DIGITELTS

by MADISON

Servicio Cualificado de Sellado de Tiempo

Declaración de Prácticas y Políticas

Control Documental

Nombre	Declaración de Prácticas y Políticas Servicio Cualificado de Sellado de Tiempo de DIGITEL TS		
Distribución	**Público**		
Versión	V1.4		
Fecha	21/05/2026		
Aprobado	Comité de Riesgos y Seguridad de DIGITEL TS	Fecha	23/07/2026
Estado	Aprobado		

Control de Cambios

Versión	Fecha	Descripción
V1.0	01/04/2024	Versión inicial
V1.2	01/05/2024	Corrección de erratas
V1.3	01/05/2025	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 319 401 V3.1.1 (2024-06)
V1.4	21/05/2026	1. Revisión anual 2. Adaptación a la normativa siguiente: ▪ Reglamento de Ejecución (UE) 2025/1929 de la Comisión, de 29 de septiembre de 2025, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a en lo que respecta a la vinculación de la fecha y la hora con los datos y al establecimiento de la exactitud de las fuentes de información temporal para el suministro de sellos cualificados de tiempo electrónicos ▪ Reglamento de Ejecución (UE) 2025/2530 de la Comisión, de 16 de diciembre de 2025, por el que se establecen disposiciones de

		aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a los requisitos para los prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados 3. Cambio del título del documento

1. Introducción

1.1. Presentación

La presente Declaración de Prácticas y Políticas (en adelante DPP) describe las prácticas y las políticas adoptadas por DIGITEL TS, en su condición de Prestador de Servicios de Confianza (PSC), para la prestación del servicio cualificado de sellado de tiempo.

Este documento describe los principios generales de funcionamiento del servicio cualificado de sellado de tiempo gestionado por la Autoridad de Sellado de Tiempo (TSA) de DIGITEL TS, especificando los procesos, prácticas y políticas generales de la Autoridad de Sellado de Tiempo para la emisión de los sellos cualificados de tiempo, así como las medidas organizativas, técnicas y de seguridad implementadas y las responsabilidades de los participantes en este servicio.

El servicio cualificado de sellado de tiempo gestionado por la TSA de DIGITEL TS crea y registra evidencias digitales de la existencia de un dato en un instante determinado en la línea de tiempo, de una forma fiable, mejorando significativamente la fiabilidad de los datos electrónicos.

Adicionalmente, para facilitar la comprensión de los usuarios de los servicios amparados en esta DPP, DIGITEL TS publica un documento complementario denominado "Declaración de Divulgación de TSA" (en inglés TSA Disclosure Statement) para el servicio cualificado de sellado de tiempo, que recoge de forma simplificada la información más relevante del servicio. No obstante, dicha declaración de divulgación no pretende sustituir a la DPP ni a las políticas contenidas en esta.

En caso de contradicción entre este documento de Declaración de Prácticas y Políticas del servicio cualificado de sellado de tiempo prestado por DIGITEL TS y otros documentos relativos a dicho servicio, prevalecerá lo establecido en este documento.

DIGITEL TS presta su servicio cualificado de sellado de tiempo conforme al artículo 42 del Reglamento (UE) 2014/910 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") .

En adición, DIGITEL TS presta este servicio de confianza conforme a lo establecido en los siguientes Reglamentos de Ejecución por los que se establecen disposiciones de aplicación del Reglamento eIDAS:

- Reglamento de Ejecución (UE) 2025/2530 de la Comisión, de 16 de diciembre de 2025, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a los requisitos para los prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados.
- Reglamento de Ejecución (UE) 2025/1929 de la Comisión, de 29 de septiembre de 2025, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a la vinculación de la fecha y la hora con los datos y al establecimiento de la exactitud de las fuentes de información temporal para el suministro de sellos cualificados de tiempo electrónicos.

DIGITEL TS tiene en cuenta además lo estipulado en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza .

Para garantizar la ciberseguridad y la ciberresiliencia de los servicios amparados en esta DPP, DIGITEL TS ha alineado sus operaciones a los requisitos de seguridad de redes y de la información establecidos en la Directiva (UE) 2022/2555 (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.

Esta declaración de Prácticas y Políticas del servicio cualificado de sellado de tiempo 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	Electronic Signatures and Infrastructures (ESI); 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 (TSAs)
RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
RFC 5816	ESSCertIDv2 Update for RFC 3161
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

1.2. Nombre e identificación del documento

Nombre:	Declaración de Prácticas y Políticas Servicio Cualificado de Sellado de Tiempo de DIGITEL TS
Versión:	Ver página inicial
Localización:	https://pki.digitelts.es/

1.2.1. Identificadores de políticas de certificados y del servicio

La Autoridad de Certificación de DIGITEL TS ha asignado a cada política de certificados unos identificadores de objeto (OID), para su identificación en sus certificados por las aplicaciones.

Asimismo, la Autoridad de Sellado de Tiempo de DIGITEL TS ha asignado a la política de su servicio cualificado de sellado de tiempo un identificador de objeto (OID), para su identificación en sus sellos cualificados de tiempo por las aplicaciones.

A continuación se detallan todos los OID de políticas de los tipos de certificados de entidad final expedidos por DIGITEL TS y de servicios de sellado de tiempo prestados por DIGITEL TS aplicables a los sellos cualificados de tiempo expedidos por DIGITEL TS bajo esta DPP:

OID ETSI	OID DIGITEL TS	POLÍTICA
	1.3.6.1.4.1.54225.10.1	**Políticas de certificados de sello electrónico para servicios de confianza prestados por DIGITEL TS**
0.4.0.2042.1.2 [ETSI EN 319 411-1 NCP+]	**1.3.6.1.4.1.54225.10.1.1**	Certificado de sello electrónico para TSU
		Políticas de servicios de sellado de tiempo prestados por DIGITEL TS
0.4.0.2023.1.1 [ETSI EN 319 421 BTSP]	---------- [Sin OID]	Servicio cualificado de sellado de tiempo

1.3. Participantes en el servicio de sellado de tiempo

1.3.1. Prestador de servicios de sellado de tiempo (TSA)

Bajo esta DPP, DIGITEL TS es un Prestador Cualificado de Servicios de Confianza (PCSC) 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 de servicios de confianza en general (ETSI EN 319 401), y a los prestadores de servicios de confianza 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 su servicio cualificado de sellado de tiempo.

La TSA de DIGITEL TS es la entidad de confianza en la que los usuarios (suscriptores y terceras partes receptoras de sellos de tiempo) confían para la emisión de sellos de tiempo.

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 certificados de las TSU de la TSA de DIGITEL TS son emitidos por la siguiente jerarquía de Autoridades de Certificación de DIGITEL TS:

DIGITEL TS CA ROOT 01

Autoiridad de Certificación Raíz de la jerarquía de DIGITEL TS que emite certificados a otras Autoridades de Certificación Subordinadas, y cuyo certificado de clave pública ha sido autofirmado.

Datos de identificación:

Common Name	**DIGITEL TS CA ROOT 01**
Huella digital (SHA1)	f23aa0a06261b3685ce5f05de058f801d3031f15
Válido desde:	28-04-2022 15:55:07

Válido hasta:	22-04-2047 15:55:06
Longitud RSA	4096 bits

DIGITEL TS QUALIFIED CA TSA G1

Autoridad de Certificación Subordinada que expide los certificados de las TSU de la TSA de DIGITEL TS para que emitan sellos cualificados de tiempo. Su certificado ha sido firmado digitalmente por la Autoridad de Certificación Raíz DIGITEL TS CA ROOT 01.

Common Name	**DIGITEL TS QUALIFIED CA TSA G1**
Huella digital (SHA1)	b844d3988972165a54b85f09fc8d9b757aaddbb8
Valido desde	06-05-2022 13:35:16
Válido hasta:	03-05-2035 13:35:15
Longitud RSA	4096 bits

1.3.2. Suscriptor

Son las personas físicas y las organizaciones que formalizan una relación contractual con DIGITEL TS para la prestación del servicio de sellado cualificado de tiempo.

El suscriptor del servicio cualificado de sellado de tiempo es, por tanto, el cliente del prestador de servicios de confianza DIGITEL TS, de acuerdo con la legislación mercantil, y tiene los derechos y obligaciones que se definen por el prestador del servicio de confianza, sin

perjuicio de los derechos y obligaciones de los solicitantes de sellos de tiempo, si bien el suscriptor será responsable del incumpimiento de las obligaciones de los solicitantes de sellos de tiempo.

1.3.3. Solicitantes de sellos de tiempo

Son los usuarios en cada suscriptor que solicitan los sellos de tiempo a la TSA de DIGITEL TS, conforme a lo indicado en el punto anterior.

Adicionalmente, DIGITEL TS es el solicitante de los sellos de tiempo emitidos para su uso por el servicio cualificado de entrega electrónica certificada conforme a lo estipulado en la Declaración de Prácticas y Políticas de este servicio.

1.3.4. Partes que confían

Son las personas físicas y las organizaciones que confían en los sellos cuaiificados de tiempo emitidos por las TSU de la TSA de DIGITEL TS.

Como paso previo a confiar en los sellos cualificados de tiempo, las partes que confían deben verificarlos como se establece en esta Declaración de Prácticas y Políticas y, en su caso, en las correspondientes instrucciones disponibles en la página web de la Autoridad de Certificación de DIGITEL TS disponible en: https://pki.digitelts.es/

1.3.5. Otros participantes

DIGITEL TS podrá utilizar en la prestación de su servicio cualificado de sellado de tiempo los servicios de proveedores tecnológicos, incluidos proveedores de servicios de computación en la nube, bajo contratos que establezcan obligaciones de seguridad y confidencialidad acordes con esta DPP y la normativa aplicable.

La utilización de dichos proveedores no exime a DIGITEL TS de su responsabilidad como Prestador Cualificado de Servicios de Confianza.

1.4. Administración de políticas

1.4.1. Organización que administra el documento

Autoridad de Sellado de Tiempo de DIGITEL TS

DIGITEL ON TRUSTED SERVICES S.L.U.

C/ Enrique Cubero 9, Edificio Madison Arena - 47014 Valladolid (España)

+34 91 015 05 10

pki@digitelts.es

1.4.2. Datos de contacto de la organización

- Razón Social: DIGITEL ON TRUSTED SERVICES S.L.U.
- Denominación Comercial: Autoridad de Sellado de Tiempo de DIGITEL TS
- NIF: B47447560
- Domicilio Social: C/ Enrique Cubero 9, Edificio Madison Arena - 47014 Valladolid (España)
- Servicio de Atención al Cliente (SAC): +34 91 015 05 10
- Correo electrónico: info@digitelts.com
- Web: https://www.digitelts.es
- Identificación en el Registro Mercantil de Valladolid: Tomo 891, Folio 38, Sección 8, Hoja VA-11307

1.4.3. Responsables en el procedimiento de gestión del documento

El sistema documental y de organización de la TSA de DIGITEL TS garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones de servicio relacionados con el mismo.

