Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:19 PM

DECLARACIÓN DE AUTORIDAD DE SELLADO DE TIEMPO

Servicio de Valor Añadido

EDITORA PEGASO VERDE
CERTIFICADOS DIGITALES / FIRMAS DIGITALES
Tecnología digital a tu alcance

Información del documento	
Nombre de documento: **Declaración de Autoridad de Sellado de Tiempo**	
Versión: **1.2**	Aprobado por: **Responsable del SVA**
Año: **2024**	Dirigido a: **INDECOPI**

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:21 PM

Control de versiones		
Versión	**Fecha**	**Descripción**
1.0	01-03-2022	Elaboración de documento inicial.
1.1	01-09-2022	Cambio de nombre del documento. Actualización de acuerdo a la nueva versión de la política del proveedor.
1.2	25-11-2024	Cambio de nombre del documento y eliminación de Política

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:23 PM

ÍNDICE

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:25 PM

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:27 PM

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:28 PM

1 INTRODUCCIÓN

EDITORA PEGASO VERDE E.I.R.L. que en adelante llamaremos “EDITORA PEGASO VERDE”, es una empresa peruana fundada el 10 de mayo del 2012, la cual brinda servicios de soporte de sistemas, y se encarga de la administración de base de datos y de la comunicación virtual de las siguientes empresas: General Services Green Pegasus, Courier Pegaso Verde y Courier Green Pegasus. De esta manera, se incursionará en la actividad de Entidad de Registro de Certificados Digitales, así como la prestación del servicio de firma digital.

Entre sus servicios se encuentran sus funciones como Entidad de Registro, para lo cual EDITORA PEGASO VERDE se encuentra acreditada ante el INDECOPI para su debido ejercicio.

En calidad de Entidad de Registro, brinda los servicios de verificación de sus clientes, tanto para representantes legales, empleados o agentes automatizados, para la emisión, re-emisión o revocación de certificados digitales; así como el registro de las evidencias generadas.

Entre los tipos de certificados digitales que provee son Certificado digital para Factura Electrónica según lo solicitado por SUNAT en el Perú; Certificado Digital para Organizaciones; Certificados para Profesionales; Certificado Digital para Persona Natural; y Certificado Digital para Agente Automatizado.

La Entidad de Registro de EDITORA PEGASO VERDE se encuentra soportada por la Entidad de Certificación de CAMERFIRMA PERÚ S.A.C., la cual forma parte de los Prestadores de Servicios de Certificación Digital acreditados por el INDECOPI.

En el año 2022, se acreditó como Servicio de Valor Añadido (SVA), para brindar dichos servicios en Perú y dar cumplimiento a la regulación peruana establecida por la Autoridad Administrativa Competente (AAC), INDECOPI.

Como Autoridad de Sellado de Tiempo (TSA), EDITORA PEGASO VERDE asume las responsabilidades de representación de los servicios de sello de tiempo brindados por CAMERFIRMA.

La infraestructura tecnológica y operativa de la TSA EDITORA PEGASO VERDE es provista por CAMERFIRMA. Dicha infraestructura ha obtenido la certificación Webtrust for Certification Authorities, y es verificada anualmente por auditores autorizados.

2 OBJETIVO

Este documento tiene como objetivo especificar la Política de Certificación del Certificado CAMERFIRMA que es proveedor de EDITORA PEGASO VERDE para Sellos de tiempo para la administración de sus servicios como Prestador de Servicios de Valor añadido tipo Autoridad de Sellado de Tiempo, y en el marco del cumplimiento de los requerimientos de la “Guía de Acreditación de Prestadores de Servicios de Valor Añadido (SVA)” establecida por el INDECOPI.

Además, está basada en la especificación del estándar RFC 3628 – Policy Requirements for Time-Stamping Authorities (TSAs), de IETF y del ETSI TS 102 023 V1.2.1 (2003-01) Electronic Signatures and Infrastructures (ESI) Policy requirements for time-stamping authorities.

