DIGITELTS

by MADISON®

PDS

Certificados de TSA

Contenido

Control de versiones

Fecha	Versión	Descripción	Autor
	1.0	Versión Inicial	Digitel TS

Documentos relacionados

Documento	Descripción

1 TEXTO DE DIVULGACIÓN

1.1 Certificados de TSA

Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación de la Autoridad de Certificación de DIGITELTS.

Este documento sigue la estructura definida en el Anexo A de la norma ETSI EN 319 411-1, de acuerdo con las indicaciones del apartado 4.3.4 de la norma ETSI EN 319 412-5.

1.1.1 Información para contactos

- Organización responsable
  - DIGITEL ON TRUSTED SERVICES, S.L.U
  - Enrique Cubero, 9, 47014 – Valladolid
  - NIF: B-47447560
- Datos de contacto
  - Teléfono: +34 91 015 05 10
  - Email: pki@digitelts.es
- Área que administra el documento
  - Departamento técnico de DIGITELTS
  - Teléfono: +34 91 015 05 10
  - Email: pki@digitelts.es
- Datos para procesos de revocación
  - Departamento técnico de DIGITELTS
  - Teléfono: +34 91 015 05 10
  - Email: revoke@digitelts.es

1.1.2 Tipos y finalidades de los certificados

- **Certificado de sello electrónico para unidades de sellado de tiempo**

Los OID de este certificado son:

- En la jerarquía propia: **1.3.6.1.4.1.54225.10.1.1**
- En ETSI la política QCP-l: **0.4.0.194112.1.1**

Los certificados de sello electrónico de TSU son certificados cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 421 y ETSI EN 319 422.

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

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

- El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
  - Content Commitment
  - Firma digital
- El campo “extend key usage” tiene activada la función:
  - TimeStamping
- En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
  - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

  - En el campo “Qualified Certificate Statements” no aparece la declaración QcSSCD (0.4.0.1862.1.4), ya que este certificado no se usa con un dispositivo cualificado.
- El campo “User Notice” describe el uso de este certificado.

1.1.3 Entidad de Certificación emisora

Los certificados indicados son emitidos por la Autoridad de Certificación de DIGITEL, identificada mediante los datos indicados anteriormente.

1.1.4 Límites de uso del certificado

- **Límites de uso para los creadores de sellos**

Se debe utilizar el servicio de sellado cualificado de tiempo electrónico, prestado por la Autoridad de Certificación de DIGITELTS exclusivamente para los usos autorizados en el contrato firmado entre ésta y el SUSCRIPTOR, y que se reproducen posteriormente (sección “obligaciones de los firmantes”).

Se debe utilizar el servicio de sellado de tiempo electrónico de acuerdo con las instrucciones, manuales o procedimientos suministrados por la Autoridad de Certificación de DIGITEL.

Se debe cumplir cualquier ley y regulación que pueda afectar al uso de las herramientas criptográficas que emplee.

No se pueden adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de sellado de tiempo electrónico de la Autoridad de Certificación de DIGITEL, sin previo permiso expreso.

- **Límites para los verificadores**

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

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados no pueden emplearse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC).

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como 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.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, visibles en el web de la Autoridad de Certificación de DIGITELTS https://pki.digitelts.es

El empleo de los certificados digitales en operaciones que contravienen este texto de divulgación, o los contratos con los suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a la Autoridad de Certificación de DIGITEL, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse

de la utilización del mismo fuera de los límites y condiciones de uso recogidas en este texto de divulgación, o en los contratos con los suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

1.1.5 Obligaciones de los suscriptores

- **Generación de claves**

El suscriptor autoriza a la Autoridad de Certificación de DIGITELTS a generar las claves, privada y pública, para la emisión de este certificado.

- **Solicitud de certificados**

El suscriptor se obliga a realizar las solicitudes de los certificados de acuerdo con el procedimiento y, si es necesario, los componentes técnicos suministrados por la Autoridad de Certificación de DIGITEL, de conformidad con lo que se establece en la declaración de prácticas de certificación (DPC) y en su documentación de operaciones.