El Comité de Riesgos y Seguridad de DIGITEL TS ostenta la capacidad para revisar y aprobar este procedimiento de revisión del documento.

1.4.4. Revisión del documento

La TSA de DIGITEL TS revisa este documento una vez al año, o tras la ocurrencia de algún incidente significativo o cambios significativos en las operaciones o en los riesgos. El

responsable del servicio será el responsable del mantenimiento de este documento siguiendo las indicaciones de la Política de Seguridad de DIGITEL.

El responsable de seguridad enviará al Comité de Riesgos y Seguridad de DIGITEL TS cambios, sugerencias y propuestas de modificaciones de este documento para su aprobación.

El Comité de Riesgos y Seguridad de DIGITEL TS analiza y aprueba las modificaciones propuestas a este documento y notificará al Organismo de Supervisión español en materia de servicios de confianza aquellas modificaciones significativas del servicio cualificado de sellado de tiempo amparado en esta Declaración de Prácticas y Políticas.

A efectos de este documento se consideran modificaciones significativas las definidas en el artículo 1 del Reglamento de Ejecución eIDAS (UE) 2025/2530. La notificación al Organismo de Supervisión español en materia de servicios de confianza se llevará a cabo con una antelación mínima de un mes antes de llevar a cabo las citadas modificaciones en los servicios de confianza cualificados, conforme estipula el artículo 24. 2 letra a) del Reglamento eIDAS.

Los cambios en esta Declaración de Prácticas y Políticas que puedan afectar a la aceptación del servicio por los suscriptores o por las partes que confían, serán informados con la publicación de este documento en la página web de DIGITEL TS https://pki.digitelts.es/.

Fases del procedimiento de cambios:

1. Recogida de propuestas.
2. Análisis y estudio de las propuestas.
3. Redacción de los borradores.
4. Presentación en el Comité de Riesgos y Seguridad de DIGITEL TS para comentarios y notificación al Organismo de Supervisión español.
5. Redacción final.
6. Notificación al Organismo de Supervisión español.

7. Al menos un mes después del paso anterior, presentación en el Comité de Riesgos y Seguridad de DIGITEL TS para su aprobación.
8. Inmediatamente después del paso anterior, publicación en la página web de DIGITEL TS https://pki.digitelts.es/.

La TSA de DIGITEL TS realiza una nueva revisión de este documento ante la inclusión de cambios suficientemente relevantes para la gestión del servicio cualificado de sellado de tiempo. La descripción de los cambios se incluirán en el apartado Control de Cambios en el inicio de este documento.

1.4.5. Aprobación del documento

Las modificaciones de esta Declaración de Prácticas y Políticas del servicio cualificado de sellado de tiempo, de la Política de Seguridad y de la Declaración de Divulgación de TSA son aprobadas por el Comité de Riesgos y Seguridad de DIGITEL TS, el cual de forma adicional se responsabilizará de su correcta implementación.

La TSA de DIGITEL TS comunica de forma permanente los cambios que se produzcan en sus obligaciones publicando nuevas versiones de su documentación jurídica en su página web https://pki.digitelts.es/

1.5. Definiciones y acrónimos

1.5.1. Definiciones

Concepto	Definición
Autoridad de Certificación	Es la entidad responsable de la emisión y gestión de los certificados digitales.

Autoridad de sellado de tiempo (TSA)	Prestador de servicios de confianza que presta servicios de sellado de tiempo mediante una o varias unidades de sellado de tiempo
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.
período de validez del certificado	Intervalo de tiempo comprendido desde «notBefore» («no antes de») hasta «notAfter» («no después de») inclusive, durante el cual la autoridad de certificación («CA») garantiza que mantendrá información sobre el estado del certificado. Los términos notBefore y notAfter se definen en el RFC 5280 de la IETF
Tiempo Universal Coordinado (UTC)	Escala de tiempo basada en el segundo, tal y como se define en la Recomendación UIT-R TF.460-6
segundo intercalar	Ajuste del UTC mediante la omisión o la adición de un segundo adicional en el último segundo de un mes UTC

sello de tiempo	Datos en formato electrónico que vinculan otros datos electrónicos a un momento concreto, estableciendo la prueba de que dichos datos existían en ese momento
Unidad de sellado de tiempo (TSU)	Conjunto de hardware y software que se gestiona como una unidad y tiene una única clave de firma de sellos de tiempo activa en cada momento
Declaración de divulgación de la TSA o (PDS)	Conjunto de declaraciones sobre las prácticas y políticas de una TSA que requieren especialmente énfasis o divulgación a los suscriptores y a las partes que confían en el servicio, por ejemplo, para cumplir requisitos reglamentarios
Reglamento eIDAS	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 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 de Ejecución eIDAS	Hace referencia a los Reglamentos de Ejecución por los que se establecen disposiciones de aplicación del Reglamento (UE) n. o 910/2014 del Parlamento Europeo y del Consejo en varias materias. A efectos del servicio de

emision de certificados se consideran relevante los siguientes:

- Reglamento de Ejecución (UE) 2025/1929 de la Comisión, de 29 de septiembre de 2025, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a la vinculación de la fecha y la hora con los datos y al establecimiento de la exactitud de las fuentes de información temporal para el suministro de sellos cualificados de tiempo electrónicos.

- Reglamento de Ejecución eIDAS (UE) 2025/2530: por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a los requisitos para los prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados

1.5.2. Siglas

Acrónimo	Definición
AC (o también CA)	Certification Authority Autoridad de Certificación
DPP	Declaración de Prácticas y Políticas
DPPC (o también CPS y CPs)	Certification Practice Statement and Certificate Policies Declaración de Prácticas y Políticas 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 Declaración 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
VPN	Virtual Private Network. Red privada virtual

EUCC	Esquema europeo de certificación de la ciberseguridad basado en los criterios comunes

2. Publicación de información y repositorios

2.1. Publicación de información del prestador

La TSA de DIGITEL TS publica la siguiente información en la dirección web https://pki.digitelts.es/:

- La Declaración de Prácticas y Políticas del servicio cualificado de sellado de tiempo, y el historial de sus versiones.
- La Declaración de Divulgación de TSA (TSA Disclosure Statement) – Términos y Condiciones, y el historial de sus versiones.
- Los certificados de las TSU vigentes (no expirados), indicando como "Desactivado" aquellos cuyas claves privadas han sido desactivadas de forma permanente, por lo que no volverán a ser usadas para la firma de sellos de tiempo.

Esta información se encuentra disponible las 24 horas de los 7 días de la semana. En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de la Autoridad de Sellado de Tiempo de DIGITEL TS, ésta realizará los mayores esfuerzos para asegurar que esta información no se encuentre indisponible durante más de 24 horas.

2.1.1. Términos y condiciones

La Autoridad de Sellado de tiempo de DIGITEL TS informa a las partes que confían en el servicio cualificado de sello de tiempo a través de esta Declaración de Prácticas y Políticas del servicio cualificado de sellado de tiempo y de la Declaración de Divulgación de TSA y regula la concreta prestación del servicio a los usuarios y suscriptores, mediante la documentación contractual de los términos y condiciones.

Dicha información, y los términos y condiciones, se suministra por medios electrónicos durante el proceso de contratación y de solicitud y emisión del certificado, y su aceptación es obligatoria y previa a la emisión del certificado. Asimismo, la aceptación expresa de los términos y condiciones y la PDS –aplicable queda incluida en la hoja de solicitud del certificado.

2.2. Frecuencia de publicación

La información del prestador de servicios de certificación, incluyendo las PDS y la Declaración de Prácticas y Políticas de Certificación, se publica en cuanto se encuentra disponible.

Los cambios en la Declaración de Prácticas de Confianza se rigen por lo establecido en la sección 1.4 de este documento.

2.3. Control de acceso

La Autoridad de Certificación de DIGITEL TS no limita el acceso de lectura a las informaciones establecidas en la sección 1, pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros, para proteger la integridad y autenticidad de la información, especialmente la información de estado de revocación de certificados TSU.

3. Gestión del servicio cualificado de sellado de tiempo

3.1. Despliegue y mantenimiento del servicio

La TSA de DIGITEL TS ha sido desplegada en sus propias infraestructuras y en caso de tercerizar el servicio o alguna de sus operaciones críticas, la TSA de DIGITEL TS asume la responsabilidad sobre su provisión conforme se indica en esta Declaración de Prácticas y Políticas del servicio cualificado de sellado de tiempo.

3.2. Política del servicio cualificado de sellado de tiempo

La TSA opera sus servicios de acuerdo con las reglas establecidas en la presente Declaración de Prácticas y Políticas, la PDS, los términos y condiciones del servicio y los documentos internos adicionales que definen los requerimientos técnicos, operativos y procedimentales.

La TSA de DIGITEL TS presta el servicio cualificado de sellado de tiempo de conformidad con los requisitos de política definidos por el estándar ETSI EN 319 421 para una Política de Sellado de Tiempo de Mejores Prácticas [BTSP] con **OID 0.4.0.2023.1.1** para las TSA que emiten sellos de tiempo, respaldados por certificados de clave pública, con una precisión de 1 segundo.

Para más información acerca del servicio puede utilizar la presente Declaración de Prácticas de Políticas del servicio, así como la Declaración de Divulgación de TSA, 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 las normas ETSI EN 319 421 y ETSI EN 319 422.
- Los algoritmos de hash aceptados por el servicio son SHA256, SHA384 y SHA512.
- 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.

3.3. Usos admitidos del servicio

Se debe utilizar el certificado de TSU exclusivamente para los usos autorizados en esta DPP 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.

3.4. Usos no autorizados o prohibidos

Bajo la presente DPP no se permite el uso que sea contrario a la legislacion 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 Declaración de Prácticas y Políticas del servicio.

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 de TSU, estos deberán utilizarse tal y como son suministrados por la CA de DIGITEL TS.