Esta política al depender de una política superior de entidad raíz, se encuentra en conformidad con lo dispuesto por la PC de Chambers of Commerce Root, que podrá localizar en la siguiente dirección http://www.camerfirma.com/area-de- usuario/jerarquia-politicas-y-practicas-de-certificacion/ y que establece las normas, políticas y procedimientos para la emisión de certificados de segundo nivel.

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 a 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.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:30 PM

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

3 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación de la Autoridad de Sellado de Tiempo de EDITORA PEGASO VERDE en el marco del cumplimiento de los requerimientos de la “Guía de Acreditación de Prestadores de Servicios de Valor Añadido (SVA)” establecida por el INDECOPI, comprende la representación de lo siguiente:

EDITORA PEGASO VERDE es responsable de exigir a sus proveedores el cumplimiento de los requisitos establecidos por la Autoridad Administrativa Competente de la IOFE y es responsable ante sus clientes de la calidad y seguridad de los servicios brindados.

4 DEFINICIONES Y ABREVIACIONES

Prestador de Servicios de Valor Añadido	Entidad que presta servicios que implican el uso de la firma digital en el marco de la regulación establecida por la IOFE.
Servicios de valor añadido	Servicios compuestos por tecnología y sistemas de gestión que utilizan certificados digitales garantizando la autenticidad e integridad de los mismos durante su aplicación.
Política de servicios de valor añadido	Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.
Suscriptor	Entidad que requiere los servicios provistos por el SVA de EDITORA PEGASO VERDE y que está de acuerdo con los términos y condiciones de los servicios conforme a lo declarado en el presente documento.
Tercero que confía	Persona que recibe un documento, log, o notificación electrónica generada durante la ejecución de los servicios de valor añadido, y que confía en la validez de las transacciones realizadas.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:32 PM

5 COMUNIDAD Y ÁMBITO DE APLICACIÓN

Este documento puede ser utilizado por terceros receptores de los sellos de tiempo de EDITORA PEGASO VERDE provistos por CAMERFIRMA y suscriptores del servicio de emisión de sellos de tiempo como base para confirmar la fiabilidad de los servicios descritos en él. La política de la autoridad de sellos de tiempo está basada en criptografía de clave pública, fuentes seguras de tiempo y certificados digitales.

