European Agency of Digital Trust

Política de Sello de Tiempo

ÁREA DOCUMENTAL DE OPERACIONES

EADTrust Policy Committee

EADTRUST EUROPEAN AGENCY OF DIGITAL TRUST

Mayo 2021

Versión 5.0

Nota sobre derechos de autor

Versiones del documento

Esta publicación podría incluir inexactitudes técnicas o errores tipográficos.

Según evoluciona el estado de la técnica y el contexto legislativo, puede ser necesario incluir cambios en este documento, por lo que se recomienda comprobar en la página web de EADTrust la última versión de la publicación.

European Agency of Digital Trust puede realizar mejoras y cambios en los productos y en los programas descritos en esta publicación en cualquier momento.

Certificación ISO 9001. ISO 27001 e ISO 20000-1

EADTrust ha superado diversas auditorías, y, en particular las relativas a las normas ISO 9001. ISO 27001 e ISO 20000-1, con el siguiente alcance:

> *El Sistema Integrado de Gestión de la Información que da soporte a consultoría, auditoría, desarrollo y provisión de los siguientes servicios electrónicos de confianza: Autoridades de Certificación (PKI) que cumplen los requerimientos de las normas EN 319 401 v2.2.1, EN 319 411-1 v1.2.2, EN 319 411-2 v2.2.2, EN 319 421 v1.1.1 para Sellado de Tiempo, Emisión de Certificados, Validación de OCSP, Firma Electrónica Centralizada, Extensión de Firma Electrónica, Notificación Electrónica Fehaciente (Correo Electrónico Certificado), Publicación Electrónica Fehaciente, Comprobación fehaciente de contenidos digitales, Foro Electrónico de Accionistas, Emisión y Gestión de Claves, Cartulario (Custodia Digital de Documentos Electrónicos), Custodia de Evidencias Electrónicas (Retención de Datos), Voto Electrónico, Facturación Electrónica, Digitalización Certificada, Gestión de firma manuscrita digitalizada y Gestión de firma avanzada vocal, para garantizar la validez legal de todo tipo de gestiones que las utilizan, de acuerdo a la declaración de aplicabilidad vigente.*

Certificados

Norma	Certificado
ISO 20000-1:2011	10242586 / 10242587
ISO 27001:2013	10242584 / 10242585
ISO 9001:2015	10242588 / 10242589

Tabla de Contenidos

Control documental

Esta sección refleja la información del documento, sus propiedades y el historial de versiones.

TABLA1. HISTORIAL DE VERSIONES.

Versión	Fecha	Documentos sustituidos	Descripción
1.0	30/03/11	Ninguno	Política de sellado de tiempo
2.0	12/03/17	Versión 1	Sustitución completa debido a cambios regulatorios y cumplimiento con el Reglamento europeo UE 910/2014 (eIDAS).
2.1	12/06/18	Versión 1.2	Adecuación al Reglamento (UE) 679/2016 De Protección de Datos Personales (RGPD).
2.2	21/08/18	Versión 2.1	Modificación del perfil de persona jurídica para sellado de tiempo. Actualización de versiones a las que se hace referencia o de las normas EN 319 401, EN 319 411-1 y EN 319 411-2. Corrección de errores tipográficos.
2.3	17/05/2019	Versión 2.2	Nueva modificación del perfil de persona jurídica para sello de tiempo. Revisión de OID de política de sellado de tiempo. Corrección de errores tipográficos.
2.4	10/09/2019	Versión 2.3	Revisión total del documento por indicación del Auditor en correspondencia con ETSI EN 319 421
2.5	24/09/2019	Versión 2.4	Revisión de detalles del documento por indicación del Auditor en correspondencia con ETSI EN 319 421
3.0	25/11/2019	Versión 2.5	Revisión para consolidar todas las mejoras identificadas en la auditoria eIDAS y las versiones internas de este documento.
4.0	23/04/2020	Versión 3.0	Revisión y actualización de la política como parte del proceso de mejora continua
4.1	12/06/2020	Versión 4.0	Se introducen los oid de test
5.0	06/05/2021	Versión 4.1	Se introducen los OIDs de preproducción, producción y test y los endpoints. Revisión de los tipos de sellos de tiempo

TABLA2. HISTORIAL DE VERSIONES.

Propiedades del documento.	
Propietario	EADTrust European Agency of Digital Trust, S.L.
Fecha	6 de mayo de 2021

Distribución	Público
Nombre / Código	OPR-PC-V4.1-Sello_Tiempo_EADTrust

1.- Introducción

EADTrust European Agency of Digital Trust, S.L. (en adelante, EADTrust), es un Prestador de Servicios Electrónicos de Confianza radicado en Madrid, España, que opera bajo la supervisión del Ministerio de Economía y Empresa (Secretaría de Estado para el Avance Digital), si bien la denominación del organismo supervisor puede cambiar por criterios políticos e incluso adscribirse a diferente Ministerio.
En el ejercicio de su actividad empresarial EADTrust ha definido sus prácticas según los requisitos del REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios electrónicos de confianza para las transacciones electrónicas en el mercado interior y que deroga la Directiva 1999/93/CE (en adelante, eIDAS) y los estándares internacionales establecidos en ETSI, actualmente definidos como: ETSI EN 319 401; ETSI EN 319 421 "Electronic signatures and infraestructures (ESI); Policy and Security Requirements of trust Providers issuing Time-Stamps" y ETSI EN 319 422 "Electronic Signatures and Infraestructures (ESI); Time_stamping protocol and time-stamp token profiles".
EADTrust, presta servicios electrónicos de confianza cualificados (definidos en el Reglamento UE 910/2014) y no cualificados (basados en otros enfoques de uso de la criptografía y de la gestión de evidencias digitales). La indicación de servicios "no cualificados" simplemente identifica los servicios de confianza no previstos en el citado Reglamento eIDAS.
Estas prácticas también se estructuran y fundamentan en la Declaración de Prácticas de Certificación (DPC), la Política de Certificados (CP, en inglés) 6844 (IETF, 2013), y los Requisitos Básicos de la Política de Certificado para la Emisión y la Gestión de los Certificados de Confianza Pública (CA/ Browser Fórum, 2018).
Asimismo, en lo relacionado con el tratamiento de los datos personales recabados para la ejecución de este servicio, EADTrust S.L. se rige por lo establecido en el Reglamento General de Protección de Datos (conocido, abreviadamente, como RGPD). La denominación completa de la citada norma es “REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)”.También será de aplicación la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales (LOPD GDD). Además, se toma en consideración la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, (abreviadamente LSSI o LSSI-CE).

