Servicios Cualificados[1] para la Gestión de Dispositivos Cualificados de Creación de Firma y Sello Electrónicos a Distancia

Declaracion de Prácticas y Políticas

[1] Estos servicios no adquirirán la condición de servicios de confianza cualificados hasta que sean reconocidos como tales por el Organismo de Supervisión de España y la cualificación haya sido indicada en la lista de confianza nacional.

Índice

Control Documental

Nombre	Declaración de Prácticas y Políticas de los Servicios Cualificados[2] de Gestión de Dispositivos Cualificados de Creación de Firma y Sello Electrónicos a Distancia de DIGITEL TS		
Distribución	**Público**		
Versión	V1.0		
Fecha	15/07/2026		
Aprobado	Comité de Riesgos y Seguridad de DIGITEL TS	Fecha	23/07/2026
Estado	Aprobado		

Control de Cambios

Versión	Fecha	Descripción
V1.0	15/07/2026	Versión inicial

[2] Estos servicios no adquirirán la condición de servicios de confianza cualificados hasta que sean reconocidos como tales por el Organismo de Supervisión de España y la cualificación haya sido indicada en la lista de confianza nacional.

1 INTRODUCCIÓN

1.1 VISIÓN GENERAL

DIGITEL TS es una Autoridad de Certificación y un Prestador Cualificado de Servicios de Confianza que, entre otros servicios de confianza cualificados, emite certificados cualificados de firma y sello electrónicos de acuerdo con la legislación vigente.

DIGITEL TS presta sus servicios cualificados[3] para la gestión de dispositivos cualificados de creación de firma y sello electrónicos a distancia conforme a los artículos 29 bis y 39 bis del 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 (en adelante, "Reglamento eIDAS").

Los servicios cualificados[3] para la gestión de dispositivos cualificados de creación de firma y sello electrónicos a distancia prestados por DIGITEL TS incluyen el servicio de firma remota (conocido por las siglas en inglés SSAS de Server Signing Application Service) que es usado por los firmantes y los creadores de sellos que disponen de certificados cualificados de firma y sellos electrónicos emitidos DIGITEL TS en soporte centralizado (certificados cualificados de firma y sello electrónicos remotos) para crear firmas electrónicas y sellos electrónicos cualificados.

En la Declaración de Prácticas y Políticas de Certificación de DIGITEL TS (en adelante DPPC) se recogen los conceptos básicos sobre certificados electrónicos, firma y sello electrónicos, Infraestructura de Clave Pública (PKI), etc. por lo que se recomienda que se consulte dicha DPPC en caso de no tener conocimiento de dichos conceptos.

Las prácticas relacionadas con el servicio SSAS se adaptan a la estructura organizativa, los procedimientos operativos, las instalaciones y el entorno informático de DIGITEL TS.

1.2 ALCANCE

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 de los servicios cualificados[3] para la gestión de dispositivos cualificados de creación de firma y sello electrónicos a distancia, incluyendo el servicio de firma remota (Server Signing Application Service o SSAS) que permite crear firmas electrónicas y sellos electrónicos cualificados en nombre de los firmantes y creadores de sellos.

Los componentes del servicio SSAS incluyen una aplicación de firma en servidor (Server Signing Application o SSA) y un dispositivo cualificado de creación de firma y sello electrónicos (Qualified

[3] Estos servicios no adquirirán la condición de servicios de confianza cualificados hasta que sean reconocidos como tales por el Organismo de Supervisión de España y la cualificación haya sido indicada en la lista de confianza nacional.

Signature and Seal Creation Device o QSCD) conforme a lo establecido en el Reglamento eIDAS.

La presente Declaración de Prácticas y Políticas es aplicable a las claves privadas de todos los certificados cualificados de firma y sello electrónicos emitidos por DIGITEL TS en soporte centralizado (certificados cualificados de firma y sello electrónicos remotos) que se definen en la Declaración de Prácticas y Políticas de Certificación de DIGITEL TS.

En caso de contradicción entre este documento de Declaración de Prácticas y Políticas de los servicios cualificados[4] para la gestión de dispositivos cualificados de creación de firma y sello electrónicos a distancia y otros documentos relativos a dicho servicio, prevalecerá lo establecido en este documento.

1.3 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Nombre:	Declaración de Prácticas y Políticas de los Servicios Cualificados[4] de Gestión de Dispositivos Cualificados de Creación de Firma y Sello Electrónicos a Distancia de DIGITEL TS
Versión:	Ver página inicial
Localización:	https://pki.digitelts.es/

DIGITEL TS presta el servicio SSAS conforme a la política EUSPv2 (EU SSAS Policy v2) definida en ETSI TS 119 431-1 v1.3.1 (2024-12) con el OID 0.4.19431.1.1.4.

1.4 PARTICIPANTES EN EL SERVICIO DE FIRMA REMOTA

1.4.1 PROVEEDOR DEL SERVICIO DE FIRMA REMOTA (SSASP)

DIGITEL TS actúa como SSASP y no delega a entidades terceras ninguna parte del servicio.