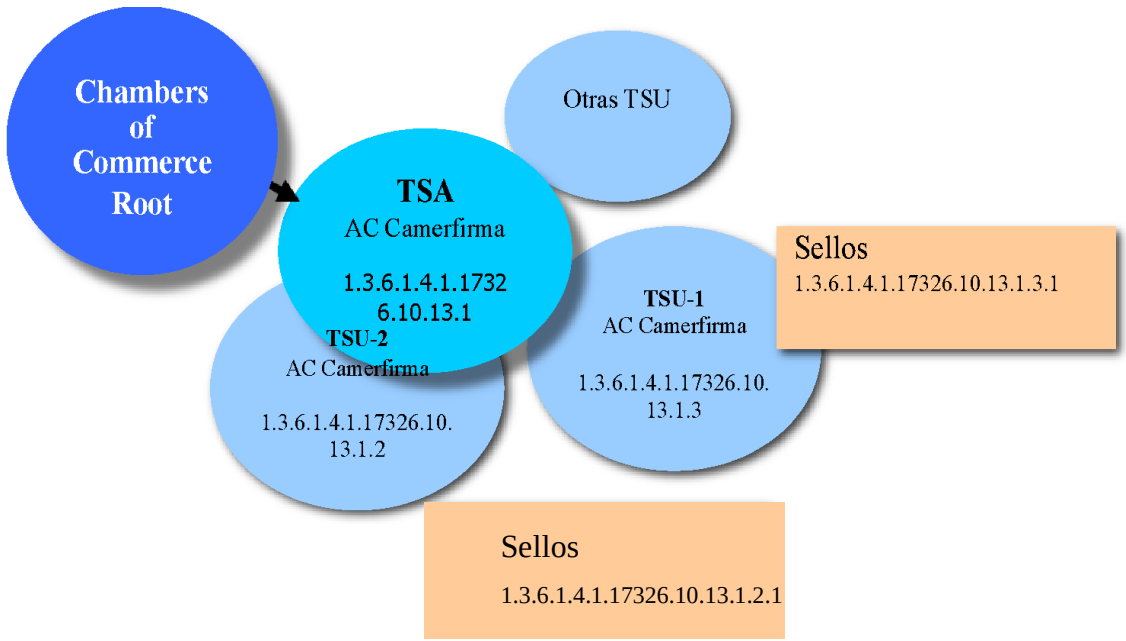
5.1 TSA-TSU

Una TSA (Autoridad de Sellado de tiempo) es un elemento 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.

La TSA puede subcontratar todos o algunos componentes de la TSA incluidos los servicios de emisión de sellos usando las claves de TSU, aunque en todo momento será la última responsable del servicio.

El servicio de sellado de tiempo se compone de una autoridad TSA y una o más Unidades de Sellado de Tiempo (TSU). Esta última 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.

El servicio de sellado de tiempo de CAMERFIRMA tiene la siguiente estructura:



Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:34 PM

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.

En el esquema gestionado por Camerfirma representado en la ilustración previa, la TSU-1 emite sellos de tiempo desde unas claves gestionadas en software y sin garantías de disponibilidad y rendimiento. La TSU-2 emite sellos de tiempo desde claves gestionadas en dispositivo hardware y con las garantías de servicio descritas en este documento.

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

5.2 SUSCRIPTOR

Bajo esta Política, el Suscriptor es una entidad que posee un certificado Camerfirma de TSU para la creación de un servicio de sellado de tiempo o la propia AC Camerfirma SA.

5.3 PARTE USUARIA

En esta Política se entiende por Parte Usuaria a la persona que voluntariamente confía en los sellos de tiempo emitidos bajo esta política y se sujeta a lo dispuesto en ella por lo que no se requerirá acuerdo posterior alguno.

La Parte Usuaria también puede denominarse como “Tercero que Confía”.

5.4 SOLICITANTE

A los efectos de esta Política, se entenderá por Solicitante la persona física que solicita un certificado para la implantación de una unidad de sellado de tiempo de TSU Camerfirma o un servicio de emisión de sellos de tiempo bajo alguna de las TSU existentes.

5.5 ÁMBITO DE APLICACIÓN Y USOS

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

5.6 USOS PROHIBIDOS Y NO AUTORIZADOS

Bajo la presente Política no se permite el uso que sea contrario a la normativa peruana y comunitaria, a los convenios internacionales ratificados por el estado peruano, 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.

5.7 CONTACTOS

Esta política de certificación está administrada y gestionada por EDITORA PEGASO VERDE.

Para cualquier consulta contactar:

- Nombre: Nemesio Lizardo Esquivel Tornero
- Dirección de correo electrónico: drlizardoesquivel@hotmail.com

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:36 PM

6 CLÁUSULAS GENERALES

6.1 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.

6.1.1 TSA

La TSA garantizará:

- Cumplir lo dispuesto en esta política.
- Proteger su información contra pérdidas, destrucciones y falsificaciones.
- Proteger sus claves privadas de forma segura.
- Emitir certificados a las TSU de forma segura
- Revocar los certificados según lo dispuesto en esta política y publicar la correspondiente ARL.
- Informar a las AC's delegadas de los cambios que se produzcan en las presentes políticas
- El acceso permanente a los servicios de sellado de tiempo excluyéndose las tareas de mantenimiento programadas y aquellas descritas en el apartado 6.2.1 de estas políticas.
- La exactitud de la fecha y hora incorporada en los sellos de tiempo basadas en el sistema UTC. Como mínimo la exactitud del sistema estará por debajo de las centésimas de segundo.
- 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.
- Que los sellos de tiempo emitidos estarán libres de datos falsos y errores

6.1.2 SOLICITANTE

El solicitante de un Certificado de TSU estará obligado a cumplir con lo dispuesto por la normativa aplicable y además a:

1. Respetar lo dispuesto en esta política de certificación.
2. Suministrar a la TSA la información necesaria para realizar una correcta identificación.
3. Confirmar la exactitud y veracidad de la información suministrada.
4. Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

6.1.3 SUSCRIPTOR

El suscriptor para hacer uso del Sistema de Certificación TSA, asume la obligación de conocer y comprender plenamente las características y limitaciones determinadas en

esta Declaración de Prácticas de Certificación y de las Políticas y contratos comerciales vinculados.