4. Obligaciones y responsabilidades

DIGITEL TS, como Entidad que emite sellos de tiempo de acuerdo con la presente DPP asume las siguientes obligaciones:

4.1. Obligaciones de la TSA

- Emitir sellos de tiempo conforme a los establecido en la presente DPP.
- Proteger sus claves privadas de forma segura.
- 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.
- Publicar esta DPP en su página web.
- Informar sobre las modificaciones de esta DPP 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.
- Emitir tokens de sello de tiempo (TST) seguros para usuarios de servicios de sellado de tiempo
- Asumir la responsabilidad de proporcionar los servicios de sellado de tiempo conforme a la normativa aplicable.
- Operar con diferentes unidades identificables de sellado de tiempo (TSUs), cada una de las cuales puede tener su propia clave de firma.
- Estar identificada en el certificado digital utilizado para los servicios de sellado de tiempo.
- Ofrecer 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 de tiempo se mantienen dentro de los márgenes de precisión establecidos en el contrato entre el cliente y DIGITEL TS de 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 perdida de fiabilidad del sistema.

- Conservar la información sobre el certificado de TSU emitido y las evidencias del servicio de sellado de tiempo por el período mínimo exigido por la normativa vigente.
- Custodiar los registros de auditoría del servicio por los plazos definidos en la normativa aplicable.
- Definir controles de seguridad alineados con las mejores prácticas para proteger el sistema y las claves privadas de los servicios.
- Notificar a las partes interesadas cualquier cambio significativo en este documento conforme se estipula en el apartado 1.4 de esta DPP.
- Gestionar los incidentes de seguridad relacionados con el servicio y notificar a las partes interesadas, incluidos los organismos de supervisión y autoridades de control competentes los incidentes significativos ocurrido en el servicio en los plazos definidos en la normativa aplicable.
- Emitir sello de tiempo conforme a esta DPP y a los estándares de aplicación.
- Ofrecer el servicio con los requisitos de disponibilidad y precisión.
- Sincronizarse con las fuentes de tiempo conforme a esta DPP.
- 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.

4.2. 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, en consecuencia, está obligado a:

- Cumplir con la presente DPP de DIGITEL TS y con los contratos suscritos con la TSA de DIGITEL TS
- Utilizar los servicios teniendo en cuenta las limitaciones definidas en la presente DPP
- Informar inmediatamente a la TSA de DIGITEL TS de cualquier incidencia del servicio que pueda afectar al servicio prestado o la validez de los sellos de tiempo.
- 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.

4.3. 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 cuanta cualquier limitación en el uso del sello de tiempo indicado en la presente DPP o en los acuerdos de servicio.

4.3.1. Responsabilidades

- DIGITEL TS opera su TSA de acuerdo con la presente DPP, y los términos de cualquier otro acuerdo vinculante entre DIGITEL TS y usuarios del servicio de sellado de tiempo.
- DIGITEL TS 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.

- DIGITEL TS 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
- DIGITEL TS no será responsable de daños consecuencia de infracciones cometidas por el suscriptor o terceras partes en los términos y condiciones aplicables.
- DIGITEL TS 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, DIGITEL TS 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 DIGITEL TS.

4.4. Procedimiento de emisión de certificados de TSU

Conforme se estipula en la Declaración de Prácticas y Políticas de Certificación de DIGITEL TS

4.5. Procedimiento de emisión de un sello de tiempo

Con objeto de la prestación del Servicio de Sellado de Tiempo, DIGITEL TS 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 Declaración de Prácticas y Políticas de Certificación de DIGITEL TS

Los Sellos de Tiempo emitidos bajo esta DPP son firmados por certificados específicos, emitidos bajo la Cadena de Certificación de la Autoridad de Certificación Subordinada con CN = DIGITEL TS 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 Declaración de Prácticas y Políticas de Certificación de DIGITEL TS

4.6. Provisión y disponibilidad del servicio de sellado de tiempo

La emisión de Sellos de Tiempo se realiza ante la petición del usuario. Cuando éste desee obtener un Sello de Tiempo para un documento electrónico, calcular un valor o conjunto de valores hash a partir de este. Éste se incluye en una estructura de petición de sello de tiempo, y es enviado a DIGITEL TS para que proceda a la emisión del Sello de Tiempo correspondiente.

Este Sello de Tiempo vincula, a través de la firma electrónica de DIGITEL TS, los datos recibidos y la fecha y hora de la recepción.

Los algoritmos admitidos están descritos en el apartado *6.2 Perfil de una petición de sello de tiempo* de este documento.

DIGITEL TS no realiza 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. DIGITEL TS no verifica 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, durante todo el año, con excepción de las paradas programadas.

Las peticiones de sellos de tiempo electrónico utilizan las especificaciones descritas en la RFC 3161.

5. Administración y operación de la TSA

5.1. Gestión de la Seguridad

La gestión de la seguridad de la TSA de DIGITEL TS está descrita en el apartado *5. Controles de seguridad física, de gestión y de operaciones* de la Declaración de Prácticas y Políticas de Certificación de DIGITEL TS.

5.2. Clasificación y gestión de activos

La TSA de DIGITEL TS 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 Declaración de Prácticas y Políticas de Certificación de DIGITEL TS.

5.3. 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 DPPC.

5.4. Controles criptográficos

5.4.1. Generación de la claves de las TSU

DIGITEL TS 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 las TSU de la TSA de DIGITEL TS son generadas siguiendo un procedimiento específico. La duración máxima del certificado de las TSU de será de 6 años.

DIGITEL TS garantiza que la generación de las claves de la TSU se llevará a cabo, para nuevas TSU, dentro de un dispositivo HSM con la certificación FIPS 140-3 Level 3 (hasta el 31/12/2030) o Common Criteria EAL4 o superior.

Los algoritmos de generación de claves de la TSU, la longitud de clave de firma resultante y el algoritmo de firma utilizado para firmar sellos de tiempo y certificados de clave pública de la TSU, respectivamente se definen en el apartado 6.1 de la Declaración de Prácticas y Políticas de Certificación de DIGITEL TS.

5.4.2. Protección de la clave privada de la TSU

Las TSU de la Autoridad de Sellado de Tiempo de DIGITEL TS utilizan claves almacenadas en dispositivos HSM con la certificación FIPS 140-3 Level 3[1] (hasta el 31/12/2030) o Common Criteria EAL4 o superior.

5.4.3. Distribución de la clave pública de la TSU

La TSA de DIGITEL TS publica en la dirección web https://pki.digitelts.es/ los certificados vigentes (no expirados) de sus TSU, indicando como "Desactivado" aquellos cuyas claves privadas han sido desactivadas de forma permanente, por lo que no volverán a ser usadas para la firma de sellos de tiempo.

5.4.4. Renovación de clave privada de la TSU

La Autoridad de Certificación de DIGITEL TS no renueva certificados de TSU, sino que emite certificados a nuevas TSU.

5.4.5. Fin del ciclo de vida de la claves de la TSU

Conforme a lo establecido en la norma ETSI EN 319 421, la clave privada de una TSU no podrá ser usada después de su fecha de expiración definida por la TSA, la cual no podrá ser posterior a la fecha de expiración del certificado de TSU asociado.

La TSA de DIGITEL TS ha definido para las claves privadas de todas sus TSU con certificados vigentes actualmente un periodo de validez de 4 años, siendo el periodo de validez de todos los certificados de TSU asociados 6 años, lo cual garantiza que todos los sellos de tiempo emitidos por las TSU podrán ser validados durante un tiempo mínimo de 2 años.

[1] [1] En el momento de la edición de la versión V1.4 del presente documento, las TSU activas de la Autoridad de Sellado de Tiempo de DIGITEL TS siguen utilizando dispositivos HSM con certificación FIPS 140-2 Level 3, si bien estos dispositivos serán migrados próximamente a nuevos HSM con la certificación FIPS 140-3 Level 3 (hasta el 31/12/2030) o Common Criteria EAL4 o superior, conforme a un plan de transición presentado al Organismo de Supervisión

A continuación, se indica para cada TSU de la TSA de DIGITEL TS con certificado actualmente vigente (no expirado), el valor del atributo CN del campo subject, el algoritmo y tamaño de sus claves y las fechas de expiración de su clave privada y su certificado asociado, indicando como **(Desactivada)** aquellas TSU cuyas claves privadas han sido desactivadas de forma permanente, por lo que no volverán a ser usadas para la firma de sellos de tiempo.

CN	Algoritmo y tamaño claves	Expiración Clave privada	Expiración Certificado
DIGITEL TS QUALIFIED TSU 01 G1 **(Desactivada)**	RSA 4096 bits	30/06/2026	28/06/2028
DIGITEL TS QUALIFIED TSU 01 G2 **(Desactivada)**	RSA 4096 bits	30/06/2026	28/06/2028
DIGITEL TS QUALIFIED TSU 01 G3 EDCSA	EDCSA 256 bits	16/03/2027	14/03/2029
DIGITEL TS QUALIFIED TSU 01 G4 EDCSA	EDCSA 256 bits	16/03/2027	14/03/2029
DIGITEL TS QUALIFIED TSU 01 G5 EDCSA	EDCSA 256 bits	16/03/2027	14/03/2029
DIGITEL TS QUALIFIED TSU 01 G6 EDCSA	EDCSA 256 bits	16/03/2027	14/03/2029
DIGITEL TS QUALIFIED TSU RSA2048 01 G7 **(Desactivada)**	RSA 2048 bits	10/03/2027	08/03/2029
DIGITEL TS QUALIFIED TSU RSA2048 01 G8 **(Desactivada)**	RSA 2048 bits	10/03/2027	08/03/2029

Las claves privadas de TSU expiradas, incluyendo sus copias de seguridad, serán destruidas de forma que dichas claves sean irrecuperables.

En el caso de finalización del servicio cualificado de sellado de tiempo de la TSA de DIGITEL TS, todas las claves privadas de sus TSU, incluyendo sus copias de seguridad, serán destruidas de forma que dichas claves sean irrecuperables.

5.4.6. Compromiso de la clave privada de una TSU

En caso de compromiso de una clave privada una TSA de la TSA de DIGITEL TS se aplicará el procedimiento indicado en el apartado *4.9.11 Requisitos especiales en caso de compromiso de la clave privada* de la Declaración de Prácticas y Políticas de Certificación de DIGITEL TS.

En caso de compromiso de la clave privada de una TSU de la TSA de DIGITEL TS no se emitirán sellos de tiempo a través de esa TSU.

En el caso de comprometerse la precisión mínima de +/- 1 segundo definida, no se emitirán sellos de tiempo hasta que se corrija la calibración.