2.- Presentación

European Agency of Digital Trust como autoridad de Sello de Tiempo, (en lo adelante EADTrust o la TSA), podrá emitir diferentes tipos de sellos de tiempo descritos a continuación.

2.1.- Tipos de Sellado de Tiempo

2.1.1.- Sello de Tiempo Cualificado

El servicio de Sellado de Tiempo cualificado se suministrará a través de la TSA Madrid, desplegada en las instalaciones de EADTrust.

En el caso de los sellos de tiempo cualificados, es requisito del Reglamento eIDAS que se creen haciendo uso de firmas avanzadas lo que permite que estas estén basadas o no en certificados cualificados. EADTrust contempla en su servicio de sello de tiempo cualificado la posibilidad de usar diferentes tipos de certificados

(no cualificado, cualificado sin HSM, cualificado con HSM). En función del tipo de certificado seleccionado, los *endpoints* a los que se dirigirán las peticiones variarán.

EADTrust se compromete a mayores garantías de seguridad respecto a la gestión de los certificados utilizados en su TSU y en su gestión.

2.1.2.- Sello de Tiempo No Cualificado

EADTrust suministrará el servicio de Sellado de Tiempo no cualificado, a través de la TSA Dublín desplegada en Cloud. Este servicio tiene altas presunciones de veracidad técnica, ya que se gestiona de la misma manera que los servicios cualificados.

Asimismo, se ofrecerá también la posibilidad de consumir el servicio desde el CPD de EADTrust en Madrid. El uso de TSU en Madrid reduce los tiempos de latencia, pero no cuenta de la capacidad elástica de la TSU Dublín.

2.2.- Variantes del servicio

A los efectos de esta política, se establecen las siguientes variantes 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.

2.3.- 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
- Precisión del sello de tiempo, que por defecto será de un (1) segundo.
- Custodia del sello producido por EADTrust.

3.- 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. La vigente en la actualidad es la siguiente:

- La Política de Sellado de Tiempo (best practices policy for time-stamp) se identifica y referencia en ETSI OID 0.4.0.2023.1.1

El proveedor de servicios de confianza ha establecido diferentes OIDs para los diferentes tipos de sellos de tiempo emitidos (cualificados y no cualificados). Asimismo, ha establecido tres entornos (Preproducción, producción y test) con sus correspondientes OIDs para facilitar la puesta en marcha del servicio.

Igualmente, las peticiones de los sellos de tiempo se realizarán a su correspondiente *endpoint*, que varía en función del certificado utilizado para firmar el hash (no cualificado, cualificado sin HSM y cualificado con HSM).

A continuación, se presentan los OIDs y los *endpoints*:

1. Los OIDs y endpoints del Sello de Tiempo cualificado son:

Entorno	URL	Certificado usado	OID
TSU Preproducción	https://saturno-tsa.eadtrust.eu/qtnqc	No Cualificado	1.3.6.1.4.1.501.2.2.5
TSU Preproducción	https://saturno-tsa.eadtrust.eu/qtqc	Cualificado No HSM	1.3.6.1.4.1.501.2.2.5
TSU Preproducción	https://saturno-tsa.eadtrust.eu/qtqc-hsm	Cualificado HSM	1.3.6.1.4.1.501.2.2.5
TSU Producción	https://cronos-tsa.eadtrust.eu/qtnqc	No Cualificado	1.3.6.1.4.1.501.2.2.1
TSU Producción	https://cronos-tsa.eadtrust.eu/qtqc	Cualificado No HSM	1.3.6.1.4.1.501.2.2.1
TSU Producción	https://cronos-tsa.eadtrust.eu/qtqc-hsm	Cualificado HSM	1.3.6.1.4.1.501.2.2.1
TSU Test	https://tempus-tsa.eadtrust.eu/qtnqc	No Cualificado	1.3.6.1.4.1.501.2.2.3
TSU Test	https://tempus-tsa.eadtrust.eu/qtqc	Cualificado No HSM	1.3.6.1.4.1.501.2.2.3
TSU Test	https://tempus-tsa.eadtrust.eu/qtqc-hsm	Cualificado HSM	1.3.6.1.4.1.501.2.2.3

(ETSI-EN-319-421 REQ 8.1)

2. Los OIDs y endpoints del Sello de Tiempo no cualificado son:

Entorno	URL	Certificado usado	OID
TSU Preproducción	https://saturno-tsa.eadtrust.eu/nqtnqc	No Cualificado	1.3.6.1.4.1.501.2.2.4
TSU Producción	https://cronos-tsa.eadtrust.eu/nqtnqc	No Cualificado	1.3.6.1.4.1.501.2.2.0
TSU Producción (AWS)	https://eon-tsa.eadtrust.eu/nqtnqc	No Cualificado	1.3.6.1.4.1.501.2.2.0
TSU Test	https://tempus-tsa.eadtrust.eu/nqtnqc	No Cualificado	1.3.6.1.4.1.501.2.2.2
TSU Test (AWS)	https://jano-tsa.eadtrust.eu/nqtnqc	No Cualificado	1.3.6.1.4.1.501.2.2.2

(ETSI-EN-319-421 REQ 8.2)

Este árbol OID se identifica con el nombre de la plataforma de EADTrust de gestión de identidades SPRITEL (Secure Platform for Registered Identities and Trusted Electronic Ledger, Plataforma Segura para identidades registradas y Custodia Electrónica Confiable) base de la Autoridad de Registro de EADTrust.

4.- 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.

4.1.- Prestador de Servicios de Sellado de Tiempo

EADTrust puede operar diferentes TSU (timestamping Unit), que podrán desplegarse en las infraestructuras propias o en las instalaciones de las entidades cliente. Para ofrecer garantías de alta disponibilidad, continuidad de negocio, u otros criterios de seguridad que lo justifiquen.