El suscriptor de un Certificado de TSU estará obligado a:

1. Respetar lo dispuesto en esta política de certificación.
2. Proteger sus claves privadas de forma segura.
3. Emitir sello de tiempo conforme a esta Política y a los estándares de aplicación.
4. En caso de utilizar recursos técnicos propios para la emisión de los certificados.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:38 PM

5. La utilización de la fuente de tiempo suministrada por la TSA y utilizar mecanismos técnicos que permitan detectar cualquier variación sobre esta.

6.1.4 PARTE USUARIA

Las terceras partes que voluntariamente confíen en los Sistemas de Certificación de esta TSA (Partes Usuarias) asumen la obligación de:

- Verificar el estado de activación en que se encuentra el Certificado de la TSA 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 cuenta cualquier limitación en el uso del sello de tiempo indicado en la política o en las prácticas de certificación correspondientes.
- Tomar en consideración cualquier límite prescrito en otros acuerdos de servicio.

6.2 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 el presente documento 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.

EDITORA PEGASO VERDE 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 se 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 y eIDAS.

Asimismo, EDITORA PEGASO VERDE es responsable de gestionar la implementación y velar por el cumplimiento del presente documento, así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

Responsable de los documentos de la TSA:

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:40 PM

- Nombre: Nemesio Lizardo Esquivel Tornero
- Dirección de correo electrónico: drlizardoesquivel@hotmail.com

6.2.1 EXONERACIÓN DE RESPONSABILIDAD

La TSA y las ER 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 el presente documento 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 el presente documento 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.

6.2.2 LÍMITE DE RESPONSABILIDAD EN CASO DE PÉRDIDAS POR TRANSACCIONES

La TSA no se responsabilizará por las pérdidas por transacciones.

6.2.3 RESPONSABILIDAD FINANCIERA

La TSA no asume ningún tipo de responsabilidad financiera.

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

6.3 INTERPRETACIÓN Y EJECUCIÓN

6.3.1 LEGISLACIÓN

La ejecución, interpretación, modificación o validez de las presentes Políticas se regirá por lo dispuesto en la legislación vigente aplicable.

6.3.2 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.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:41 PM

6.3.3 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.

6.3.4 PROCEDIMIENTO DE RESOLUCIÓN DE DISPUTAS

El procedimiento de resolución de disputas se indicará en los respectivos acuerdos con los clientes.

6.3.5 TARIFAS DE EMISIÓN DE CERTIFICADOS Y RENOVACIÓN

Los precios de los servicios de certificación o cualquier otro servicio relacionado estarán disponibles para los usuarios en la página Web de EDITORA PEGASO VERDE:

www.editorapegasoverde.net

6.3.6 TARIFAS DE ACCESO A LOS CERTIFICADOS

Sin estipular.

6.3.7 TARIFAS DE ACCESO A LA INFORMACIÓN RELATIVA AL ESTADO DE LOS CERTIFICADOS O LOS CERTIFICADOS REVOCADOS

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

6.3.8 TARIFAS POR EL ACCESO AL CONTENIDO DE ESTAS POLÍTICAS DE CERTIFICACIÓN

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

6.3.9 POLÍTICA DE REINTEGROS

Sin estipular.

6.4 POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN

6.4.1 DECLARACIÓN DE PRÁCTICAS DE LA TSA

La TSA demostrará que cuenta 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 la 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.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:43 PM

- 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.

6.4.2 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 auditoria.
- 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.

6.5 PUBLICACIÓN Y REPOSITORIOS

6.5.1 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 encontrará disponible en Internet.

Las Prácticas de Certificación de referencia serán así mismo públicas y se pondrán a disposición del público en una dirección de Internet.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:45 PM

6.5.2 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 usuarios.