6. Sellado de tiempo

6.1. Fuente de tiempo

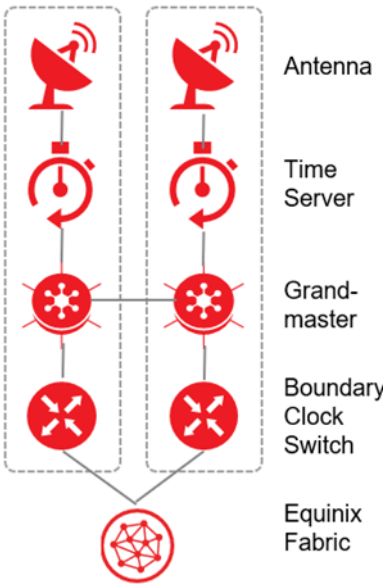
Los servidores de las TSU de la TSA de DIGITEL TS tienen un procedimiento de sincronización de tiempo coordinado mediante **Equinix Precision Time**, dicho servicio basado en suscripción provee una sincronización de tiempo preciso, seguro y confiable para aplicaciones empresariales.

El servicio *NTP Equinix Precision Time* dispone de las siguientes características:

- Fuentes de tiempo NTP Stratum 1 con antenas GNSS de alta precisión con oscilador de rubidio.
- Ubicación geográfica de las fuentes de tiempo localizadas en Frankfurt y Londres.
- Comunicación con las fuentes de tiempo mediante protocolo NTP.
- Redundancia del servicio mediante la configuración de 2 IPs diferentes de fuentes de tiempo NTP.
- Niveles de precisión del servicio de entre 30–40 µs.
- Acuerdo del nivel del servicio (SLA) garantizado de un 99,99% de disponibilidad.
- Aislamiento de la ruta de red de extremo a extremo mediante la ampliación del dominio de capa 2 desde los *appliance* de DIGITEL TS hasta las fuentes del tiempo a través del direccionamiento IP privado.

- Comunicaciones privadas de extremo a extremo mediante la red troncal de alto rendimiento de **Equinix Fabric**[2].

- Soporte para hasta 1000 clientes NTP.



Adicionalmente, se realiza una sincronización de tiempo de los servidores de las TSU de la TSA de DIGITEL TS mediante el protocolo NTP con la fuente de tiempo UTC Statrum 1 de la Sección de Hora del Real Instituto y Observatorio de la Armada en San Fernando (ROA).

Se realiza una monitorización en todo momento de ambas sincronizaciones de tiempo.

6.2. 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

[2] https://www.equinix.es/interconnection-services/equinix-fabric

- Los algoritmos de hash aceptados serán SHA256, SHA384 y SHA512. En cualquier caso, DIGITEL TS sigue las recomendaciones de la industria en cuanto a suites criptográficas.
- El cliente y el servidor de sellado de tiempo admitirán el protocolo de sellado de tiempo a través de HTTPS, tal como se define en la cláusula 3.4 de IETF RFC 3161.

6.3. Perfil de certificado de TSU

Los OID de este certificado son:

- En DIGITEL TS: **1.3.6.1.4.1.54225.10.1.1**
- En ETSI, política NCP+: **0.4.0.2042.1.2**

Este certificado es un certificado de sello electrónico de acuerdo con el Reglamento eIDAS, con las indicaciones adicionales para la creación de sellos cualificados de tiempo de acuerdo con el artículo 42 del Reglamento eIDAS, y da cumplimiento a lo dispuesto en las normas técnicas ETSI EN 319 411-1 (política **NCP+**), ETSI EN 319 421 y ETSI EN 319 422.

Este certificado permite a Unidades de Sellado de Tiempo (TSU) de la Autoridad de Sellado de Tiempo (TSA) de DIGITEL TS emitir los sellos cualificados de tiempo electrónicos cuando reciben una solicitud bajo las especificaciones en la norma técnica RFC 3161.

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

- La extensión Key Usage, marcada como crítica, tiene activada la funcion de firma digital
- La extensión Extended Key Usage, marcada como crítica, tiene activada la función de sellado de tiempo

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

6.4.1. Controles de Seguridad física

La TSA de DIGITEL TS, basándose en los resultados de sus evaluaciones de riesgos, ha establecido controles de seguridad física y ambiental alineados con el Reglamento (UE) 910/2014 (Reglamento Eidas) y con lo establecido en artículo 21 de la Directiva (UE) 2555/2022 (NIS2) y su Reglamento de Ejecución 2690 de fecha 17 de octubre de 2024, con el fin de proteger los recursos de las instalaciones donde se encuentran los sistemas y los equipamientos empleados para las operaciones de registro y aprobación de las solicitudes, generación técnica de los certificados, gestión de la TSA y de los sistemas relacionados con la gestión del sellado de tiempo y la gestión del hardware criptográfico.

En concreto, la política de seguridad física y ambiental aplicable a los servicios cualificados ha establecido prescripciones para las siguientes contingencias:

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

Estas medidas resultan aplicables a las instalaciones donde gestionan los servicios cualificados de sello de tiempo bajo la plena responsabilidad de la Autoridad de Sellado de

Tiempo de DIGITEL TS, que la presta desde sus instalaciones de alta seguridad, tanto principales como, en su caso, de operación en contingencia, que son debidamente, probadas, revisadas y en su caso actualizadas de forma periódica, o tras incidentes significativos, o con motivo de cambios significativos en las operaciones o en los riesgos.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso.

6.4.2. Ubicación y construcción

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

La sala donde se realizan las operaciones del servicio cualificado en el Centro de Proceso de Datos:

- Cuenta con redundancia en sus infraestructuras.
- Cuenta con varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.
- Las operaciones de mantenimiento no requieren que el Centro esté offline en ningún momento.

La Autoridad de Sellado de Tiempo de DIGITEL TS dispone de instalaciones que protegen físicamente la prestación de los servicios cualificados de sellado de tiempo, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de estos.

6.4.3. Acceso físico

La TSA de DIGITEL TS dispone de tres niveles de seguridad física (Entrada del Edificio donde se ubica el CPD, acceso a la sala del CPD y acceso al RAC) para la protección del servicio cualificado, debiendo accederse desde los niveles inferiores a los niveles superiores.

El acceso físico a las dependencias de la TSA de DIGITEL TS donde se llevan a cabo procesos del servicio cualificado de sello de tiempo está limitado y protegido mediante una combinación de medidas físicas y procedimentales. De esta forma se siguen las siguientes indicaciones:

- Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro de este, incluyendo filmación por circuito cerrado de televisión y su archivo.
- El acceso a las salas se realiza con lectores de tarjeta de identificación y huella biométrica y es gestionado por un sistema informático que mantiene un log de entradas y salidas automático.
- Para el acceso al rack donde se ubican los procesos criptográficos es necesario la autorización previa de la TSA de DIGITEL TS a los administradores del servicio de hospedaje que disponen de la llave para abrir la cabina.

En cuanto al acceso a las salas de acceso restringido en el CPD existe un listado con las personas autorizadas a pedir acceso a las personas que dependen directamente de ellos como empleado o como externos.

Para la intervención de un tercero en el CPD se requiere que los responsables de la gestión del CPD conozcan previamente el detalle de la intervención y se planifique en tiempo.

Para ello hay que abrir una solicitud de acceso donde indicar:

- Personal que accederá a la sala y rol

- Identificar elementos a los que es necesario acceder (elemento o rack completo en el caso de que sea dedicado)
- Acciones que se van a realizar.
- Fecha de la visita
- Duración.

El personal externo a DIGITEL TS que acceda al CPD con motivo de estas intervenciones deberá estar acompañado por uno de los responsables de la gestión del CPD durante todo el tiempo que se encuentre en el área segura.

6.4.4. Alimentación eléctrica y aire acondicionado

Las instalaciones de la TSA de DIGITEL TS disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado

6.4.5. Exposición al agua

Según lo dispuesto en el apartado 5.1.4 de la Declaración de Prácticas y Políticas de Certificación de DIGITEL TS. Las instalaciones están ubicadas en una zona de bajo riesgo de inundación.

Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad

6.4.6. Protección y prevención de incendios

Las instalaciones y activos de la TSA de DIGITEL TS cuentan con sistemas automáticos de detección y extinción de incendios.

6.4.7. Almacenamiento de soportes

Únicamente personal autorizado tiene acceso a los medios de almacenamiento.

La información de más alto nivel de clasificación se guarda en una caja fuerte fuera de las instalaciones de los Centros de Procesos de Datos.

6.4.8. Tratamiento de residuos

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

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

En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

6.4.9. Copia de seguridad fuera de las instalaciones

No se realizan copias de respaldo fuera de las instalaciones, ya que las copias de respaldo de cada centro de proceso de datos se almacenan en el otro centro de proceso de datos, de forma cruzada, generando así la redundancia necesaria.

6.5. Controles de procedimientos

La TSA de DIGITEL TS garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal al servicio de la TSA de DIGITEL TS ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

6.6. Roles de confianza

Según lo dispuesto en el apartado 5.2.1 de la Declaración de Prácticas y Políticas de Certificación de DIGITEL TS

- **Auditor de Sistemas (*System Auditors*[3] en ETSI 319 401):** autorizado para ver los archivos y registros de auditoría de los sistemas que soportan el servicio cualificado de sellado de tiempo de DIGITEL TS.
- **Administrador de Sistemas (*System Administrators*[4] en ETSI 319 401):** responsable del funcionamiento correcto del hardware y software de los sitemas que soportan el servicio cualificado de sellado de de tiempo. Autorizado para instalar, configurar, mantener los sistemas y gestionar el servicio, incluida la recuperación de los sistemas.
- **Operador del Sistema (*System Operators*[5] en ETSI 319 401):** responsables de las operaciones diarias de los sistemas para el servicio cualificado de sellado de tiempo. Autorizados a realizar copias de seguridad del sistema.
- **Responsable de Seguridad (*Security Officers*6 en ETSI 319 401):** encargado de coordinar, controlar y hacer cumplir las prácticas de seguridad relacionadas con el servicio cualificiado de sellado de tiempo, definidas por las políticas de seguridad de DIGITEL TS. Se encarga de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

6.6.1.Número de personas requeridas por tarea

La TSA de DIGITEL TS garantiza que 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.

[3] REQ-7.2-14X d) ETSI EN 319401
[4] EQ-7.2-14X b) ETSI EN 319401
[5] EQ-7.2-14X c) ETSI EN 319401
[6] EQ-7.2-14X a) ETSI EN 319401

- Activación de la clave privada de la TSA.
- Cualquier actividad realizada sobre los recursos HW y SW que dan soporte al servicio cualificado de sello de tiempo.

6.6.2. Identificación y autentificación para cada rol

Las personas asignadas para cada rol de confianza serán designadas formalmente para desempeñar funciones de confianza. Estas funciones deben ser aceptadas por la persona designada a desempeñarlas. El personal que ocupa puestos de confianza está libre de conflicto de intereses que puedan afectar a su imparcialidad en las operaciones de la Autoridad de Certificación de DIGITEL TS.