Las características del sello de tiempo son las siguientes:

- Los algoritmos de hash soportados son los de la familia SHA-2
- La TSU emite sellos de tiempo, en referencia a UTC (tiempo universal coordinado) con una precisión mejor que 1 segundo. Se monitoriza esta precisión y se bloquea la posibilidad de emisión de sellos de tiempo si llega a ser peor de 1 segundo. Se tiene en cuenta la posibilidad de reflejar segundos intercalares si fuera necesario en el contexto de mantenimiento del patrón.
- Se limita el uso de los sellos de tiempo de EADTrust a la función de garantizar la existencia de ciertos datos electrónicos con anterioridad a un determinado momento y a su empleo por los organismos o entidades que lo hayan contratado. Un posible uso es el empleo de sellos de tiempo para crear versiones longevas de firmas electrónicas y sellos electrónicos aplicados a documentos electrónicos.
- EADTrust custodia de forma segura los sellos de tiempo expedidos, de forma que puede dar testimonio de su generación más allá del período de vigencia de los certificados, al margen de que los propios sellos de tiempo se incorporen a otros contextos de uso, como por ejemplo la extensión de firmas electrónicas.
- El subscriptor debe hacer uso del servicio mediante el mecanismo de autenticación proporcionado por EADTrust y cumplir sus compromisos de pago. En caso de instalación en sus infraestructuras, deberá proporcionar un sistema de alimentación eléctrica y de comunicaciones adecuado. Deberá configurar los firewalls de forma que permitan la administración remota.
- Los terceros que confían en los sellos de tiempo de EADTrust deberían ser capaces de comprobar los sellos de tiempo y los certificados que los acompañan. Las TSU solo emiten sellos de tiempo mientras el certificado está vigente y si fuera preciso revocarlo, se deja de usar la clave privada asociada. Aunque no se prevé que pueda quedar expuesta la clave privada, la consulta de la revocación de certificado permite descartar cualquier riesgo en ese sentido.

4.2.- 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:

a. Suscriptores de los servicios de sellado de tiempo.
b. Terceros que confían en los sellos emitidos.

4.2.1.- 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 período de suscripción.

4.2.2.- Terceros que confían en los sellos emitidos

5.- 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.

5.1.- 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).

6.- Límites y prohibiciones de uso

6.1.- 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.

6.2.- 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.

7.- Administración de la política

7.1.- Organización que administra el documento

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

7.2.- Datos de contacto de la organización

Nombre del PSC	European Agency of digital Trust, S. L.

Dirección	C/ Alba,15, 28043 Madrid-Spain
Dirección de mail	policy@eadtrust.eu
Teléfono	(+34) 902365612 / (+34) 917160555

8.- Publicación de Información y Repositorio de Sellos

8.1.- 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: www.eadtrust.eu.
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 de manera inmediata en los plazos que más adelante se describen en este documento y en Declaración de Prácticas de Servicios de Confianza.

8.2.- 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 Servicios de Confianza a los servicios de sellado
- Los documentos de condiciones generales vinculantes con suscriptores y terceros que confían en sellos de tiempo
- Las modificaciones de los documentos anteriormente indicados

8.3.- 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 el documento de política o Declaración de Prácticas de Certificación. La información de estado de revocación de certificados se publicará conforme se indica en la Declaración de Prácticas de Certificación.

9.- Control de acceso

EADTrust no limitará el acceso de lectura a los documentos públicos indicados anteriormente en esta Política, pero sí 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.

10.- Requisitos de Operación del Ciclo de Vida de los Sellos de Tiempo

10.1.- Solicitud de sello de tiempo

10.1.1.- 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.

10.1.2.- Procedimiento de alta

Antes del alta como suscriptor, EADTrust informará al suscriptor de los términos y condiciones aplicables al servicio. La citada información se comunicará en soporte duradero, en papel o electrónicamente y en lenguaje fácilmente comprensible, y tendrá los siguientes contenidos mínimos:

- 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.

10.2.- 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 algoritmos de resumen SHA-2 o posteriores
- La solicitud no deberá contener extensiones
- En caso de verificación incorrecta de la solicitud, se devolverán los mensajes de error apropiados (RFC 3161, sección 2.4.2).

10.3.- 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

- 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 correspondiente de esta política.
- Generar sellos de tiempo conteniendo las informaciones incluidas en la sección 17 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 15.2de esta política.

10.4.- Entrega del sello de tiempo

10.4.1.- 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).

10.4.2.- Publicación del sello de tiempo

EADT no publica los sellos de tiempo. En su defecto se conservará almacenados en las bases de datos habilitados a este efecto y en las copias de seguridad de estas bases de datos pudiendo obtenerse un listado completo o parcial de los emitidos para un subscriptor mediante solicitud previa.

10.4.3.- 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.

10.4.4.- Finalización de la suscripción

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

11.- Controles de Seguridad Física, De Gestión y de Operaciones

11.1.- Controles físicos

EADTrust está sujeta a las validaciones anuales de la norma UNE-ISO/IEC 27001 que regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los sistemas de información.

EADTrust tiene establecidos 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 a los servicios de generación certificados ofrece protección frente:

- Controles físicos de entrada.
- Seguridad de oficinas, despachos e instalaciones.
- Protección contra las amenazas externas y ambientales.
- Trabajo en áreas seguras.
- Áreas de carga y descarga.
- Emplazamiento y protección de equipos.
- Instalaciones de suministro.
- Seguridad del cableado.
- Mantenimiento de los equipos.
- Retirada de materiales propiedad de la empresa.
- Seguridad de los equipos fuera de las instalaciones.
- Reutilización o eliminación de equipos.

- Política de dispositivos móviles.

11.1.1.- Localización y construcción de las instalaciones

EADTrust cuenta con infraestructura adecuada para prestar servicios de confianza digital en sus instalaciones de Madrid, y además para ciertos servicios (OCSP, por ejemplo) podrán contratarse Prestadores de Servicios de Housing y de Cloud Computing, como por ejemplo Amazon[1] y OVH[2].

11.1.2.- Acceso físico

Las instalaciones de EADTrust cuentan con un sistema completo de control de acceso físico que consiste en:

- Seguridad perimetral que se extiende desde el suelo hasta el techo para evitar el acceso no autorizado.
- Control sobre el acceso físico a la instalación.
    - Sólo se permite el acceso al personal autorizado.
    - Los derechos de acceso al área de seguridad son revisados y actualizados periódicamente.
    - Todo el personal está identificado y no es posible circular en el edificio sin estar identificado y acompañado por un empleado.
    - El personal que no está en la lista de acceso de EADTrust y que puede estar trabajando en el sitio está debidamente supervisado.
- El acceso a las instalaciones que acogen los servidores implica la videograbación de la actividad y requiere identificación biométrica y control dual de los accesos.
- Se lleva a cabo el registro de los accesos a las instalaciones que acogen los servidores.
- Se cuenta con medidas adicionales de limitación de accesos al edificio en las oficinas de EADTrust.

11.1.3.- Electricidad y aire acondicionado

El centro de procesamiento de datos dispone de energía y aire acondicionado suficientes para crear un entorno operativo fiable.

Los equipos de servicio son de bajo consumo y de baja disipación térmica por lo que pueden continuar en uso incluso si falla el aire acondicionado por un período prolongado.

Los sistemas de alimentación ininterrumpida garantizan un tiempo de funcionamiento superior a 10 horas en caso de que se produzca un corte prolongado de suministro eléctrico.

