres y que permita un rápido acceso a las mismas conforme al plan de contingencias.

Así mismo, las instalaciones estarán equipadas con los elementos y materiales adecuados para poder albergar información de alto valor.

4.1.2 Acceso físico

El acceso físico a las zonas de seguridad estará limitado al personal autorizado previa autenticación.

4.1.3 Alimentación eléctrica y aire acondicionado

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la alimentación eléctrica y el aire acondicionado son suficientes para soportar las actividades del sistema de la TSA

4.1.4 Exposición al agua

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de TSA está protegido de la exposición al agua.

4.1.5 Protección y prevención de incendios

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de TSA está protegido con un sistema antincendios.

4.1.6 Sistema de almacenamiento.

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de almacenamiento usado por el sistema de TSA está protegido de riesgos medioambientales como la temperatura, el fuego, la humedad y la magnetización.

4.1.7 Eliminación de residuos

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los medios usados para almacenar o transmitir la información de carácter sensible como las claves, datos de activación o archivos de la TSA serán destruidos, así como que la información que contengan será irrecuperable.

4.1.8 Backup remoto

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las instalaciones usadas para realizar back-up externo, que tendrán el mismo nivel de seguridad que las instalaciones principales.

4.2. Controles procedimentales

4.2.1 Roles de confianza

Los roles de confianza, en los cuales se sustenta la seguridad de la TSA, serán claramente identificados.

Los roles de confianza incluyen las siguientes responsabilidades:

- **Responsable de seguridad:** asume la responsabilidad por la implementación de las políticas de seguridad, así como gestión y revisión de logs.
- **Administradores de sistema:** Están autorizados para instalar, configurar y mantener de los sistemas y aplicaciones de confianza de la TSA que soportan las operaciones de Certificación.
- **Operador de sistema:** Está autorizado para realizar funciones relacionadas con el sistema de backup y de recuperación.
- **Administrador de CA:** Responsable de la Administración y control de gestión de los sistemas de confianza de la TSA.
- **Operador de CA:** Realizan funciones de apoyo en el control dual de las operaciones de la CA.
- **Auditor de CA:** Realiza las labores de supervisión y control de la implementación de las políticas de seguridad.

La TSA debe asegurarse que existe una separación de tareas para las funciones críticas de la CA, para prevenir que una persona use el sistema el sistema de TSA y la clave de la TSA sin detección.

La separación de los roles de confianza será detallada en la DPC.

4.2.2 Número de personas requeridas por tarea

Las siguientes tareas requerirán al menos un control dual:

- La generación de la clave de la TSA/TSU.
- La recuperación y back-up de la clave privada de la TSA/TSU.
- Activación de la clave privada de la TSA.

- Cualquier actividad realizada sobre los recursos HW y SW que dan soporte a la autoridad de certificación.

4.2.3 Identificación y autentificación para cada rol

La TSA establecerá los procedimientos de identificación y autenticación de las personas implicadas en roles de confianza.

4.3. Controles de seguridad de personal

4.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el personal cumple con los requisitos mínimos razonables para el desempeño de sus funciones. En concreto:

TSA General

- La TSA empleará personal que posea el conocimiento, experiencia y calificaciones necesarias y apropiadas para el puesto.
- Los roles de seguridad y responsabilidades especificadas en la política de seguridad de la TSA, serán documentadas en la descripción del trabajo.
- Se deberá describir el trabajo del personal de la TSA (temporal y fijo) desde el punto de vista de realizar una separación de tareas, definiendo los privilegios con los que cuentan, los niveles de acceso y una diferenciación entre las funciones generales y las funciones específicas de la TSA.
- El personal llevará a cabo los procedimientos administrativos y de gestión de acuerdo con los procedimientos especificados para la gestión de la seguridad de la información.

Registro, generación de certificados y gestión de revocaciones

- Deberá ser empleado el personal de gestión con responsabilidades en la seguridad que posea experiencia en tecnologías de firma electrónica y esté familiarizado con procedimientos de seguridad.
- Todo el personal implicado en roles de confianza deberá estar libre de intereses que pudieran perjudicar su imparcialidad en las operaciones de la TSA
- El personal de la TSA será formalmente designado para desempeñar roles de confianza por el responsable de seguridad

- La TSA no asignará funciones de gestión a una persona cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de estas funciones.