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.

6.6.3. Segregación de tareas

DIGITEL TS garantiza la separación de las funciones y áreas de responsabilidad que puedan entrar en conflicto en el marco de la gestión operativa del servicio cualificado de sello de tiempo electrónico, con el fin de minimizar las posibilidades de modificación no autorizada o involuntaria, o de uso indebido, de los activos del servicio.

6.7. Controles de seguridad de personal

6.7.1.Requisitos de historial, calificaciones, experiencia y autorización

Todo el personal que realiza tareas calificadas como confiables lleva al menos un año trabajando en el centro de producción y tiene contratos laborales fijos.

El personal de DIGITEL TS en funciones de confianza y, en su caso, sus subcontratistas en funciones de confianza cumplen el requisito de poseer los conocimientos especializados, la experiencia y las cualificaciones necesarios obtenidos a través de formación y credenciales formales, o de la experiencia real, o de una combinación de ambas cosas.

Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas. DIGITEL TS realiza acciones de formación para el personal que ocupa puestos de confianza en materia de seguridad, privacidad y servicios de confianza. Estas formaciones se actualizan con periodicidad mínima anual para incluir las nuevas amenazas y las prácticas de seguridad actuales.

El personal en puestos de confianza no tiene intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

En general, la TSA de DIGITEL TS retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

La TSA de DIGITEL TS no asignará a un puesto de confianza o de gestión a una persona que no sea idónea para el puesto, especialmente por haber sido condenada por delito o falta que afecte su idoneidad para el desempeño de las funciones. Por este motivo, previamente se realiza una investigación hasta donde permita la legislación aplicable, relativa a los siguientes aspectos:

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

6.7.2. Procedimientos de investigación de historial

La TSA de DIGITEL TS, antes de contratar a una persona o de que ésta acceda al puesto de trabajo, realiza las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años
- Referencias profesionales
- Estudios, incluyendo titulación alegada.

La TSA de DIGITEL TS realiza dichas comprobaciones con observancia estricta del 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 (RGPD), y con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos (LOPDGDD).

La investigación se repetirá con una periodicidad suficiente.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

En la solicitud para el puesto de trabajo se informa acerca de la necesidad de someterse a una investigación previa, advirtiéndose de que la negativa a someterse a la investigación implicará el rechazo de la solicitud.

6.7.3. Requisitos de formación

La TSA de DIGITEL TS forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo evidencias de dichas formaciones.

Los programas de formación son actualizados y mejorados con periodicidad anual. La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad de la Autoridad de Certificación de DIGITEL TS. Uso y operación de dispositivos y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de gestión de incidentes, gestión de situaciones de crisis y gestión de la continuidad de negocio,
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.
- Procesos de identidad de solicitantes de certificados y medidas de seguridad de documentos de identificación.

Adicionalmente, DIGITEL TS desarrolla programas de sensibilización y formación en materia de ciberseguridad para los empleados, los miembros de los órganos de dirección; así como, para proveedores directos y otros proveedores de servicios. En particular sobre:

- Ciberamenazas relevantes y medidas de gestión de riesgos aplicadas.
- Puntos de contacto y recursos disponibles para obtener información adicional y asesoramiento en materia de ciberseguridad.
- Prácticas básicas de ciberhigiene.

Estos programas de sensibilización y formación están alineados con la Directiva NIS2 y con los compromisos de DIGITEL TS de fomentar la cultura en materia de ciberseguridad y ciberresiliencia digital.

6.7.4. Requisitos y frecuencia de actualización formativa

La TSA de DIGITEL TS actualiza la formación del personal de acuerdo con las necesidades, y con la frecuencia suficientes para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación,

o cuando se produzcan cambios en las prácticas de ciberhigiene, así como en el panorama actual de amenazas y los riesgos de ciberseguridad para la prestación del servicio.

6.7.5. Secuencia y frecuencia de rotación laboral

Sin estipulación.

6.7.6. Sanciones para acciones no autorizadas

La TSA de DIGITEL TS dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable y, en especial, coordinado con el sistema sancionador del convenio colectivo que resulte de aplicación al personal.

Las acciones disciplinarias incluyen la suspensión y el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

6.7.7. Requisitos de contratación de profesionales

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por la TSA de DIGITEL TS. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios cualificados de sello de tiempo sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la DPP del servicio, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de sello de tiempo, no obstante, lo cual, la TSA de DIGITEL TS será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios cualificados de sello de tiempo por tercero distinto a la TSA de DIGITEL TS.

En todo caso, estos terceros deberán cumplir los mismos requisitos exigidos para los empleados de DIGITEL TS, tanto de formación previa como, conocimientos especializados, experiencia y/o

cualificación de habilidades para ejecutar las funciones específicas de los roles de confianza de la TSA de DIGITEL TS.

6.7.8. Suministro de documentación al personal

El prestador de servicios cualificados de sello de tiempo suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

6.8. Procedimientos de registro de auditoría de seguridad

La TSA de DIGITEL TS está sujeta a las validaciones cada dos años por medio de auditorías sobre protección de datos y cada 3 años de ISO 27001, con revisiones anuales. DIGITEL TS realiza, también, un análisis de riesgo anual. Además, dispone de una revisión interna mensual y auditoría externa anual de revisión de seguridad con el objetivo de identificar y analizar las vulnerabilidades potencialmente explotables.

Asimismo, DIGITEL TS ha implantado los requisitos de seguridad y principios básicos del Esquema Nacional de Seguridad (ENS) obteniendo una certificación de Nivel Medio conforme a lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

6.8.1. Tipos de eventos registrados

La TSA de DIGITEL TS produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Caídas del sistema y fallos de hardware, actividades de firewall y router e intentos de acceso al sistema
- Intentos de accesos no autorizados al sistema de la TSA a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.

- Cambios en la configuración y mantenimiento del sistema.
- Acceso o cambios en archivos de configuración críticos y copias de seguridad.
- Registros de las aplicaciones de la TSA.
- Encendido y apagado de la aplicación de la TSA
- Cambios en los detalles de la TSA y/o sus claves.
- Cambios en la creación de políticas de certificados TSU
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de este.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida de las claves de la TSU y de sus certificados
- Tráfico de red saliente y entrante.
- Eventos relacionados con la sincronización de los relojes de la TSA/TSU con UTC, incluidos los eventos de recalibración o sincronización de los relojes utilizados para el servicio de sellado de tiempo electrónico. También los eventos de perdida de sincronización.
- Las actividades de los cortafuegos y enrutadores
- Registros de acceso físico.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al servicio de sellado de tiempo.
- Registros de eventos y registros de herramientas de seguridad, como antivirus, sistemas de detección de intrusiones o cortafuegos.
- Uso de los recursos del sistema, así como su rendimiento.
- Acceso y uso de sus equipos y dispositivos de red.
- Activación, parada y pausa de los distintos registros.

Adicionalmente la TSA de DIGITEL TS registra:

- Acontecimientos medioambientales que impacten en los servicios
- Cambios en la Política de Seguridad
- La documentación presentada por el suscriptor del servicio cualificado de sellado de tiempo

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.

- Tipo de entrada.

La TSA de DIGITEL TS revisa sus logs periódicamente y en cualquier caso cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

La TSA de DIGITEL TS conserva las evidencias de la prestación del servicio cualificado de sellos de tiempo, incluidos los logs de auditoría, al menos durante 15 años desde el cese del servicio.

La conservación de esta información se lleva a cabo en condiciones de seguridad y los registros están protegidos de manipulación, borrado o eliminación mediante la firma de los ficheros que los contienen.

El acceso a los ficheros de logs está reservado solo a las personas autorizadas. Asimismo, los dispositivos son manejados en todo momento por personal autorizado.

Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

6.8.2. Procedimiento de copias de seguridad

La TSA de DIGITEL TS dispone de un procedimiento adecuado de copias de seguridad de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de seguridad de los logs.

La TSA de DIGITEL TS tiene implementado un procedimiento de copia de seguridad seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs.

6.9. Localización del sistema de acumulación de registros

La información de la auditoria de eventos es recogida automáticamente por el sistema operativo, las comunicaciones de red y por el software de gestión de sellos de tiempo, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

6.10. Notificación del evento de auditoría al causante del evento

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

6.11. Análisis de vulnerabilidades

Toda la infraestructura del servicio cualificado de sello de tiempo es objeto de una evaluación de vulnerabilidades mensualmente (con pruebas de penetración al menos una vez al año) y siempre que una parte crítica de la infraestructura se vea afectada. Esta evaluación es llevada a cabo por proveedores externos con personal cualificado, y cubre los siguientes elementos:

- Pentesting: sobre las URLs externas, redes y sistemas de información.
- Análisis de vulnerabilidades de los sistemas de información y parcheo.

Las vulnerabilidades detectadas se tratarán según los procedimientos existentes, los cuales incluyen clasificación, categorización, identificación y aplicación de parches. Serán priorizadas en función de su criticidad, estableciéndose un plazo máximo de resolución de 48 horas para las categorizadas como críticas.

6.12. Archivos de informaciones

6.12.1. Tipos de registros archivados

La TSA de DIGITEL TS, garantiza que toda la información relativa al servicio cualificado de sellado de tiempo y a la emisión de certificados de TSU se conserva durante un período de tiempo apropiado conforme a lo establecido en la legislación aplicable.

Los siguientes documentos implicados en el ciclo de vida del Servicio cualificado de sellado de tiempo son almacenados por la TSA de DIGITEL TS:

- Todos los datos de auditoría de sistema (PKI, TSA y OCSP).
- Todos los datos relativos a los certificados de TSU, incluyendo los contratos con los titulares y los datos relativos a su identificación y su ubicación.
- Solicitudes de emisión y revocación de certificados TSU, incluidos todos los informes relativos al proceso de revocación.
- CRLs emitidas o registros del estado de los certificados de TSU generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos del servicio cualificado de sellado de tiempo
- Las Declaraciones de Prácticas y Políticas del servicio cualificado de sellado de tiempo publicadas.
- Todos los datos de auditoría identificados en la sección 4
- Información de solicitudes de sellos de tiempo cualificados
- Documentación aportada para justificar las solicitudes del servicio
- Sincronización y eventos relacionados con la perdida de sincronización del reloj con las fuentes de tiempo UTC

6.12.2. Período de conservación de registros

La TSA de DIGITEL TS archiva los registros especificados anteriormente durante 15 años tras la finalización del servicio o desde la finalización de la vigencia del certificado al que están asociadas.

6.12.3. Protección del archivo

La TSA de DIGITEL TS protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo es protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.