- **Veracidad de la información**

El suscriptor se responsabiliza de que toda la información incluida en su solicitud del certificado sea exacta, completa para la finalidad del certificado y esté actualizada en todo momento.

El suscriptor tiene que informar inmediatamente a la Autoridad de Certificación de DIGITEL:

- De cualquier inexactitud detectada en el certificado una vez se haya emitido.
- De los cambios que se produzcan en la información aportada y/o registrada para la emisión del certificado.
- De la pérdida, robo, sustracción, o cualquier otro tipo de pérdida de control de la clave privada por el custodio.

- **Obligaciones de custodia**

El suscriptor se obliga a custodiar toda la información que genere en su actividad como entidad de registro.

A custodiar el código de identificación personal o cualquier soporte técnico entregado por la Autoridad de Certificación de DIGITEL, las claves privadas y, si fuese necesario, las especificaciones propiedad de la Autoridad de Certificación de DIGITELTS que le sean suministradas.

En caso de pérdida o robo de la clave privada del certificado, o en caso de que se sospeche que la clave privada ha perdido fiabilidad por cualquier motivo, dichas circunstancias han de ser notificadas inmediatamente a la Autoridad de Certificación de DIGITELTS por medio del suscriptor.

- **Obligaciones de uso correcto**

Se debe utilizar el certificado exclusivamente para los usos autorizados en la DPC y en cualquier otra instrucción, manual o procedimiento suministrado al suscriptor.

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

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

Además:

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

- **Transacciones prohibidas**

El firmante se obliga a no utilizar sus claves privadas, los certificados o cualquier otro soporte técnico entregado por la Autoridad de Certificación de DIGITELTS en la realización de transacción alguna prohibida por la ley aplicable.

Los servicios de certificación digital y de sellado de tiempo electrónico prestados por la Autoridad de Certificación de DIGITELTS no han sido diseñados ni permiten su utilización o reventa como equipos de control de situaciones peligrosas, o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo o sistemas de control de armamento, en las que un error pudiera directamente causar la muerte, daños físicos o daños medioambientales graves.

1.1.6 Obligaciones de los verificadores

- **Decisión informada**

La Autoridad de Certificación de DIGITELTS informa al verificador que tiene acceso a información suficiente para tomar una decisión informada en el momento de verificar un certificado y confiar en la información contenida en dicho certificado.

Adicionalmente, el verificador reconocerá que el uso del Registro y de las Listas de Revocación de Certificados (en lo sucesivo, "las LRCs" o "las CRLs) de la Autoridad de Certificación de DIGITEL, se rigen por su DPC y se comprometerá a cumplir los requisitos técnicos, operativos y de seguridad descritos en la mencionada DPC.

- **Requisitos de verificación del sello de tiempo**

La comprobación será ejecutada normalmente de forma automática por el software del verificador y, en todo caso, de acuerdo con la DPC, con los siguientes requisitos:

- Es necesario utilizar el software apropiado para la verificación de un sello de tiempo con los algoritmos y longitudes de claves autorizados en el certificado y/o ejecutar cualquier otra operación criptográfica, y establecer la cadena de certificados en que se basa el sello de tiempo a verificar, ya que éste se verifica utilizando esta cadena de certificados.
- Es necesario asegurar que la cadena de certificados identificada es la más adecuada para el sello de tiempo que se verifica, ya que un sello de tiempo puede basarse en más de una cadena de certificados, y es decisión del verificador asegurarse el uso de la cadena más adecuada para verificarla.

- Es necesario comprobar el estado de revocación de los certificados de la cadena con la información suministrada al Registro de la Autoridad de Certificación de DIGITELTS (con LRCs, por ejemplo) para determinar la validez de todos los certificados de la cadena de certificados, ya que únicamente puede considerarse correctamente verificado un sello de tiempo si todos y cada uno de los certificados de la cadena son correctos y se encuentran vigentes.
- Es necesario asegurar que todos los certificados de la cadena autorizan el uso de la clave privada por el suscriptor del certificado, ya que existe la posibilidad de que alguno de los certificados incluya límites de uso que impidan confiar en el sello de tiempo que se verifica. Cada certificado de la cadena dispone de un indicador que hace referencia a las condiciones de uso aplicables, para su revisión por los verificadores.
- Es necesario verificar técnicamente la firma de todos los certificados de la cadena antes de confiar en el certificado utilizado para el sellado de tiempo electrónico.