4.3.2 Procedimientos de comprobación de antecedentes

La TSA no podrá asignar funciones que impliquen el manejo de elementos críticos del sistema a aquellas personas que no posean la experiencia necesaria en la propia TSA que propicie la confianza suficiente en el empleado. Se entenderá como experiencia necesaria el haber pertenecido al Departamento en cuestión durante al menos 6 meses.

4.3.3 Requerimientos de formación

La TSA debe realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el personal que realiza tareas de operaciones de TSA o AR, recibirá una formación relativa a:

- Los principales mecanismos de seguridad de TSA y/o AR.
- Todo el software de PKI y sus versiones empleados en el sistema de la TSA.
- Todas las tareas de PKI que se espera que realicen.
- Los procedimientos de resolución de contingencias y continuidad de negocio.

4.3.4 Requerimientos y frecuencia de la actualización de la formación

La formación debe darse con una frecuencia anual para asegurar que el personal está desarrollando sus funciones correctamente.

4.3.5 Frecuencia y secuencia de rotación de tareas

No estipulado.

4.3.6 Sanciones por acciones no autorizadas

La TSA deberá fijar las posibles sanciones por la realización de acciones no autorizadas.

4.3.7 Requerimientos de contratación de personal

Ver apartado 4.3.1.

4.3.8 Documentación proporcionada al personal

Todo el personal de la TSA deberá recibir los manuales de usuario en los que se detallen al menos los procedimientos para el registro de certificados, creación, actualización, renovación, revocación y la funcionalidad del software empleado.

5. Requerimientos Operacionales

5.1. 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 servicio de sellado de tiempo se realiza mediante oferta comercial, indicando en dicha oferta las condiciones de uso del servicio.

5.1.1 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.

5.1.2 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.

5.1.3 Unicidad de los nombres

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

5.1.4 Procedimiento de resolución de disputas de nombres

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

5.1.5 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.

5.1.6 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.

5.2. Autenticación.

5.2.1 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.

5.2.2 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 de sello 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.

5.2.3 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.

-

5.3. 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.

5.4. 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 se renueva a más tardar 1 año antes de su caducidad, 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.

5.5. 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.

5.6. Reemisión después de una revocación

La AC no realizará reemisiones.

5.7. Aceptación de certificados de TSU

Aceptando el certificado, el Suscriptor del Sello de tiempo confirma y asume la exactitud del contenido del mismo, 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.

5.8. 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 del mismo. Al hablar de revocación nos referiremos siempre a la pérdida de validez definitiva.

5.8.1 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 concurran 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.

5.8.2 Quién puede solicitar la revocación

La revocación puede ser solicitada por:

- El representante de la Entidad.
- El Suscriptor del Sello de tiempo.
- La TSA.

5.8.3 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.

5.9. Validación del estado de un certificado

5.9.1 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 revocación que haya sido previamente validada.

5.9.2 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.

5.9.3 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.

5.9.4 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.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 http://www.camerfirma.com.

6. 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

6.1. Estándares para los módulos criptográficos

Todas las operaciones criptográficas deben ser desarrolladas en un módulo validado por al menos FIPS-140-1 nivel 3 o por un nivel de funcionalidad y seguridad equivalente.

6.1.1 Control multipersona (n de entre m) de la clave privada

Se requerirá un control multipersona para la activación de la clave privada de la TSA. Este control deberá ser definido adecuadamente por la DPC en la medida en que no se trate de información confidencial o pueda comprometer de algún modo la seguridad del sistema.

6.1.2 Depósito de la clave privada (key escrow)

La clave privada de la TSA debe ser almacenada en un medio seguro protegido criptográficamente y al menos bajo un control dual.

La clave del suscriptor (TSA) deberá estar almacenada en un formato seguro y particionada de tal forma que ni pueda ser manipulada de forma individual.

6.1.3 Copia de seguridad de la clave privada

La TSA deberá realizar una copia de back up de su propia clave privada que haga posible su recuperación en caso de desastre o de pérdida o deterioro de la misma de acuerdo con el apartado anterior.