La TSA de DIGITEL TS asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas.

6.12.4. Procedimientos de copia de seguridad

La TSA de DIGITEL TS como mínimo realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos y realiza copias de respaldo completas semanalmente para casos de recuperación de datos.

6.13. Compromiso de claves y recuperación de desastre

6.14. Procedimientos de gestión de incidencias y compromisos

DIGITEL TS dispone de un Plan de Continuidad del negocio en el que se indican las actuaciones a realizar en casos de desastre. Se cuenta con un sistema de copia de seguridad que almacena de forma segura aquellos datos necesarios para reanudar las operaciones de los sistemas que dan soporte a la TSA de DIGITEL TS. Se incluye también las oportunas referencias al centro de respaldo alternativo que garantice que toda la información esencial y las aplicaciones puedan recuperarse ante un desastre o fallo.

El Plan de continuidad de negocio incluye también las medidas en caso de compromiso o sospecha de compromiso de claves privadas de la TSU o la perdida de calibración de un reloj del servicio de sellado de tiempo.

Las medidas definidas en el Plan de Continuidad de negocio se fundamentan en los resultados del análisis del impacto potencial de perturbaciones graves en las operaciones de la CA y a TSA de DIGITEL TS.

La TSA de DIGITEL TS prueba los medios alternativos mediante simulacros al menos una vez al año. De esta forma, se establecen procedimientos de entrenamiento, prueba y mantenimiento de este plan. Todo el personal, se entrena en el proceso de recuperación del Plan de Contingencia. Esto es particularmente importante dado que los procedimientos son significativamente diferentes de las operaciones normales y se requiere un desempeño excelente para garantizar la restauración de los equipos y sistemas.

Las actividades indicadas en el plan de recuperación de desastres se diseñan acorde con los parámetros de continuidad (RTO y RPO) definidos para los servicios.

Para garantizar de forma proactiva la continuidad del servicio, se cuenta con una estructura redundada en dos CPD's en configuración activo-activo, lo que permite un nivel de redundancia adecuado para garantizar los niveles de servicio. En caso de producirse un desastre que llegase a inhabilitar uno de ellos, el otro CPD puede asumir la carga de forma completa incluso bajo condiciones de alta carga de demanda.

Ambos Centros de proceso de datos se encuentran ubicados en un prestador de servicios de alojamiento con nivel de disponibilidad mínimo Tier III, así como en posesión de las principales certificaciones de gestión de la seguridad y del servicio (ISO 27001, ISO 20000).

De forma adicional, se mantiene una lista actualizada del personal que sustenta las funciones críticas, así como el mínimo número de personas que tienen que estar disponibles para garantizar su continuidad. Se han determinado los backups existentes para los perfiles críticos y adoptado las medidas necesarias para garantizar que estos perfiles pueden asumir este rol, a través de sesiones de transferencia de conocimiento, traspaso de procedimientos operativos, custodia distribuida de credenciales con control dual para identificadores con alto nivel de privilegio, entre otros.

Existen mecanismos de teletrabajo que permiten acceder a los sistemas productivos de forma remota.

6.15. Terminación del servicio

En caso de cese de los servicios, la TSA de DIGITEL TS sigue siendo responsable de mantener accesible durante un período de tiempo, toda la información pertinente referente a los datos expedidos y recibidos como parte de la prestación de sus servicios de confianza, en particular al objeto de que sirvan de prueba en los procedimientos legales o para garantizar la continuidad del servicio, incluida la manera en la se mantiene accesible la información una vez que el servicio ha cesado .

Para dar satisfacción a esta responsabilidad, DIGITEL TS ha desarrollado un plan de cese actualizado que ordena las medidas a tomar en caso del cese planificado o no de la empresa como prestadora de servicios de confianza, y también en caso de cierre planificado o no, del servicio cualificado de sello de tiempo amparado en esta Declaracion de Prácticas y Políticas, o cuando proceda, en los casos de desmantelamiento de cualquier componente técnico o servicio utilizado para prestar el servicio cualificado soportado en esta DPP.

Este plan cubre las acciones siguientes:

- Provisión de la cantidad necesaria, mediante seguro de responsabilidad civil, para cubrir los costes a efectos de contingencia de cierre.
- Comunicación del cese a todos Suscriptores del cese del servicio con una anticipación mínima de 2 meses.
- Comunicación del cese a proveedores y contratistas y revocación de toda autorización a entidades subcontratadas para actuar en alguna operativa del servicio.
- Revocación de toda autorización a entidades subcontratadas para actuar en nombre de la TSA en la prestación del servicio cualificado de sellado de tiempo.
- la TSA deberá revocar todos los certificados TSU no expirados.
- las claves privadas de las TSU, o cualquier parte de las claves, incluidas las copias, serán destruidas de manera que no puedan ser recuperadas.
- la TSU terminada no asignará ni generará nuevos pares de claves privadas y públicas y no deberá emitir nuevos tokens de sellos de tiempo.

- La TSA podrá transferir la gestión del servicio a otro prestador de servicios de confianza que los asuma. La TSA informará, cuando sea el caso, sobre las características de la TSA cualificada al que se propone la transferencia de la gestión del servicio y recabará previamente el consentimiento de los suscriptores del mismo.
- En caso de traspaso del servicio a un nuevo proveedor, DIGITEL TS llevará a cabo un Plan de traspaso que garantice la continuidad del servicio en condiciones de seguridad y privacidad. Para ello firmará un acuerdo de Traspaso con el nuevo proveedor y ejecutarán de manera conjunta un plan de traspaso para garantizar la entrega ordenada y segura del servicio. El nuevo proveedor asumirá el compromiso de mantener y poner a disposición de las partes que confían toda la información del servicio generada antes de la salida de DIGITEL TS como proveedor por el plazo de 15 años, contados desde la fecha del cese de su prestación por DIGITEL TS conforme a lo establecido en la normativa aplicable.
- En caso de que al cese de operaciones el servicio no se transfiera a otro prestador, DIGITEL TS pondrá en deposito ante notario público toda la informacion relacionada con la prestación del servicio, por el plazo de 15 años estipulado en la legislación aplicable.
- Comunicará al Organismo de Supervisión nacional en materia de servicios de confianza, con una antelación mínima de 3 meses, el cese de su actividad y el destino de los certificados de TSU y de las evidencias del servicio cualificado de sellado de tiempo especificando si se transfiere su provisión y a quién, de manera que este pueda verificar la correcta aplicación del plan de terminación de los servicios, incluyendo la forma en que se hace accesible la información, de conformidad con el artículo 24.2 letras a); h) e i) y el artículo 46 ter, apartado 4, letra i) del Reglamento (UE) eIDAS.
- Comunicará, también al supervisor nacional de servicios de confianza con una antelación mínima de 3 meses, la apertura de cualquier proceso concursal que se siga contra la TSA de DIGITEL TS, así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

7. Controles de seguridad técnica

La TSA de DIGITEL TS emplea sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de emisión de certificados de TSU conforme a lo establecido en el apartado 6.1.1 de la Declaración de Prácticas y Políticas de Certificación de DIGITEL TS.

7.1. Controles de seguridad informática

7.1.1. Requisitos técnicos específicos de seguridad informática

La TSA de DIGITEL TS emplea sistemas y aplicaciones fiables para ofrecer sus servicios cualificados de sellado de tiempo. Se han realizado controles y auditorias informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en prestación de este servicio cualificado.

Respecto a la seguridad de la información, la TSA de DIGITEL TS sigue el esquema de certificación sobre sistemas de gestión de la información ISO 27001.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de la TSA de DIGITEL TS, en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log
- Plan de backup y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red.

Cada servidor de la TSA de DIGITEL TS incluye las siguientes funcionalidades:

- Control de acceso a los servicios de sello de tiempo y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del suscriptor, la TSA y los datos de auditoría.
- Auditoría de eventos relativos a la seguridad.
- Autodiagnóstico de seguridad relacionado con los servicios cualificados de sello de tiempo
- Mecanismos de recuperación de claves y del sistema de la TSA.

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software, protección física y procedimientos.

7.2. Controles de seguridad del ciclo de vida

7.2.1. Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por la TSA de DIGITEL TS de acuerdo con estándares de desarrollo y control de cambios.

Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

7.2.2. Controles de gestión de seguridad

La TSA de DIGITEL TS desarrolla las actividades precisas para la formación y concienciación de los empleados, incluida la alta dirección; así como a sus proveedores en materia de ciberseguridad y buenas prácticas de ciberhigiene. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación. En la realización de esta función dispone de un plan de formación anual. La TSA de DIGITEL TS exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores del servicio d cualificado de sellado de tiempo.

Por otro lado, DIGITEL TS revisa su Política de Seguridad con el fin de mantener la idoneidad, adecuación y eficacia de esta. La revisión se lleva a cabo a intervalos planificados y como mínimo anualmente o siempre que se produzcan incidentes significativos o cambios significativos en las operaciones o en los riesgos, o en la organización.

7.2.2.1 Clasificación y gestión de información y bienes

La TSA de DIGITEL TS mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de la TSA de DIGITEL TS detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en cuatro niveles: Uso Público, Uso Interno, Confidencial y Secreto.

7.2.2.2 Operaciones de gestión

La TSA de DIGITEL TS dispone de un procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.

En el documento de seguridad de la TSA de DIGITEL TS se desarrolla en detalle el proceso de gestión de incidencias.

La TSA de DIGITEL TS tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

7.2.2.3 Tratamiento de los soportes y seguridad

Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

7.2.2.4 Planificación del sistema

El departamento de Sistemas de la TSA de DIGITEL TS mantiene un registro de las capacidades de los equipos. Juntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

7.2.2.5 Reportes de incidencias y respuesta

La TSA de DIGITEL TS dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

7.2.2.6 Procedimientos operacionales y responsabilidades

La TSA de DIGITEL TS define actividades, asignadas a personas con un rol de confianza, distintas de las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

7.2.2.7 Gestión del sistema de acceso

La TSA de DIGITEL TS realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.

En particular:

- Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
- La TSA de DIGITEL TS dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- La TSA de DIGITEL TS dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones de certificación.

- El personal de la TSA de DIGITEL TS es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.
- El acceso se produce mediante VPN y certificado electrónico de autenticación en USB y PIN.

7.2.2.8 Generación del certificado

La autenticación para el proceso de emisión de certificados de TSU se realiza mediante un sistema *m de n* operadores para la activación de la clave privada de la Autoridad de Certificación de DIGITEL TS.

7.2.2.9 Gestión de la revocación

La revocación de los certificados de TSU se realiza mediante autenticación fuerte a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador de la Autoridad de Certificación de DIGITEL TS.