En caso de corte eléctrico prolongado, se procederá a la parada ordenada de sistemas

11.1.4.- Exposición al agua

[1] Aspectos de cumplimiento de Amazon: https://aws.amazon.com/es/compliance/

[2] Aspectos de cumplimiento de OVH: https://www.ovh.com/world/private-cloud/documentation/certifications.xml

EADTrust ha tomado las precauciones necesarias para minimizar el impacto de la exposición al agua.

11.1.5.- Prevención y protección contra incendios

El centro de procesamiento de datos de EADTrust tiene barreras físicas que se extienden desde el suelo hasta el techo, así como sistemas automáticos de medida de humedad y temperatura que registrarán situaciones anómalas antes de que pueda producirse un incendio.

Cuenta con equipos de extinción debidamente señalizados y adecuados al tipo de equipamiento existente. La puerta ignífuga cuenta con una protección adicional de espuma ignífuga.

11.1.6.- Almacenamiento de soportes

Los soportes que contienen información de backup se almacenan de forma segura.

11.1.7.- Eliminación de residuos

Existe una política para regular los procedimientos que rigen la destrucción de los medios de información.

Los soportes de almacenamiento que contienen información confidencial se destruyen para garantizar que los datos no sean legibles o recuperables después de la eliminación. EADTrust ha adoptado una política de gestión de residuos diseñada para poder superar una auditoría ISO 14001.

11.1.8.- Copia de seguridad externa

EADTrust mantiene copias de seguridad de los soportes de almacenamiento en un entorno seguro y protegido contra accidentes y una distancia suficiente para evitar daños en caso de un desastre en el sitio originario.

11.2.- Controles de procedimiento

11.2.1.- Puestos de confianza

Un "puesto de confianza" se define como las funciones asignadas a una persona que pueden conllevar problemas de seguridad si no se realizan satisfactoriamente, ya sea de forma accidental o intencionada.

Para asegurar que las personas de confianza cumplan adecuadamente sus deberes, se abordan las siguientes consideraciones:

- La primera es que la tecnología está diseñada y configurada para prevenir errores y conducta inadecuada.
- La segunda es que las tareas se distribuyen entre varios individuos de manera que cualquier conducta impropia requeriría la complicidad de varios de ellos.

EADTrust tiene definiciones completas de todas las funciones desempeñadas en la organización. Se definen los deberes y responsabilidades asociados a cada función, y cada uno tiene un conjunto de procedimientos documentados que regulan la práctica anexa a cada uno.

11.2.2.- Número de personas requeridas por tarea

Para reforzar la seguridad del sistema, se asigna más de una persona a cada función, con la excepción de la función de operador, que puede realizar el administrador.

Se puede asignar varias personas a la misma función.

11.2.3.- Identificación y autenticación para cada puesto

Los roles de confianza requieren la comprobación de la identidad por medios seguros. Todos los roles de confianza son realizados por individuos.

EADTrust tiene documentación específica que da más detalles de cada función.

11.2.4.- Puestos que requieren separación de deberes

EADTrust sigue la política de seguridad CIMC (Certificate Issuing and Management Component)[3] que se define en su modelo de seguridad.

11.3.- Controles de personal

11.3.1.- Antecedentes, cualificaciones, experiencia y requisitos de aplicación

EADTrust emplea personal con la experiencia y con las cualificaciones necesarias para desempeñar sus responsabilidades laborales.

Todo el personal con funciones de confianza está libre de cualquier interés que pueda afectar su imparcialidad con respecto a las operaciones de EADTrust.

11.3.2.- Procedimientos de comprobación de antecedentes penales

Según la legislación española no es aplicable la solicitud de antecedentes penales a los trabajadores por parte de las empresas. Existe una prohibición general de discriminar a cualquier trabajador, por cualquier motivo, tanto en el empleo como en el acceso al mismo. Así se prevé específicamente en el artículo 14 de la Constitución Española, el artículo 4.2 del Estatuto de los Trabajadores y el artículo 73.2 de la Ley General Penitenciaria.

[3] https://www.commoncriteriaportal.org/files/ppfiles/cert-issu-v15-sec-eng.pdf.

Conforme a la legislación española y por criterio reiterado de los tribunales, debe primar el derecho a la intimidad y a la reinserción laboral.

11.3.3.- Requisitos de formación

EADTrust proporciona a su personal la formación necesaria para desempeñar sus responsabilidades laborales de manera competente y satisfactoria. La formación del personal incluye lo siguiente:

- Una copia de la Declaración de Prácticas de Servicios Electrónicos de Confianza.
- Sensibilización sobre la seguridad.
- Funcionamiento del software y hardware para cada función específica.
- Procedimientos de seguridad para cada función específica.
- Procedimientos de gestión y operación para cada función específica.
- Procedimiento de recuperación de desastres.

Entre los requisitos de seguridad aplicable se encuentran los recogidos en el Sistema de Gestión de la Seguridad de la Información desarrollado en el marco de la certificación ISO 27001.

11.3.4.- Frecuencia y requisitos de cursos de perfeccionamiento

Cualquier cambio significativo en las operaciones de la PKI de EADTrust requerirá un plan de formación y la implementación del plan será documentada.

11.3.5.- Rotación y secuencia laboral

No aplica

11.3.6.- Sanciones para acciones no autorizadas

Incidentes de seguridad de la información. EADTrust tiene un plan de gestión de incidentes de seguridad.

Sanciones para acciones no autorizadas. Se aplicarán en correspondencia con lo previsto en la legislación laboral vigente, en función de la gravedad de las actuaciones.

11.3.7.- Requisitos de contratación del personal

EADTrust mantiene una política de contratación de personal que busca los perfiles adecuados para su actividad y cuenta con criterios de idoneidad para la asignación de roles y responsabilidades.

EADTrust cumple con sus obligaciones en materia de igualdad y, en el marco de las relaciones con sus empleados, tiene asumido un compromiso fehaciente para la promoción e implantación efectiva de los principios de igualdad de oportunidades entre mujeres y hombres, y de no discriminación por razón de género, raza, origen, religión, etc.

En este mismo sentido manifiesta su compromiso de trabajo para garantizar la accesibilidad de sus servicios e instalaciones a todas las personas, independientemente de sus capacidades técnicas, cognitivas o físicas.

11.3.8.- Documentación proporcionada al personal

Todo el personal con funciones de confianza recibe:

- Una copia de la Declaración de Prácticas de Certificación
- Una copia del Manual de Acogida que incluye consideraciones específicas de confidencialidad y seguridad.
- Documentación que define las obligaciones y procedimientos asociados a cada rol.
- El personal también tiene acceso a los manuales de operaciones de los distintos componentes del sistema.