Las copias de las claves privadas del suscriptor (TSA) se regirán por lo dispuesto en el punto anterior.

6.1.4 Archivo de la clave privada

La clave privada de la TSA no podrá ser archivada de acuerdo una vez finalizado su ciclo de vida.

Las claves privadas de la TSU no podrán ser archivadas una vez finalizado su ciclo de vida.

6.1.5 Introducción de la clave privada en el módulo criptográfico

Las claves que se generaran dentro del módulo criptográfico. Solo saldrán cifradas del dispositivo. Tanto para extraerlas como introducirlas en el dispositivo se utilizará al menos la colaboración de dos personas.

6.1.6 Método de activación de la clave privada

La clave privada de la TSA deberá ser activada conforme al apartado 3.1.1., dentro del cual se sobreentiende que se realiza la activación de la clave privada luego de su generación.

6.1.7 Método de desactivación de la clave privada

No estipulado.

6.1.8 Método de destrucción de la clave privada

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la clave privada de la TSA no será usada una vez finalizado su ciclo de vida.

Todas las copias de la clave privada de firma de la TSA deberán ser destruidas o deshabilitadas de forma que la clave privada no pueda ser recuperada.

6.2. Otros aspectos de la gestión del par de claves

6.2.1 Archivo de la clave pública

La TSA deberá conservar todas las claves públicas de verificación.

6.2.2 Periodo de uso para las claves públicas y privadas

El periodo de uso de la clave privada de la TSA será de 30 años.

El periodo de uso de la clave privada de la TSU será de 5 años.

6.3. Controles de seguridad informática

La TSA empleará sistemas fiables y productos que estén protegidos contra modificaciones.

En particular se aplicarán como referencia los controles de seguridad descritos en ISO17799 para la gestión de sistemas de información, así como los requerimientos para sistemas confiables para la gestión de certificados de firma electrónica descritos en CWA14167-1.

7. Perfiles de Certificado y CRL

7.1. 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 for certificates issued to legal persons*".

7.1.1 Número de versión

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

7.1.2 Extensiones del certificado raíz de la jerarquía

Extensión del certificado:

Versión: 3

Número de serie: a3:da:42:7e:a4:b1:ae:da

Signature Algorithm: sha1WithRSAEncryption

Subject:

C = EU,

L = Madrid (see current address at www.camerfirma.com/address),

serialNumber = A82743287,

O = AC Camerfirma S.A.,

CN = Chambers of Commerce Root – 2008

Validity:

Not Before: Aug 1 12:29:50 2008 GMT

Not After : Jul 31 12:29:50 2038 GMT

RSA Public-Key: (4096 bit)

X509v3 Subject Key Identifier:

F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02:9E:17:19

X509v3 Key Usage: critical

Certificate Sign, CRL Sign

X509v3 Certificate Policies:

Policy: X509v3 Any Policy

CPS: http://policy.camerfirma.com

7.1.3 Extensiones del certificado CA de la jerarquía

Extensión del certificado:

Versión: 3

Número de serie: 25:a4:54:bc:34:55:12:38

Signature Algorithm: sha256WithRSAEncryption

Subject:

C = ES,

OU = AC CAMERFIRMA,

O = AC Camerfirma S.A.,

serialNumber = A82743287,

L = Madrid (see current address at https://www.camerfirma.com/address),

CN = Camerfirma TSA II - 2014

Validity:

Not Before: Dec 16 16:45:33 2014 GMT

Not After : Dec 15 16:45:33 2037 GMT

RSA Public-Key: (4096 bit)

X509v3 Subject Key Identifier:

17:C5:40:BC:2A:F8:45:B8:AB:33:BF:F8:6F:49:6C:F6:17:CA:B7:D4

X509v3 Key Usage: critical

Certificate Sign, CRL Sign

X509v3 Extended Key Usage:

Time Stamping

X509v3 Certificate Policies:

Policy: X509v3 Any Policy

CPS: http://policy.camerfirma.com

X509v3 CRL Distribution Points:

http://crl.camerfirma.com/chambersroot-2008.crl

http://crl1.camerfirma.com/chambersroot-2008.crl

7.1.4 Extensiones del certificado TSU CAMERFIRMA PERU SAC

Extensión del certificado:

Versión: 3

Número de serie: da:38:f6:d0:40:5e:d4:17

Signature Algorithm: sha256WithRSAEncryption

Subject:

serialNumber = 20566302447

O = CAMERFIRMA PERU SAC

CN = TSU CAMERFIRMA PERU SAC

C = PE

Validity:

Not Before: Oct 4 11:14:54 2017 GMT

Not After : Oct 3 11:14:54 2023 GMT

RSA Public-Key: (2048 bit)

X509v3 Subject Key Identifier:

29:56:91:09:4F:E5:56:21:C6:01:24:76:7F:9D:0F:DB:7A:C3:77:9A

X509v3 Key Usage: critical

Digital Signature, Non Repudiation

X509v3 Extended Key Usage:

Time Stamping

X509v3 Certificate Policies:

Policy: X509v3 1.3.6.1.4.1.17326.10.13.1.3

CPS: http://policy.camerfirma.com

X509v3 CRL Distribution Points:

http://crl.camerfirma.com/camerfirma_tsaii-2014.crl

http://crl1.camerfirma.com/camerfirma_tsaii-2014.crl

7.1.5 Extensiones del resto de certificados de TSU

Las fichas con el detalle de dichos certificados se pueden solicitar en https://www.camerfirma.com/contacto-soporte/ o al teléfono +34 91 344 37 43.

7.1.6 Extensiones específicas

El certificado, emitido bajo la presente Política, podrá incluir por petición del Suscriptor 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.

7.2. Sello de tiempo.

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

7.2.1 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 de referencia 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 desviación máxima de 100ms

7.3. Identificadores de objeto (OID) de los algoritmos criptográficos

El identificador de objeto del algoritmo de firma puede ser:

- 1.2.840.113549.1.1.11 - sha256WithRSAEncryption
- 1.2.840.113549.1.1.13 - sha512WithRSAEncryption

El campo Subject Public Key Info (1.2.840.113549.1.1.1) incorpora el valor rsaEncryption.

7.4. 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.

7.4.1 Número de versión

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

7.4.2 CRL y extensiones

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

7.5. OCSP Profile

7.5.1 Número de versión

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

7.5.2 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.

8. Especificación de la Administración

8.1. Autoridad de las políticas

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

8.2. 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 http://www.camerfirma.com.

Camerfirma 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.

8.3. Publicación y copia de la política

Una copia de esta política estará disponible en formato electrónico en la página web de AC Camerfirma SA http://www.camerfirma.com

8.4. 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 a su seguridad, toda o parte de esa DPC no estarán disponible públicamente.

9. ANEXO I – Proceso de Sellado de tiempo.

El procedimiento de sellado implica:

- Usuario petiionario:

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

- Unidad de sellado 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 Sellado de Tiempo.

Generación de Sello de Tiempo

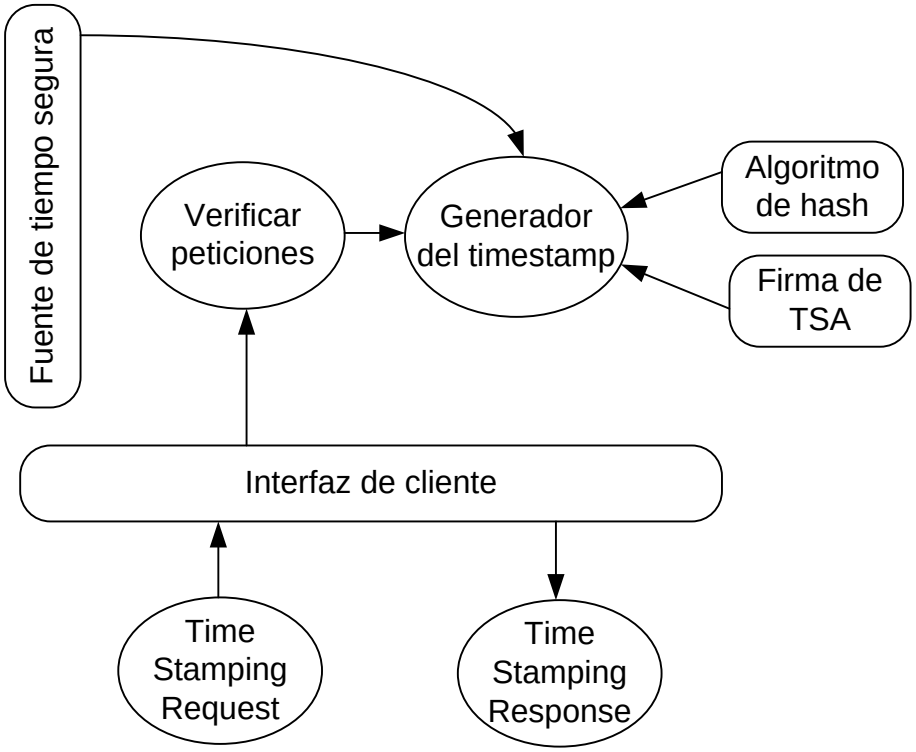
Esta función es la responsable de crear un sello de tiempo que asocie el instante de tiempo actual, un número de serie único, los datos proporcionados para el sellado de tiempo y garantizar los requerimientos de política a la que se adhiere.