En concreto:

a) El certificado de la TSA y TSUs son públicos y se encontrarán disponibles en la página Web de CAMERFIRMA.
b) La información a la que se refiere el punto a) 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.

6.5.3 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 EC 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.

6.5.4 CONTROLES DE ACCESO

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

6.6 AUDITORIAS

6.6.1 FRECUENCIA DE LAS AUDITORIAS

Se realizará una auditoria con una periodicidad mínima bianual, salvo que se establezca un plazo menor por la normativa vigente.

6.6.2 IDENTIFICACIÓN Y CUALIFICACIÓN DEL AUDITOR

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

6.6.3 RELACIÓN ENTRE AUDITOR Y LA TSA

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

6.6.4 TÓPICOS CUBIERTOS POR LA AUDITORIA

La auditoría deberá verificar en todo caso:

a) Que la TSA tiene un sistema que garantice la calidad del servicio prestado
b) Que la TSA cumple con los requerimientos de esta Política de Certificación

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:47 PM

c) 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.

6.7 CONFIDENCIALIDAD

6.7.1 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 EC 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.

6.7.2 TIPO DE INFORMACIÓN CONSIDERADA NO CONFIDENCIAL

Se considerará como información no confidencial:

a) La contenida en la presente Política y en las Prácticas de Certificación
b) La información contenida en los certificados de TSA y TSU.
c) Cualquier información cuya publicidad sea impuesta normativamente
d) 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.

6.7.3 DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN DE CERTIFICADOS

La forma de difundir la información relativa a la revocación de un certificado se realizará mediante la publicación de las correspondientes CRL y mediante protocolo de acceso en línea OCSP.

6.7.4 ENVÍO A LA AUTORIDAD COMPETENTE

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

6.8 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.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:49 PM

7 GESTIÓN DE CLAVES DE LA TSA

7.1 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.

7.2 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.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:51 PM

7.3 DISTRIBUCIÓN DE LA CLAVE PÚBLICA DE LA TSU-TSA

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.

7.4 CAMBIO DE CLAVES DE 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).

7.5 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.

7.6 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:

a) el hardware criptográfico usado para la firma de sellos de tiempo no se manipula durante su transporte
b) el hardware criptográfico usado para la firma de sellos de tiempo no se manipula mientras está almacenado
c) el uso del hardware criptográfico usado para la firma de sellos de tiempo requiere el uso de al menos dos empleados de confianza.
d) el hardware criptográfico usado para la firma de sellos de tiempo está funcionando correctamente; y;

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:53 PM

e) 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.

8 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:

8.1 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 TSAs 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.

8.2 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.

9 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 efectosprobatorios 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.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:55 PM

- 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.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:57 PM

10 CONTROLES DE SEGURIDAD FÍSICA, PROCEDIMENTAL Y DE PERSONAL

10.1 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 anti-incendios, 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.

10.2 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.

10.3 ACCESO FÍSICO

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

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:22:58 PM

10.4 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

10.5 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.

10.6 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 anti-incendios.

10.7 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.

10.8 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.

10.9 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.

11 CONTROLES PROCEDIMENTALES

11.1 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.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:23:00 PM

- **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.

11.2 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.

11.3 IDENTIFICACIÓN Y AUTENTIFICACIÓN PARA CADA ROL

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

12 CONTROLES DE SEGURIDAD DE PERSONAL

12.1 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.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:23:02 PM

- 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.

12.2 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.

12.3 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.

12.4 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.

12.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

No estipulado.

12.6 SANCIONES POR ACCIONES NO AUTORIZADAS

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

12.7 REQUERIMIENTOS DE CONTRATACIÓN DE PERSONAL

Ver apartado 12.1.

12.8 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.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:23:04 PM

13 CONTROLES DE SEGURIDAD TÉCNICA

13.1 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.

13.2 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.

13.3 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.

13.4 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.

13.5 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.

13.6 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.

