

DIGITELTS

by MADISON*



POLÍTICA DEL SERVICIO CUALIFICADO DE SELLADO DE TIEMPO

DIGITELTS Qualified Trust Service Provider

1	Introducción	6
2	Definiciones y acrónimos	7
2.1	Definiciones	7
2.2	Acrónimos	9
3	Política de la TSA y requerimientos generales	12
3.1	Política de Sellado de Tiempo y Declaración de Prácticas de la TSA	12
3.2	Nombre del documento e identificación	12
3.3	Identificadores de certificados	12
3.4	Participantes en el servicio de sello de tiempo	13
3.4.1	Prestador de servicios de sellado de tiempo (TSA)	13
3.4.2	Suscriptor	15
3.4.3	Entidades finales	15
3.4.4	Usuarios	16
4	Política de sellado de tiempo	16
4.1	Despliegue y mantenimiento de los servicios de confianza	16
4.2	Política de sellado de tiempo	16
4.3	Obligaciones y responsabilidades	18
4.3.1	Obligaciones de uso correcto	18
4.3.2	Obligaciones de la Entidad Emisora de Sellos de Tiempo	19
4.3.3	Obligaciones del suscriptor de sellos de tiempo	21
4.3.4	Obligaciones de terceras partes verificadoras de sellos de tiempo	22
4.3.5	Responsabilidades	22
4.4	Procedimiento de emisión de un sello de tiempo	23
4.5	Provisión y disponibilidad del servicio de sellado de tiempo	24
4.6	Administración y operación de la TSA	24
4.6.1	Gestión de la Seguridad	24
4.6.2	Clasificación y gestión de activos	25

4.6.3	Seguridad del personal	25
4.7	Controles criptográficos	25
4.7.1	Generación de la clave de la TSA	25
4.7.2	Protección de la clave privada de la TSU	25
4.7.3	Distribución de la clave pública de la TSU	25
4.7.4	Renovación de clave privada de la TSU	25
4.7.5	Fin del ciclo de vida de la clave de la TSU	26
4.7.6	Compromiso de la clave privada del certificado de TSA	26
4.8	Sellado de tiempo	26
4.8.1	Fuente de tiempo	26
4.8.2	Perfil de una petición de sello de tiempo	27
4.8.3	Perfil de certificado de TSU	27

Control documental

Líder	Área de servicios de confianza		
Tipo	Política		
Distribución	Público		
Fecha	2025		
Descripción	POLÍTICA DEL SERVICIO CUALIFICADO DE SELLADO DE TIEMPO		
Aprobado	Comité de Riesgos y Seguridad DIGITELTS	Fecha	24 de 06 de 2025
Estado	Aprobado		

Control de Cambios

Versión	Fecha	Detalle
V1.0	Abril 2024	Versión Inicial
V1.2	Mayo 2024	Corrección de erratas
V1.3	Abril 2025	1.-Revisión anual 2.-Adaptación a la normativa siguiente: - Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) N.º 910/2014. - Directiva (UE) 2022/2555 (Directiva NIS 2) y su Reglamento de Ejecución 2024/2690 de 17/10/2024. - Estándar ETSI EN 319401 V3.1.1 (2024-06) - Estándar ETSI EN 319 421V1.3.0 (2025-01)

1 Introducción

DIGITELTS es un Prestador de Servicios de Confianza Cualificado conforme al Reglamento (UE) del Parlamento y del Consejo, de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital (en adelante, “Reglamento eIDAS”) y se encuentra cualificado para la prestación del servicio de sellado de tiempo, cumpliendo con los requisitos establecidos en el artículo 42 del Reglamento eIDAS. Así como, conforme a lo estipulado en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza .

Asimismo, para garantizar la ciberseguridad de sus operaciones como prestador cualificado de servicios de sellado de tiempo, la TSA de Digitel TS ha alineado sus procesos a los requisitos de seguridad de redes y ciberresiliencia digital definidos en la Directiva (UE) 2555/2022 (Directiva NIS2) y su Reglamento de Ejecución (UE) 2024/2690; así como, a la normativa de desarrollo que se dicte incluida la normativa de transposición al ordenamiento jurídico español.