Sello de tiempo -*Time Stamp Token* (TST)

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

9.1. Recepción del sello:

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



9.2. 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.

9.3. 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 "TimeStamp

Request" 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**.

Posteriormente se obtiene de la fuente segura de tiempo (ver apartado en este documento) y se genera el token de tiempo que es firmado electrónicamente con las claves privadas de sellado de Camerfirma.

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 sellado de tiempo de Camerfirma se realizará:

- Mediante protocolo HTTP/HTTPS con autentificación en cliente, con el fin de poder validar las peticiones realizadas.

- Mediante usuario y contraseña.

9.4. 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.

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 el sello de tiempo es posterior a la fecha en que se emitió este.
- Comprobar que el certificado emisor del sello 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 limite prescrito en la Declaración de Practicas de Certificación de AC Camerfirma o en cualquier otro aspecto descrito en las condiciones de uso del servicio.

10. ANEXO II - Camerfirma Perú.

10.1. Presentación

AC Camerfirma S.A. (Camerfirma) es una empresa que fue creada en el año 1999 con domicilio en España, donde se establece como prestador de servicios de certificación al amparo de la LEY 59/2003, de 19 de diciembre, de firma electrónica en España.

Camerfirma desde el comienzo de su trayectoria como sociedad anónima en el año 2000, mantiene una estrecha relación con los mercados de Sudamérica y cuenta en su labor con numerosos proyectos de consultoría y de implantación de PKI con las Cámaras de Comercio sudamericanas.

En el año 2014, Camerfirma logró acreditarse como Entidad de Certificación en Perú bajo el nombre de Camerfirma Perú S.A. (Camerfirma Perú). En el año 2016, se acreditó como prestador de servicios de intermediación digital y servicios de emisión de Sellos de Tiempo (Timestamp), para brindar dichos servicios en Perú y dar cumplimiento a la regulación peruana establecida por la Autoridad Administrativa Competente (AAC), INDECOPI.

Como entidad de Sellado de Tiempo – TSA, Camerfirma Perú asume las responsabilidades de representación de los servicios de sello de tiempo brindados por Camerfirma.

La infraestructura tecnológica y operativa de la TSA Camerfirma Perú es provista por Camerfirma. Dicha infraestructura está sujeta a las acreditaciones de calidad y seguridad descritas posteriormente en este documento, como: WebTrust for Certification Authorities.

10.2. Contacto

Nombre: Javier Urios

Cargo: Gerente General de Camerfirma Perú

Dirección de correo electrónico: xurios@cocep.org.pe

10.3. Responsabilidad

Camerfirma Perú asume las responsabilidades de representación de los servicios de sello de tiempo brindados por Camerfirma, a fin de ejecutar las garantías y cláusulas contractuales con los clientes. En tal sentido establece y garantiza el cumplimiento de los niveles de servicio y requerimientos contractuales acordados con cada cliente; sin embargo, no participa de los roles de confianza que administran los sistemas de sellado

de tiempo, sino que estos están circunscritos a la infraestructura y organización administrada conforme a la certificación WebTrust.