11.4.- Procedimientos de registro de auditoría

Los registros de auditoría se utilizan para reconstruir los eventos significativos registrados en el software de EADTrust o de la Autoridad de Registro y el usuario o evento que dio origen al registro. Los registros también se utilizarán en el arbitraje para resolver cualquier posible conflicto comprobando la validez de una firma en un momento dado.

11.4.1.- Tipos de eventos registrados

EADTrust registra y guarda los registros de auditoría de todos los eventos relativos al sistema de seguridad de la AC.

Se registrarán los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los registros de auditoría.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.

Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de este.

EADTrust también conserva, ya sea manualmente o electrónicamente, la siguiente información:

- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Informes de compromisos y discrepancias.
- Control de material destinado a gestión de claves.
- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

11.4.2.- Frecuencia de procesamiento del registro

Los registros de auditoría son revisados regularmente por el auditor de EADTrust.

11.4.3.- Periodo de retención del registro de auditoría

EADTrust almacena la información de los registros de auditoria al menos durante 10 años. Los auditores tienen derecho a acceder a los registros de auditoría.

La eliminación o modificación no autorizada de las entradas de registro se evita escribiendo registros de auditoría utilizando medios no aptos para su reescritura o borrado sin detección, para ello se utiliza un sistema de hashes encadenados y firma digital.

En el caso de la bitácora (en papel) se usan técnicas de cumplimentación que limitan la posibilidad de manipulación o eliminación de información.

11.4.4.- Procedimientos de copia de seguridad para registros de auditoría

Los sistemas de gestión de copias de respaldo están contemplados entre las medidas de seguridad adoptadas por la entidad.

Cuando haya cualquier gestión de CA se hace la copia de respaldo de la situación anterior y además la actuación se registra en la bitácora. Siempre habrá respaldo de la última modificación, y, en su caso, en ubicaciones separadas a las de prestación del servicio.

11.4.5.- Evaluaciones de vulnerabilidades

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de EADTrust.

Anualmente se revisan los procesos de gestión de riesgos y vulnerabilidades dentro del marco de revisión de la certificación **UNE-ISO/IEC 27001** que están reflejados en el documento de Análisis de riesgos de EADTrust.

En este documento se especifican los controles implantados para garantizar los objetivos de seguridad requeridos.

Además, se contratan externamente auditorías de “White Hat Ethical Hacking” o “Penetration Testing”

11.5.- 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 11.6.1 de esta política.

11.6.- Tipos de eventos registrados

EADTrust custodia y conserva 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.

11.6.1.- 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 o lo establecido en la Declaración de Prácticas de Servicios de Confianza.

11.6.2.- 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.

11.6.3.- 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.

12.- Renovación de claves

EADTrust ha definido un plan de renovación programada de las claves de las Entidades de Sellado de Tiempo, que garantiza la continuidad de los servicios.

13.- Compromiso de claves y recuperación de desastre

13.1.- Corrupción de recursos, aplicaciones o datos

Cuando tenga lugar un evento de corrupción de recursos, aplicaciones o datos, EADTrust iniciará 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.

13.2.- 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, llevará a cabo los siguientes pasos:

- 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 12 de esta política.

13.3.- Compromiso de la clave privada de la entidad

EADTrust considera 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 realizará 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.

13.4.- Desastre sobre las instalaciones

EADTrust ha previsto, desarrolla, mantiene, prueba y, si es necesario, ejecutará 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 indica cómo restaurar los servicios de los sistemas de información.
La ubicación de los sistemas de recuperación de desastres dispondrá de las protecciones físicas de seguridad detalladas en el plan de seguridad.
EADTrust es 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 esta sincronizada con la base de datos de producción, dentro de los límites temporales especificados en el plan de seguridad u otro documento que lo sustituya, de EADTrust.

14.- Terminación del servicio

EADTrust asegura 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, asegura 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 ejecuta, 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 declara en sus prácticas las previsiones que tiene para el caso de terminación del servicio. Estas incluyen:

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

15.- Controles de Seguridad Técnica

EADTrust emplea sistemas y productos fiables, 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.

15.1.- Fiabilidad de la fuente de tiempo

La fuente de tiempo utilizada en los sistemas de EADTrust es la proporcionada por un sistema de alta precisión sincronizado con la constelación de satélites GPS y Galileo, en concreto se usa un servidor con un receptor simultáneo multisatélite y soporte para GPS, GLONASS, GALILEO y BEIDOU.
Existe una opción de contingencia que prevé la sincronización con la referencia horaria del Real Instituto y Observatorio de la Armada en San Fernando (Cádiz), a través de la Sección de Hora, que resulta accesible mediante el servicio NTP, conforme al RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification.
Este organismo tiene entre sus misiones la del mantenimiento de la unidad básica de Tiempo, declarado a efectos legales como Patrón Nacional de dicha unidad, así como el mantenimiento y difusión oficial de la escala de “Tiempo Universal Coordinado”, considerada a todos los efectos como la base de la hora legal en todo el territorio nacional, según el Real Decreto 1308/1992, de 23 de octubre.
Todos los sistemas que constituyen la infraestructura de Clave Pública de EADTrust están sincronizados en fecha y hora.

El sistema de fuente de tiempo de intranet puede configurarse en base al protocolo NTP o PTP, si bien la precisión necesaria en entornos de uso convencional es de 1 segundo. La precisión interna de la fuente se deriva de la proporcionada por la constelación de satélites:

- **GPS**. US Naval Observatory estableció una escala de tiempo atómico, llamada **Tiempo GPS**, cuya unidad de medida es el segundo atómico internacional. El tiempo de satélite es mantenido, en cada satélite, por dos o por cuatro relojes atómicos. Los relojes de los satélites son monitorizados por las estaciones de seguimiento y los centros de control de la Tierra que en ocasiones los reajustan para mantener cada reloj dentro del Tiempo GPS.
- **Galileo** es el programa europeo de radionavegación y posicionamiento por satélite, desarrollado por la Unión Europea (UE) conjuntamente con la Agencia Espacial Europea. Este programa dota a la Unión Europea de una tecnología independiente del GPS estadounidense y el GLONASS ruso. Galileo proporciona una referencia temporal de alta precisión.

Los tokens de sellado de tiempo se sellan con los certificados EADTrust de TSU, emitidos bajo la Cadena de Certificación descrita en la Declaración de Prácticas de Certificación. Se prevé el uso de certificados cualificados y no cualificados para el servicio de sello de tiempo cualificado. La validez de los certificados cualificados orientados al sellado de tiempo se establece en los propios certificados.

- 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.

15.2.- Generación e instalación del par de claves

15.2.1.- Generación del par de claves

La generación de las claves de firma de la TSU de EADTrust, se lleva a cabo en un entorno físicamente seguro, por personal designado con roles de confianza, bajo al menos, control dual. El personal de referencia se limita a aquellos requeridos para hacerlo.

La generación de las claves de firma de la TSU se lleva a cabo empleando hardware criptográfico 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). Las claves están únicamente en un dispositivo criptográfico a la vez usado por alguna TSU, sin estar replicadas en otro dispositivo. En ningún momento una TSU tendrá activa más de una clave a la vez.

15.2.2.- 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.

15.2.3.- 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.

15.2.4.- Longitudes de claves

La longitud de las claves de las Entidades de Sellado de Tiempo será de al menos 2048 bits.

15.3.- Protección de la clave privada

15.3.1.- 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.

15.3.2.- 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 se lleva a cabo necesariamente del concurso sucesivo de más de una persona que tendrá el rol 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.

15.3.3.- 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.

15.3.4.- 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. Cuando las claves se almacenan en un módulo hardware de proceso dedicado, se proveen los controles oportunos para que éstas nunca puedan abandonar el dispositivo.

15.3.5.- Archivo de la clave privada

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

15.3.6.- 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.

15.3.7.- 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 15.3.2.

15.3.8.- 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.

15.3.9.- 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, es decir, de manera que sea prácticamente imposible recuperarlas. Esta acción se realizará cuando expire el período de validez de las mismas y sean sustituidas por otras nuevas, o cuando se retire el dispositivo criptográfico que la contiene de la TSU.

15.4.- Otros aspectos de gestión del par de claves

15.4.1.- 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 11.5 de esta política.

15.4.2.- Periodos de utilización de las claves pública y privada

Los períodos 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. Una vez finalizado el período de utilización de las claves, se garantizará la sustitución de las claves en las mismas condiciones de seguridad en las que se instalaron las anteriores, destruyendo las que caen en desuso tal y como se define en el apartado 15.3.9.

16.- Controles de seguridad informática

16.1.- Requisitos técnicos específicos de seguridad informática

Se deberá garantizar que el acceso los sistemas está limitado a individuos debidamente autorizados. 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.

16.1.1.- Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de sellado de tiempo empleadas por EADTrust son fiables.

16.2.- Controles técnicos del ciclo de vida

16.2.1.- Controles de desarrollo de sistemas

Se realiza un análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente empleado en las aplicaciones de sellado de tiempo, para garantizar que los sistemas son seguros. Se emplean procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

16.2.2.- 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 18 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.

16.2.3.- 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.

16.3.- Controles de seguridad de red

Se garantiza que el acceso a las diferentes redes de EADTrust está limitado a individuos debidamente autorizados. En particular:
Se implementan controles para proteger la red interna de dominios externos accesibles por terceras partes.
Los cortafuegos se configuran de forma que se impidan accesos y protocolos que no sean necesarios para la operación de la Entidad de Sellado de Tiempo.
Los datos sensibles se protegen cuando se intercambien a través de redes no seguras (incluyendo como tales los datos de registro del suscriptor)
Se garantiza que los componentes locales de red se encuentran ubicados en entornos seguros, así como la auditoría periódica de sus configuraciones.

16.4.- Controles de ingeniería de módulos criptográficos

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

17.- Perfiles de Sellos de Tiempo

Los sellos tendrán el contenido y campos ajustados a las siguientes normas:

- ETSI EN 319 422 V1.1.1 (2016-03) - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- IETF RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- IETF RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs).
- XML Timestamping Profile of the OASIS Digital Signature Services Version 1.0. OASIS Standard. 11 April 2007.

En el caso de los sellos de tiempo cualificados, es requisito del Reglamento eIDAS que se creen haciendo uso de firmas avanzadas lo que permite que estas estén basadas o no en certificados cualificados. EADTrust contempla en su servicio de sello de tiempo cualificado la posibilidad de usar ambos tipos de certificados.

17.1.- Perfil de certificado cualificado de persona jurídica para sello de tiempo cualificado

El perfil de los certificados cualificados de persona jurídica para sello de tiempo cualificado se encuentra descrito en la Política específica.

17.2.- Perfil de certificado no cualificado de persona jurídica para sello de tiempo cualificado y no cualificado

El perfil de los certificados no cualificados de persona jurídica para sello de tiempo cualificado y no cualificado, se encuentra descrito en la Política específica.

18.- Auditoría de Conformidad

EADTrust ha superado anualmente desde 2009 diversas auditorías de su Sistema Integrado de Gestión con respecto a varias normas.

En estos momentos, **EADTrust** está certificado respecto a las normativas **“UNE EN ISO 9001:2015“, “UNE ISO/IEC, 27001:2014” y “UNE ISO/IEC 20000-1:2011”** a través de la entidad **LRQA Business Assurance**, con el siguiente alcance:

> *El Sistema Integrado de Gestión de la Información que da soporte a consultoría, auditoría, desarrollo y provisión de los siguientes servicios electrónicos de confianza: Autoridades de Certificación (PKI) que*

cumplen los requerimientos de las normas EN 319 401 v2.2.1, EN 319 411- 1 v1.2.2, EN 319 411-2 v2.2.2, EN 319 421 v1.1.1 para Sellado de Tiempo, Emisión de Certificados, Validación de OCSP, Firma Electrónica Centralizada, Extensión de Firma Electrónica, Notificación Electrónica Fehaciente (Correo Electrónico Certificado), Publicación Electrónica Fehaciente, Comprobación fehaciente de contenidos digitales, Foro Electrónico de Accionistas, Emisión y Gestión de Claves, Cartulario (Custodia Digital de Documentos Electrónicos), Custodia de Evidencias Electrónicas (Retención de Datos), Voto Electrónico, Facturación Electrónica, Digitalización Certificada, Gestión de firma manuscrita digitalizada y Gestión de firma avanzada vocal, para garantizar la validez legal de todo tipo de gestiones que las utilizan, de acuerdo a la declaración de aplicabilidad vigente. Estos son los certificados:

Norma	Certificado
ISO 20000-1:2011	10242586 / 10242587
ISO 27001:2013	10242584 / 10242585
ISO 9001:2015	10242588 / 10242589

EADTrust ha superado varias auditorías de tipo "Penetration testing" para verificar la resistencia de su infraestructura a diversos ataques de seguridad potenciales y se estima una cadencia aproximadamente anual para repetir las auditorías de este tipo.

EADTrust se somete con la periodicidad indicada en el Reglamento UE 910/2014 a auditorías de cumplimiento de los requisitos relativos a los prestadores de servicios electrónicos de confianza cualificados, en base a las normas:

- ETSI EN 319 401 V2.2.1 (2018-04) - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

- ETSI EN 319 411-1 V1.2.2 (2018-04) - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2 V2.2.2 (2018-04) - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

- ETSI EN 319 421 V1.1.1 (2016-03) - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

En el marco de los requisitos de CAB Fórum, las auditorías son anuales.

19.- Requisitos Empresariales y Legales

19.1.- Tarifas

EADTrust recibirá las contraprestaciones económicas correspondientes, de acuerdo con las tarifas aprobadas por su Órgano de Dirección.

19.2.- Tarifas de emisión de certificados

Las tarifas que los usuarios deben abonar en contraprestación al servicio, se recogen en el documento términos y condiciones de emisión para cada tipo de certificado.

19.3.- Tarifas de consulta OCSP

Los servicios OCSP de EADTrust respecto a sus propios certificados son gratuitos.

Los servicios OCSP de EADTrust respecto a los certificados de otros prestadores están sujetos a un coste de alta, un coste mensual y un coste unitario que se comunicará previa solicitud. Este servicio solamente se presta a empresas.

20.- Consideraciones de protección de datos de carácter personal

Todos los datos correspondientes a las personas físicas están sujetos a la normativa sobre protección de datos de carácter personal. De conformidad con lo establecido en el Reglamento (UE) 679/2016 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE), también conocido como RGPD.

En España, es de aplicación lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre de 2018, de protección de datos personales y garantía de derechos digitales, también conocida como LOPD-GDD.

Conforme establece la citada legislación de protección de datos, se consideran datos de carácter personal cualquier información relativa a personas físicas identificadas o identificables.

La información personal que no haya de ser incluida en los certificados y en el mecanismo indicado de comprobación del estado de los certificados, es considerada información personal de carácter privado.

Los siguientes datos son considerados información privada:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección correspondiente.
- Claves privadas generadas y/o almacenadas por la Entidad de Certificación.
- Cualquier otra información que pudiera identificarse como “Información privada”.

Los datos recabados por el prestador de servicios electrónicos de confianza tendrán la consideración legal que corresponda a su naturaleza, siendo normalmente datos de nivel básico. La información confidencial de acuerdo con la normativa de protección de datos es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado. A estos efectos EADTrust considera pública y no confidencial la siguiente información:

- Los certificados expedidos.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados, así como el resto de informaciones de estado de revocación.

Los certificados de sitio web publicados en el registro de "Certificate Transparency" pueden ser descargados y analizados por terceros, normalmente en contextos de gestión de debida diligencia en la expedición de certificados.

20.1.- Consentimiento para usar datos de carácter personal

EADTrust S.L informa que los datos personales a los que tenga acceso en el marco de la prestación de sus servicios serán incorporados al registro de actividades de tratamiento del que es Responsable. EADTrust fundamenta el tratamiento de datos fundamentalmente en: el interés legítimo que tiene en responder solicitudes de información sobre sus servicios, la ejecución de un contrato o en el consentimiento expreso del titular del dato. Los titulares de datos pueden retirar ese consentimiento en cualquier momento.

Los datos recabados son los mínimos necesarios para la prestación de los servicios y se conservan por los períodos que establece la Ley. No se ceden a terceros, salvo obligación legal; ni se realizan perfiles o se toman decisiones automatizadas en base a estos datos.

EADTrust le informa igualmente que, en caso de solicitar los servicios amparados en esta DPC por vía telefónica, su voz podrá ser grabada durante las conversaciones telefónicas que mantenga con la Autoridad de Registro (AR) o la Autoridad de Certificación (AC), con el fin de permitir una tramitación segura de la solicitud de emisión o revocación de certificados. Previo a la grabación se le ofrecerá la información básica de protección de datos estipulada en el RGPD y se le recabará su consentimiento expreso. Los datos personales recabados por esta vía se incorporarán al registro de actividades de tratamiento del que es responsable EADTrust.

Cuando el servicio de emisión o revocación de certificados se provea en la modalidad de verificación y autenticación de identidad mediante video conferencia o videograbación, EADTrust requerirá captar la imagen y la voz del Solicitante. La base legal para este tratamiento es la ejecución del contrato de prestación de servicios en esta modalidad conforme dispone el artículo 6.1 b) del Reglamento General de Protección de Datos. Estos datos son necesarios para la adecuada prestación del servicio y se incorporarán al registro de actividades de tratamiento de EADTrust.

Para más información sobre el ejercicio de los derechos al amparo del RGPD y sobre el tratamiento de sus datos personales por EADTrust consulte la nota legal más extensa, incluida en: www.eadtrust.rgpd.de

20.2.- Comunicación a terceros de datos de carácter personal

Los datos de carácter personal solo podrán ser comunicados a terceros, siempre que el titular del derecho lo consienta expresamente o por obligación legal de EADTrust.

21.- Responsabilidad contractual y extracontractual

21.1.- Limitación de responsabilidad

EADTrust no asumirá responsabilidad alguna por los daños derivados o relacionados con la no ejecución o la ejecución defectuosa de las obligaciones del titular de un certificado.

EADTrust no será responsable de la utilización incorrecta de los Certificados ni de las claves, ni de cualquier daño indirecto que pueda resultar de la utilización de los Certificados.

EADTrust no será responsable de los daños que puedan derivarse de aquellas operaciones en que se hayan incumplido las limitaciones de uso del Certificado.

EADTrust no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones contenidas en esta DPC si tal falta de ejecución o retraso fuera consecuencia de un supuesto de fuerza mayor, caso fortuito o, en general, cualquier circunstancia en la que no se pueda tener un control directo.

EADTrust no será responsable del contenido de aquellos documentos firmados electrónicamente por los titulares de certificados.

EADTrust no garantiza los algoritmos criptográficos ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si guardó la diligencia debida de acuerdo al estado actual de la técnica, y procedió conforme a lo dispuesto en esta DPC y en la normativa de aplicación.

21.1.1.- Responsabilidades

EADTrust responderá en el caso de incumplimiento de sus obligaciones según se indica en el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, y en la normativa reguladora de los servicios electrónicos de confianza, así como en la DPC y en esta política específica.

EADTrust responderá por los daños y perjuicios que causen al firmante o terceros de buena fe cuando incumpla las obligaciones que impone el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014 y la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

La responsabilidad del prestador de servicios de confianza regulada en la ley será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, si bien corresponderá al prestador de servicios de confianza demostrar que actuó con la diligencia profesional que le es exigible siendo responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en razón del incumplimiento de las obligaciones establecidas en el Reglamento 910/2014.

Se presumirá la intencionalidad o la negligencia de un prestador cualificado de servicios de confianza salvo cuando el prestador cualificado de servicios de confianza demuestre que los perjuicios a que se refiere el párrafo primero del artículo 13 del Reglamento 910/2014 se produjeron sin intención ni negligencia por su parte.

Cuando EADTrust, como prestador cualificado de servicios de confianza, informe debidamente a los suscriptores con antelación sobre las limitaciones de la utilización de los servicios que presta y estas limitaciones sean reconocibles para un tercero, el prestador de servicios de confianza no será responsable de los perjuicios producidos por una utilización de los servicios que vaya más allá de las limitaciones indicadas.

De manera particular, EADTrust como prestador de servicios de confianza responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado electrónico.

EADTrust como prestador de servicios de certificación asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de confianza.

21.1.2.- Exención de responsabilidades de EADTrust

EADTrust no asume ninguna responsabilidad por perjuicios ocasionados en las siguientes circunstancias:

- En caso de guerra, catástrofes naturales o cualquier otro supuesto de caso fortuito o de fuerza mayor: alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico y/o telefónico, virus informáticos, deficiencias en los servicios de telecomunicaciones o el compromiso de las claves asimétricas derivado de un riesgo tecnológico imprevisible.
- Ocasionados durante el periodo comprendido entre la solicitud de un certificado y su entrega al usuario.
- Ocasionados durante el periodo comprendido entre la revocación de un certificado y el momento de publicación de la siguiente CRL.
- Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos y esta DPC.
- Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por la infraestructura de Certificación de EADTrut.
- Ocasionados por el mal uso de la información contenida en el certificado.
- La Autoridad de Certificación no será responsable del contenido de aquellos documentos firmados electrónicamente ni de cualquier otra información que se utilice en un proceso de autenticación en la que esté involucrado un certificado emitido por ella.

21.1.3.- Perjuicios derivados del uso de servicios de sello de tiempo y certificados

A excepción de lo establecido por las disposiciones de la DPC, esta política específica y lo determinado por Ley, EADTrust no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados, usuarios del servicio de sello de tiempo o terceros que confían en los certificados y sellos de tiempo emitidos.

21.1.4.- Seguro de responsabilidad civil

EADTrust cuenta con un Seguro de Responsabilidad Civil adecuado a sus actividades, según lo dispuesto en la normativa reguladora de los servicios electrónicos de confianza.

21.2.- Enmiendas y cambios

21.2.1.- Procedimiento para realizar cambios

Las modificaciones de este documento serán aprobadas por el órgano de aprobación y gestión de políticas de certificación de EADTrust.

Estas modificaciones estarán recogidas en un documento de actualización de la Declaración de Prácticas de Servicios Electrónicos de Confianza y en esta política específica, cuyo mantenimiento está garantizado por EADTrust.

Las versiones actualizadas de la Declaración de Prácticas de Servicios Electrónicos de Confianza y de esta política específica, junto con la relación de modificaciones realizadas pueden ser consultadas en la dirección www.eadtrust.eu
y más concretamente en http://policy.eadtrust.eu

EADTrust podrá modificar la Declaración de Prácticas de Servicios Electrónicos de Confianza y esta política específica para lo que actuará según el siguiente procedimiento:

- La modificación estará justificada desde el punto de vista técnico, legal o comercial.
- Se deberán contemplar todas las implicaciones técnicas y legales de la nueva versión de especificaciones.
- Se establecerá un control de modificaciones, para garantizar, que las especificaciones resultantes cumplen con los requisitos que se intentaban cumplir y que dieron pie al cambio.
- Se valorarán las implicaciones que puedan tener sobre los usuarios el cambio de especificaciones, por si fuera preciso comunicarles el cambio.

21.2.2.- Mecanismo y periodo de modificación

En la fase preparatoria de las auditorías bienales, EADTrust revisará el presente documento para asegurarse de que permanece actualizado en relación con los cambios que se vayan produciendo en los siguientes aspectos:

- Marco legislativo de aplicación.
- Pautas de funcionamiento de Servicios Electrónicos de Confianza publicadas por el Organismo Nacional de Supervisión
- Publicación de estándares.
- Mejoras o no conformidades identificadas en las auditorías.
- Mejoras realizadas en los servicios o lanzamiento de nuevos servicios.
- Adopción de productos y servicios de terceros que se integren con los ofrecidos por EADTrust.

EADTrust podrá realizar modificaciones de este documento sin necesidad de informar previamente a los usuarios, como, por ejemplo:

- Correcciones de errores tipográficos en el documento
- Cambios en la información de contacto.

EADTrust podrá realizar modificaciones de este documento de las que se informará a los usuarios por email, tales como:

- Cambios en las especificaciones o condiciones del servicio.
- Modificaciones de URLs.

21.2.3.- Circunstancias bajo las cuales debe modificarse el OID

Se asignarán OID específicos para las funciones y significados de información que sean significativos para los suscriptores y para los terceros que confían.

21.3.- Quejas. Reclamaciones y jurisdicción

En caso de una queja del usuario o de un tercero interesado, este podrá dirigir su queja al mail: info@eadtrust.eu
o por correo postal; aportando copia de su identificación; así como todos los documentos y toda la información que considere oportuna para fundamentar su queja.

La CA de EADTrust en un plazo de 48 horas le remitirá por la misma vía de comunicación utilizada por el solicitante, un informe fundamentado de respuesta.

El plazo definido anteriormente podrá ser extendido en caso de que la resolución de la queja revista complejidad para su solución. Esta ampliación será comunicada al usuario.

En caso de que el usuario no esté conforme con la resolución de la queja. Este podrá presentar una solicitud de recurso de apelación ante la Dirección General de EADTrust. Para ello solo deberá comunicarse vía e mail

a info@eadtrust.eu, indicando en el asunto que se trata de un recurso de apelación, también podrá emplearse la vía del correo postal.

Para la resolución de apelaciones se seguirá el procedimiento descrito anteriormente.

Las reclamaciones dirigidas a EADTrust se gestionarán de forma directa para intentar llegar a un acuerdo que resuelva el incidente o, en su caso, comprobar si es una cobertura incluida en el seguro.

La actividad de EADTrust se rige por la Ley española y por los Tribunales de Madrid, salvo que el usuario ostente la condición de consumidor, lo que redundará en que se aplique la normativa de protección de consumidores.