13.7 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

La clave privada de la TSA deberá ser activada conforme al apartado 7.1., dentro del cual se sobreentiende que se realiza la activación de la clave privada luego de su generación.

13.8 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

No estipulado.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:23:06 PM

13.9 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.

14 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

14.1 ARCHIVO DE LA CLAVE PÚBLICA

La TSA deberá conservar todas las claves públicas de verificación.

14.2 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.

15 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.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:23:08 PM

16 PERFILES DE CERTIFICADO Y CRL

16.1 PERFIL DE CERTIFICADO

Todos los certificados emitidos bajo esta política serán conformes a:

- Estándar X.509 versión 3.
- RFC 2459 "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”.

16.1.1 NÚMERO DE VERSIÓN

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

16.1.2 EXTENSIONES DEL CERTIFICADO TSA

EXTENSIÓN DEL CERTIFICADO		**VALOR**
Versión **Serial Number (certificate)** **Algoritmo de firma**		V3 12 Sha1RSA
Emisor (issuer)	C N O OU C	Chambers of Commerce Root Camerfirma SA CIF A82743287 http://www.chambersign.org EU
Válido desde Válido hasta		jueves, 19 de mayo de 2005 9:20:50 domingo, 20 de mayo de 2035 9:20:50
Asunto.	C C N O L E S N	ES TSA Camerfirma TSA CA AC Camerfirma SA Madrid (see current address at www.camerfirma.com/address) ac_camerfirma_tsa_ca@camerfirma.com A82743287
Clave pública		RSA 2.048 Bits
Identificador de clave de asunto		bf fa 7e ae b9 9d aa 65 69 72 c6 32 16 8d e0 10 2e a5 9b 22
Identificador de clave del emisor		Id. de clave=e3 94 f5 b1 4d e9 db a1 29 5b 57 8b 4d 76 06 76 e1 d1 a2 8a Emisor de certificado: Dirección del directorio: CN=Chambers of Commerce Root OU=http://www.chambersign.org O=AC Camerfirma SA CIF A82743287 C=EU Número de serie del certificado=00
Punto de distribución CRL		http://crl.chambersign.org/chambersroot.crl

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:23:09 PM

Nombre alternativo del sujeto	ac_camerfirma_tsa_ca@camerfirma.com
Nombre alternativo del Emisor	chambersroot@chambersign.org
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.17326.10.13.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://cps.camerfirma.com/cps/ac_camerfirma_tsa_ca.html
Restricción básica<critica>	Tipo de asunto= Entidad emisora de certificados (CA) Restricción de longitud de ruta=11

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:23:11 PM

Uso de la clave <critica>	Firma digital, Firma de certificados, Firma CRL sin conexión, Firma CRL (86)
Algoritmo de identificación	Sha1
Huella digital	e3 f1 5b b2 da ea 3b 0e 8d 61 75 17 af 9d fe a1 fd ca 6a f0

16.1.3 EXTENSIONES DEL CERTIFICADO TSU

EXTENSIÓN DEL CERTIFICADO		**VALOR**
Versión		V3
Serial Number (certificate)		05
Algoritmo de firma		Sha1RSA
Emisor (issuer)	C	ES
	CN	TSA Camerfirma TSA CA
	O	AC Camerfirma SA
	L	Madrid (see current address at www.camerfirma.com/address
	E	ac_camerfirma_tsa_ca@camerfirma.com
	SN	A82743287
Válido desde		<fecha de inicio de la validez>
Válido hasta		<fecha de fin de la validez>
Asunto.	C	ES
	CN	TSU 1 AC Camerfirma
	O	AC Camerfirma SA
	L	Madrid (see current address at www.camerfirma.com/address
	E	tsa_camerfirma@camerfirma.com
	SN	A82743287
Clave pública		RSA 1024
Identificador de clave de asunto		SHA-1 Clave
Identificador de clave del emisor		Id. de clave Emisor de certificado Número de serie del certificado
Punto de distribución CRL		http://crl.camerfirma.com/tsa_camerfirma.crl http://crl1.camerfirma.com/tsa_camerfirma.crl
Nombre alternativo del sujeto		Nombre RFC822=tsa_camerfirma@camerfirma.com