Este servicio crea y registra evidencias digitales de la existencia de un dato en un instante determinado en la línea de tiempo, de una forma fiable y de confianza, mejorando significativamente la fiabilidad de los datos electrónicos.

El presente documento describe la política de la Autoridad de Sellado de Tiempo (TSA) de Digitel TS, especificando los procesos y políticas generales de la Autoridad de Sellado de Tiempo para la generación del token de tiempo electrónico y sus servicios.

Se especifican procesos y detalles técnicos adicionales a la Declaración de Prácticas de Certificación (DPC) de DIGITELTS.

Se ha utilizado el estándar RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” del Internet Engineering Task Force (IETF) como guía de asistencia en la redacción de este documento.

La política de sellado de tiempo cualificado de la TSA de Digitel TS es conforme a los siguientes estándares:

Referencia	Documento referenciado
ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 421	Policy and Security Requirements for Trust Service Providers issuing Time Stamps
ETSI EN 319 422	Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
RFC-3628	Policy Requirements for time-stamping authorities

2 Definiciones y acrónimos

2.1 Definiciones

Concepto	Definición
Autoridad de Certificación	Es la entidad responsable de la emisión y gestión de los certificados digitales.
Autoridad de sellado de tiempo electrónico	Prestador de servicios de certificación que proporciona la certeza sobre la preexistencia de determinados documentos electrónicos a un momento dado.

Certificado	Archivo que asocia la clave pública con algunos datos identificativos del Sujeto/Firmante y es firmada por la AC.
Clave pública	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos.
Clave privada	Valor matemático conocido únicamente por el titular y usado para la creación de una firma digital o el descifrado de datos. La clave privada de la AC será usada para la firma de certificados y firma de CRL's. La clave privada del servicio TSA será usada para la firma de los sellos de tiempo electrónico.
CRL	Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la AC.
OID	Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.
FUNCIÓN HASH	Operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado.

HASH O HUELLA DIGITAL	Resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.
Par de claves	Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.

2.2 Acrónimos

Acrónimo	Definición
AC (o también CA)	Certificate Authority Autoridad de Certificación
DPC (o también CPS)	Certification Practice Statement. Declaración de Prácticas de Certificación
CRL (o también LRC)	Certificate Revocation List. Lista de certificados revocados
DN	Nombre distintivo dentro del certificado digital Distinguished Name.

ETSI EN	European Telecommunications Standards Institute – European Standard.
FIPS	Federal Information Processing Standard Publication
HSM	Hardware Security Module Módulo de seguridad en Hardware
NTP	Network Time Protocol Protocolo de tiempo en red.
OCSP	On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
OID	Object Identifier. Identificador de objeto
PDS	PKI Disclosure Statements Texto de Divulgación de PKI.
PKI	Public Key Infrastructure. Infraestructura de clave pública

	Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
SHA	Secure Hash Algorithm. Algoritmo seguro de Hash
TCP/IP	Transmission Control. Protocol/Internet Protocol. Sistema de protocolos, definidos en el marco de la IEFT.
TSA	Time Stamping Authority Autoridad de Sellado de Tiempo Electrónico
TSU	Time Stamping Unit Unidad de Sellado de Tiempo.
UTC	Coordinated Universal Time // Tiempo universal coordinado
	Virtual Private Network. Red privada virtual

VPN

3 Política de la TSA y requerimientos generales

3.1 Política de Sellado de Tiempo y Declaración de Prácticas de la TSA

La Política y Declaración de Prácticas de sellado de tiempo se definen como:

- La Política de la TSA define los aspectos que deben ser cumplidos tanto por el suscriptor como por la Autoridad emisora de sellos de tiempo. Se incluyen las reglas y procesos que aplica la TSA cuando genera un token de sello de tiempo.
- La Declaración de Prácticas (DPC) es una declaración de cómo está implementado el servicio de sellado de tiempo para cumplir con los requerimientos de la política.

Esta política de TSA describe los procesos y políticas específicas de forma complementaria a los procesos descritos en la DPC de DIGITELTS.

3.2 Nombre del documento e identificación

Este documento es la política de sellado de tiempo cualificado de DIGITELTS.

Nombre del documento: DIGITELTS-DPP_QTSA

Versión 1.3

3.3 Identificadores de certificados

La Autoridad de Certificación de DIGITELTS ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por las aplicaciones.

OID	Tipos de certificados
1.3.6.1.4.1.54225.10.1.1	Certificado de Sello electrónico de TSU

En caso de contradicción entre este Documento de Política del Servicio de Confianza y otros documentos de prácticas y procedimientos, prevalecerá lo establecido en esta política.

3.4 Participantes en el servicio de sello de tiempo

3.4.1 Prestador de servicios de sellado de tiempo (TSA)

DIGITELTS es un prestador de servicios de confianza, que actúa como Autoridad de Sellado de Tiempo (TSA) de acuerdo con lo dispuesto en el **Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo**, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital (Reglamento eIDAS). Así como, con lo estipulado en **la Ley 6/2020, de 11 de noviembre**, reguladora de determinados aspectos de los servicios electrónicos de confianza y las **normas técnicas de la ETSI** aplicables a los prestadores en general (ETSI EN 319 401), y a los prestadores que expiden sellos de tiempo (ETSI EN 319 421 y ETSI EN 319 422), al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

La TSA de Digitel TS es la entidad de confianza en el que el usuario (suscriptores y terceras partes receptoras de sellos de tiempo) confían para la emisión de tokens de tiempo electrónico.

La TSA de Digitel TS podrá subcontratar todos o algunos de sus componentes, aunque en todo momento mantiene la responsabilidad última sobre todos los servicios relacionados con

la emisión de los sellos de tiempo. La TSA tiene la responsabilidad sobre las TSU (Unidades de sellado de tiempo) las cuales emiten los sellos de tiempo en representación de la TSA.

Los servicios de sellado cualificado de tiempo electrónico son emitidos por las siguientes jerarquías de certificación de DIGITELTS:

DIGITELTS CA ROOT 01

Se trata de la entidad de certificación raíz de la jerarquía que emite certificados a otras entidades de certificación, y cuyo certificado de clave pública ha sido autofirmado.

Datos de identificación:

Common Name	DIGITELTS CA ROOT 01
Huella digital	f23aa0a06261b3685ce5f05de058f801d3031f15

DIGITELTS Qualified CA TSA G1

Se trata de la Autoridad del Servicio de Sellado de Tiempo electrónico que expide los certificados de las Unidades de Tiempo Electrónico (TSU) para que emitan tokens cualificados de tiempo electrónico. La clave pública de la TSA ha sido firmada digitalmente por la DIGITELTS CA ROOT 01.

Common Name	DIGITELTS QUALIFIED CA TSA G1
Huella digital	b844d3988972165a54b85f09fc8d9b757aaddbb8

Valido desde

06-05-2022 13:19:47

3.4.2 Suscriptor

Los subscriptores del servicio de sellado de tiempo electrónico son las empresas, entidades u organizaciones que adquieren los certificados de TSU a la Autoridad de Certificación de DIGITELTS.

El suscriptor del servicio adquiere un derecho de uso del certificado de TSU, para su uso propio, o al objeto de facilitar la certificación de la emisión del token de tiempo electrónico.

El suscriptor del servicio de certificación es, por tanto, el cliente del prestador de servicios de confianza, de acuerdo con la legislación mercantil, y tiene los derechos y obligaciones que se definen por el prestador del servicio de confianza, que son adicionales y se entienden sin perjuicio de los derechos y obligaciones de los creadores de sellos de tiempo electrónicos, como se autoriza y regula en las normas técnicas europeas aplicables.

En general y para evitar cualquier conflicto de intereses, el suscriptor y el prestador de servicios de confianza serán entidades separadas. No obstante, lo anterior, se declara como excepción el caso de la emisión de certificados para la propia Autoridad de Certificación de DIGITELTS. Cuando se produce esta excepción consistente en la emisión de un certificado donde el suscriptor es la misma Autoridad de Certificación de DIGITELTS, la emisión del certificado sigue el procedimiento **Proc_EmisionTSU_DTS**, en el que se contempla la validación de la petición, que es realizada por un servicio o responsable perteneciente a la empresa DIGITELTS y que dispone de la correspondiente autorización.

3.4.3 Entidades finales

Las entidades finales son las personas y organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales para los usos de sellado de tiempo electrónico.

Serán entidades finales de los servicios de certificación de la Autoridad de Certificación de DIGITELTS las siguientes:

- Suscriptores del servicio de certificación.
 - Creadores de sellos.
 - Usuarios.

3.4.4 Creadores de sellos

Son las personas que solicitan los tokens de tiempo electrónico a la TSA de Digitel TS

3.4.5 Usuarios

Las partes usuarias son las personas y las organizaciones que confían en los servicios de sellado de tiempo prestados por la TSA de Digitel TS

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en esta declaración de prácticas de confianza y, en su caso, en las correspondientes instrucciones disponibles en la página web de la Autoridad de Certificación de DIGITELTS. la Autoridad de Certificación de DIGITELTS <https://pki.digitelts.es>

4 Política de sellado de tiempo

4.1 Despliegue y mantenimiento de los servicios de confianza

La TSA de DIGITELTS ha sido s ha sido desplegada en sus propias infraestructuras y en caso de tercerizar el servicio o alguna de sus operaciones críticas, la TSA de DIGITELTS asume la responsabilidad sobre su provisión conforme se indica en esta Política y en la DPC.

4.2 Política de sellado de tiempo

La TSA opera sus servicios de acuerdo con las reglas establecidas en la presente Política, la DPC y documentos internos adicionales que definen los requerimientos técnicos, operativos

y procedimentales. DIGITELTS puede de forma discrecional ofrecer servicios de TSA específicos a un solicitante.

La Política define cómo DIGITELTS se adhiere a los requerimientos identificados en la DPC y otros documentos internos.

Los procedimientos definidos y su correcta implementación son auditados anualmente por una entidad externa independiente.

Para más información acerca de las jerarquías de certificación y las Entidades de Certificación de DIGITELTS, puede utilizar la Declaración de Prácticas de Certificación y, a la Política de Divulgación de los servicios de sellado de tiempo, disponibles en <https://pki.digitelts.es/>

Las características del servicio de sellado de tiempo cualificado son las siguientes:

- Los sellos de tiempo emitidos por el servicio de sellado de tiempo cualificado son conforme a la norma ETSI EN 319 421 y ETSI EN 319 422.
- Los algoritmos de hash que aceptamos es SHA256, SHA512 y EDCSA256.
- La TSA asegura la precisión de tiempo compatible con los estándares mínimos de tiempo UTC de +/- 1 segundo.
- La TSA de DIGITEL TS no emitirá tokens de sello de tiempo si no se puede asegurar dicha precisión.

4.3 Usos admitidos

Se debe utilizar el certificado de TSU exclusivamente para los usos autorizados en esta Política, la DPC y en cualquier otra instrucción, manual o procedimiento suministrado al suscriptor, concretamente para la emisión de token de tiempo electrónicos. .

Los tokens de tiempo electrónicos 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 de tiempo.

4.4 Usos no autorizados o prohibidos

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

Los sellos de tiempo 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 extracontractuales, daños directos o indirectos que puedan derivarse de usos distintos a los permitidos y/o prohibidos quedan a cargo del suscriptor. En ningún caso podrán el suscriptor o los terceros perjudicados reclamar a Digitel TS compensación o indemnización alguna por daños o responsabilidades provenientes del uso de los sellos para los usos distintos a los permitidos y/o prohibidos.

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

4.5 Obligaciones y responsabilidades

DIGITELTS, como Entidad que emite sellos de tiempo de acuerdo con la presente Política de Sellado de Tiempo asume las siguientes obligaciones:

4.5.1 Obligaciones de uso correcto

Se debe cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas empleadas.

No se podrán adoptar medidas de inspección, alteración o descompilación de los servicios de certificación digital prestados.

Además:

- Que cuando se utilice cualquier certificado, y mientras el certificado no haya expirado ni haya sido suspendido o haya sido revocado, se habrá aceptado dicho certificado y estará operativo.
- Que no se actúa como entidad de certificación y, por lo tanto, se obliga a no utilizar las claves privadas correspondientes a las claves públicas contenidas en los certificados con el propósito de firmar certificado alguno.
- Que en caso de quedar comprometida la clave privada, su uso queda inmediata y permanentemente suspendido.

4.5.2 Obligaciones de la CA y la TSA Entidad Emisora de certificados de TSU y Sellos de Tiempo

La Autoridad de Sellado de Tiempo de DIGITELTS:

- Proteger sus claves privadas de forma segura.
- Emitir certificados de TSU conforme a esta Política y a los estándares de aplicación.
- Emitir certificados de TSU según la información que obra en su poder.
- Publicar los certificados de TSU emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.
- Revocar los certificados de TSU según lo dispuesto en la DPC y publicar las mencionadas revocaciones en la CRL.
- Informar a los Suscriptores de la revocación de sus certificados de TSU, en tiempo y forma de acuerdo con la legislación española vigente.
- Publicar esta Política y las Prácticas correspondientes en su página web.
- Informar sobre las modificaciones de esta Política y de su Declaración Prácticas de Certificación a los Suscriptores/Creadores del Sello.

- Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida o destrucción o falsificación.
- Emite tokens de sello de tiempo (TST) seguros para usuarios de servicios de sellado de tiempo (se incluyen tanto suscriptores como terceras partes).
- Asume la responsabilidad de proporcionar los servicios de sellado de tiempo conforme a la normativa aplicable.
- Puede operar con diferentes unidades identificables de sellado de tiempo (TSUs), cada una de las cuales puede tener su propia clave de firma.
- Está identificada en el certificado digital utilizado para los servicios de sellado de tiempo.
- Ofrece sus servicios a todos los suscriptores y terceras partes verificadoras de sellos de tiempo que se comprometan a cumplir con sus obligaciones
- Garantizar que la hora y fecha incluidas en los sellos se mantienen dentro de los márgenes precisión establecida en el contrato entre el cliente y DIGITEL TS que en ningún caso pueden ser superiores a un segundo.
- Emitir sellos de tiempo según la información enviada por el cliente y libres de errores de entrada de datos.
- Establecer los mecanismos de generación de la información relevante en las actividades descritas, protegiéndolas ante pérdida, destrucción o falsificación.
- Suministrar una fuente fiable de tiempo a las TSU delegadas y establecer los mecanismos técnicos necesarios para detectar cualquier variación de los datos de tiempo utilizados por las TSU, notificando a los usuarios cualquier desviación o pérdida de fiabilidad del sistema.
- Conservar la información sobre el certificado de TSU emitido por el período mínimo exigido por la normativa vigente.

4.5.3 Obligaciones del suscriptor del certificado de TSU

- Suministrar a la TSA de Digitel TS la información necesaria para realizar una correcta identificación.
- Realizar el pago del certificado de TSU conforme a la forma y medios establecidos por la TSA.
- Realizar los esfuerzos que razonablemente estén a su alcance para confirmar la exactitud y veracidad de la información suministrada.
- Notificar cualquier cambio en los datos aportados para la creación del certificado de TSU durante su periodo de validez.
- Respetar lo dispuesto en esta Política y en la DPC de Digitel TS.
- Proteger sus claves privadas de forma segura.
- Asegurarse de que su certificado de TSU no ha caducado ni este revocado antes de ofrecer el servicio de sellado de tiempo.
- Emitir sello de tiempo conforme a esta Política y a los estándares de aplicación.
- Ofrecer el servicio con los requisitos de disponibilidad y precisión.
- Informar inmediatamente a la TSA acerca de cualquier situación que pueda afectar a la validez del Certificado, o a la seguridad de las claves.
- Sincronizarse con las fuentes de tiempo marcadas por el Prestador.
- Someterse a la auditoria de sus sistemas por parte de la TSA o un tercero autorizado.
- Facilitar el acceso de la TSA a su servicio de sellado a los aplicativos con el objeto de establecer los controles correspondientes respecto a la corrección de la marca de hora.
- Facilitar el acceso de la TSA para recopilar información de los sellos emitidos o bien enviar un informe periódico sobre el número de sellos emitidos.

4.5.4 Obligaciones del suscriptor de los sellos de tiempo

El suscriptor de sellos de tiempo puede utilizar el Servicio de Sellado de Tiempo únicamente según especificaciones de ETSI EN 319 422.

El suscriptor debe verificar que el token de sello de tiempo ha sido correctamente firmado por la autoridad de sellado de tiempo, y que la clave privada utilizada para firmar el token de sello de tiempo no ha sido revocada.

El suscriptor debe cumplir con la presente Política de Sellado de Tiempo de DIGITELTS, disponible en <https://pki.digitelts.es/>

4.5.5 Obligaciones de terceras partes verificadoras de sellos de tiempo

Cuando se recibe un token de sello de tiempo, la tercera parte debe verificar que el token está correctamente firmado y que la clave privada utilizada para firmar el sello de tiempo no ha sido revocada.

Mientras el certificado utilizado para generar sellos de tiempo no esté caducado, es posible comprobar su validez en la CRL o OCSP correspondiente.

En el caso de que la verificación se realice después del periodo de validez del certificado, la tercera parte deberá comprobar que la función hash empleada, los algoritmos y longitud de claves criptográficas se pueden seguir considerando seguras.

Asimismo, deberán tener en cuenta cualquier limitación en el uso del sello de tiempo indicado en la política y prácticas de certificación correspondiente.

Tomar en consideración cualquier limite prescrito en otros acuerdos de servicio.

4.5.6 Responsabilidades

- DIGITELTS opera su TSA de acuerdo con la política de TSA de DIGITELTS, su DPC, y los términos de cualquier otro acuerdo vinculante entre DIGITELTS y usuarios del servicio de sellado de tiempo.
- DIGITELTS realiza esfuerzos para proporcionar alta disponibilidad en sus servicios, pero no ofrece una garantía total en cuanto a disponibilidad, ni la precisión en los sellos de tiempo.

- DIGITELTS no es responsable en ningún caso de pérdida de beneficios, daños indirectos o consecuentes, o pérdida de datos, en la medida en que la legislación vigente lo permita
 - DIGITELTS no será responsable de daños consecuencia de infracciones cometidas por el suscriptor o terceras partes en los términos y condiciones aplicables.
 - DIGITELTS no será bajo ninguna circunstancia responsable de daños consecuencia de eventos de fuerza mayor como desastres naturales, caídas de electricidad o telecomunicaciones, fuego, interacciones externas no predecibles como virus o ataques de hackers, acciones gubernamentales, o huelgas.
 - En cualquier caso, DIGITELTS realizará todas las medidas razonables para mitigar los efectos de tales eventos. Cualquier daño consecuencia de un retraso causado por un evento de fuerza mayor no será cubierto por DIGITELTS.

4.6 Publicación y repositorios

Conforme se estipula en el apartado 2 de la DPC de Digitel TS

4.7 Procedimiento de emisión de certificados de TSU

Conforme se estipula en la DPC de Digitel TS para la emisión y revocación de otro tipo de certificados electrónicos.

4.8 Procedimiento de emisión de un sello de tiempo

Con objeto de la prestación del Servicio de Sellado de Tiempo, DIGITELTS realiza la gestión de las claves correspondientes de conformidad con lo descrito en el apartado 6.2 *Protección de la clave privada y controles de los módulos criptográficos* de la DPC.

Los Sellos de Tiempo emitidos bajo esta política son firmados por certificados específicos, emitidos bajo la Cadena de Certificación de la Autoridad de Certificación subordinada con CN = DIGITELTS QUALIFIED CA TSA G1

Para obtener más información sobre la citada Cadena de Certificación de la Autoridad de Certificación raíz consultar el apartado 1.3.1 Prestador de servicios de certificación de la DPC.

4.9 Provisión y disponibilidad del servicio de sellado de tiempo

La emisión de Sellos de Tiempo se realizará ante la petición del usuario. Cuando éste desee obtener un Sello de Tiempo para un documento electrónico, calculará un valor o conjunto de valores hash a partir de este. Éste se incluirá en una estructura de petición de sello de tiempo, y será enviado a DIGITELTS para que proceda a la emisión del Sello de Tiempo correspondiente.

Este Sello de Tiempo vinculará, a través de la firma electrónica de DIGITELTS, los datos recibidos y la fecha y hora de la recepción.

Los algoritmos admitidos están descritos en el apartado 4.9.2 *Perfil de una petición de sello de tiempo* de este documento.

DIGITELTS no realizará comprobación o tratamiento alguno sobre la representación de los datos a sellar recibidos más allá de su inclusión en el propio Sello de Tiempo y en los sistemas de registro de eventos. DIGITELTS no verificará en modo alguno el contenido, ni la veracidad de la representación de los datos a sellar ni del origen de estos.

El Servicio de Sellado de Tiempo se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de la Autoridad de Certificación de DIGITELTS, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.8 de la DPC.

Las peticiones de sellos de tiempo electrónico utilizan las especificaciones descritas en la RFC3161.

4.10 Administración y operación de la TSA

4.10.1 Gestión de la Seguridad

La gestión de la seguridad de la TSA de DIGITELTS está descrita en el apartado 5. *Controles de seguridad física, de gestión y de operaciones* de la DPC.

4.10.2 Clasificación y gestión de activos

La TSA de DIGITELTS asegura que la información y otros activos reciben el tratamiento apropiado en cuanto a seguridad, según se define en el apartado 5.7 *Compromiso de claves y recuperación de desastre* de la DPC.

4.10.3 Seguridad del personal

Los controles de seguridad del personal están definidos en el apartado 5 *Controles de seguridad física, de gestión y de operaciones* de la DPC.

4.11 Controles criptográficos

4.11.1 Generación de la clave de la TSA

DIGITELTS genera las claves criptográficas en un entorno físicamente securizado y realizado por personal con roles de confianza bajo al menos control dual de la operativa. Las claves de la TSA de DIGITELTS son generadas siguiendo un procedimiento específico. La duración máxima del certificado de la TSA será de 5 años.

4.11.2 Protección de la clave privada de la TSU

Los sellos de tiempo que dan soporte a las autoridades de sellado de tiempo de DIGITELTS utilizan claves generadas según lo especificado en la DPC y se encuentran almacenadas en dispositivos de Primekey SignServer Appliance cumpliendo con los requisitos del perfil de protección FIPS 140-2 Level 3 validated HSM.

4.11.3 Distribución de la clave pública de la TSU

El certificado de la TSA de DIGITELTS está publicado en <https://www.pki.digitelts.es>

4.11.4 Renovación de clave privada de la TSU

La Autoridad de Certificación de DIGITELTS no renueva certificados.

4.11.5 Fin del ciclo de vida de la clave de la TSU

La TSA de DIGITELTS no permite firmar respuestas timestamp con un certificado caducado o revocado.

En el caso de finalización de servicios de la TSA de DIGITELTS, todas las claves privadas de los certificados de la TSA incluyendo copias de seguridad serán destruidas de forma que dichas claves sean irre recuperables.

4.11.6 Compromiso de la clave privada del certificado de TSA

- En caso de compromiso de una clave privada del servicio TSA de DIGITELTS se aplicará el procedimiento indicado en el punto 4.9.11 *Requisitos especiales en caso de compromiso de la clave privada* de la DPC.
 - En caso de compromiso de una clave privada del servicio TSA de DIGITELTS no se emitirán tokens timestamp.
- En el caso de comprometerse la precisión mínima de +/- 1 segundo definida no se emitirán sellos de tiempo hasta que se corrija la calibración.

4.12 Sellado de tiempo

4.12.1 Fuente de tiempo

Los registros están fechados con una fuente fiable vía NTP con conexión a la plataforma EQUINIX.

Los servidores de la Autoridad de Certificación de DIGITELTS están conectados a las fuentes primarias Equinix Precision Time NTP, con un nivel Stratum 1, desde Frankfurt, balanceada mediante dos IP como fuentes de tiempo en los appliance de la Autoridad de Certificación.

La hora empleada para registrar los sucesos del registro de auditoría deberá ser sincronizada con la UTC, como mínimo, una vez al día.

No es necesario que esta información se encuentre firmada digitalmente.

4.12.2 Perfil de una petición de sello de tiempo

- La petición de sello de tiempo deberá seguir la estructura definida en IETF RFC 3161 y RFC 5816.
- La petición debe seguir las indicaciones de ETSI EN 319 422
- Los algoritmos de hash aceptados serán SHA256 y SHA512. En cualquier caso, DIGITELTS sigue las recomendaciones de la industria en cuanto a suites criptográficas.

4.12.3 Perfil de certificado de TSU

Los OID de este certificado son:

- En la jerarquía propia: 1.3.6.1.4.1.54225.10.1.1
- En ETSI la política NCP+: 0.4.0.2042.1.2

Los certificados de sello electrónico de TSU son certificados que siguen las indicaciones de la política ETSI “NCP+” y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 421 y ETSI EN 319 422.

Este certificado permite a Unidades de Sellado de Tiempo o TSU emitir los sellos de tiempo electrónico cuando reciben una solicitud bajo las especificaciones de la RFC3161.

La información de usos en el perfil de certificado indica lo siguiente:

- El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones: Firma digital
- El campo “extend key usage” tiene activada la función: TimeStamping
- Este certificado no dispone de los campos QcStatements.

- El campo “User Notice” describe el uso de este certificado.

4.12. Controles de seguridad físicos, lógicos y de personal de la TSA

4.12.1. Controles de Seguridad física

Según lo dispuesto en la DPC de Digitel TS

4.12.2. Ubicación y construcción

Según lo dispuesto en la DPC de Digitel TS

4.12.3. Acceso físico

Según lo dispuesto en la DPC de Digitel TS

4.12.4 Alimentación eléctrica y aire acondicionado

Según lo dispuesto en la DPC de Digitel TS

4.12.5 Exposición al agua

Según lo dispuesto en la DPC de Digitel TS

4.12.6 Protección y prevención de incendios

Según lo dispuesto en la DPC de Digitel TS

4.12.7 Sistema de almacenamiento

Según lo dispuesto en la DPC de Digitel TS

4.12.8 Eliminación de residuos

Según lo dispuesto en la DPC de Digitel TS

4.13 Controles procedimentales y de personal

4.13.1 Roles de confianza

4.13.1.1 Número de personas requeridas por tarea

Las siguientes tareas requieren al menos un control dual:

- La generación de la clave de la TSA/TSU.
- La recuperación y back-up de la clave privada de la TSA/TSU.
- Activación de la clave privada de la TSA.
- Cualquier actividad realizada sobre los recursos HW y SW que dan soporte a la autoridad de certificación.

4.13.1.2 Identificación y autenticación para cada rol

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante tarjetas criptográficas y códigos de activación.

4.13.1.2.3. Controles de seguridad de personal

Según lo dispuesto en la DPC de Digitel TS

4.14 Procedimientos de registro de auditoría

Según lo dispuesto en la DPC de Digitel TS

4.15 Continuidad de negocio

Según lo dispuesto en la DPC de Digitel TS

4.16 Cese de la TSA

Según lo dispuesto en la DPC de Digitel TS