1.4.2 SUSCRIPTOR Y FIRMANTE O CREADOR DE UN SELLO

Según lo dispuesto en la DPPC.

El término firmante se utiliza en esta DPP, conforme a su uso en ETSI TS 119 431-1, para referirse indistintamente a los términos firmante y creador de un sello según lo dispuesto en la DPPC y el Reglamento eIDAS, excepto en aquellos casos en los que se usan ambos términos conjuntamente.

1.4.3 PARTES QUE CONFÍAN

Según lo dispuesto en la DPPC.

1.4.4 OTROS PARTCIPANTES

[4] Estos servicios no adquirirán la condición de servicios de confianza cualificados hasta que sean reconocidos como tales por el Organismo de Supervisión de España y la cualificación haya sido indicada en la lista de confianza nacional.

Según lo dispuesto en la DPPC.

1.5 ADMINISTRACIÓN DE LA POLÍTICA

Según lo dispuesto en la DPPC.

1.5.1 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Según lo dispuesto en la DPPC.

1.5.2 DATOS DE CONTACTO DE LA ORGANIZACIÓN

Según lo dispuesto en la DPPC.

1.5.3 RESPONSABLES EN EL PROCEDIMIENTO DE GESTIÓN DEL DOCUMENTO

Según lo dispuesto en la DPPC.

1.5.4 REVISIÓN DEL DOCUMENTO

Según lo dispuesto en la DPPC.

1.5.5 APROBACIÓN DEL DOCUMENTO

Según lo dispuesto en la DPPC.

1.6 REFERENCIAS NORMATIVAS

La prestación de este servicio se realiza de acuerdo con las siguientes documentos normativos:

- 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.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- 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 en lo que respecta a los requisitos para los prestadores de servicios de confianza cualificados que presten servicios de confianza cualificados.
- Reglamento de Ejecución (UE) 2025/1943 de la Comisión, de 29 de septiembre de 2025, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 en lo que respecta a las normas de referencia para los certificados cualificados de firma electrónica y los certificados cualificados de sello electrónico.
- Reglamento de Ejecución (UE) 2025/1567 de la Comisión, de 29 de julio 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 gestión de dispositivos

cualificados de creación de firma electrónica a distancia y de dispositivos cualificados de creación de sello electrónico a distancia como servicios de confianza cualificados

- Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- 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 (Directiva NIS2), aplicable a los prestadores de servicios de confianza en virtud del artículo 19 del Reglamento eIDAS modificado.

Igualmente, este documento se ha redactado siguiendo las directrices definidas en las siguientes especificaciones técnicas:

Referencia	Documento referenciado
ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI EN 319 411-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI TS 319 431-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev
CEN 419 241-1	Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements
CEN 419 241-2	Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing
CEN 419 221-5	Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services

1.7 DEFINICIONES Y SIGLAS

Además de las definiciones y siglas recogidos en la DPPC de DIGITEL TS, la presente Declaración de Prácticas y Políticas del servicio de firma remota utiliza los siguientes términos y abreviaturas tal y como se definen en la ETSI TS 119 431 -1:

- **Referencia a medios de identificación electrónica:** datos usados en el SSAS como referencia a unos medios de identificación electrónica que permiten autenticar a un firmante.
- **Autenticación:** un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico.
- **Aplicación de firma en servidor (SSA):** una aplicación que, asociada a un dispositivo de creación de firma (QSCD/SCDev) o un dispositivo de creación de firma en remoto (QSCD/SCDev remoto), permite generar una firma digital.
- **Identificación electrónica (eID)** el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica.
- **Medios de identificación electrónica:** una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea.
- **Dispositivo cualificado de creación de firma / sello electrónico (QSCD o SCDev):** dispositivo de creación de firma que cumple con los requisitos del Anexo II del Reglamento eIDAS.
- **QSCD/SCDev remoto**: es un SCDev ampliado con control remoto proporcionado por un Módulo de Activación de Firma (SAM) ejecutado en un entorno protegido contra manipulaciones. Este módulo utiliza los datos de activación de firma (SAD), recogidos a través de un protocolo de activación de firma (SAP), para garantizar con un alto nivel de confianza que las claves de firma se utilizan bajo el control exclusivo del firmante.
- **Componente de servicio de aplicación de firma en servidor (SSAS):** componente de servicio operado por un PSC, compuesto de una aplicación de firma en servidor (SSA) y un QSCD / SCDev, empleado para la creación de firmas electrónicas cualificadas en nombre del firmante.
- **Proveedor de servicio de aplicación de firma en servidor (SSASP)**: PSC que opera un SSAS.
- **Servicio de confianza:** servicio electrónico consistente en la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo, servicios de entrega electrónica certificada y certificados de estos servicios; o la creación, verificación y validación de certificados ara la autenticación de sitios web; o la preservación de firmas,

sellos o certificados electrónicos.