7.2.2.10 Estado de la revocación

La aplicación del estado de la revocación del certificado de TSU dispone de un control de acceso basado en la autenticación con certificados o con doble factor de identificación para evitar el intento de modificación de la información del estado de la revocación.

7.3. Controles de seguridad de red

La TSA de DIGITEL TS protege el acceso físico a los dispositivos de gestión de red y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos. Los cortafuegos están configurados de manera que impidan todos los protocolos y accesos que no sean necesarios para el funcionamiento de DIGITEL TS como prestador de servicios cualificados de sello de tiempo.

La información confidencial que se transfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL o de VPN con autenticación por doble factor.

8. Auditoría de conformidad

La TSA de DIGITEL TS realiza auditorías de conformidad para asegurar el cumplimiento y adecuación con las políticas, normativas, planes y procedimientos de seguridad del sistema de gestión de seguridad de la información. Dichas auditorías, su alcance y periodicidad, se describen en el correspondiente *Plan de Auditoría de DIGITEL*, que se actualiza de forma anual. Como resultado de estas se elaboran planes de acciones correctivas como respuesta a las no conformidades y desviaciones detectadas.

La TSA de DIGITEL TS realiza auditorías de conformidad del Reglamento eIDAS y la Directiva NIS2 por medio de evaluaciones de conformidad anuales sobre el servicio cualificado de sellado de tiempo

- Servicio Los controles para la realización de las auditorías de cumplimiento se basan en las siguientes guías de referencia:
- ETSI EN 319 401 General Policy Requirements for Trust Service Providers.
- ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Timestamps.
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI).
- Time-stamping protocol and time-stamp token profiles

En el marco de auditorías de cumplimiento DIGITEL TS verifica el cumplimiento de los controles definidos en los Reglamentos de Ejecución del Reglamento eIDAS aplicables al servicio cualificado de sello de tiempo detallados previamente en esta DPP.
La TSA de DIGITEL TS realiza las pertinentes auditorías sobre protección de datos con periodicidad bienal.

DIGITEL TS es una empresa comprometida con la seguridad y la calidad de sus servicios mediante la obtención y mantenimiento de la certificación ISO/IEC 27001:2022.

Asimismo, DIGITEL TS ha certificado los sistemas de información que dan soporte a los servicios electrónicos cualificados amparados en esta DPP con la categoría media, conforme a las exigencias del Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

8.1. Frecuencia de la auditoría de conformidad

Se realizan evaluaciones de conformidad eIDAS con carácter bienal, además de revisiones anuales.

- Se realizan auditorías relativas a la protección de los datos personales bianuales.
- Se realizan auditorías de ISO 27001 cada 3 años con seguimiento anual.
- Se realizan análisis internas de vulnerabilidades cada mes, y externa cada año.
- Se realiza un análisis de intrusión cada año.

8.2. Identificación y cualificación del auditor

Las auditorías son realizadas por una firma de auditoría independiente externa que demuestra competencia técnica y experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios cualificados de sellado de tiempo, y los elementos relacionados.

El auditor responsable de la evaluación de conformidad eIDAS debe estar acreditado según ETSI EN 319 403.

8.3. Relación del auditor con la entidad auditada

Los auditores internos o externos responsables de ejecutar las auditorías son independientes funcionalmente del servicio de producción objeto de auditoría.

8.4. Listado de elementos objeto de auditoría

La auditoría verifica:

- Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.
- Que la entidad cumple con los requerimientos de la DPP y otra documentación vinculada con la provision de servicios cualificados de sellado de tiempo, bajo el marco del Reglamento (UE) 910/2014 eIDAS y sos Actos de Ejecución aplicables al servicio.
- Que la DPP y demás documentación jurídica vinculada, se ajusta a lo acordado por la TSA de DIGITEL TS y con lo establecido en la normativa vigente.
- Que la entidad cumple los requisitos de ciberseguridad y resiliencia digital establecidos en la Directiva (UE) 2022/2555 NIS2 y su normativa de desarrollo.
- Que la entidad gestiona de forma adecuada sus sistemas de información.

En particular, los elementos objeto de auditoría serán, entre otros, los siguientes:

- Procesos de la TSA/TSU y elementos relacionados.
- Sistemas de información.
- Protección del centro de proceso de datos.
- Documentación asociada.
- Analisis de riesgos, procesos de seguridad y gestión de incidentes que garanticen el cumplimento la Directiva NIS2 y su normativa de desarrollo.

8.5. Acciones que emprender como resultado de una falta de conformidad

Una vez recibido por la Dirección de DIGITEL TS el informe de la auditoría de cumplimiento realizada, se analizan, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta un plan correctivo que solvente dichas deficiencias.

Si la TSA de DIGITEL TS es incapaz de desarrollar y/o ejecutar dicho plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicarlo inmediatamente al Comité de Riesgos y Seguridad de DIGITEL TS que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.

- Revocar la clave de la TSU y regenerar la infraestructura.
- Poner en marcha la terminaciónr el servicio cualificado de sellado de tiempo
- Otras acciones complementarias que resulten necesarias.

8.6. Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se entregan al Comité de Riesgos y Seguridad de DIGITEL TS en un plazo máximo de 15 días tras la ejecución de la auditoría, para su análisis y tratamiento.

9. Requisitos comerciales y legales

9.1. Tarifas

9.1.1. Tarifa de emisión o renovación de certificados

Se puede establecer una tarifa por la prestación del servicio cualificado de sello de tiempo que se informará oportunamente a los suscriptores en el contrato de prestación del servicio.

9.1.2.Tarifa de acceso a certificados de TSU

No se ha establecido ninguna tarifa por el acceso a los certificados

9.1.3.Tarifa de acceso a información de estado de certificado de TSU

No se ha establecido ninguna tarifa por el acceso a la información de estado de certificados de TSU.

9.1.4. Tarifas de otros servicios

Sin estipulación

9.1.5.Política de reintegro

Sin estipulación

9.2. Responsabilidad financiera

La TSA de DIGITEL TS dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios, en relación con la gestión de la finalización de los servicios y plan de cese.

9.2.1. Cobertura de seguro

La TSA de DIGITEL TS dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional que cumple con lo indicado en el artículo 24.2.c) del Reglamento (UE) 910/2014, y con el artículo 9.3.b) de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, con un mínimo asegurado de 3.000.000 de euros.

9.2.2. Otros activos

Sin estipulación.

9.3. Confidencialidad de la información

9.3.1. Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales:

- Solicitudes y respuestas del servicio cualificado de sello de tiempo
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por TSA y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Política y planes de seguridad.
- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.
- Toda otra información identificada como “Confidencial”.

9.3.2. Informaciones no confidenciales

La Declaración de Prácticas y Políticas del servicio cualificado de sellado de tiempo, los términos y condiciones del servicio, la declaración de divulgación de TSA.

9.3.3. Divulgación legal de información

La TSA de DIGITEL TS divulga la información confidencial únicamente en los casos legalmente previstos.

En concreto, los registros que avalan la fiabilidad del servicio cualificado de sello de tiempo, así como los registros relacionados con la fiabilidad de los datos y los relacionados con la operativa, serán divulgados en caso de ser requerido para ofrecer evidencia de la prestación del servicio en un procedimiento judicial, incluso sin consentimiento del suscriptor del servicio.

9.3.4. Divulgación de información por petición de su titular

La TSA de DIGITEL TS incluye, en la política de privacidad prevista en la sección 9.4, prescripciones para permitir la divulgación de la información del suscriptor, directamente a los mismos o a terceros.

9.3.5. Otras circunstancias de divulgación de información

Sin estipulación.

9.4. Protección de la información personal

DIGITEL TS ha desarrollado una política de privacidad, y documentado en esta Declaración de Prácticas y Políticas del servicio cualificado de sello de tiempo los aspectos y procedimientos de seguridad correspondientes de conformidad con el 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 (RGPD - Reglamento General de Protección de Datos) y la Ley

Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)

Asimismo, DIGITEL TS dispone de un Registro de Actividades de Tratamiento de datos de carácter personal, donde está recogido el tratamiento de los datos personales en el marco de la prestación de los servicios cualificados de sello de tiempo amparados en esta DPP, cuya finalidad es la gestión de los certificados de TSU emitidos y la prestación de los servicios cualificados de sellos de tiempo asociados.

Para garantizar la privacidad y la seguridad de los datos tratados, DIGITEL TS ha adoptado las medidas técnicas y organizativas adecuadas al análisis de riesgos realizado en relación a este tratamiento, asegurando la licitud y proporcionalidad del tratamiento, así como que se han respetado los principios de privacidad por diseño y por defecto.

De conformidad con lo establecido en el artículo 4 del Reglamento General de Protección de Datos (RGPD), se consideran datos personales cualquier información relativa a personas físicas identificadas o identificables.

Para la prestación del servicio de confianza cualificado de sello de tiempo, se precisa recabar y almacenar ciertas informaciones, que incluyen datos personales. Tales informaciones son recabadas a través de los suscriptores, en base a la relación corporativa que les une (por ser empleados, cargos, socios…) o en ciertos casos, directamente de los interesados, con cumplimiento estricto del RGPD, la LOPDGDD, el Reglamento (UE) 910/2014, y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (LSEC). Asimismo, la TSA de DIGITEL TS precisa recabar y almacenar datos personales para mantener la relación con clientes, así como la gestión comercial y de los servicios contratados en idénticas condiciones de cumplimiento normativo.

La base legal para el tratamiento de los datos personales es la ejecución del contrato de servicios de confianza (artículo 6.1.b) del RGPD). Asimismo, la base legal para el mantenimiento de relaciones comerciales es el consentimiento del interesado.

Los datos que se solicitan a los interesados son estrictamente los necesarios para la suscripción del contrato y la prestación del servicio cualificado de sello de tiempo. La no comunicación de los datos supone la imposibilidad de prestación del servicio. Los datos personales proporcionados se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recaban y para determinar las posibles responsabilidades que se pudieran derivar de la finalidad, además de los períodos establecidos en la normativa de servicios de confianza, y aquellos que resulten del ejercicio de las correspondientes acciones de reclamación en la vía administrativa y judicial. Más en concreto, conforme al artículo 9.3.a) de la LSEC, los datos necesarios para la prestación del servicio de expedición del certificado se conservarán durante el plazo de quince años desde la expiración del certificado.

Con carácter general no se comunicarán los datos personales a terceros, salvo obligación legal, entre las que pudieran estar las comunicaciones a administraciones públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento de sus datos de carácter personal. En algunos casos, podría ser necesario comunicar la información proporcionada a terceras partes para poder prestar el servicio solicitado.

Cualquier persona tiene derecho a obtener confirmación sobre los tratamientos de sus datos que se llevan a cabo por la TSA de DIGITEL TS. Puede ejercer sus derechos de acceso, rectificación, supresión y portabilidad de sus datos, de limitación y oposición a su tratamiento, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, cuando procedan ante la TSA de DIGITEL TS en las direcciones indicadas en el apartado 1.5 de este documento.

La TSA de DIGITEL TS no adopta decisiones automatizadas, ni siquiera la elaboración de perfiles.

La TSA de DIGITEL TS no realiza transferencias de datos personales a terceros países.

En caso de que la TSA de DIGITEL TS detecte que se ha producido una violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de

confianza prestado o en los datos personales correspondientes, lo notificará al supervisor nacional competente en materia de servicios electrónicos de confianza, al equipo de respuesta a incidentes de seguridad (CSIRT) de referencia, o en su caso, a la autoridad competente designada en materia de ciberseguridad, en un plazo máximo de 24 horas desde que tenga conocimiento de la violación, y a la Autoridad de Protección de Datos correspondiente, en un plazo máximo de 72 horas tras tener conocimiento de los hechos, conforme estipula el artículo 23 de la Directiva (UE) 2555/2022 y el artículo 24.2 f) *ter* del Reglamento eIDAS.

9.5. Derechos de propiedad intelectual

9.5.1. Propiedad de la Declaración de Prácticas y Políticas del servicio cualificado de sello de tiempo

Únicamente la TSA de DIGITEL TS goza de derechos de propiedad intelectual sobre esta Declaración de Prácticas y Políticas y la documentación relacionada con la prestación del servicio.

9.6. Obligaciones y responsabilidad civil

9.6.1. Obligaciones de la TSA

La TSA de DIGITEL TS garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la DPP, siendo el único responsable del cumplimiento de los procedimientos descritos, incluso si una parte o la totalidad de las operaciones se subcontratan externamente.

La TSA de DIGITEL TS presta los servicios cualificados de sello de tiempo conforme con esta Declaración de Prácticas y Políticas, la declaración de divulgación de TSA y los términos y condiciones del servicio.

Con anterioridad a la prestación del servicio al suscriptor, la TSA de DIGITEL TS informa al suscriptor de los términos y condiciones relativos al mismo, su precio y sus limitaciones mediante un contrato de suscriptor.

Este requisito de información también se cumple mediante un documento de declaración de divulgación de TSA, que incorpora el contenido del Anexo B de la norma técnica ETSI EN 319 421, documento que puede ser transmitido por medios electrónicos, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

La TSA de DIGITEL TS comunica de forma permanente los cambios que se produzcan en sus obligaciones publicando nuevas versiones de su documentación jurídica en su web https://pki.digitelts.es/ a suscriptores y terceros que confían en el servicio mediante dicho PDS, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en las secciones anteriores.
- Indicación de la política aplicable.
- Manifestación de que la información derivada de la prestación del servicio es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la TSA sin revocación de certificados de TSU válidos.
- Límites de uso del certificado TSU, incluyendo las establecidas en la sección 4.2 de la DPPC
- Forma en que se garantiza la responsabilidad patrimonial de la TSA.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la TSA acepta o excluye su responsabilidad.
- Periodo de archivo de información del servicio
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.

9.6.2. Garantías ofrecidas a suscriptores y terceros que confían en certificados

Finalmente la TSA de DIGITEL TS garantiza al suscriptor y al tercero que confían en el servicio

- Que el certificado de TSU para la emisión de sellos cualificados de tiempo contiene las informaciones que debe contener de acuerdo con la política NCP+.
- Que el servicio de sello de tiempo se ofrece con la precision indicada en esta DPP.

9.7. Exención de garantía

La TSA de DIGITEL TS rechaza toda garantía que no sea legalmente exigible conforme las Leyes aplicables al servicio, excepto las expresamente contempladas en la sección 9.6.2.

9.8. Limitaciones de responsabilidad

La TSA de DIGITEL TS en su actividad de prestación de servicios cualificados de sello de tiempo, responderá por el incumplimiento de lo establecido en la DPP, y allí donde sea aplicable, por lo que dispone Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y el Reglamento (UE) 910/2014 eIDAS.

Sin perjuicio de lo anterior, la TSA de DIGITEL TS no garantizará los algoritmos y estándares criptográficos utilizados ni responderá de los daños causados por ataques externos a los mismos, siempre que hubiere aplicado la diligencia debida según el estado de la técnica en cada momento, y hubiere actuado conforme a lo dispuesto en la presente DPP, en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, y en el Reglamento (UE) 910/2014, donde sea aplicable.

La TSA de DIGITEL TS será responsable del daño causado ante el Suscriptor o cualquier persona que de buena fe confíe en el servicio, siempre que exista dolo o culpa grave por parte de la TSA.

En ningún caso será responsable de las acciones u omisiones de terceros distintos de la TSA de DIGITEL TS o de los perjuicios de cualquier tipo que se pudieran irrogar a solicitantes, representantes, entidades representadas, usuarios o, en su caso, terceros involucrados cuando dichos perjuicios no se deban a errores imputables a la TSA de DIGITEL TS en los referidos procedimientos del servicio cualificado de sello de tiempo.

En todo caso y con independencia de la naturaleza de la declaración de voluntad que se sustancie o la condición pública o privada de quien firma o confía en el servicio cualificado, así como de la cuantía de los perjuicios que se pudieran causar, la cantidad máxima por la que la TSA de DIGITEL TS responderá en el supuesto de actuación negligente en el cumplimiento de las obligaciones asumidas será de SEIS MIL EUROS (6.000€).

En el supuesto de liquidación de la compañía por cualquier motivo o de terminación de las actividades relativas al servicio cualificado de sello de tiempo, la TSA de DIGITEL TS se atendrá a la normativa vigente en cada momento, informando en todo caso con suficiente antelación a los suscriptores del servicio y otras partes interesadas y, en su caso, transferirá otro Prestador de Servicios Cualificados de sello de tiempo que los asuma, con expreso consentimiento de sus suscriptores.

En el supuesto de que esta transferencia del servicio no fuera posible por cualquier motivo, se procederá, previo aviso a los suscriptores a depositar el servicio ante notario público.

9.9. Periodo de validez

9.9.1.Plazo

La DPP y las PDS entran en vigor en el momento de su publicación.

9.9.2. Sustitución y derogación de la DPP

La presente DPP, y la PDS quedan derogadas en el momento que una nueva versión de los documentos sea publicada. La nueva versión sustituirá íntegramente el documento anterior.

9.9.3. Efectos de la finalización

Para los certificados de TSU vigentes y para los sellos de tiempo emitidos bajo una DPP anterior, la nueva versión prevalecerá a la anterior en todo lo que no se oponga a ésta.

9.10. Notificaciones individuales y comunicaciones con los participantes

Se establece en el contrato con el suscriptor, los medios y plazos para las notificaciones.

De modo general, se utilizará el sitio web https://pki.digitelts.es/ para realizar cualquier tipo de notificación y comunicación general, así como el correo electrónico o postal para notificaciones y comunicaciones individualizadas.

En caso de problemas de seguridad o de pérdida de integridad que puedan afectar a una persona física o jurídica, se le notificará dicha incidencia sin ningún retraso.

9.11. Enmiendas

9.11.1. Procedimiento para los cambios

Elementos que pueden cambiar sin necesidad de notificación

Los únicos cambios que pueden realizarse a esta Declaración de Prácticas y Políticas del Servicio Cualificado de Sellado de Tiempo sin requerir de notificación son las correcciones tipográficas o de edición o los cambios en los detalles de contacto.

Cambios con notificación

Los elementos de esta DPP pueden ser cambiados unilateralmente por la TSA de DIGITEL TS sin preaviso. Las modificaciones pueden traer causa justificativa en motivos legales, técnicos o comerciales.

Cuando se produzcan cambios significativos que afecten a los servicios amparados en esta DPP, dichas modificaciones serán notificadas al Organismo de Supervisión correspondiente con un mes de antelación y tras su aprobación definitiva, se publicará la nueva documentación con un periodo de entrada en vigor que posibilite la posible rescisión de los suscriptores que no acepten los cambios. El momento de entrada en vigor se anunciará suficientemente en el momento de publicación de los cambios.

A efectos de esta DPP se consideran cambios significativos los regulados en el artículo 1 del Reglamento de Ejecución eIDAS (UE) 2015/2530.

Mecanismo de notificación

Todos los cambios propuestos que puedan afectar sustancialmente a los suscriptores, usuarios o terceros serán notificados inmediatamente a los interesados mediante la publicación en la Web de la TSA de DIGITEL TS.

9.11.2. Periodo y procedimiento de notificación

Las personas, instituciones o entidades afectadas pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los 30 días siguientes a la notificación. Cualquier acción tomada como resultado de unos comentarios queda a la discreción de la organización responsable de la administración de las políticas.

9.12. Reclamaciones y resolución de conflictos

La TSA de DIGITEL TS establece, en el contrato de suscriptor, y en la PDS, los procedimientos de mediación y resolución de conflictos aplicables.

9.13. Normativa aplicable

La TSA de DIGITEL TS establece, en el contrato de suscriptor y en la PDS, que la legislación aplicable a la prestación de los servicios cualificados de sellado de tiempo, es la ley española. Específicamente son de aplicación, en lo que proceda, las siguientes normas:

- 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 mediante 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 de Ejecución (UE) 2025/2530 de la Comisión, de 29 de septiembre de 2025,por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a los requisitos

para los prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados.

- Reglamento de Ejecución (UE) 2025/1929 de la Comisión, de 29 de septiembre de 2025, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a la vinculación de la fecha y la hora con los datos y al establecimiento de la exactitud de las fuentes de información temporal para el suministro de sellos cualificados de tiempo electrónicos.
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI2)(NIS 2).

- Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024, por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y en el que se detallan los casos en que un incidente se considera significativo con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales, y los proveedores de servicios de confianza.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- 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).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Las prácticas y politicas del servicio cualificado de sellado de tiempo de la TSA de DIGITEL TS siguen las directrices de los siguientes estándares:

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles.
- RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs).
- RFC 5816: ESSCertIDv2 Update for RFC 3161.
- RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

9.13.1. Cumplimiento de la normativa aplicable

La TSA de DIGITEL TS cumple el Reglamento (UE) 910/2014, Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, así como el resto de la normativa relacionada en el punto anterior.

La TSA de DIGITEL TS establece, en el contrato de suscriptor y en la PDS, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles. La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.