Asimismo Camerfirma Perú es responsable de gestionar la implementación y velar por el cumplimiento de la presente política y la declaración de prácticas, así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

10.4. Conformidad.

Camerfirma Perú, como Autoridad emisora de sellos de tiempo, cumple los requerimientos legales establecidos en la Guía de Acreditación de Entidades Prestadoras de Servicios de Valor Añadido, el Reglamento y la Ley de Firmas y Certificados Digitales – Ley 27269.

11. ANEXO III - Declaración de Practicas de la TSA.

- AC Camerfirma 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 identifican las obligaciones de todos los agentes (internos y externos) implicados en el soporte al servicio de sellado de tiempos.
- AC Camerfirma 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 Practicas.
- 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.

11.1. Declaración Informativa de la TSA-TSU.

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

Esta información se puede encontrar en http://www.camerfirma.com/servicios/sellado-de-tiempo/

12. Anexo IV. Acrónimos

AC	Autoridad de Certificación.
AR	Autoridad de Registro.
CPS	*Certification Practice Statement*. Declaración de Prácticas de Certificación.
CRL	*Certificate Revocation List.* Lista de certificados revocados.
CSR	*Certificate Signing Request.* Petición de firma de certificado.
DCCF	Dispositivo cualificado de creación de firma.
DES	*Data Encryption Standard*. Estándar de cifrado de datos.
DN	*Distinguished Name.* Nombre distintivo dentro del certificado digital.
DSA	*Digital Signature Algorithm.* Estándar de algoritmo de firma.
DSCF	Dispositivo seguro de creación de firma.
DSADCF	Dispositivo seguro de almacén de datos de creación de firma.
FIPS	*Federal Information Processing Standard Publication.*
IETF	*Internet Engineering Task Force*
ISO	*International Organization for Standardization.* Organismo Internacional de Estandarización
ITU	*International Telecommunications Union.* Unión Internacional de Telecomunicaciones
LDAP	*Lightweight Directory Access Protocol*. Protocolo de acceso a directorios
OCSP	*On-line Certificate Status Protocol.* Protocolo de acceso al estado de los certificados
OID	*Object Identifier*. Identificador de objeto
PA	*Policy Authority.* Autoridad de Políticas
PC	Política de Certificación
PIN	*Personal Identification Number*. Número de identificación personal

PKI	*Public Key Infrastructure*. Infraestructura de clave pública
RSA	Rivest-Shamir-Adleman. Tipo de algoritmo de cifrado
SHA	*Secure Hash Algorithm.* Algoritmo seguro de Hash
SSL	*Secure Sockets Layer*. 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	*Transmission Control. Protocol/Internet Protocol*. Sistema de protocolos, definidos en el marco de la IEFT. 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	*Time-Stamping Authority*
TSU	*Time-Stamping Unit*
TST	*Time-Stamp Token*
UTC	*Coordinated Universal Time*

13. Anexo V. Definiciones

Autoridad de Certificación (AC)	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.
Autoridad de Políticas (AP)	Persona o conjunto de personas responsable de todas las decisiones relativas a la creación, administración, mantenimiento y supresión de las políticas de certificación y DPC.
Autoridad de Registro (AR)	Entidad responsable de la gestión de las solicitudes e identificación y registro de los solicitantes de un certificado.
Certificación cruzada	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.
Certificado	Archivo que asocia la clave pública con algunos datos identificativos del suscriptor y es firmada por la AC.
Clave pública	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**.
Clave privada	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.
CPS	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).

CRL	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.
Datos de Activación	Datos privados, como PIN o contraseñas empleados para la activación de la clave privada.
DCCF	*Dispositivo cualificado de creación de firma.* dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II del Reglamento (UE) 910/2014.
DSADCF	*Dispositivo seguro de almacén de los datos de creación de firma.* Elemento software o hardware empleado para custodiar la clave privada del suscriptor de forma que solo él tenga el control sobre la misma.
DSCF	*Dispositivo Seguro de creación de firma*. 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.
Entidad	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.
Firma digital	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: a) que los datos no han sido modificados (integridad). b) que la persona que firma los datos es quien dice ser (identificación). c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen).
OID	Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.

Par de claves	Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.
PKI	Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública.
Política de certificación (PC)	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.
Suscriptor	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.
Tercero que confía	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.