- **Confianza en un certificado no verificado**

Si el verificador confía en un certificado no verificado, asumirá todos los riesgos derivados de esta actuación.

- **Uso correcto y actividades prohibidas**

El verificador se obliga a no utilizar ningún tipo de información de estado de los certificados o de ningún otro tipo que haya sido suministrada por la Autoridad de Certificación de DIGITEL, en la realización de transacción alguna prohibida para la ley aplicable a la citada transacción.

El verificador se obliga a no inspeccionar, interferir o realizar ingeniería inversa de la implantación técnica de los servicios públicos de sellado de tiempo electrónico o de certificación de la Autoridad de Certificación de DIGITEL, sin previo consentimiento escrito.

Adicionalmente, el verificador se obliga a no comprometer intencionadamente la seguridad de los servicios públicos de sellado de tiempo electrónico ni de certificación de la Autoridad de Certificación de DIGITEL.

Los servicios de sellado de tiempo electrónico y de certificación digital prestados por la Autoridad de Certificación de DIGITELTS no han sido diseñados ni permiten la utilización o reventa, como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo, o sistemas de control de armamento, donde un error podría causar la muerte, daños físicos o daños medioambientales graves.

- **Cláusula de indemnidad**

El tercero que confía en el certificado se compromete a mantener indemne a la Autoridad de Certificación de DIGITELTS de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.

- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.
- Falta de comprobación de la totalidad de medidas de aseguramiento prescritas en la DCP o resto de normas de aplicación.

La Autoridad de Certificación de DIGITELTS no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

1.1.7 Obligaciones de la Autoridad de Certificación de DIGITELTS

- **En relación con la prestación del servicio de certificación digital**

La Autoridad de Certificación de DIGITELTS se obliga a:

a) Emitir, entregar, administrar, suspender, revocar y renovar certificados, de acuerdo con las instrucciones suministradas por el suscriptor, en los casos y por los motivos descritos en la DPC de la Autoridad de Certificación de DIGITEL.
b) Ejecutar los servicios con los medios técnicos y materiales adecuados, y con personal que cumpla las condiciones de cualificación y experiencia establecidas en la DPC.
c) Cumplir los niveles de calidad del servicio, en conformidad con lo que se establece en la DPC, en los aspectos técnicos, operativos y de seguridad.
d) Notificar al suscriptor, con anterioridad a la fecha de expiración de los certificados, de la posibilidad de renovarlos, así como la suspensión, alzamiento de esta suspensión o revocación de los certificados, cuando se produzcan dichas circunstancias.
e) Comunicar a las terceras personas que lo soliciten, el estado de los certificados, de acuerdo con lo que se establece en la DPC para los diferentes servicios de verificación de certificados.

- **En relación con las comprobaciones del registro**

La Autoridad de Certificación de DIGITELTS se obliga a la emisión de certificados en base a los datos suministrados por el suscriptor, por lo cual podrá realizar las comprobaciones que considere oportunas.

En el caso que la Autoridad de Certificación de DIGITELTS detecte errores en los datos que se deben incluir en los certificados o que justifican estos datos, podrá realizar los cambios que considere necesarios antes de emitir el certificado o suspender el proceso de emisión y gestionar con el suscriptor la incidencia correspondiente. En caso de que la Autoridad de Certificación de DIGITELTS corrija los datos sin gestión previa de la incidencia correspondiente con el suscriptor, deberá notificar los datos finalmente certificados al suscriptor.

La Autoridad de Certificación de DIGITELTS se reserva el derecho a no emitir el certificado, cuando considere que la justificación documental resulte insuficiente para la correcta identificación y autenticación del suscriptor y/o del dominio.

Las anteriores obligaciones quedarán en suspenso en los casos en que el suscriptor actúe como autoridad de registro y disponga de los elementos técnicos correspondientes a la generación de claves, emisión de certificados y grabación de dispositivos de firma corporativos.

- **Periodos de conservación**

La Autoridad de Certificación de DIGITELTS archiva los registros correspondientes a las solicitudes de emisión y revocación de certificados durante al menos 15 años.

La Autoridad de Certificación de DIGITELTS almacena la información de los logs durante un periodo de 15 años.

1.1.8 Garantías limitadas y rechazo de garantías

- **Garantía de la Autoridad de Certificación de DIGITELTS por los servicios de certificación digital**

Se garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Autoridad de Certificación de DIGITEL.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación de este.
- Que los certificados cumplen con todos los requisitos materiales establecidos en la DPC.
- Que los servicios de revocación y el empleo del depósito cumplen con todos los requisitos materiales establecidos en la DPC.

La Autoridad de Certificación de DIGITELTS garantiza al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el depósito, que el certificado ha sido emitido al suscriptor y firmante identificado en el mismo y que el certificado ha sido aceptado.
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la DPC.

- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y depósito.

Adicionalmente, la Autoridad de Certificación de DIGITELTS garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado cualificado de sello electrónico, de acuerdo con el anexo III del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE y con las indicaciones adicionales para la creación de sellos cualificados de tiempo de acuerdo con el artículo 42 de este mismo Reglamento.
- Que, en el caso de que genere las claves privadas del suscriptor, se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la Autoridad de Certificación de DIGITEL, con los límites que se establezcan. En ningún caso Autoridad de Certificación de DIGITELTS responderá por caso fortuito y en caso de fuerza mayor.
- La clave privada de la entidad de certificación utilizada para emitir certificados no ha sido comprometida, a menos que la Autoridad de Certificación de DIGITELTS no haya comunicado lo contrario mediante el Registro de certificación, de acuerdo con la DPC.
- No ha originado ni ha introducido declaraciones falsas o erróneas en la información de ningún certificado, ni ha dejado de incluir información necesaria aportada por el suscriptor y validada por la Autoridad de Certificación de DIGITEL, en el momento de la emisión del certificado.
- Todos los certificados cumplen los requisitos formales y de contenido de la DPC, incluyendo todos los requisitos legales en vigor y aplicables.
- Queda vinculada por los procedimientos operativos y de seguridad descritos en la DPC.

- **Exclusión de la garantía**

La Autoridad de Certificación de DIGITELTS rechaza toda otra garantía diferente a la anterior que no sea legalmente exigible.

Específicamente, la Autoridad de Certificación de DIGITELTS no garantiza software alguno utilizado por cualquier persona para firmar, verificar firmas, cifrar, descifrar, o utilizar de otra forma certificado digital alguno emitido por la Autoridad de Certificación de DIGITEL, excepto en los casos en que exista una declaración escrita en sentido contrario.

1.1.9 Acuerdos aplicables y DPC

- **Acuerdos aplicables**

Los acuerdos aplicables a los certificados son los siguientes:

- Contrato de servicios de certificación, que regula la relación entre la Autoridad de Certificación de DIGITELTS, y la persona jurídica suscriptora de los certificados.
- Condiciones generales del servicio incorporadas en este texto de divulgación del certificado o PDS.
- DPC, que regula la emisión y utilización de los certificados.

- **DPC (Declaración de Prácticas de Confianza)**

Los servicios de certificación y de sellado de tiempo de la Autoridad de Certificación de DIGITELTS se regulan técnica y operativamente por su DPC,

por sus actualizaciones posteriores, así como por documentación complementaria.

La DPC y la documentación de operaciones se modifica periódicamente y se puede consultar en la dirección: https://pki.digitelts.es

1.1.10 Reglas de confianza para firmas longevas

La Autoridad de Certificación de DIGITELTS informa a los solicitantes de los certificados que no ofrece un servicio que garantice la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

1.1.11 Política de intimidad

La Autoridad de Certificación de DIGITELTS no puede divulgar ni puede ser obligada a divulgar información confidencial alguna en lo referente a certificados sin una solicitud específica previa que provenga de:

a) La persona con respecto a la cual la Autoridad de Certificación de DIGITELTS tiene el deber de mantener la información confidencial, o
b) Una orden judicial, administrativa o cualquier otra prevista en la legislación vigente.