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:23:13 PM

Bases del certificado		[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.17326.10.13.1.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://cps.camerfirma.com/cps/ac_camerfirma_tsa_ca [1,2]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario Calificador: Texto de aviso=**TSU Software AC Camerfirma**
Restricción básica<critica>		Tipo de asunto=Entidad final Restricción de longitud de ruta=Ninguno
Uso de la clave <critica>		Firma digital, Sin repudio (c0)
Uso Mejorado de Clave		Impresión de fecha (1.3.6.1.5.5.7.3.8)
Algoritmo de identificación		Sha1
Huella digital		<fingerprint>

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:23:15 PM

16.1.4 SELLOS DE TIEMPO

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

TimeStampResp: = SEQUENCE {

status PKIStatusInfo,

timeStampToken OPTIONAL }

El campo status está basado en la definición de la estructura PKIStatusInfo de la RFC2510:

PKIStatusInfo ::= SEQUENCE {

status

PKISTATUS,

statusString PKIFreeText OPTIONAL,

failInfo PKIFailureInfo OPTIONAL }

Status: Si este campo está a cero o a uno indica que el sello viene en el mensaje de respuesta. Para cualquier otro valor indica que no viene en el mensaje de respuesta.

PKIStatus ::= INTEGER {

granted (0),

grantedWithMods (1),

rejection (2),

waiting (3),

revocationWarning (4),this message contains a warning that a revocation is imminent

revocationNotification (5)notification that a revocation has occurred}

StatusString: Se usa para indicar eventos de error.

FailInfo: indica las causas por las que no se ha generado el sello de tiempo. Siendo los posibles errores:

PKIFailureInfo ::= BIT STRING {

badAlg (0),

Unrecognized or unsupported Algorithm Identifier badRequest (2),

Transaction not permitted or supported badDataFormat (5),

The data submitted has the wrong format timeNotAvailable (14),

The TSA's time source is not available unacceptedPolicy (15),

The requested TSA policy is not supported unacceptedExtension (16),

The requested extension is not supported

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:23:17 PM

addInfoNotAvailable (17) The additional information requested could not be understood or is not available

systemFailure (25) the request cannot be handled due to system failure}

El campo **timestampToken** contiene el sello de tiempo generado. Se define como:

TimeStampToken ::= ContentInfo contentType is id-signedData ([CMS]) Content is SignedData ([CMS])

ContentInfo es una estructura que encapsula la información firmada en una estructura TSTInfo. Está definida en la RFC2630 y tiene los siguientes campos:

TSTInfo ::= SEQUENCE {

version	INTEGER { v1(1) },	
policy	TSAPolicyId,	
messageImprint	MessageImprint,	
serialNumber	INTEGER,	
genTime	GeneralizedTime,	
accuracy	Accuracy	OPTIONAL,
ordering	BOOLEAN	DEFAULT FALSE,
nonce	INTEGER	OPTIONAL,
tsa	[0] GeneralName	OPTIONAL,
extensions	[1] IMPLICIT Extensions	OPTIONAL } version: indica la

versión del sello

policy: si se ha generado el sello, será igual al del mensaje de petición messageImprint: será igual al del mensaje de petición

serialNumber: es un entero asignado por la TSA y debe ser único para cada sello que genere. Por tanto, un sello será identificado por el nombre de la TSA que lo generó y el número de serie asignado

genTime: es el instante de tiempo en el que se creó el sello. Tanto ISO como el IETF expresan el instante de tiempo referido a la escala UTC, para evitar confusiones con las horas locales. El formato debe ser el siguiente:

CC YY MM DD hh mm ss Z

CC representa el siglo (19-99)

YY representa el año (00-99)

MM representa el mes (01-12)

DD representa el día (01-31)

hh representa la hora (00-23)

mm representa los minutos (00-59)

ss representa los segundos (00-59)

Z viene de zulu, que es como se conoce a la escala UTCaccuracy: en los casos que sea necesario, proporciona una precisión incluso de microsegundos:

Accuracy ::= SEQUENCE {

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:23:19 PM

seconds [1] Integer OPTIONAL,

millis [2] Integer (1..999) OPTIONAL,

micros [3] Integer (1..999) OPTIONAL,

}

nonce: aparece si lo hace en el mensaje de petición, y tendrá el mismo valor

tsa: sirve para identificar a la TSA

extensions: están definidas en la RFC 2459

16.1.5 ACCESO AL SERVICIO

El método de comunicación entre las entidades y el servicio de sellado de tiempo se realizará mediante protocolo HTTPS con autentificación en cliente, con el fin de poder validar las peticiones realizadas.

16.1.6 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 milisegundos.
- 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

16.1.7 IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

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.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:23:21 PM

16.1.8 RESTRICCIONES DE LOS NOMBRES

No estipulado

16.2 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.

Para el certificado de TSA:

C	V2
Emisor	CN = Chambers of Commerce Root OU = http://www.chambersign.org O = TSA Camerfirma SA CIF A82743287

	C = EU
Periodo máximo de validez	6 Meses
Algoritmo de firma	Sha1withRSA
2.5.29.20 Nº de serie	Presente
Identificador de clave de autoridad	Id. de clave=e3 94 f5 b1 4d e9 db a1 29 5b 57 8b 4d 76 06 76 e1 d1 a2 8a Emisor de certificado: Dirección del directorio: CN=Chambers of Commerce Root OU=http://www.chambersign.org O=AC Camerfirma SA CIF A82743287 C=EU Número de serie del certificado=00
Versión	V2

Para el certificado de TSU:

Versión	V2
Emisor	CN = AC Camerfirma TSA CA O = AC Camerfirma SA Número de serie = A82743287 L = Madrid (see current address at www.camerfirma.com/address) E = ac_camerfirma_tsa_ca@camerfirma.com C = ES
Periodo máximo de validez	1 Mes
Algoritmo de firma	Sha1withRSA
2.5.29.20 Nº de serie	Presente

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:23:23 PM

Identificador de clave de autoridad	Id. de clave=bf fa 7e ae b9 9d aa 65 69 72 c6 32 16 8d e0 10 2e a5 9b 22 Emisor de certificado: Dirección del directorio: CN=Chambers of Commerce Root OU=http://www.chambersign.org O=AC Camerfirma SA CIF A82743287 C=EU Número de serie del certificado=12

16.2.1 NÚMERO DE VERSIÓN

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

16.2.2 CRL Y EXTENSIONES

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

17 ESPECIFICACIÓN DE LA ADMINISTRACIÓN

17.1 AUTORIDAD DE LAS POLÍTICAS

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

17.2 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 EDITORA PEGASO VERDE.

En la Web de EDITORA PEGASO VERDE se mantendrá un histórico con las versiones anteriores de las políticas.

Los usuarios 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 usuarios de la política, la PA puede discrecionalmente asignar un nuevo OID a la política modificada.

17.3 PUBLICACIÓN Y COPIA DE LA POLÍTICA

Una copia de esta política estará disponible en formato electrónico en una dirección de Internet definida en la DPC.

17.4 PROCEDIMIENTOS DE APROBACIÓN DE LA DPC

Para la aprobación y autorización de una TSA se deberán respetar los procedimientos especificados por la PA. Las partes de la DPC de una TSA que contenga información relevante en relación a su seguridad, toda o parte de esa DPC no estará disponible públicamente.

Firmado digitalmente por:
NEMESIO LIZARDO ESQUIVEL TORNERO
DNI:40075571, ABOGADO, CAL 22468
Fecha: 28/11/2024 02:23:25 PM

18 CUMPLIMIENTO DE REQUERIMIENTOS LEGALES

EDITORA PEGASO VERDE, 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.

19 CONFORMIDAD

Este documento ha sido aprobado por la Autoridad de la TSA de EDITORA PEGASO VERDE, y tiene carácter normativo sobre todos los servicios de sellado de tiempo, por lo que cualquier incumplimiento por parte de las personas mencionadas en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectiv