Política de sellado de tiempo

EADTRUST

(**E**uropean **A**gency of **D**igital **Trust,** S.L.)

Miembro de

Observatorio del Notariado para la Sociedad de la Información

UBL

European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

AENOR
Asociación Española de Normalización y Certificación

FORO evidencias electrónicas

Histórico de versiones			
Versión	Fecha	Documentos sustituidos	Descripción / Detalles
2	9/09/09		

Cambios desde la última versión
Maquetación corporate

Difusión	
Propietario:	EADTRUST European Agency of Digital Trust, S.L
Preparado por:	Ivan Basart
Modificado por	
Aprobado por:	
Firma:	
Fecha:	9 de Septiembre 2009
Distribución:	Publica

Referencias de archivo	
Nombre archivo:	Política SelladoTiempo EADTrust

CONTENIDO

A. INTRODUCCIÓN

EADTRUST (European Agency of Digital Trust, S.L.) en adelante EADTrust es una compañía ubicada en el estado español dedicada a la prestación de servicios relacionados con la seguridad informática y, en concreto, con la firma electrónica.

Dentro de estas prestaciones englobadas en la marca EADTrust, se ofrecen servicios de Prestador de Servicios de Certificación, tal como quedan definidos en el punto 2 del artículo 2 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica:

> *Se denomina **prestador de servicios de certificación** la persona física o jurídica que expide certificados electrónicos o presta **otros servicios en relación con la firma electrónica.***

En este contexto, el presente documento contiene la política de servicios DSS EADTrust de EADTRUST (European Agency of Digital Trust).

A.1 Presentación

EADTrust podrá emitir diferentes tipos de sellos de tiempo descritos a continuación.

A.1.1 Tipos de sellado de tiempo

A los efectos de esta política, se establecen los siguientes tipos de sellado de tiempo:

- ✓ Sellado de tiempo inicial. Los sellos de tiempo podrán ser generados inicialmente para un documento electrónico.
- ✓ Resellado de tiempo. Los sellos de tiempo podrán ser generados posteriormente para el mantenimiento de un documento o sello previamente existentes.

A.1.2 Opciones del servicio

Los sellos de tiempo podrán ofrecer opciones, entre las que se pueden mencionar las siguientes:

- ✓ Formato del sello de tiempo, que podrá ser RFC3161 o XMLTimeStamp.
- ✓ Precisión del sello de tiempo, que por defecto será de un (1) segundo.
- ✓ Custodia del sello producido por EADTrust.

A.2 Identificación del Documento

Este documento es la "Política de sellado de tiempo de EADTrust".

EADTrust debe asignar, a cada política de sellado de tiempo, un identificador de objeto (OID), para su identificación por las aplicaciones.

Adicionalmente, EADTrust custodiará en su repositorio y publicará a través del sitio web de EADTrust, un documento con los OIDs correspondientes a las políticas de sellado de tiempo vigentes en cada momento.

A.3 Participantes en los servicios de sellado de tiempo

Esta política de sellado de tiempo regula la prestación de servicios de emisión de sellos de tiempo al público.

Los participantes en los servicios de sellado de tiempo serán los siguientes:

- Prestadores de Servicios de Sellado de Tiempo.
- Entidades y usuarios finales.

A.3.1 Prestador de Servicios de Sellado de Tiempo

EADTrust dispondrá de una o más Entidades de Sellado de Tiempo para la prestación de los servicios, para ofrecer garantías de alta disponibilidad, continuidad de negocio, u otros criterios de seguridad que lo justifiquen.

A.3.2 Entidades y usuarios finales

Las entidades y usuarios finales serán las personas y organizaciones destinatarias de los servicios de sellado de tiempo, incluyendo su emisión, gestión y uso, y entre ellas, las siguientes:

1) Suscriptores de los servicios de sellado de tiempo.
2) Terceros que confían en los sellos emitidos.

A.3.3 Suscriptores

Los suscriptores son las personas y las organizaciones que se suscriben a servicios de sellado de tiempo y que podrán solicitar sellos durante el periodo de suscripción.

A.3.3.1 Terceros que confían en los sellos emitidos

Los terceros que confían en los sellos emitidos son las personas y las organizaciones que reciben sellos de tiempo.

Como paso previo a confiar en los sellos emitidos, los terceros deben verificarlos, tal como se establece en este documento de política y en las correspondientes condiciones generales de uso.

A.4 Uso de los sellos

Esta sección lista las aplicaciones para las que pueden emplearse los sellos, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los sellos.

A.4.1 Usos permitidos

Los sellos iniciales se podrán solicitar para cualquier tipo de documento, firmado o no electrónicamente, y para cualquier tipo de objeto digital,

incluso código ejecutable, garantizándose la existencia de dichos contenidos a la fecha indicada dentro del sello.

También podrán solicitarse sellos sobre sellos anteriormente expedidos (resellado).

A.4.2 Límites y prohibiciones de uso

A.4.2.1 Límites de uso

Los sellos se emplearán para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Los sellos pueden incorporar límites de uso por razón de la materia y de la cuantía, que se establecen en las extensiones del certificado de Entidad de Sellado de Tiempo emitido por EADTrust, así como en la correspondiente política de sellado de tiempo, que se indicarán en las correspondientes condiciones generales de emisión y uso de sellos de tiempo.

A.4.2.2 Prohibiciones de usos

Los sellos no se han diseñado, no se pueden destinar y no se autoriza su uso en equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Todas las responsabilidades legales, contractuales o extra contractuales, daños directos o indirectos que puedan derivarse de usos limitados y/o prohibidos quedan a cargo del suscriptor. En ningún caso podrán el suscriptor o los terceros perjudicados reclamar a EADTrust compensación o indemnización alguna por daños o responsabilidades provenientes del uso de los sellos para los usos limitados y/o prohibidos.

A.5 Administración de la política

A.5.1 Organización que administra el documento

EADTRUST (European Agency of Digital Trust, S.L.)

A.5.2 Datos de contacto de la organización

EADTRUST (European Agency of Digital Trust, S.L.)

http://www.eadtrust.net

A.5.3 Procedimientos de gestión del documento

EADTrust debe disponer de un comité de aprobación de procedimientos y prácticas de la Entidad de Sellado de Tiempo (ETSI TS 102023, sección 7.1.1.f), formado por miembros de la alta dirección, que vele porque esta política se implante adecuadamente (ETSI TS 102023, sección 7.1.1.g).

Se deben practicar análisis de riesgos periódicamente, para evaluar los activos de la Entidad de Sellado de Tiempo, las vulnerabilidades y amenazas a dichos activos que puedan producir un impacto en el negocio, con la finalidad de determinar la idoneidad de los controles y procedimientos establecidos por esta política, o la necesidad de cambios en dichos controles y procedimientos (ETSI TS 102023, sección 7.1.1.a).

EADTrust debe disponer de una Declaración de Prácticas de Certificación específica para declarar sus controles y procedimientos de acuerdo con esta política de sellado de tiempo (ETSI TS 102023, sección 7.1.1.b), así como los controles y procedimientos de cualquier entidad subcontratada para colaborar en la prestación del servicio (ETSI TS 102023, sección 7.1.1.c).

El comité de aprobación de procedimientos y prácticas debe velar por la existencia de un procedimiento de revisión periódica de la Declaración de Prácticas de Certificación (ETSI TS 102023, sección 7.1.1.h).

B. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE SELLOS

B.1 Repositorio(s) de sellos

EADTrust deberá disponer de uno o varios Repositorios de Sellos. Estos repositorios serán accesibles a través del sitio web de EADTrust.

El servicio de Repositorio estará disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de EADTrust, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección D.7.4 y la Declaración de Prácticas de Certificación aplicable.

B.2 Publicación de información

EADTrust publicará las siguientes informaciones, de sus Repositorios:

- Los sellos emitidos, a solicitud del suscriptor.
- Los certificados de Entidades de Sellado de Tiempo.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados, correspondientes a las Entidades de Sellado de Tiempo propias.
- La política de sellado de tiempo
- La Declaración de Prácticas de Certificación aplicable a los servicios de sellado (ETSI TS 102023, sección 7.1.1.d).
- Los documentos de condiciones generales vinculantes con suscriptores y terceros que confían en sellos de tiempo (ETSI TS 102023, sección 7.1.1.e).
- Las modificaciones de los documentos anteriormente indicados (ETSI TS 102023, sección 7.1.1.i).

B.3 Frecuencia de publicación

La información anteriormente indicada, incluyendo políticas y la Declaración de Prácticas de Certificación, se publicará inmediatamente tras su aprobación.

Los cambios en los documentos de política y en la Declaración de Prácticas de Certificación se regirán por lo establecido en la sección A.5 del documento de política o Declaración de Prácticas de Certificación.

La información de estado de revocación de certificados se publicará de acuerdo con lo establecido en la política de certificación correspondiente a la Entidad de Sellado de Tiempo.

B.4 Control de acceso

EADTrust no limitará el acceso de lectura a las informaciones establecidas en la sección B.2, pero establecerá controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Repositorio, para proteger la integridad y autenticidad de la información publicada.

EADTrust empleará sistemas fiables para el Repositorio, de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Los sellos sólo estén disponibles para consulta si el suscriptor ha prestado su consentimiento.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

C. REQUISITOS DE OPERACIÓN DEL CICLO DE VIDA DE LOS SELLOS DE TIEMPO

C.1 Solicitud de sello de tiempo

C.1.1 Legitimación para solicitar la emisión

Antes de la emisión de sellos de tiempo, debe existir un procedimiento de alta de suscriptor al servicio de sellado, en el que se determinarán las personas y sistemas que podrán solicitar sellos de tiempo, y de acuerdo con qué calidades y opciones.

C.1.2 Procedimiento de alta

Antes del alta como suscriptor, EADTrust debe informar al suscriptor de los términos y condiciones aplicables al servicio (ETSI TS 102023, sección 7.1.1.e).

La citada información se comunicará en soporte duradero, en papel o electrónicamente y en lenguaje fácilmente comprensible, y tendrá los siguientes contenidos mínimos (ETSI TS 102023, sección 7.1.2):

- ✓ La información de contacto de la Entidad de Sellado de Tiempo.
- ✓ La política de sellado de tiempo aplicable.
- ✓ Al menos un algoritmo de resumen criptográfico que se pueda emplear para representar los datos para los que se solicita el sello de tiempo.
- ✓ El periodo previsto de vida de la firma electrónica empleada para firmar el sello de tiempo (Esta duración dependerá del algoritmo de resumen, algoritmo de firma y longitud de clave privada empleados por la Entidad de Sellado de Tiempo).
- ✓ La precisión del tiempo del sello, con respecto al Tiempo Universal Coordinado.
- ✓ La disponibilidad del servicio, incluyendo los tiempos previstos de recuperación y de parada programados.
- ✓ Cualesquiera limitaciones en el uso del servicio de sellado de tiempo.
- ✓ Las obligaciones del suscriptor del servicio de sellado de tiempo.
- ✓ Las obligaciones del tercero que confía en sellos de tiempo.
- ✓ Información sobre cómo verificar el sello de tiempo, de forma que el tercero pueda decidir de forma razonable confiar o no en el mismo, así como cualesquiera limitaciones en el periodo de validez del sello.
- ✓ El periodo durante el cual la Entidad de Sellado de Tiempo retiene registros de auditoría.
- ✓ El sistema jurídico que resulte aplicable a la prestación del servicio, incluyendo el cumplimiento de los requisitos establecidos por la legislación aplicable.
- ✓ Limitaciones de responsabilidad.
- ✓ Procedimientos de reclamaciones y resolución de disputas.

- ✓ Si la Entidad de Sellado de Tiempo ha sido declarada conforme con la política de sellado aplicable, y en este caso, por qué organismo independiente.

Tras la adhesión a las condiciones generales del servicio por el suscriptor, EADTrust procederá a su alta en el sistema, habilitando los medios técnicos para recibir solicitudes de sello.

EADTrust soportará protocolos de transporte (RFC 3161, sección 3) de las solicitudes de sellado de tiempo que sean síncronos o asíncronos, y entre ellos, al menos dispondrá de la posibilidad de solicitar el servicio empleando HTTP (ETSI TS 101861, sección 6).

C.2 Procesamiento de la solicitud de sello de tiempo

Una vez recibida una solicitud de sello de tiempo, EADTrust debe verificar los siguientes aspectos:

- La procedencia y la autenticidad de la solicitud, mediante el protocolo de seguridad apropiado al medio de transporte empleado, incluyendo al menos SSL/TLS para el protocolo HTTP (RFC 3161 no establece ningún método para autenticar al solicitante de sellos, sino que esta posibilidad debe implantarse mediante la seguridad del protocolo de transporte de las solicitudes, como es HTTPS).
- La corrección técnica (RFC 3161, sección 2.4.1) de la solicitud, de acuerdo con el protocolo escogido y, en concreto, que la solicitud contiene:
  - ✓ El número de versión.
  - ✓ Un resumen criptográfico válido conforme a uno de los algoritmos apropiados, según se expone posteriormente.
  - ✓ Opcionalmente, el número de ocurrencia única (*nonce*), generado por el suscriptor.
- Se considerarán válidos los siguientes algoritmos de resumen (ETSI TS 101861, sección 4.2.2, con exclusión de MD5 por su pérdida de robustez desde el momento de aprobación de la especificación técnica): SHA-1 (obligatoriamente) y RIPEMD-160 (opcionalmente), con exclusión expresa de MD5 y otros algoritmos.
- La solicitud no deberá contener extensiones (ETSI TS 101861, sección 4.2.1).

En caso de verificación incorrecta de la solicitud, se devolverán los mensajes de error apropiados (RFC 3161, sección 2.4.2).

C.3 Emisión del sello de tiempo

Tras la verificación de la solicitud se procederá a la emisión del sello de tiempo, de forma segura.

EADTrust deberá (ETSI TS 102023, sección 7.3.1):

- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de sellado de tiempo a los que sirven de soporte.
- Emplear fuentes de tiempo fiables, de acuerdo con los requisitos establecidos en la sección de esta política.
- Generar sellos de tiempo conteniendo las informaciones incluidas en la sección F de esta política.
- Emplear una clave específica para la firma de los sellos generados, de acuerdo con los requisitos de gestión de claves especificados en la sección E de esta política.

C.4 Entrega del sello de tiempo

C.4.1 Entrega del sello de tiempo

EADTrust deberá entregar el sello al solicitante, mediante el protocolo de transporte empleado para la solicitud.

La respuesta protocolaria deberá contener el resultado de la solicitud y, en su caso, el sello emitido (RFC 3161, sección 2.4.2).

C.4.2 Publicación del sello de tiempo

EADTrust publicará el sello, siempre que el subscriptor haya dado su consentimiento, en el Repositorio a que se refiere la sección B.1 de esta política, con los controles de acceso pertinentes.

C.4.3 Notificación de la emisión a terceros

EADTrust podrá establecer casos y métodos en que se notifique la emisión a terceros, de acuerdo con las necesidades de los suscriptores.

C.5 Finalización de la suscripción

Transcurrido el plazo contractualmente establecido, finalizará la suscripción al servicio, y no se podrán seguir solicitando sellos de tiempo.

D. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

EADTrust deberá implantar los siguientes controles:

- Seguridad física (ETSI TS 102023, sección 7.4.4).
- Gestión de la seguridad (ETSI TS 102023, secciones 7.4.1, 7.4.2 y 7.4.5).
- Personal (ETSI TS 102023, sección 7.4.3)
- Auditoría de seguridad (ETSI TS 102023, sección 7.4.11).
- Archivo de operaciones (ETSI TS 102023, sección 7.4.11).
- Renovación de claves (ETSI TS 102023, sección 7.2.4).
- Compromiso de claves y recuperación de desastre (ETSI TS 102023, sección 7.4.8).
- Terminación del servicio (ETSI TS 102023, sección 7.4.8).

D.1 Controles de seguridad física

EADTrust debe disponer de instalaciones que protejan físicamente la prestación del servicio de sellado de tiempo del compromiso causado por acceso no autorizado a los sistemas o a los datos.

La protección física se logrará mediante la creación de perímetros de seguridad claramente definidos en torno al servicio, pudiendo compartirse estos espacios con los restantes servicios que presta EADTrust

EADTrust establecerá controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones.

La política de seguridad física y ambiental aplicable al servicio de sellado de tiempo deberá establecer prescripciones para las siguientes contingencias:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobos.
- Allanamiento y entrada no autorizada.
- Recuperación del desastre.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para el servicio de sellado de tiempo.

D.1.1 Localización y construcción de las instalaciones

La localización de las instalaciones debe permitir la presencia de fuerzas de seguridad en un plazo de tiempo razonablemente inmediato desde que una incidencia fuera notificada a los mismos (en el caso de no contar con presencia física permanente de personal de seguridad del prestador de servicios de certificación)

La calidad y solidez de los materiales de construcción de las instalaciones deberá garantizar unos adecuados niveles de protección frente a intrusiones por la fuerza bruta.

D.1.2 Acceso físico

EADTrust deberá establecer al menos cuatro (4) niveles de seguridad con restricción de acceso a los diferentes perímetros y barreras físicas definidas.

Para el acceso a las dependencias donde se lleven a cabo procesos relacionados con el ciclo de vida del sello de tiempo, será necesaria la autorización previa, identificación en el momento del acceso y registro del mismoEsta identificación, ante el sistema de control de accesos, deberá realizarse mediante reconocimiento de algún parámetro biométrico del individuo, excepto en caso de visitas escoltadas.

La generación de claves criptográficas de las Entidades de Sellado de Tiempo, así como su almacenamiento, deberá realizarse en dependencias específicas para estos fines, y requerirán de acceso y permanencia duales.

D.1.3 Electricidad y aire acondicionado

Los equipos informáticos deberán estar convenientemente protegidos ante fluctuaciones o cortes del suministro eléctrico, que pudieran dañarlos o interrumpir el servicio.

Las instalaciones contarán con un sistema de estabilización de la corriente, así como de un sistema de generación propio con autonomía suficiente para mantener el suministro durante el tiempo que requiera el cierre ordenado y completo de todos los sistemas informáticos.

Los equipos informáticos deberán estar ubicados en un entorno donde se garantice una climatización (temperatura y humedad) adecuada a sus condiciones óptimas de trabajo.

D.1.4 Exposición al agua

EADTrust deberá disponer de sistemas de detección de inundaciones adecuados para proteger los equipos y activos ante tal eventualidad, en el caso de que las condiciones de ubicación de las instalaciones lo hagan necesario.

D.1.5 Prevención y protección de incendios

Todas las instalaciones y activos de EADTrust deben contar con sistemas automáticos de detección y extinción de incendios.

En concreto, los dispositivos criptográficos y los soportes que almacenen claves, deberán contar con un sistema específico y adicional al resto de la instalación, para la protección frente al fuego.

D.1.6 Almacenamiento de soportes

El almacenamiento de soportes de información debe realizarse de forma que se garantice tanto su integridad como su confidencialidad, de acuerdo con la clasificación de la información que se haya establecido.

Deberá contarse para ellos con dependencias o armarios ignífugos.

El acceso a estos soportes, incluso para su eliminación, deberá estar restringido a personas específicamente autorizadas.

D.1.7 Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se deberá realizar mediante mecanismos que garanticen la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se procederá al formateo, borrado permanente, o destrucción física del soporte.

En el caso de documentación en papel, éste deberá someterse a un tratamiento físico de destrucción.

D.1.8 Copia de respaldo fuera de las instalaciones

Periódicamente, EADTrust almacenará copia de respaldo de los sistemas de información, en dependencias físicamente separadas de aquellas en las que se encuentran los equipos.

D.2 Controles de gestión

EADTrust debe garantizar que sus sistemas se operan de forma segura, para lo cual deberá establecer e implantar procedimientos para las funciones que afecten a la provisión de sus servicios.

D.2.1 Funciones fiables

EADTrust deberá identificar funciones o roles con la condición de fiables.

Las personas que deban ocupar tales puestos deberán ser formalmente nombrados por la alta dirección EADTrust.

Las funciones fiables deberán incluir:
- ✓ Personal responsable de la seguridad.
- ✓ Administradores del sistema.
- ✓ Operadores del sistema.

✓ Auditores del sistema.

Las funciones fiables deberán realizarse teniendo en cuenta que debe existir una separación de funciones sensibles, así como una concesión de mínimo privilegio, cuando sea posible.

Para determinar la sensibilidad de la función, se tendrán en cuenta los siguientes elementos:

✓ Deberes asociados a la función.
✓ Nivel de acceso.
✓ Monitorización de la función.
✓ Formación y concienciación.
✓ Habilidades requeridas.

EADTrust deberá identificar y autenticar al personal antes de acceder a la correspondiente función fiable.

D.2.2 Roles que requieren separación de tareas

Las siguientes tareas deberán ser realizadas, al menos, por dos personas:

✓ Gestión del acceso físico.
✓ Gestión de aplicaciones informáticas de la Entidad de Sellado de Tiempo.
✓ Gestión de bienes de equipo criptográfico.
✓ Gestión de claves de la Entidad de Sellado de Tiempo.
✓ Gestión de configuración y control de cambios.
✓ Gestión del archivo.

D.3 Controles de personal

D.3.1 Requisitos de historial, calificaciones, experiencia y autorización

EADTrust deberá emplear personal cualificado y con la experiencia necesaria, para la prestación de los servicios ofrecidos, en el ámbito del sellado de tiempo, la firma electrónica y los procedimientos de seguridad y de gestión adecuados.

Este requisito se aplicará al personal de gestión, especialmente en relación con procedimientos de personal de seguridad.

La calificación y la experiencia podrán suplirse mediante una formación y entrenamiento apropiados.

El personal en puestos fiables deberá encontrarse libre de intereses personales que entre en conflicto con el desarrollo de la función que tenga encomendada.

No se podrá asignar a un puesto fiable o de gestión a una persona que no sea idóneo para el puesto, especialmente por haber sido condenada por delito o falta que afecte a su idoneidad para el puesto. Por este motivo, se

deberá realizar una investigación, de acuerdo con lo establecido en la sección siguiente, relativa a los siguientes aspectos:

- ✓ Estudios, incluyendo titulación alegada.
- ✓ Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales y comprobación de que realmente se hizo el trabajo alegado.

D.3.2 Procedimientos de investigación de historial

EADTrust deberá realizar la investigación antes de que la persona sea contratada y/o acceda al puesto de trabajo.

En la solicitud para el puesto de trabajo se informará acerca de la necesidad de someterse a una investigación previa.

Se deberá advertir de que la negativa a someterse a la investigación implicará el rechazo de la solicitud.

Se deberá obtener consentimiento inequívoco del afectado por la investigación previa y procesar y proteger todos sus datos personales de acuerdo con la LOPD y el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos.

D.3.3 Requisitos de formación

EADTrust deberá formar al personal en puestos fiables y de gestión, hasta que alcancen la cualificación necesaria, de acuerdo con lo establecido en la sección D.3.1 de esta política.

La formación deberá incluir los siguientes contenidos:

- ✓ Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- ✓ Versiones de maquinaria y aplicaciones en uso.
- ✓ Tareas que debe realizar la persona.
- ✓ Gestión y tramitación de incidentes y compromisos de seguridad.
- ✓ Procedimientos de continuidad de negocio y emergencia.

EADTrust deberá realizar una actualización en la formación del personal al menos cada dos años.

D.3.4 Secuencia y frecuencia de rotación laboral

EADTrust podrá establecer métodos de rotación laboral para la prestación del servicio en turnos, con el objeto de cubrir las necesidades de 24x7 del servicio.

D.3.5 Sanciones para acciones no autorizadas

EADTrust deberá disponer de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, que deberá encontrarse adecuado a la legislación laboral aplicable y, en especial,

coordinado con el sistema sancionador del convenio colectivo que resulte de aplicación al personal.

Las acciones disciplinarias podrán incluir la suspensión y el despido de la persona responsable de la acción dañina.

D.3.6 Requisitos de contratación de profesionales externos

EADTrust podrá contratar profesionales externos a EADTrust para cualquier función, incluso para un puesto fiable, en cuyo caso deberá someterse a los mismos controles que los restantes empleados.

En el caso de que el profesional no deba someterse a tales controles, deberá estar constantemente acompañado por un empleado fiable, cuando se encuentre en las instalaciones de EADTrust.

D.3.7 Suministro de documentación al personal

EADTrust suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de que sea suficientemente competente a tenor de lo establecido en la sección D.3.1 de esta política.

D.4 Procedimientos de auditoría de seguridad

D.4.1 Tipos de eventos registrados

EADTrust debe guardar registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- ✓ Encendido y apagado de los sistemas.
- ✓ Inicio y terminación de la aplicación de autoridad de sellado de tiempo.
- ✓ Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema.
- ✓ Generación y cambios en las claves de la Entidad de Sellado de Tiempo.
- ✓ Operaciones que afecten a los relojes.
- ✓ Cambios en las políticas de emisión de sellos de tiempo.
- ✓ Intentos de entrada y salida del sistema.
- ✓ Intentos no autorizados de entrada en la red de la Entidad de Sellado de Tiempo.
- ✓ Intentos no autorizados de acceso a los ficheros del sistema.
- ✓ Intentos fallidos de lectura en un sello custodiado, y de lectura y escritura en el Repositorio.
- ✓ Eventos relacionados con el ciclo de vida del sello, como solicitud, emisión o publicación en el Repositorio.
- ✓ Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación del mismo.

EADTrust debe también guardar, ya sea manual o electrónicamente, la siguiente información:

- ✓ La ceremonia de generación de claves y las bases de datos de gestión de claves.
- ✓ Los registros de acceso físico.
- ✓ Mantenimientos y cambios de configuración del sistema.
- ✓ Cambios en el personal.
- ✓ Informes de compromisos y discrepancias.
- ✓ Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor o del poseedor de claves.
- ✓ Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Sellado de Tiempo.

D.4.2 Frecuencia de tratamiento de registros de auditoría

Los registros de auditoría se examinarán por lo menos una vez a la semana en busca de actividad sospechosa o no habitual.

El procesamiento de los registros de auditoría consistirá en una revisión de los registros la cual incluye la verificación de que los registros no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros.

Las acciones llevadas a cabo a partir de la revisión de auditoría también deben ser documentadas.

D.4.3 Periodo de conservación de registros de auditoría

Los registros de auditoría se deben retener en el recinto durante por lo menos dos meses después de procesarlos y a partir de ese momento se archivarán de acuerdo con la sección D.5.2 de esta política.

D.4.4 Protección de los registros de auditoría

Los ficheros de registros, tanto manuales como electrónicos, deben protegerse de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico.

D.4.5 Procedimientos de copia de respaldo

Se deberán generar, al menos, copias incrementales de respaldo de registros de auditoría diariamente y copias completas semanalmente.

D.4.6 Localización del sistema de acumulación de registros de auditoría

El sistema de acumulación de registros de auditoría deberá ser, al menos, un sistema interno de EADTrust, compuesto por los registros de la aplicación, por los registros de red y por los registros del sistema operativo, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado.

D.4.7 Notificación del evento de auditoría al causante del evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no será preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

Se podrá comunicar si el resultado de su acción ha tenido éxito o no, pero no que se ha auditado la acción.

D.4.8 Análisis de vulnerabilidades

Los eventos en el proceso de auditoría deberán ser guardados, en parte, para monitorizar las vulnerabilidades del sistema.

Los análisis de vulnerabilidad deben ser ejecutados, repasados y revisados a través de un examen de esos eventos monitorizados.

Estos análisis deben ser ejecutados diariamente, mensualmente y anualmente de acuerdo con su definición en el plan de auditoría o documento que lo sustituya, de EADTrust.

D.5 Archivo de informaciones

EADTrust debe garantizar que toda la información relativa a los sellos de tiempo se guarda durante un período de tiempo apropiado, según lo establecido en la sección D.5.2 de esta política.

D.5.1 Tipos de eventos registrados

EADTrust debe guardar todos los eventos que tengan lugar durante el ciclo de vida de un sello de tiempo, incluyendo la renovación del mismo.

Se debe guardar un registro de lo siguiente:

- ✓ Altas y bajas de suscriptores.
- ✓ Listados de sellos emitidos.
- ✓ Los sellos custodiados, cuando se preste el servicio.

D.5.2 Periodo de conservación de registros

EADTrust debe guardar los registros especificados en la sección anterior de esta política de forma permanente, con un mínimo de quince (15) años.

D.5.3 Protección del archivo

EADTrust debe:

- ✓ Mantener la integridad y la confidencialidad del archivo que contiene los datos referentes a los sellos emitidos.
- ✓ Archivar los datos anteriormente citados de forma completa y confidencial.
- ✓ Mantener la privacidad de los datos del suscriptor.

D.5.4 Procedimientos de copia de respaldo

EADTrust debe realizar copias de respaldo incrementales diarias de todos sus documentos electrónicos, según la sección D.5.1 de esta política. Debe, además, realizar copias de respaldo completas semanalmente para casos de recuperación de datos, de acuerdo con la sección D.7 de esta política.

D.5.5 Localización del sistema de archivo

EADTrust debe disponer de un sistema de mantenimiento de datos de archivo tal y como se especifica en la sección D.5.4 de esta política.

D.5.6 Procedimientos de obtención y verificación de información de archivo

Sólo personas autorizadas por EADTrust podrán tener acceso a los datos de archivo, ya sea en las mismas instalaciones de EADTrust o en su ubicación externa.

D.6 Renovación de claves

EADTrust deberá establecer un plan de renovación programada de las claves de las Entidades de Sellado de Tiempo, que garantice la continuidad de los servicios.

D.7 Compromiso de claves y recuperación de desastre

D.7.1 Corrupción de recursos, aplicaciones o datos

Cuando tenga lugar un evento de corrupción de recursos, aplicaciones o datos, EADTrust debe iniciar las gestiones necesarias, de acuerdo con el plan de seguridad, el plan de emergencia y el plan de auditoría, o documentos que los sustituyan, para hacer que el sistema vuelva a su estado normal de funcionamiento.

D.7.2 Revocación de la clave pública de la entidad

En el caso de que EADTrust deba revocar la clave pública de una Entidad de Sellado de Tiempo, deberá llevar a cabo lo siguiente:

- ✓ Desactivar el uso de la clave privada de la Entidad de Sellado de Tiempo.
- ✓ Solicitar la revocación y seguir los procedimientos correspondientes descritos en la Declaración de Prácticas de Certificación para los certificados de Entidad de Sellado de Tiempo.

- ✓ Realizar todos los esfuerzos necesarios para informar de la revocación a todos los suscriptores a los cuales EADTrust haya emitido sellos, así como a los terceros, mediante la publicación de la revocación en el repositorio.
- ✓ Realizar una renovación de claves, en caso de que la revocación no haya sido debida a la terminación del servicio por parte de EADTrust, según lo establecido en la sección D.6 de esta política.

D.7.3 Compromiso de la clave privada de la entidad

EADTrust debe considerar el compromiso o la sospecha de compromiso de la clave privada de las Entidades de Sellado de Tiempo como un desastre.

En caso de compromiso, EADTrust debe realizar como mínimo las siguientes acciones:

- ✓ Informar a todos los suscriptores y terceros del compromiso.
- ✓ Indicar que los sellos que han sido entregados usando la clave de esta Entidad de Sellado de Tiempo ya no son válidos.

D.7.4 Desastre sobre las instalaciones

EADTrust debe desarrollar, mantener, probar y, si es necesario, ejecutar un plan de emergencia para el caso de que ocurra un desastre, ya sea por causas naturales o causado por el hombre, sobre las instalaciones, el cual indique cómo restaurar los servicios de los sistemas de información.

La ubicación de los sistemas de recuperación de desastres debe disponer de las protecciones físicas de seguridad detalladas en el plan de seguridad.

EADTrust debe ser capaz de restaurar la operación normal de los servicios de sellado de tiempo, en las 24 horas siguientes al desastre.

La base de datos de recuperación de desastres utilizada por EADTrust debe estar sincronizada con la base de datos de producción, dentro de los límites temporales especificados en el plan de seguridad.

D.8 Terminación del servicio

EADTrust debe asegurar que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios de la Entidad de Sellado de Tiempo y, en particular, asegurar un mantenimiento continuo de los sellos custodiados que sean requeridos para proporcionar evidencia en caso de investigación civil o criminal.

Antes de terminar sus servicios, EADTrust debe ejecutar, como mínimo, los siguientes procedimientos:

- Informar a todos los suscriptores y terceros que confían en sellos.
- Retirar toda autorización de subcontrataciones que actúan en su nombre en el proceso de emisión de sellos.
- Ejecutar las tareas necesarias para transferir las obligaciones de mantenimiento de los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros que confían en sellos.
- Destruir las claves privadas de la Entidad de Sellado de Tiempo.

EADTrust debe declarar en sus prácticas las previsiones que tiene para el caso de terminación del servicio. Estas deben incluir:

- Notificación a las entidades afectadas.
- Transferencia de sus obligaciones a otras personas.

E. CONTROLES DE SEGURIDAD TÉCNICA

EADTrust deberá emplear sistemas y productos fiables (ETSI TS 102023, sección 7.4.7), que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de sellado de tiempo a los que sirven de soporte.

Asimismo, debe garantizar el empleo de fuentes de tiempo fiables para garantizar la precisión del sello.

E.1 Fiabilidad de la fuente de tiempo

Los valores de tiempo incluidos en los sellos serán trazables al menos a un valor de tiempo real distribuido por un laboratorio oficial de Tiempo Universal Coordinado, debiéndose consultar en primer lugar al Real Observatorio de la Armada.

EADTrust debe asegurar que el reloj de las Entidades de Sellado de Tiempo se encuentra sincronizado con Tiempo Universal Coordinado con la precisión declarada en el sello (ETSI TS 102023, sección 7.3.2).

- La calibración de los relojes debe ser mantenida de forma que no resulte previsible un desplazamiento en el tiempo de los mismos.
- Los relojes serán protegidos contra amenazas que pudieran resultar en un cambio no detectado que descalibre el reloj.
- Se asegurará que se detectarán los desplazamientos y saltos del reloj, que impidan su sincronización con Tiempo Universal Coordinado.
- Se asegurará que se mantiene la sincronización del reloj cuando se notifica un segundo de salto, notificado por el órgano competente.

E.2 Generación e instalación del par de claves

E.2.1 Generación del par de claves

Los pares de claves de las Entidades de Sellado de Tiempo deben ser generados empleando hardware criptográfico (ETSI TS 102023, sección 7.2.1) que cumpla ISO 15408: EAL 4 (o superior), de acuerdo con lo establecido en CEN CWA 14167 parte 2, según proceda, o de acuerdo con un objetivo de seguridad o perfil de protección equivalente; o FIPS 140-2 Nivel 3 (o superior).

E.2.2 Envío de la clave pública al emisor del certificado

La clave pública de la Entidad de Sellado de Tiempo será certificada por EADTrust.

El método de remisión de la clave pública a la Entidad de Certificación será PKCS #10, otra prueba criptográfica equivalente o cualquier otro método aprobado por EADTrust.

E.2.3 Distribución de la clave pública de la Entidad de Sellado de Tiempo

Las claves de las Entidades de Sellado de Tiempo deben ser comunicadas a los terceros que confían en sellos, asegurando la integridad de la clave y autenticando su origen.

La clave pública de cada Entidad de Sellado de Tiempo se publicará en el Repositorio, en forma de certificado firmado por una Entidad de Certificación de EADTrust, junto a una declaración referente a que la clave autentica a la Entidad de Sellado de Tiempo.

Los usuarios podrán acceder al Repositorio para obtener las claves públicas de las Entidades de Sellado de Tiempo.

Adicionalmente, en aplicaciones S/MIME, el mensaje de datos podrá contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

E.2.4 Longitudes de claves

La longitud de las claves de las Entidades de Sellado de Tiempo será al menos de 1024 bits (ETSI TS 101861, sección 5.2.4), recomendándose el empleo de claves de al menos 2048 bits.

E.3 Protección de la clave privada

E.3.1 Estándares de módulos criptográficos

Para los módulos que gestionan claves de las Entidades de Sellado de Tiempo se deberá asegurar el nivel exigido por los estándares indicados en las secciones anteriores.

E.3.2 Control por más de una persona sobre la clave privada

El acceso de operación a las claves privadas de las Entidades de Sellado de Tiempo deberá requerir necesariamente del concurso sucesivo de más de una persona que tendrá el role o bien de custodio de un dispositivo criptográfico o bien de conocedor de una clave de acceso.

Los dispositivos criptográficos quedarán almacenados en las dependencias de EADTrust, y para su acceso será necesaria una persona adicional.

E.3.3 Repositorio de la clave privada

Las claves privadas de las Entidades de Certificación se almacenarán en espacios ignífugos y protegidos por controles de acceso físico dual.

E.3.4 Copia de respaldo de la clave privada

No se podrán realizar copias de respaldo de las claves privadas de las Entidades de Sellado de Tiempo (ETSI TS 102023, sección 7.2.1).

Cuando las claves se almacenen en un módulo hardware de proceso dedicado, deberán proveerse los controles oportunos para que éstas nunca puedan abandonar el dispositivo.

E.3.5 Archivo de la clave privada

No se archivarán claves privadas de Entidades de Sellado de Tiempo.

E.3.6 Introducción de la clave privada en el módulo criptográfico

Las claves privadas se podrán generar directamente en los módulos criptográficos o en módulos criptográficos externos, de los que se exportarán las claves cifradas para su introducción en los módulos de producción.

En este caso, las claves privadas de las Entidades de Sellado de Tiempo quedarán almacenadas en ficheros cifrados con claves fragmentadas y en dispositivos criptográficos (de las que no podrán ser extraídas).

Dichos dispositivos serán empleados para introducir la clave privada en el módulo criptográfico.

E.3.7 Método de activación de la clave privada

La clave privada de cada Entidad de Sellado de Tiempo se activará mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección E.3.2.

E.3.8 Método de desactivación de la clave privada

La desactivación de la clave privada se producirá en los casos de apagado del módulo criptográfico, o mediante los procedimientos soportados por el módulo criptográfico.

E.3.9 Método de destrucción de la clave privada

Las claves privadas serán destruidas en una forma que impida su robo, modificación, divulgación no autorizada o uso no autorizado.

E.4 Otros aspectos de gestión del par de claves

E.4.1 Archivo de la clave pública

Las Entidades de Sellado de Tiempo archivarán sus claves públicas de forma permanente, de acuerdo con lo establecido en la sección D.5 de esta política.

E.4.2 Periodos de utilización de las claves pública y privada

Los periodos de utilización de las claves serán los determinados por la duración del certificado de la Entidad de Sellado de Tiempo, transcurrido el cual no podrán continuar utilizándose.

Dicho periodo no podrá ser superior al periodo previsto de validez criptográfica del algoritmo y longitud de clave empleados para la producción de sellos (ETSI TS 102023, sección 7.2.4).

E.5 Controles de seguridad informática

E.5.1 Requisitos técnicos específicos de seguridad informática

Se deberá garantizar que el acceso los sistemas está limitado a individuos debidamente autorizados (ETSI TS 102023, sección 7.4.6). En particular:

- ✓ Se debe garantizar una administración efectiva del nivel de acceso de los usuarios (operadores, administradores, así como cualquier usuario con acceso directo al sistema) para mantener la seguridad del sistema, incluyendo gestión de cuentas de usuarios, auditoría y modificaciones o denegación de acceso oportunas.
- ✓ Se debe garantizar que el acceso a los sistemas de información y aplicaciones se restringe de acuerdo a lo establecido en la política de control de acceso, así como que los sistemas proporcionan los controles de seguridad suficientes para implementar la segregación de funciones identificada en las prácticas, incluyendo la separación de funciones de administración de los sistemas de seguridad y de los operadores. En concreto, el uso de programas de utilidades del sistema estará restringido y estrechamente controlado.
- ✓ El personal deberá ser identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del sello de tiempo.
- ✓ El personal será responsable y deberá poder justificar sus actividades, por ejemplo mediante un archivo de eventos.
- ✓ Deberá evitarse la posibilidad de revelación de datos sensibles mediante la reutilización de objetos de almacenamiento (por ejemplo ficheros borrados) que queden accesibles a usuarios no autorizados.
- ✓ Los sistemas de seguridad y monitorización deben permitir una rápida detección, registro y actuación ante intentos de acceso irregular o no autorizado a sus recursos (por ejemplo, mediante sistema de detección de intrusiones, monitorización y alarma)
- ✓ El acceso a los repositorios públicos de la información deberá contar con un control de accesos para modificaciones o borrado de datos.

E.5.2 Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de sellado de tiempo empleadas por EADTrust deberán ser fiables.

E.6 Controles técnicos del ciclo de vida

E.6.1 Controles de desarrollo de sistemas

Se deberá realizar un análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente

empleado en las aplicaciones de sellado de tiempo, para garantizar que los sistemas son seguros.

Se emplearán procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

E.6.2 Controles de gestión de seguridad

EADTrust deberá mantener un inventario de todos los activos informativos y realizará una clasificación de los mismos, de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración de los sistemas se auditará de forma periódica, de acuerdo con lo establecido en la sección G.1.1 de esta política.

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

E.6.3 Evaluación del nivel de seguridad del ciclo de vida

EADTrust se someterá a evaluaciones independientes, auditorías y, en su caso, certificaciones de seguridad del ciclo de vida de los productos que emplea.

E.7 Controles de seguridad de red

Se deberá garantizar que el acceso a las diferentes redes de EADTrust está limitado a individuos debidamente autorizados. En particular:

- Deben implementarse controles para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos deberán configurarse de forma que se impidan accesos y protocolos que no sean necesarios para la operación de la Entidad de Sellado de Tiempo.
- Los datos sensibles deberán protegerse cuando se intercambien a través de redes no seguras (incluyendo como tales los datos de registro del suscriptor)
- Se debe garantizar que los componentes locales de red se encuentran ubicados en entornos seguros, así como la auditoría periódica de sus configuraciones.

E.8 Controles de ingeniería de módulos criptográficos

Se debe garantizar que las claves de las Entidades de Sellado de Tiempo son generadas en equipamientos criptográficos, que cumplan los estándares criptográficos de seguridad que se han indicado en las secciones anteriores.

F. PERFILES DE SELLOS DE TIEMPO

Los sellos tendrán el contenido y campos descritos en esta sección, incluyendo, como mínimo, los siguientes (RFC 3161, sección 2.4.2; ETSI TS 101861, sección 5.2.1):

- Número de versión del sello.
- Indicador de política de sellado de tiempo.
- Resumen criptográfico del objeto sellado.
- Número de serie.
- Tiempo del sello.
- Precisión.
- Identificación de la Entidad de Sellado de Tiempo.

No se emplearán ni el campo Ordenación

EADTrust publicará sus perfiles de sellos en el Repositorio indicado en la sección B.

G. AUDITORIA DE CONFORMIDAD

EADTrust debe realizar periódicamente una auditoría de cumplimiento para probar que cumple, una vez ha empezado a funcionar, los requisitos de seguridad y de operación necesarios para cumplir la política de los servicios de sellado de tiempo.

G.1.1 Frecuencia de la auditoria de conformidad

Se debe llevar a cabo una auditoría de conformidad anualmente o en cualquier momento, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de claves. Estas auditorías podrán ser internas o externas.

G.1.2 Identificación y calificación del auditor

Si EADTrust dispone de un departamento de auditoría interno, éste podrá encargarse de llevar a cabo la auditoría de conformidad.

En el caso de no poseer ese departamento, o de considerarse oportuno, se deberá acudir a un auditor independiente, el cual debe demostrar experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública y sellada de tiempo.

G.1.3 Relación del auditor con la entidad auditada

Las auditorías de conformidad ejecutadas por terceros deben ser llevadas a cabo por una entidad independiente de EADTrust, no debiendo tener ningún conflicto de intereses que menoscabe su capacidad de llevar a cabo servicios de auditoría.

G.1.4 Listado de elementos objeto de auditoria

Los elementos objeto de auditoría serán los siguientes:

- ✓ Procesos de sellado de tiempo.
- ✓ Sistemas de información.
- ✓ Protección del centro de proceso
- ✓ Documentación del servicio.

Los detalles de cómo llevar a cabo la auditoría de cada uno de estos elementos se detallarán en el plan de auditoría de EADTrust.

G.1.5 Acciones a emprender como resultado de una falta de conformidad

Una vez recibido el informe de la auditoría de cumplimiento llevada a cabo, EADTrust debe discutir, con la entidad que ha ejecutado la auditoría y las deficiencias encontradas y desarrollar y ejecutar un plan correctivo que solvente dichas deficiencias.

Si EADTrust no es capaz de desarrollar y/o ejecutar el mencionado plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema deberá realizarse una de las siguientes acciones:

- ✓ Revocar la clave de las Entidades de Sellado de Tiempo, tal y como se describe en la sección D.7.2 de esta política.
- ✓ Terminar los servicios de sellado de tiempo, tal y como se describe en la sección 0 de esta política.

H. REQUISITOS COMERCIALES Y LEGALES

H.1 Tarifas

H.1.1 Tarifa de emisión o renovación de sellos

EADTrust podrá establecer una tarifa por la emisión o por la renovación de los sellos.

H.1.2 Tarifa de acceso a sellos

EADTrust no podrá establecer ninguna tarifa por el acceso a los sellos que en su caso se publiquen.

H.1.3 Tarifas de otros servicios

Sin estipulación.

H.1.4 Política de reintegro

EADTrust no podrá reintegrar las tarifas del servicio, excepto por funcionamiento erróneo, debiendo documentar en su Declaración de Prácticas de Certificación los casos en que se reintegrarán dichas tarifas.

H.2 Capacidad financiera

EADTrust deberá disponer de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios.

H.2.1 Otros activos

Sin estipulación.

H.2.2 Cobertura de seguro para suscriptores y terceros que confían en sellos

Sin estipulación.

H.3 Confidencialidad

H.3.1 Informaciones confidenciales

Las siguientes informaciones, como mínimo, serán mantenidas confidenciales por EADTrust:

- ✓ Sellos generados y almacenadas por EADTrust, cuando el suscriptor solicite la custodia sin publicación en el Repositorio.
- ✓ Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- ✓ Registros de auditoría interna y externa, creados y/o mantenidos por EADTrust y sus auditores.
- ✓ Planes de continuidad de negocio y de emergencia.
- ✓ Política y planes de seguridad.
- ✓ Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.

✓ Toda otra información identificada como "Confidencial".

H.3.2 Informaciones no confidenciales

La siguiente información será considerada no confidencial:

✓ La información contenida en el Repositorio.
✓ Toda otra información que no esté indicada en la sección anterior de esta política.

H.3.3 Divulgación legal de información

EADTrust divulgará la información confidencial en los casos legalmente previstos para ello.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el sello de tiempo serán divulgados en caso de ser requerido para ofrecer evidencia del sellado en caso de un procedimiento judicial, incluso sin consentimiento del suscriptor del servicio.

Se indicarán estas circunstancias en la política de intimidad prevista en la sección H.4 de esta política.

H.3.4 Divulgación de información por petición de su titular

EADTrust incluirá, en la política de intimidad prevista en la sección H.4 de esta política, prescripciones para permitir la divulgación de la información del suscriptor, directamente a los mismos o a terceros.

H.3.5 Otras circunstancias de divulgación de información

Sin estipulación.

H.4 Protección de datos personales

Para la prestación del servicio, EADTrust precisa recabar y almacenar ciertas informaciones, que incluyen informaciones personales. Tales informaciones serán recabadas directamente de los afectados, con su consentimiento explícito o en los casos es los que la ley permita recabar la información sin consentimiento del afectado.

Se recabarán los datos exclusivamente necesarios para la prestación del servicio de sellado de tiempo.

EADTrust no divulgará ni cederá datos personales, excepto en los casos previstos en las secciones H.3.2 a H.3.5 de esta política, y en la sección 0, en caso de terminación de la Entidad de Certificación.

La información confidencial de acuerdo con la LOPD será protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

H.5 Derechos de propiedad intelectual

EADTrust será propietaria de las Declaraciones de Prácticas de Certificación y de las Políticas de Sellado de Tiempo.

H.6 Obligaciones y responsabilidad civil

H.6.1 Obligaciones de EADTrust

EADTrust debe garantizar, bajo su plena responsabilidad, que cumple con todos los requisitos establecidos en cada política para la que emite sellos de tiempo.

Será la única entidad responsable del cumplimiento de los procedimientos descritos en esta política, incluso cuando una parte o la totalidad de las operaciones sean subcontratadas externamente.

EADTrust debe prestar sus servicios de sellado de tiempo conforme con su Declaración de Prácticas de Certificación vigente, en la que se detallarán sus funciones, procedimientos de operación y medidas de seguridad.

Se debe vincular a los suscriptores y a los terceros que confían en sellos mediante condiciones generales de emisión y uso, que deberán estar en lenguaje escrito y comprensible.

H.6.2 Garantías ofrecidas a suscriptores y terceros que confían en sellos

EADTrust, en las condiciones generales de emisión y uso, establecerá y rechazará garantías, y limitaciones de responsabilidad aplicables.

EADTrust, como mínimo, garantizará:

- ✓ Que los sellos de tiempo cumplen con todos los requisitos materiales establecidos de la Declaración de Prácticas de Certificación.
- ✓ Que el servicio de Repositorio cumple con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

H.6.3 Rechazo de otras garantías

EADTrust podrá rechazar toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección H.6.2.

H.6.4 Limitación de responsabilidades

EADTrust limitará su responsabilidad en las condiciones de esta política y en los acuerdos generales y/o particulares establecidos con los suscriptores.

H.6.5 Caso fortuito y fuerza mayor

EADTrust incluirá cláusulas para limitar su responsabilidad en caso fortuito y en caso de fuerza mayor, en las condiciones generales de emisión y uso.

H.6.6 Ley aplicable

EADTrust deberá establecer, en las condiciones generales de emisión y uso, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la ley española.

H.6.7 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

EADTrust deberá establecer, en las condiciones generales de emisión y uso, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- ✓ En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- ✓ En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, se velará porque, al menos los requisitos contenidos en las secciones H.6.1 (Obligaciones y responsabilidad), G (Auditoría de conformidad) y H.3 (Confidencialidad), continúen vigentes tras la terminación de los servicios.
- ✓ En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- ✓ En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

H.6.8 Cláusula de jurisdicción competente

EADTrust deberá establecer, en las condiciones generales de emisión y uso, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles.

La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

H.6.9 Resolución de conflictos

EADTrust deberá establecer, en las condiciones generales de emisión y uso, los procedimientos de mediación y resolución de conflictos aplicables.