Sin embargo, el suscriptor acepta que determinada información, personal y de otro tipo, proporcionada en la solicitud de certificados, sea incluida en sus certificados y en el mecanismo de comprobación del estado de los certificados, y que la información mencionada no tenga carácter confidencial, por imperativo legal.

La Autoridad de Certificación de DIGITELTS no cede a ninguna persona los datos entregados específicamente para la prestación del servicio de certificación.

El tratamiento de dichos datos por motivo de la prestación del servicio de certificación, se produce en el marco en el que la Autoridad de Certificación de DIGITELTS es responsable del tratamiento de los datos personales a que se refiere el artículo 28 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), y 33 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) y en su virtud es conforme con los requisitos del RGPD y de la LOPDGDD, y garantiza la protección de los derechos del interesado.

1.1.12 Política de privacidad

La Autoridad de Certificación de DIGITELTS dispone de una política de privacidad en el apartado 9.4 de la DPC, y regulación específica de la privacidad en relación con el proceso de registro, la confidencialidad del registro, la protección del acceso a la información personal, y el consentimiento del usuario.

Asimismo, se contempla que la documentación justificativa de la aprobación de la solicitud debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante el plazo de 15 años desde la expiración del

certificado, incluso todo en caso de pérdida anticipada de vigencia por revocación.

1.1.13 Política de reintegro

La Autoridad de Certificación de DIGITELTS no reintegrará el coste del servicio de certificación en ningún caso.

1.1.14 Ley aplicable y jurisdicción competente

Las relaciones con la Autoridad de Certificación de DIGITELTS se regirán por la ley española en materia de servicios de confianza vigente en cada momento, así como por la legislación civil y mercantil en lo que sea de aplicación.

La jurisdicción competente es la que se indica en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

En caso de discrepancia entre las partes, las partes intentarán la previa resolución amistosa. A tal fin, las partes deberán dirigir una comunicación a la Autoridad de Certificación de DIGITELTS por cualquier medio que deje constancia a la dirección de contacto indicada en el punto 1.1.1 de esta PDS.

Si las partes no alcanzasen un acuerdo al respecto, cualquiera de ellas podrá someter el conflicto a la jurisdicción civil, con sujeción a los Tribunales del domicilio social de la Autoridad de Certificación de DIGITELTS.

1.1.15 Acreditaciones y sellos de calidad

La Autoridad de Certificación de DIGITELTS se encuentra incluida en la lista española de prestadores de confianza (TSL): https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf

La Autoridad de Certificación de DIGITELTS dispone de la certificación "eIDAS-compliant" para los siguientes servicios:

- Servicio de expedición de sellos electrónicos cualificados de tiempo

De acuerdo con lo indicado en el Reglamento UE 910/2014, la Autoridad de Certificación de DIGITELTS realizará auditorías de conformidad cada 2 años y en los años intermedios una de seguimiento.

1.1.16 Vinculación con la lista de prestadores

La Autoridad de Certificación de DIGITELTS es prestador cualificado de servicios de certificación por lo que forma parte de la Lista de Prestadores cualificados (TSL) que mantiene el supervisor nacional y que se puede obtener en la siguiente dirección:

- https://sedeaplicaciones.minetur.gob.es/Prestadores/

La Autoridad de Certificación de DIGITELTS está incluida en la "Trust List" de la Unión Europea como Prestador cualificado de servicios electrónicos de confianza:

- https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/ES/35

1.1.17 Divisibilidad de las cláusulas, supervivencia, acuerdo íntegro y notificación

Las cláusulas del presente texto de divulgación son independientes entre sí, motivo por el cual, si cualquier cláusula es considerada inválida o inaplicable, el resto de las cláusulas de las PDS seguirán siendo aplicables, excepto acuerdo expreso en contrario de las partes.

Los requisitos contenidos en las secciones de "Obligaciones y responsabilidad", de "Auditoría de conformidad" y de "Confidencialidad" de la DPC de la Autoridad de Certificación de DIGITELTS continuarán vigentes tras la terminación del servicio.

Este texto contiene la voluntad completa y todos los acuerdos entre las partes.