- **Proveedor de servicios de confianza (PSC):** entidad que provee de servicios de confianza. En este caso hace referencia a DIGITEL TS.

2 RESPONSABILIDAD DE PUBLICACIÓN Y REPOSITORIOS

2.1 REPOSITORIOS

Los repositorios de DIGITEL TS para la publicación de la información de certificación están disponibles las 24 horas del día, los 7 días de la semana.

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de DIGITEL TS, DIGITEL TS realizará los mayores esfuerzos para asegurar que estos repositorios no se encuentren inaccesibles durante más de 24 horas.

2.2 PUBLICACIÓN DE INFORMACIÓN DE LA POLITICA DE SSAS

2.2.1 PRÁCTICAS Y POLÍTICAS DE SSAS

DIGITEL TS pone a disposición del público la versión actual de esta Declaración de Practicas y Políticas del servicio de firma remota en el sitio web siguiente: https://pki.digitelts.es/

Una vez publicada una nueva versión de esta Declaración de Practicas y Políticas del servicio de firma remota, DIGITEL TS mantendrá a disposición del público la versión anterior en el mismo sitio web, al menos hasta la terminación de los servicios incluidos en esa versión.

2.2.2 TÉRMINOS Y CONDICIONES

Como parte del servicio de firma remota, DIGITEL TS publica términos y condiciones del servicio de emisión de certificados cualificados que son vinculantes para los usuarios finales al igual que esta Declaración de Practicas y Políticas del servicio de firma remota y la Declaración de Prácticas y Políticas de Certificación.

Los destinatarios de los términos y condiciones del servicio de emisión de certificados son los suscriptores y las partes que confían.

2.3 Frecuencia de Publicación

Según lo dispuesto en la DPPC.

2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

Según lo dispuesto en la DPPC.

3 SUBCOMPONENTES DEL SERVICIO SSAS

3.1 SUBCOMPONENTES DEL SERVICIO DEL SERVICIO SSAS

El servicio de firma remota que provee DIGITEL TS comprende los subcomponentes siguientes:

- **Servicio de generación de claves de firma remota o en nube**: genera claves de firma en el dispositivo remoto. La prueba de posesión de claves de firma generadas se transmite al servicio de registro de la CA-DIGITEL TS que emite el certificado asociado.
- **Servicio de vinculación del certificado:** vincula el certificado generado por el servicio de generación de certificados de la CA-DIGITEL TS con las claves de firma correspondientes.
- **Servicio de vinculación de medios de identificación electrónica (eID)**: vincula las referencias de medios de identificación electrónica con las correspondientes claves de firma para proporcionar un único control.
- **Servicio de activación de la firma**: verifica los datos de activación de la firma y activa la clave de firma correspondiente para crear una firma digital.
- **Servicio de destrucción de la clave de firma**: destruye las claves de firma de forma que se garantice que las claves de firma no puedan volver a utilizarse.

4 INICIALIZACIÓN DE LAS CLAVES DE FIRMA

4.1 GENERACIÓN Y PROTECCIÓN DE LAS CLAVES DE FIRMA

DIGITEL TS ofrece un servicio de firma remota en **QSCD Nube (plataforma centralizada QSCD)**.

Se utiliza un sistema de generación y almacenamiento remoto de claves, que permite al firmante (o al creador de un sello, en el caso de persona jurídica) acceder a la clave privada bajo su control exclusivo (o bajo su control, en el caso de persona jurídica) desde diferentes dispositivos.

Las claves se almacenan en un QSCD **Trident, the distributed remote Qualified Signature Creation Device version 3.1.3**, que se ajusta a los requisitos que se establecen en el Anexo II del Reglamento eIDAS, y está certificado con referencia **OCSI/ACC/I4P/02/2024/RA** conforme al artículo 30 del mismo Reglamento.

Las claves gestionadas son aptas para la creación de firmas electrónicas cualificadas y sellos electrónicos cualificados.

Las claves del firmante son creadas y almacenadas por DIGITEL TS, bajo estricto control único del firmante, que accederá a ellas por medio del PIN de activación de firma que conocerá solamente el firmante y que DIGITEL TS recomienda no tener por escrito, y vinculado a su dispositivo.

En el caso de certificados de sello se puede identificar al firmante por MTLS para autenticar máquina a máquina.

El proceso de generación de claves se divide en dos fases:

- En la primera fase del proceso, el firmante recibirá un email con un QR para proceder a instalar una APP de DIGITEL TS para vincular el dispositivo móvil del firmante con su eID. Esta vinculación se explica en el siguiente punto.
- En la segunda fase del proceso, el servicio SSAS genera una petición de certificado en base a los datos proporcionados por la Autoridad de Registro de DIGITEL TS en formato PKCS#10, que es enviada a la CA-DIGITEL TS para finalizar la emisión del certificado asociado al par de claves.

La Autoridad de Registro es la encargada de solicitar la creación de par de claves y de vincularlas a la identidad del firmante y al certificado electrónico emitido.

Tras la emisión del certificado, el SSAS de DIGITEL TS almacena de manera segura e íntegra las claves del firmante.

Para acceder a sus clave privada el firmante deberá activarla enviando el PIN de activación suministrado en el momento de emisión del certificado y a su vez tendrá que aceptar la operación desde la APP vinculada a su dispositivo móvil que funcionará como segundo factor.

Todas las claves generadas por el SSAS de DIGITEL TS se asocian a certificados emitidos por la CA de DIGITEL TS.

4.2 MEDIOS DE EID VINCULADOS A LA IDENTIDAD

DIGITEL TS, bien por sí misma, mediante video identificación o a través de una Autoridad de Registro, validará la identidad del firmante de acuerdo con los requisitos establecidos en la Declaración de Prácticas de Certificación del certificado solicitado por el firmante con un nivel de garantía alto.

Una vez aprobada la solicitud, el firmante recibe un correo electrónico con la notificación de este hecho y cómo proceder a la generación y activación del certificado en la nube. Para ello recibirá un mail que contiene un QR para instalar una APP en su dispositivo móvil, con el cual se vinculará su identidad y acceso a certificados.

Para autenticarse se le solicitará una contraseña de usuario que se utilizará para conectarse al SSAS junto con un token JWT generado en un servicio de autenticación que está vinculado al HSM, dotando al proceso de autenticación de un segundo factor.

El dispositivo se vincula al usuario mediante la generación de un par claves, locales al dispositivo, donde la clave pública se comparte con el servidor.

Por otra parte, se registra el dispositivo en Firebase para la recepción de notificaciones Push, y el identificador de Push sirve como identificador único del dispositivo que tiene que usarse en la operación.

4.3 VINCULACIÓN DE CERTIFICADOS ELECTRÓNICOS

Mediante la petición de generación de claves, el usuario tiene que identificarse con sus credenciales para vincular el certificado; sólo puede hacerlo desde su dispositivo y ahí se le solicita el PIN de operaciones del certificado. Una vez se valida toda la información se genera y vincula el certificado al usuario y dispositivo.

4.4 PROVISIÓN DE MEDIOS DE EID

Las claves privadas de los firmantes se encuentran debidamente protegidas por la plataforma centralizada QSCD de DIGITEL TS.

El proceso de identificación/autenticación del firmante para acceder a la plataforma de DIGITEL TS se lleva a cabo por medios garantizan un nivel de seguridad alto conforme al Reglamento de Ejecución 2015/1502. El dispositivo vinculado actúa como segundo factor de posesión que además dispone de comunicación cifrada y autenticada con el SSAS, ya que en el momento de vinculación se registra con el usuario, su dispositivo y la clave pública con la que se comunicarán posteriormente.

Las peticiones de firma se realizan por API. Para activar las operaciones de firma, el firmante recibirá una notificación push a la APP para validar/aceptar la operación. Esta operación sólo podrá realizarse desde el dispositivo que se ha vinculado a su eID.

En caso de que la autenticación sea por MTLS no se solicita PIN, ni es necesaria la APP y la

operación se acepta de forma automática.

4.5 REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LAS CLAVES DE FIRMA

4.5.1 ACTIVACIÓN DE LAS CLAVES DE FIRMA

En la plataforma centralizada QSCD de DIGITEL TS, las claves se generan en un dispositivo criptográfico HSM protegido por una clave maestra del dispositivo y por los datos de activación de la clave generada y conocida solo por el propio titular del certificado asociado. La plataforma permite activar un doble control de activación vía OTP.

El protocolo de activación de firma (SAP) requiere que el firmante complete un proceso de identificación/autenticación previa al momento de uso de su clave de firma, mediante el uso de los datos de activación de firma (SAD) [SIG-6.3.1-01] [SIG-6.3.1-01].

El firmante ha de proveer un mensaje de activación de firma (SAD) mediante protocolo de activación de firma (SAP), que está diseñado para prevenir ataques [SIG-6.3.1-01][SIG-6.3.1-05].

El Protocolo de activación de firma (SAP) gestiona la petición del firmante de forma que se garantice que la clave de firma está bajo control del firmante con un alto nivel de confianza.

Las claves del firmante solo se pueden activar dentro del módulo HSM [SIG-A.5-02].

La clave del firmante solo se activa si este completa el protocolo de activación (SAP) y el mensaje de activación (SAD) que envía es correcto [SIG-6.3.1-09].

El mensaje de activación de firma (SAD) vincula un resumen criptográfico de los datos a firmar con los datos de activación del firmante mediante la firma electrónica del mensaje de activación con la clave de activación del firmante. [SIG-6.3.1-04].

Los controles de acceso implementados en el SSAS de DIGITEL TS garantizan que un firmante no tiene acceso a las claves de otros firmantes ni a otros objetos y funciones del sistema que no sean las funciones de firma [SIG-6.3.1-03].

Al activarse la clave del firmante, el SSAS de DIGITEL TS solo permite su uso para firmar el resumen criptográfico contenido en el mensaje SAD utilizado para la activación. Luego de realizar la operación de firma solicitada, el SSAS desactiva la clave del firmante y se requiere un nuevo SAD para una nueva firma.

El SSAS almacena en los metadatos del par de claves del firmante, la fecha de caducidad del certificado asociado.

Las claves de firma serán utilizables solo en casos en que se haya obtenido el consentimiento del firmante [SIG-6.3.1-09].

4.5.2 ELIMINACIÓN DE LAS CLAVES DE FIRMA

Con anterioridad a la destrucción de claves privadas del firmante, DIGITEL TS revocará el certificado electrónico asociado.

Se realizará un borrado seguro de la clave privada en los dispositivos criptográficos (HSM) que la tengan almacenada, siguiendo los pasos descritos en el manual de administración del HSM. Finalmente, se realizará un borrado seguro de todas las copias de seguridad de la clave privada.

En la plataforma centralizada QSCD, el borrado de las claves se llevará a cabo según consta en la descripción en el manual del fabricante del dispositivo entregado al titular después de la validación de su identidad o solicitándolo en https://www.digitel ts.com/contacto-soporte/

4.5.3 COPIAS DE SEGURIDAD Y RESTAURACIÓN DE CLAVES DE FIRMA

DIGITEL TS realiza una copia de backups de las claves privadas del firmante que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de las mismas. De conformidad con el artículo 29bis.1.b), del Reglamento eIDAS, la duplicación de los datos de creación de firma se realiza únicamente con fines de copia de seguridad, garantizando que la seguridad de los conjuntos de datos duplicados sea del mismo nivel que la de los originales y que el número de copias no exceda del mínimo necesario para garantizar la continuidad del servicio Tanto la generación de la copia como la recuperación de esta necesitan al menos de la participación de dos personas.

En la plataforma centralizada QSCD de DIGITEL TS se pueden realizar copias de seguridad de las claves del Titular en los términos marcados por la reglamentación correspondiente.

5 CONTROLES DE LAS INSTALACIONES, DE GESTIÓN Y OPERACIONALES

5.1 CONTROLES FÍSICOS

Según lo dispuesto en la DPPC.

5.1.1 UBICACIÓN Y CONSTRUCCIÓN

Según lo dispuesto en la DPPC.

5.1.2 ACCESO FÍSICO

Según lo dispuesto en la DPPC.

5.1.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

Según lo dispuesto en la DPPC.

5.1.4 EXPOSICIÓN AL AGUA

Según lo dispuesto en la DPPC.

5.1.5 PROTECCIÓN Y PREVENCIÓN DE INCENDIOS

Según lo dispuesto en la DPPC.

5.1.6 SISTEMA DE ALMACENAMIENTO

Según lo dispuesto en la DPPC.

5.1.7 ELIMINACIÓN DE RESIDUOS

Según lo dispuesto en la DPPC.

5.1.8 COPIA DE RESPALDO EXTERNA

Según lo dispuesto en la DPPC.

5.2 CONTROLES PROCEDIMENTALES

5.2.1 ROLES DE CONFIANZA

Según lo dispuesto en la DPPC.

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Según lo dispuesto en la DPPC.

5.2.3 IDENTIFICACIÓN Y AUTENTIFICACIÓN PARA CADA ROL

Según lo dispuesto en la DPPC.

5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE TAREAS

Según lo dispuesto en la DPPC.

5.3 CONTROLES DEL PERSONAL

5.3.1 CALIFICACIONES, EXPERIENCIA Y REQUISITOS DE AUTORIZACIÓN

Según lo dispuesto en la DPPC.

5.3.2 PROCEDIMIENTOS DE COMPROBACIÓN DE ANTECEDENTES

Según lo dispuesto en la DPPC.

5.3.3 REQUERIMIENTOS DE FORMACIÓN

Según lo dispuesto en la DPPC.

5.3.4 REQUERIMIENTOS Y FRECUENCIA DE LA ACTUALIZACIÓN DE LA FORMACIÓN

Según lo dispuesto en la DPPC.

5.3.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

No estipulado.

5.3.6 SANCIONES POR ACCIONES NO AUTORIZADAS

Según lo dispuesto en la DPPC.

5.3.7 REQUERIMIENTOS DE CONTRATACIÓN DE PERSONAL

Según lo dispuesto en la DPPC.

5.3.8 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

Según lo dispuesto en la DPPC.

5.4 PROCEDIMIENTOS DE REGISTRO DE EVENTOS

Según lo dispuesto en la DPPC.

5.4.1 TIPOS DE EVENTOS REGISTRADOS

Los tipos de eventos registrados están previstos en la DPPC de DIGITEL TS. Adicionalmente y a efectos del servicio amparado en esta DPP, DIGITEL TS registrará todos los eventos de seguridad, incluyendo los cambios relacionados con la política de seguridad, el arranque y el apagado del sistema, las caídas del sistema y fallos de hardware, actividades del firewall y del router e intentos de acceso al sistema SSASS.

El SSAS guarda registro, al menos, de los siguientes eventos:

- Inicialización de sistema, arranque, parada y cambios de configuración.
- Eventos de gestión de claves del firmante (generación, activación, uso, desactivación y

destrucción)

- Uso de claves de los firmantes.
- Autenticación de los firmantes (incluyendo intentos fallidos).
- Gestión de los datos de activación de firma del firmante (cambios de PIN)
- Arranque y parada de las funciones de auditoría.
- Cambio de la configuración de las funciones de auditoría.
- Accesos al sistema por parte de los usuarios administradores.
- El SSAS deja de procesar de forma automática peticiones en el caso de que sus funciones de auditoría no estén disponibles. [OVR-6.4.5-03]
- Todos los intentos de acceso al SSAS son registrados.

Los eventos de firma del usuario incluyen el certificado asociado a la clave de firma.

El SSAS genera un registro de auditoría continuo en el que solo es posible añadir nuevos eventos y no es posible eliminar o modificar los eventos anteriores.

El SSAS protege los eventos del registro de auditoría a nivel de entrada y de todo el registro aplicando una función HMAC que encadena cada registro con el anterior. [OVR-6.4.5-04] para evitar el borrado no autorizado.

Todos los registros de eventos del registro de auditoría del SSAS incluyen la siguiente información:

- Fecha y hora del evento.
- Tipo de evento.
- Identidad de la entidad (firmante, administrador o proceso) responsable de la acción.
- Resultado del evento (éxito o error) [OVR-6.4.5-05]

El SSAS comprueba en el arranque y periódicamente la integridad del registro de auditoría para detectar el borrado o modificación. Adicionalmente el SSAS dispone de una funcionalidad para verificar la integridad del registro de auditoría a petición de un usuario con rol de auditor en el sistema. [OVR-6.4.5-06].

Los registros de auditoría relativos al servicio amparado en esta DPP se conservarán en un formato que pueda ser procesado y presentado de tal manera que los auditores del sistema puedan interpretar la información. [SRG_AA.4.2].

Para garantizar la precisión de la fecha y hora de los eventos de auditoría el reloj de los sistemas se encuentra sincronizado por NTP tal y como se explica en el punto 6.1.3 Sincronización horaria. Existen controles para detectar problemas que puedan comprometer la sincronización. [OVR-6.4.5-07].

El SSAS denegará por defecto a todos los usuarios el acceso de lectura a los registros de auditoría,

excepto a los usuarios a los que se les haya concedido acceso de lectura explícito (por ejemplo, los que tengan el rol de Auditor del Sistema). [SRG_AA.5.1].

El sistema generará una advertencia que notifique todos los eventos inusuales al personal administrativo en los roles de confianza para su gestión. Entre otros, el sistema notificará los eventos siguientes:

- Acciones del usuario fuera del horario de uso estándar.
- Acciones del usuario ejecutadas con una velocidad anormal (para detectar intervenciones no humanas).
- Acciones del usuario que se saltan las actividades estándar dentro de los procesos definidos.
- Sesiones de usuario duplicadas

5.4.2 PERIODOS DE RETENCIÓN PARA LOS REGISTROS DE AUDITORIA

Según lo dispuesto en la DPPC.

5.4.3 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Según lo dispuesto en la DPPC.

5.4.4 PROCEDIMIENTOS DE COPIA DE RESPALDO DE LOS REGISTROS DE AUDITORÍA

Según lo dispuesto en la DPPC.

5.4.5 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORIA

Según lo dispuesto en la DPPC.

5.5 CAMBIO DE CLAVES

Según lo dispuesto en la DPPC.

5.6 RECUPERACIÓN EN CASO DE COMPROMISO DE LA CLAVE O DESASTRE

Según lo dispuesto en la DPPC.

5.6.1 PROCEDIMIENTOS DE GESTIÓN DE INCIDENCIAS Y COMPROMISOS

Según lo dispuesto en la DPPC.

5.6.2 CORRUPCIÓN DE RECURSOS, APLICACIONES O DATOS

Según lo dispuesto en la DPPC.

5.6.3 CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Según lo dispuesto en la DPPC.

5.7 TERMINACIÓN DEL SERVICIO

5.7.1 CESE DE ACTIVIDAD O DEL SERVICIO

DIGITEL TS dispone de un plan de terminación del servicio para cada servicio de confianza cualificado que presta, de conformidad con el artículo 24, apartado 2, letra i), del Reglamento eIDAS y con los requisitos establecidos en el artículo 3 del Reglamento de Ejecución (UE) 2025/2530, que garantiza la continuidad del servicio y la preservación de la información como evidencia en procedimientos judiciales.

6 CONTROLES DE SEGURIDAD TÉCNICA

6.1 GESTIÓN DE LA SEGURIDAD DE LOS SISTEMAS

6.1.1 GESTIÓN DE LOS SISTEMAS Y DE LA SEGURIDAD

6.1.1.1. ROLES PRIVILEGIADOS

En el marco de la prestación del servicio SSAS de DIGITEL TS, constituyen roles con acceso privilegiado los administradores y operadores del sistema SSAS.

6.1.1.2. ROLES SIN PRIVILEGIOS DE ACCESO

En el marco de la prestación del servicio SSAS de DIGITEL TS, constituyen roles sin acceso privilegiado, los siguientes:

- **Firmante:** está autorizado a utilizar la plataforma centralizada de firma QSCD de DIGITEL TS pasando los datos de activación de firma (SAD) como parte del protocolo de activación de firma (SAP) para firmar el documento o la representación de datos a firmar (DTBS/R), que potencialmente también puede pasar por el protocolo de activación de firma (SAP).
- **SCA:** está autorizado a enviar la solicitud representación de datos a firmar (DTBS/R) a la plataforma centralizada QSCD para que sea firmada por un firmante.
- **RA:** Está autorizada a enviar la clave pública del certificado al servicio de firma remota SSAS en respuesta a una solicitud de certificado firmada.

6.1.2 OPERACIONES DE LOS SISTEMAS

La entidad dispone de procedimientos para operar de forma correcta y segura el SSAS. **[**CEN EN 419 241-1 6.2.2.1. (SRG_SO.1.1 Y SRG_SO.1.2)]

El componte software SSA y el QSCD son operados de acuerdo con sus manuales para su instalación, administración y operación para cumplir con los objetivos de seguridad definidos en la Declaración de Seguridad de su certificación Common Criteria. [CEN EN 419 241-1 6.2.2.1. (SRG_SO.1.1 Y SRG_SO.1.2)]

6.1.3 SINCRONIZACIÓN HORARIA

DIGITEL TS garantiza que el servicio SSAS esté convenientemente sincronizado con una fuente de tiempo estándar. Los servidores de la Autoridad de Certificación de DIGITEL TS están conectados a las fuentes primarias Equinix Precision Time NTP, con un nivel Stratum 1, desde Frankfurt y Londres, balanceada mediante dos IP como fuentes de tiempo en los *appliance* de la Autoridad de Certificación.

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

6.2 CONTROLES DE SEGURIDAD INFORMÁTICA

Todos los definidos en la sección 6.5 “Controles de seguridad informática” de la DPPC de DIGITEL TS.

El SSASC se encuentra monitorizado y se generan alertas que son enviadas a los administradores del sistema cuando se detectan eventos que pueden impactar en su disponibilidad o comprometer su seguridad [6.2.6.1 (SRG_AA.1)]

Adicionalmente el sistema de monitorización permite generar alertas basadas en reglas de correlación para detectar comportamientos que pueden denotar un potencial ataque.

6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Según lo dispuesto en la DPPC.

6.4 CONTROLES DE SEGURIDAD DE LA RED

Según lo dispuesto en la DPPC.

7 AUDITORÍAS DE CONFORMIDAD

Según lo dispuesto en la DPPC.

7.1 FRECUENCIA DE LAS AUDITORÍAS

Según lo dispuesto en la DPPC.

7.1.1 AUDITORÍAS DE AC SUBORDINADA EXTERNA O CERTIFICACIÓN CRUZADA.

No aplicable.

7.1.2 AUDITORIA EN LAS AR

Según lo dispuesto en la DPPC.

7.1.3 AUDITORÍAS INTERNAS

Según lo dispuesto en la DPPC.

7.2 IDENTIFICACIÓN Y CUALIFICACIONES DEL AUDITOR

Según lo dispuesto en la DPPC.

7.3 RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

Según lo dispuesto en la DPPC.

7.4 PUNTOS CUBIERTOS POR LA AUDITORIA

Según lo dispuesto en la DPPC.

7.5 MEDIDAS TOMADAS COMO RESULTADO DE LAS DEFICIENCIAS

Según lo dispuesto en la DPPC.

7.6 COMUNICACIÓN DE RESULTADOS

Según lo dispuesto en la DPPC.

8 ASPECTOS LEGALES Y OTROS ASUNTOS

8.1 TARIFAS

8.1.1 TARIFAS DE EMISIÓN DE CERTIFICADOS Y RENOVACIÓN

Los precios de los servicios de SSAS o cualquier otro servicio relacionado están disponibles y actualizados en la página Web de DIGITEL TS https://www.digitel ts.com/certificados-digitales/ o previa consulta al departamento de soporte de digitel ts en https://www.digitel ts.com/contacto-soporte/ o al teléfono +34 91 136 91 05.

El servicio de SSAS de DIGITEL TS tiene publicado su precio concreto de venta al público, al igual que otros servicios excepto aquellos que están sujetos a una negociación comercial previa.

8.1.2 TARIFAS

Según lo dispuesto en la DPPC.

8.1.3 POLÍTICA DE REINTEGROS

Según lo dispuesto en la DPPC.

8.2 RESPONSABILIDAD FINANCIERA

8.2.1 COBERTURA DEL SEGURO

Según lo dispuesto en la DPPC.

8.2.2 OTROS ACTIVOS

No estipulado.

8.2.3 SEGURO O COBERTURA DE GARANTÍA PARA ENTIDADES FINALES

Según lo dispuesto en la DPPC.

8.3 CONFIDENCIALIDAD DE LA INFORMACIÓN DEL NEGOCIO

8.3.1 TIPO DE INFORMACIÓN A MANTENER CONFIDENCIAL

Según lo dispuesto en la DPPC.

8.3.2 TIPO DE INFORMACIÓN CONSIDERADA NO CONFIDENCIAL

Según lo dispuesto en la DPPC.

8.3.3 RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Según lo dispuesto en la DPPC.

8.4 PRIVACIDAD DE LA INFORMACIÓN PERSONAL

8.4.1 PLAN DE PRIVACIDAD

Según lo dispuesto en la DPPC.

8.4.2 INFORMACIÓN TRATADA COMO PRIVADA

Según lo dispuesto en la DPPC.

8.4.3 INFORMACIÓN NO CONSIDERADA PRIVADA

Según lo dispuesto en la DPPC.

8.4.4 RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN PRIVADA

Según lo dispuesto en la DPPC.

8.4.5 AVISO Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

Según lo dispuesto en la DPPC.

8.4.6 DIVULGACIÓN DE CONFORMIDAD CON UN PROCESO JUDICIAL O ADMINISTRATIVO

Según lo dispuesto en la DPPC.

8.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

Según lo dispuesto en la DPPC.

8.5 DERECHOS DE PROPIEDAD INTELECTUAL

Según lo dispuesto en la DPPC.

8.6 OBLIGACIONES Y RESPONSABILIDAD CIVIL

8.6.1 OBLIGACIONES Y RESPONSABILIDAD DE LA AC

Según lo dispuesto en la DPPC.

8.6.2 OBLIGACION Y RESPONSABILIDAD DE LA AR

Según lo dispuesto en la DPPC.

8.6.3 OBLIGACIÓN Y RESPONSABILIDAD DEL SUSCRIPTOR

Según lo dispuesto en la DPPC.

8.6.4 OBLIGACIÓN Y RESPONSABILIDAD DE LA PARTE QUE CONFÍA

Según lo dispuesto en la DPPC.

8.6.5 OBLIGACIÓN Y RESPONSABILIDAD DE OTROS PARTICIPANTES

No estipulado.

8.7 EXONERACIÓN DE RESPONSABILIDAD

Según lo dispuesto en la DPPC.

8.8 LIMITACIÓN DE RESPONSABILIDAD EN CASO DE PÉRDIDAS POR TRANSACCIONES

Según lo dispuesto en la DPPC.

8.9 INDEMNIZACIONES

Según lo dispuesto en la DPPC.

8.10 PLAZO Y FINALIZACIÓN

8.10.1 PLAZO

Según lo dispuesto en la DPPC.

8.10.2 FINALIZACIÓN

Según lo dispuesto en la DPPC.

8.10.3 EFECTO DE LA TERMINACIÓN Y SUPERVIVENCIA

Según lo dispuesto en la DPPC.

8.11 NOTIFICACIONES INDIVIDUALES Y COMUNICACIÓN CON LOS PARTICIPANTES

Según lo dispuesto en la DPPC.

8.12 MODIFICACIONES

8.12.1 PROCEDIMIENTO DE MODIFICACIÓN

Según lo dispuesto en la DPPC.

8.12.2 MECANISMO DE NOTIFICACIÓN Y PLAZOS

Según lo dispuesto en la DPPC.

8.12.3 CIRCUNSTANCIAS EN LAS QUE SE DEBE CAMBIAR EL OID

No estipulado.

8.13 PROCEDIMIENTO DE RESOLUCIÓN DE CONFLICTOS

Según lo dispuesto en la DPPC.

8.14 LEGISLACIÓN APLICABLE

Según lo dispuesto en la DPPC.

8.15 CONFORMIDAD CON LA LEY APLICABLE

Según lo dispuesto en la DPPC.

8.16 CLÁUSULAS DIVERSAS

8.16.1 ACUERDO COMPLETO

Según lo dispuesto en la DPPC.

8.16.2 ASIGNACIÓN

Según lo dispuesto en la DPPC.

8.16.3 SEPARABILIDAD

Según lo dispuesto en la DPPC.

8.16.4 CUMPLIMIENTO (HONORARIOS DE ABOGADOS Y EXENCIÓN DE DERECHOS)

Según lo dispuesto en la DPPC.

8.16.5 FUERZA MAYOR

Según lo dispuesto en la DPPC.

8.17 OTRAS PROVISIONES

No estipulado.