DIGITELTS

by MADISON®

Declaración de prácticas de certificación de DIGITELTS

DIGITEL TS Qualified Trust Service Provider

Control documental

Líder	Área de servicios de confianza		
	Declaración de prácticas de certificación		
Distribución	**Público**		
Fecha	2024		
Descripción	Declaración de prácticas de certificación de DIGITELTS		
Aprobado	Comité de Riesgos y Seguridad DIGITEL TS	Fecha	30 de mayo 2024
Estado	Aprobado		

Control de Cambios

Versión	Fecha	Detalle
V1.0	Mayo 2021	Versión Inicial
V2.0	01 mayo 2024	▪ Inclusión de los servicios de confianza de emisión de certificados cualificados de persona Física en software y centralizados ▪ Inclusión de los servicios de confianza de emisión de certificados cualificados de sello electrónico en software y centralizados
V2.1	21 de mayo 2024	Corrección de erratas

1 Introducción

1.1 Presentación

Este documento declara las prácticas de confianza **de la Autoridad de Certificación de DIGITELTS**.

Los tipos de certificados que se emiten son los siguientes:

- Certificado para el servicio de sellado de tiempo electrónico, para la expedición de sellos cualificados de tiempo electrónico.
- Certificado cualificado de sello electrónico de persona jurídica / entidad sin personalidad jurídica.
- Certificado cualificado de firma electrónica de persona física.

1.2 Nombre del documento e identificación

Este documento es la 'Declaración de Prácticas de Confianza de la Autoridad de Certificación de DIGITELTS'.

1.2.1 Identificadores de certificados

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

OID	Tipos de certificados de Sello electrónico de Unidades de Sellado de Tiempo
1.3.6.1.4.1.54225.10.1.1	Certificado de Sello electrónico de TSU

OID	Tipos de certificados cualificados de Sello electrónico de Persona Jurídica y ESPJ
1.3.6.1.4.1.54225.10.2.1	Sello avanzado de Persona Jurídica y ESPJ
1.3.6.1.4.1.54225.10.2.5	Sello cualificado de Persona Jurídica y ESPJ

OID	Tipos de certificados cualificados de firma electrónica para personas físicas
1.3.6.1.4.1.54225.10.3.1	Certificado de firma avanzada para personas físicas individuales
1.3.6.1.4.1.54225.10.3.5	Certificado de firma cualificada para personas físicas individuales
1.3.6.1.4.1.54225.10.3.11	Certificado de firma avanzada para personas físicas vinculadas
1.3.6.1.4.1.54225.10.3.15	Certificado de firma cualificada para personas físicas vinculadas

OID	Tipos de certificados cualificados de firma electrónica para personas físicas representantes
1.3.6.1.4.1.54225.10.3.21	Certificado de firma avanzada para personas físicas representantes de Personas Jurídicas
1.3.6.1.4.1.54225.10.3.25	Certificado de firma cualificada para personas físicas representantes de Personas Jurídicas
1.3.6.1.4.1.54225.10.3.31	Certificado de firma avanzada para personas físicas representantes de ESPJ
1.3.6.1.4.1.54225.10.3.35	Certificado de firma cualificada para personas físicas representantes de ESPJ

En caso de contradicción entre esta Declaración de Prácticas de Confianza y otros documentos de prácticas y procedimientos, prevalecerá lo establecido en esta Declaración de Prácticas.

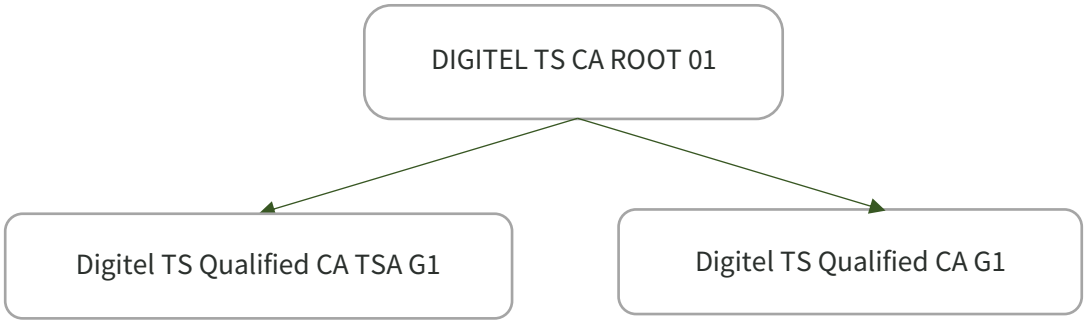
1.3 Participantes en los servicios de certificación

1.3.1 Prestador de servicios de certificación

La Autoridad de Certificación de DIGITELTS es un prestador de servicios de confianza, que actúa 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, **la Ley 6/2020, de 11 de noviembre**, reguladora de

determinados aspectos de los servicios electrónicos de confianza y las **normas técnicas de la ETSI** aplicables a los prestadores en general (ETSI EN 319 401), a los prestadores que expiden y gestionan certificados (ETSI EN 319 411-1), a los prestadores que expiden y gestionan certificados cualificados (ETSI EN 319 411-2), y a los prestadores que expiden sellos de tiempo (ETSI EN 319 421), al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

Para la prestación de los servicios de certificación, la Autoridad de Certificación de DIGITELTS ha establecido la siguiente jerarquía de entidades de certificación:



1.3.1.1 DIGITEL TS CA ROOT 01

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

Datos de identificación:

Common Name	DIGITEL TS CA ROOT 01
Huella digital	f23aa0a06261b3685ce5f05de058f801d3031f15

Válido desde:	28-04-2022 // 15:55:07
Válido hasta:	22-04-2047 // 15:55:06
Longitud RSA	4096 bits

1.3.1.2 Digitel TS Qualified CA TSA G1

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

Common Name	DIGITEL TS QUALIFIED CA TSA G1
Huella digital	`b844d3988972165a54b85f09fc8d9b757aaddbb8`
Válido desde:	06-05-2022 // 13:19:47
Válido hasta:	03-05-2035 // 13:19:46
Longitud RSA	4096 bits

1.3.1.3 DIGITEL TS QUALIFIED CA G1

Se trata de la Autoridad de Certificación cualificada que expide los certificados cualificados a las entidades finales. La clave pública de esta CA ha sido firmada digitalmente por la DIGITEL TS CA ROOT 01.

Common Name	DIGITEL TS QUALIFIED CA G1
Huella digital	5c6d8bda6146bc258b917bcbf91a2e72c7f59731
Válido desde:	06-05-2022 // 13:19:47
Válido hasta:	03-05-2035 // 13:19:46
Longitud RSA	4096 bits

1.3.2 Registradores y autoridades de Registro

En general, el prestador del servicio de certificación actúa como verificador de la identidad de los solicitantes y personas identificadas en los certificados.

También pueden actuar como registradores de los certificados sujetos a esta Declaración de Prácticas de Confianza, en aquellos tipos de certificados que dispongan de la condición de corporativos, las unidades designadas para esta función por los suscriptores de los certificados, como un departamento de personal.

También son registradores de los certificados sujetos a esta Declaración de Prácticas de Confianza destinados a los receptores, los operadores de una organización autorizada por la

Autoridad de Certificación de DIGITELTS, y bajo su responsabilidad, para realizar el procedimiento de registro presencial.

Las funciones de registro de los suscriptores se realizan por delegación y de acuerdo con las instrucciones del prestador de servicios de certificación, en los términos del artículo 24.1 del Reglamento (UE) 910/2014, y del artículo 7 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, y bajo la plena responsabilidad del prestador de servicios de confianza frente a terceros.

1.3.3 Entidades finales

Las entidades finales son las personas y organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para los usos de sellado de tiempo electrónico. Serán entidades finales de los servicios de certificación de la Autoridad de Certificación de DIGITELTS las siguientes:

- Suscriptores del servicio de certificación.
- Firmantes
- Creadores de sellos.
- Partes que confían.

1.3.3.1 Suscriptores del servicio de certificación

Los subscriptores del servicio de certificación son las empresas, entidades u organizaciones que adquieren los certificados a la Autoridad de Certificación de DIGITELTS para su uso en su ámbito corporativo empresarial u organizativo y se encuentran identificadas en los certificados.

El suscriptor del servicio de certificación adquiere un derecho de uso del certificado, para su uso propio, o al objeto de facilitar la certificación de la emisión del tiempo electrónico o la certificación de la identidad de una persona jurídica. Esta persona jurídica figura identificada en el certificado.

El suscriptor del servicio de certificación es, por tanto, el cliente del prestador de servicios de confianza, de acuerdo con la legislación mercantil, y tiene los derechos y obligaciones que se definen por el prestador del servicio de confianza, que son adicionales y se entienden sin perjuicio de los derechos y obligaciones de los creadores de sellos y firmas como se autoriza y regula en las normas técnicas europeas aplicables a la expedición de certificados electrónicos (ETSI EN 319 411-1, secciones 5.4.2 y 6.3.4) y aplicables a la expedición de certificados electrónicos cualificados (ETSI EN 319 411-2, secciones 5.4.2 y 6.3.4).

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

1.3.3.2 Firmantes

Los firmantes son las personas físicas que tienen bajo su exclusivo control, con un elevado nivel de confianza, las claves de firma digital para identificación y firma electrónica avanzada o cualificada; siendo típicamente los empleados, clientes y otras personas vinculadas a los suscriptores.

Los firmantes se encuentran, en su caso, debidamente autorizados por el suscriptor y debidamente identificados en el certificado mediante su nombre y apellidos, y número de identificación fiscal válido en la jurisdicción de expedición del certificado, sin que sea posible, en general, el empleo de seudónimos.

La clave privada de un firmante no puede ser recuperada por el prestador de servicios de certificación.

Dada la existencia de certificados para usos diferentes de la firma electrónica, como la identificación, también se emplea el término más genérico de "persona física identificada en el certificado", siempre con pleno respeto al cumplimiento de la legislación de firma electrónica en relación con los derechos y obligaciones del firmante.

1.3.3.3 Creadores de sellos

Son las personas jurídicas que disponen de certificados y crean sellos electrónicos a partir del uso de los citados certificados.

1.3.3.4 Autoridad de Sellado de Tiempo

La Autoridad de Certificación de DIGITELTS es la *Autoridad de Sellado de Tiempo electrónico* cuando ofrece el servicio de confianza de creación de sellos de tiempo electrónicos.

1.3.4 Partes que confian

Son las personas y las organizaciones que precisan confiar en los sellos de tiempo electrónicos, sellos electrónicos y firmas electrónicas.

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

1.4 Uso de los certificados

Esta sección lista las aplicaciones para las que puede emplearse cada tipo de certificado, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

1.4.1 Usos permitidos

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

1.4.1.1 Certificado de sello electrónico de TSU

Los OID de este certificado son:

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

Los certificados de sello electrónico de TSU son certificados que siguen las indicaciones de la política ETSI "**NCP+**" y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 421 y ETSI EN 319 422, y con las indicaciones adicionales para la creación de sellos cualificados de tiempo de acuerdo con el artículo 42 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

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

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

- El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones: Firma digital
- El campo "extend key usage" tiene activada la función: TimeStamping
- El campo "User Notice" describe el uso de este certificado.

1.4.1.2 Certificado de Sello avanzado de Persona Jurídica y ESPJ

Los OID de este certificado son:

- En la jerarquía propia: **1.3.6.1.4.1.54225.10.2.1**
- En ETSI la política QCP-l: **0.4.0.194112.1.1**

Este certificado es un certificado cualificado de acuerdo con el artículo 38 y con el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y da cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

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

- El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
  - Firma digital (para autenticación)
  - Compromiso con el contenido (para firma electrónica)
- En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
  - QcCompliance (0.4.0.1862.1.1), que se emite como cualificado.
  - En el campo "Qualified Certificate Statements" **no aparece** la declaración QcSSCD (0.4.0.1862.1.4).
- El campo "User Notice" describe el uso de este certificado.

1.4.1.3 Certificado de Sello cualificado de Persona Jurídica y ESPJ.

Los OID de este certificado son:

- En la jerarquía propia: **1.3.6.1.4.1.54225.10.2.5**
- En ETSI la política QCP-l-qscd: **0.4.0.194112.1.3**

Este certificado es un certificado cualificado de acuerdo con el artículo 38 y con el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y da cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados funcionan con dispositivo cualificado de creación de sello, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados son gestionados de forma centralizada, es decir, que la generación y gestión de los datos de creación de firma electrónica es realizada por el prestador, por cuenta del creador de sellos. Estos certificados garantizan la identidad del suscriptor del certificado, y permiten la generación del "*sello electrónico cualificado*"; es decir, el sello electrónico avanzado que se basa en un certificado cualificado y que ha sido generado empleando un dispositivo cualificado de creación de sellos electrónicos, por lo cual de acuerdo con lo que establece el artículo 35.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, disfrutará de la presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado.

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

- El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
  - Firma digital (para autenticación)
  - Compromiso con el contenido (para sello electrónico)
- En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
  - QcCompliance (0.4.0.1862.1.1), que se emite como cualificado.
  - En el campo "Qualified Certificate Statements" la declaración QcSSCD (0.4.0.1862.1.4) de que se usa exclusivamente en conjunción con un dispositivo cualificado de creación de sellos.
- El campo "User Notice" describe el uso de este certificado.

1.4.1.4 Certificado de firma avanzada para Persona Física Individual

Los OID de este certificado son:

- En la jerarquía propia: **1.3.6.1.4.1.54225.10.3.1**
- En ETSI la política QCP-n: **0.4.0.194112.1.0**

Este certificado es un certificado cualificado de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y da cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados garantizan la identidad del firmante y permiten la generación de la "*firma electrónica avanzada basada en certificado electrónico cualificado*".

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

- El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
  - Firma digital (para autenticación)
  - Compromiso con el contenido (para firma electrónica)
- En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
  - QcCompliance (0.4.0.1862.1.1), que se emite como cualificado.
  - En el campo "Qualified Certificate Statements" **no aparece** la declaración QcSSCD (0.4.0.1862.1.4).
- El campo "User Notice" describe el uso de este certificado.

1.4.1.5 Certificado de firma cualificada para Persona Física Individual

Los OID de este certificado son:

- En la jerarquía propia: **1.3.6.1.4.1.54225.10.3.5**
- En ETSI la política QCP-n-qscd: **0.4.0.194112.1.2**

Este certificado es un certificado cualificado de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y da cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados, funcionan con dispositivo cualificado de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados son gestionados de forma centralizada, es decir, que la generación y gestión de los datos de creación de firma electrónica es realizada por el prestador, por cuenta del firmante. Estos certificados garantizan la identidad del firmante y permiten la generación de la "firma electrónica cualificada"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

- El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
  - Firma digital (para autenticación)
  - Compromiso con el contenido (para firma electrónica)
- En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
  - QcCompliance (0.4.0.1862.1.1), que se emite como cualificado.

- En el campo “Qualified Certificate Statements” la declaración QcSSCD (0.4.0.1862.1.4) de que se usa exclusivamente en conjunción con un dispositivo cualificado de creación de firmas.

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

1.4.1.6 Certificado de firma avanzada para Persona Física Vinculada

Los OID de este certificado son:

- En la jerarquía propia: **1.3.6.1.4.1.54225.10.3.11**
- En ETSI la política QCP-n: **0.4.0.194112.1.0**

Este certificado es un certificado cualificado de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y da cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados garantizan la identidad del firmante y su vinculación con el suscriptor del certificado (indicado en el campo “Organization” del “subject” del certificado) y permiten la generación de la “firma electrónica avanzada” basada en certificado electrónico cualificado.

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

- El campo “key usage” tiene activadas, y por tanto permite realizar, las siguientes funciones:
  - Firma digital (para autenticación)
  - Compromiso con el contenido (para firma electrónica)
- En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
  - QcCompliance (0.4.0.1862.1.1), que se emite como cualificado.
  - En el campo “Qualified Certificate Statements” **no aparece** la declaración QcSSCD

(0.4.0.1862.1.4).

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

1.4.1.7 Certificado de firma cualificada para Persona Física Vinculada

Los OID de este certificado son:

- En la jerarquía propia: **1.3.6.1.4.1.54225.10.3.15**
- En ETSI la política QCP-n-qscd: **0.4.0.194112.1.2**

Este certificado es un certificado cualificado de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y da cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados, funcionan con dispositivo cualificado de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados son gestionados de forma centralizada, es decir, que la generación y gestión de los datos de creación de firma electrónica es realizada por el prestador, por cuenta del firmante. Estos certificados garantizan la identidad del firmante, su vinculación con el suscriptor del certificado (indicado en el campo “Organization” del “subject” del certificado) y permiten la generación de la “firma electrónica cualificada”; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

- El campo “key usage” tiene activadas, y por tanto permite realizar, las siguientes funciones:

- Firma digital (para autenticación)
- Compromiso con el contenido (para firma electrónica)

- En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
  - QcCompliance (0.4.0.1862.1.1), que se emite como cualificado.
  - En el campo “Qualified Certificate Statements” la declaración QcSSCD (0.4.0.1862.1.4) de que se usa exclusivamente en conjunción con un dispositivo cualificado de creación de firmas.
- El campo “User Notice” describe el uso de este certificado.

1.4.1.8 Certificado de firma avanzada para Persona Física Representante Legal de Persona Jurídica

Los OID de este certificado son:

- En la jerarquía propia: **1.3.6.1.4.1.54225.10.3.21**
- En ETSI la política QCP-n: **0.4.0.194112.1.0**
- De acuerdo con los perfiles de certificados del Ministerio de Hacienda y Administraciones Públicas: **2.16.724.1.3.5.8**

Este certificado es un certificado cualificado de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y da cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Este certificado garantiza la identidad del firmante y del subscriptor (descrito en el campo “O” -*Organization*- del “*subject*” del certificado), indica una relación de representación legal o apoderamiento general entre el firmante y el subscriptor y permiten la generación de la “*firma electrónica avanzada basada en certificado electrónico cualificado*”.

Este certificado es un certificado de representante de persona jurídica, con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las Administraciones Públicas españolas.

Este certificado incluye un campo (*Description*) en el Subject donde se indica el documento público que acredita de forma fehaciente las facultades del firmante para actuar en nombre de la entidad a la que representa y, en caso de ser obligatoria, la inscripción de los datos registrales.

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

- El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
  - Firma digital (para autenticación)
  - Compromiso con el contenido (para firma electrónica)
- En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
  - QcCompliance (0.4.0.1862.1.1), que se emite como cualificado.
  - En el campo "Qualified Certificate Statements" **no aparece** la declaración QcSSCD (0.4.0.1862.1.4).
- El campo "User Notice" describe el uso de este certificado.

1.4.1.9 Certificado de firma cualificada para Persona Física Representante Legal de Persona Jurídica

Los OID de este certificado son:

- En la jerarquía propia: **1.3.6.1.4.1.54225.10.3.25**
- En ETSI la política QCP-n-qscd: **0.4.0.194112.1.2**

- De acuerdo con los perfiles de certificados del Ministerio de Hacienda y Administraciones Públicas: **2.16.724.1.3.5.8**

Este certificado es un certificado cualificado de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y da cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados, funcionan con dispositivo cualificado de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados son gestionados de forma centralizada, es decir, que la generación y gestión de los datos de creación de firma electrónica es realizada por el prestador, por cuenta del firmante. Estos certificados garantizan la identidad del firmante, su vinculación con el suscriptor del certificado (indicado en el campo “Organization” del “subject” del certificado), indica una relación de representación legal o apoderamiento general entre el firmante y el subscriptor y permiten la generación de la “**firma electrónica cualificada**”; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

Este certificado es un certificado de representante de persona jurídica, con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las Administraciones Públicas españolas.

Este certificado incluye un campo (*Description*) en el Subject donde se indica el documento público que acredita de forma fehaciente las facultades del firmante para actuar en nombre de la entidad a la que representa y, en caso de ser obligatoria, la inscripción de los datos registrales.

- El campo “key usage” tiene activadas, y por tanto permite realizar, las siguientes funciones:
  - Firma digital (para autenticación)
  - Compromiso con el contenido (para firma electrónica)
- En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
  - QcCompliance (0.4.0.1862.1.1), que se emite como cualificado.
  - En el campo “Qualified Certificate Statements” la declaración QcSSCD (0.4.0.1862.1.4) de que se usa exclusivamente en conjunción con un dispositivo cualificado de creación de firmas.
- El campo “User Notice” describe el uso de este certificado.

1.4.1.10 Certificado de firma avanzada para Persona Física Representante Legal de Entidad Sin Personalidad Jurídica

Los OID de este certificado son:

- En la jerarquía propia: **1.3.6.1.4.1.54225.10.3.31**
- En ETSI la política QCP-n: **0.4.0.194112.1.0**
- De acuerdo con los perfiles de certificados del Ministerio de Hacienda y Administraciones Públicas: **2.16.724.1.3.5.9**

Este certificado es un certificado cualificado de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y da cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Este certificado garantiza la identidad del firmante y del subscriptor (descrito en el campo “O” -*Organization*- del “*subject*” del certificado), indica una relación de representación entre el

firmante y el subscriptor y permiten la generación de la "*firma electrónica avanzada basada en certificado electrónico cualificado*".

Estos certificados son certificados de representante de entidad sin personalidad jurídica, en el que el Representante tiene plenas capacidades para actuar en nombre de la Entidad sin Personalidad Jurídica ante las Administraciones Públicas españolas.

Este certificado incluye un campo (*Description*) en el Subject donde se indica el documento público que acredita de forma fehaciente las facultades del firmante para actuar en nombre de la entidad a la que representa y, en caso de ser obligatoria, la inscripción de los datos registrales.

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

- El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
  - Firma digital (para autenticación)
  - Compromiso con el contenido (para firma electrónica)
- En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
  - QcCompliance (0.4.0.1862.1.1), que se emite como cualificado.
  - En el campo "Qualified Certificate Statements" **no aparece** la declaración QcSSCD (0.4.0.1862.1.4).
- El campo "User Notice" describe el uso de este certificado.

1.4.1.11 Certificado de firma cualificada para Persona Física Representante Legal de Entidad Sin Personalidad Jurídica

Los OID de este certificado son:

- En la jerarquía propia: **1.3.6.1.4.1.54225.10.3.35**

- En ETSI la política QCP-n-qscd: **0.4.0.194112.1.2**
- De acuerdo con los perfiles de certificados del Ministerio de Hacienda y Administraciones Públicas: **2.16.724.1.3.5.9**

Este certificado es un certificado cualificado de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y da cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados, funcionan con dispositivo cualificado de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados son gestionados de forma centralizada, es decir, que la generación y gestión de los datos de creación de firma electrónica es realizada por el prestador, por cuenta del firmante. Estos certificados garantizan la identidad del firmante, su vinculación con el suscriptor del certificado (indicado en el campo “Organization” del “subject” del certificado), indica una relación de representación entre el firmante y el subscriptor y permiten la generación de la “**firma electrónica cualificada**”; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

Este certificado es un certificado de representante de entidad sin personalidad jurídica, con poderes totales para actuar entre otras, ante las Administraciones Públicas españolas.

Este certificado incluye un campo (*Description*) en el Subject donde se indica el documento público que acredita de forma fehaciente las facultades del firmante para actuar en nombre de la entidad a la que representa y, en caso de ser obligatoria, la inscripción de los datos registrales.

- El campo “key usage” tiene activadas, y por tanto permite realizar, las siguientes funciones:
  - Firma digital (para autenticación)
  - Compromiso con el contenido (para firma electrónica)
- En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
  - QcCompliance (0.4.0.1862.1.1), que se emite como cualificado.
  - En el campo “Qualified Certificate Statements” la declaración QcSSCD (0.4.0.1862.1.4) de que se usa exclusivamente en conjunción con un dispositivo cualificado de creación de firmas.
- El campo “User Notice” describe el uso de este certificado.

1.4.2 Límites y prohibiciones de uso de los certificados

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.

Excepto cuando se prevea expresamente en un procedimiento de la Autoridad de Certificación de DIGITELTS, 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), sin perjuicio de lo indicado en el artículo 24.1.c) del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

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 esta DPC, los documentos jurídicos vinculantes de cada certificado, o los contratos con las entidades de registro o con los creadores de sellos y/o los suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a la Autoridad de Certificación de DIGITELTS, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el titular o cualquier tercero.

La Autoridad de Certificación de DIGITELTS no tiene acceso a los datos sobre los que se puede aplicar el uso pretendido de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de la Autoridad de Certificación de DIGITELTS emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor o la persona responsable del uso de los datos de creación de sello, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado. Todo ello sin perjuicio del régimen aplicable a los servicios de la sociedad de la información, cuando sea legalmente procedente.

Asimismo, le será imputable al suscriptor o a la persona responsable del uso de los datos de creación de sello, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en esta DPC, los documentos jurídicos vinculantes con cada certificado, o los contratos o convenios con las entidades de registro o con sus 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.

1.4.3 Emisión de certificados de pruebas

La Autoridad de Certificación de DIGITEL emite certificados de pruebas para su revisión en procesos de inspección o notificación por el Supervisor y en procesos de evaluación en auditorías de conformidad. Estos certificados emitidos bajo la jerarquía en producción incluyen datos ficticios que son:

Certificados de sello electrónico de persona jurídica /ESPJ	
Organization	Empresa de ejemplo
SerialNumber	B47999990
Locality	Valladolid
OU	Operaciones test

Certificados de persona física individual	
Nombre	Pedro
Apellidos	Pruebas Pruebas
SerialNumber	00000000T

Para poder disponer de estos certificados se debe enviar un correo electrónico a la dirección pki@digitelts.es

1.5 Administración de la política

1.5.1 Organización que administra el documento

Autoridad de Certificación de DIGITELTS.

DIGITEL ON TRUSTED SERVICES S.L.U

C/ Enrique Cubero, 9, 47014 Valladolid (España)

+34 91 015 05 10

pki@digitelts.es

1.5.2 Datos de contacto de la organización

- Razón Social: DIGITEL ON TRUSTED SERVICES S.L.U
- Denominación Comercial: Autoridad de Certificación de DIGITELTS TS
- CIF: B47447560
- Domicilio Social: C/ Enrique Cubero, 9, 47014 Valladolid (España).
- Servicio de Atención al Cliente (SAC): 91 015 05 10
- Correo electrónico: comercial@digitelts.com
- Web: https://pki.digitelts.es
- Identificación en el Registro Mercantil de Valladolid: Tomo 891, Folio 38, Hoja VA-11307

1.5.3 Responsables en el procedimiento de gestión del documento

El sistema documental y de organización de la Autoridad de Certificación de DIGITELTS 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 seguridad de la información ostenta la capacidad para proponer, revisar y aprobar este procedimiento de revisión.

1.5.3.1 Revisión del documento

La Autoridad de Certificación de DIGITELTS revisa este documento una vez al año. 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 Seguridad cambios, sugerencias y propuestas de modificaciones de este documento para su aprobación.

El Comité de Seguridad tratará si las modificaciones aprobadas necesitan ser notificadas ante el supervisor español.

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 Seguridad para comentarios y aprobación.
5. Redacción final
6. Publicación en la web
7. En caso de necesidad, notificación al supervisor español.

La Autoridad de Certificación de DIGITELTS realiza una nueva revisión de este documento ante la inclusión de cambios suficientemente relevantes para la gestión de los servicios de certificación. La descripción de los cambios se incluirán en el apartado “control de versiones” de la sección “Información General” en el inicio de este documento.

1.5.4 Aprobación del documento

Las siguientes modificaciones de esta Declaración de Prácticas de Confianza, de la Política de Seguridad y de los Textos de Divulgación (PDS) son aprobadas por el Comité de Seguridad de la Información, el cuál de forma adicional se responsabilizará de su correcta implementación.

La Autoridad de Certificación de DIGITELTS 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

1.6 Definiciones y acrónimos

1.6.1 Definiciones

Concepto	Definición
Autoridad de Certificación	Es la entidad responsable de la emisión y gestión de los certificados digitales.
Autoridad de Registro	Entidad responsable de la gestión de las solicitudes, identificación y registro de los solicitantes de un certificado. Puede formar parte de la Autoridad de Certificación o ser ajena.
Autoridad de sellado de tiempo electrónico	Prestador de servicios de certificación que proporciona la certeza sobre la preexistencia de determinados documentos electrónicos a un momento dado.

Certificado	Archivo que asocia la clave pública con algunos datos identificativos del Sujeto/Firmante y es firmada por la AC.
Clave pública	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos.
Clave privada	Valor matemático conocido únicamente por el titular y usado para la creación de una firma digital o el descifrado de datos. La clave privada de la AC será usada para la firma de certificados y firma de CRL's. La clave privada del servicio TSA será usada para la firma de los sellos de tiempo electrónico.
DPC	Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta.
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.
Datos de Activación	Datos privados, como PIN's o contraseñas empleadas para la activación de la clave privada

REIDAS	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
Firma digital	El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera: a) que los datos no han sido modificados (integridad) b) que la persona que firma los datos es quien dice ser (identificación) c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)
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.
Solicitante	En el contexto de este documento, el solicitante será una persona física representante legal o apoderada con un poder especial para realizar determinados trámites en nombre y representación de una persona jurídica.
Suscriptor	En el contexto de este documento la persona jurídica propietaria del certificado (a nivel corporativo)
Partes que confian	En el contexto de este documento, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado

1.6.2 Acrónimos

Acrónimo	Definición
AC (o también CA)	Certificate Authority

	Autoridad de Certificación
AR (o también RA)	Registration Authority Autoridad de Registro
CPD	Centro de Proceso de Datos
DPC (o también CPS)	Certification Practice Statement. Declaración de Prácticas de Certificación
CRL (o también LRC)	Certificate Revocation List. Lista de certificados revocados
DN	Nombre distintivo dentro del certificado digital Distinguished Name.
DNI	Documento Nacional de Identidad
ETSI EN	European Telecommunications Standards Institute – European Standard.
FIPS	Federal Information Processing Standard Publication

HSM	Hardware Security Module Módulo de seguridad en Hardware
IETF	Internet Engineering Task Force
LSEC	Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
NIF	Número de Identificación Fiscal
NTP	Network Time Protocol Protocolo de tiempo en red.
OCSP	On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
OID	Object Identifier. Identificador de objeto

PDS	PKI Disclosure Statements Texto de Divulgación de PKI.
PIN	Personal Identification Number. Número de identificación personal
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
QSCD (o también DCCF)	Qualified Electronic Signature/Seal Creation Device. Dispositivo cualificado de creación de firma/sellos
QCP	Qualified Certificate Policy Política de certificados cualificados
QCP-l	Certificate policy for European Union (EU) qualified certificates issued to legal persons. Política de certificados cualificados (EU) para personas jurídicas.

	OID: 0.4.0.194112.1.1
QCP-n	Certificate policy for European Union (EU) qualified certificates issued to natural persons. Política de certificados cualificados (EU) para personas físicas OID: 0.4.0.194112.1.0
RFC	Request for Comments Documento RFC
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.
	Time Stamping Authority

TSA	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

2 Publicación de información y depósito de certificados

2.1 Depósito de certificados

La Autoridad de Certificación de DIGITELTS dispone de un Depósito de certificados, en el que se publican las informaciones relativas a los servicios de certificación.

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

2.2 Publicación de información del prestador

La Autoridad de Certificación de DIGITELTS publica las siguientes informaciones, en su Depósito que pueden encontrarse en la siguiente dirección: https://pki.digitelts.es/

- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- La Declaración de Prácticas de Confianza, y la historia de sus versiones.
- Los textos de divulgación (PKI Disclosure Statements – PDS), como mínimo en lengua española, y la historia de sus versiones.

2.2.1 Términos y condiciones

La Autoridad de Certificación de DIGITELTS informa a las partes que confían en los servicios de certificación digital través de los textos de divulgación (PDS) 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 en la PDS queda incluida en la hoja de solicitud del certificado.

2.3 Frecuencia de publicación

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

Los cambios en la Declaración de Prácticas de Confianza se rigen por lo establecido en la sección 1.5 de este documento.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en la sección 4.9 de esta Declaración de Prácticas de Confianza.

2.4 Control de acceso

La Autoridad de Certificación de DIGITELTS 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 del Depósito, para proteger la integridad y autenticidad de la información, especialmente la información de estado de revocación.

La Autoridad de Certificación de DIGITELTS emplea sistemas fiables para el Depósito, de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones en los datos almacenados.
- Pueda comprobarse la autenticidad de la información.
- Los certificados sólo estén disponibles para consulta si la persona física o la persona jurídica ha prestado su consentimiento.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3 Identificación y autenticación

3.1 Registro de nombres

Todos los certificados contienen un nombre diferenciado ITU X.500 en el campo `Subject`, incluyendo un componente `Common Name` (CN=), relativo a la identidad del titular del certificado, del sello electrónico o de la unidad de tiempo electrónico (TSU).

De acuerdo con el apartado 4.2.4 de la ETSI EN 319 412-2 al respecto de los certificados emitidos a personas físicas, se indica que, en caso de incluirse, el tamaño de los campos `givenName`, `surname`, `pseudonym`, `commonName`, `organizationName` y `organizationalUnitName` pueden ser más largos que el límite establecido en la IETF RFC 5280.

De acuerdo con el apartado 4.2.1 de la ETSI EN 319 412-3 al respecto de los certificados emitidos a personas jurídicas, se indica que, en caso de incluirse, el tamaño de los campos organizationName, organizationalUnitName y commonName pueden ser más largos que el límite establecido en la IETF RFC 5280.

3.1.1 Tipos de nombres

3.1.1.1 Certificados de sello de tiempo electrónico

Si la TSU es emitida a nombre de una persona física debe tenerse en cuenta las indicaciones de la ETSI EN 319 412-2, y si es emitida a una persona jurídica debe tenerse en cuenta las indicaciones de la ETSI EN 319 412-3.

- Country (C): especificará el país en el que está establecido el contrato entre el prestador y la persona usuaria de la TSU.
- OrganizationName (O): especificará el nombre oficial de la persona jurídica que gestiona la TSU.
- Common Name (CN): Nombre que identifica de forma única la TSU en la jerarquía de la TSA emisora.

3.1.1.2 Certificados de sello electrónico de persona jurídica o ESPJ

- Country (C): especificará el país en el que está establecido el contrato entre el prestador y la persona jurídica o ESPJ.
- OrganizationName (O): especificará el nombre oficial de la persona jurídica o ESPJ que gestiona el sello electrónico.
- Common Name (CN): Nombre de la plataforma donde reside el sello electrónico.
- organizationIdentifier (OI): NIF de la entidad u Organización a la que está vinculado este sello (en formato ETSI EN 319412-1)
- Serial Number (SN): NIF de la entidad u Organización
- Locality (L): Localidad de la organización

3.1.1.3 Certificados de persona física individual

- `Country` (C): especificará el país en el que está establecido el contrato entre el prestador y la persona física.
- `Common Name` (CN): Nombre y apellidos, y número identificativo de la persona física.
- `Surname`: Apellidos
- `Given Name`: Nombre
- `Title`: Cargo / otros
- `Serial Number`: DNI/NIE (en formato ETSI EN 319412-1)

3.1.1.4 Certificados de persona física vinculada

- `Country` (C): especificará el país en el que está establecido el contrato entre el prestador y la persona física.
- `Common Name` (CN): Nombre y apellidos, y número identificativo de la persona física.
- `Surname`: Apellidos
- `Given Name`: Nombre
- `Title`: Cargo / otros
- `Serial Number`: DNI/NIE (en formato ETSI EN 319412-1)
- `OrganizationName` (O): especificará el nombre oficial de la persona jurídica a la que está vinculado el firmante.
- `Organizational Unit` (OU): Departamento en la Organización a la que se encuentra vinculado el firmante u otra información sobre la Organización
- `Organizationidentifier` (OI): NIF de la persona jurídica a la que está vinculado (en formato ETSI EN 319412-1)

3.1.1.5 Certificados de persona física representante de persona jurídica

- `Country` (C): especificará el país en el que está establecido el contrato entre el prestador y la persona física representante.

- Common Name (CN): Nombre y apellidos, y número identificativo de la persona física, así como el CIF de la persona jurídica representada.
- Surname: Apellidos
- Given Name: Nombre
- Title: Cargo / otros
- Serial Number: DNI/NIE (en formato ETSI EN 319412-1)
- OrganizationName (O): especificará el nombre oficial de la persona jurídica a la que está representanto el firmante.
- Organizational Unit (OU): Departamento en la Organización de la que es representante el firmante u otra información sobre la Organización
- Organizationidentifier (OI): NIF de la persona jurídica a la que está representando (en formato ETSI EN 319412-1)
- Description: Documento público que acredita de forma fehaciente las facultades del firmante para actuar en nombre de la persona jurídica

3.1.1.6 Certificados de persona física representante de entidad sin personalidad jurídica

- Country (C): especificará el país en el que está establecido el contrato entre el prestador y la persona física representante.
- Common Name (CN): Nombre y apellidos, y número identificativo de la persona física, así como el CIF de la ESPJ representada.
- Surname: Apellidos
- Given Name: Nombre
- Title: Cargo / otros
- Serial Number: DNI/NIE (en formato ETSI EN 319412-1)
- OrganizationName (O): especificará el nombre oficial de la ESPJ a la que está representanto el firmante.

- `Organizational Unit` (OU): Departamento en la Organización de la que es representante el firmante u otra información sobre la Organización
- `Organizationidentifier` (OI): NIF de la ESPJ a la que está representando (en formato ETSI EN 319412-1)
- `Description`: Documento público que acredita de forma fehaciente las facultades del firmante para actuar en nombre de la ESPJ.

3.1.2 Significado de los nombres

Los nombres contenidos en los campos `SubjectName` y `SubjectAlternativeName` de los certificados, cuando existan, son comprensibles en lenguaje natural, de acuerdo con lo establecido en la sección anterior.

3.1.3 Empleo de anónimos y seudónimos

En ningún caso se pueden utilizar seudónimos para identificar a una persona jurídica ni a un firmante

En ningún caso se emiten certificados anónimos.

3.1.4 Interpretación de formatos de nombres

Los formatos de nombres se interpretarán de acuerdo con la legislación del país de establecimiento del suscriptor, en sus propios términos.

El campo “país” será el del país en el que se realice el contrato con el subscriptor.

En los certificados de “persona física vinculada” y en los de “persona física representante” muestra la relación entre una persona física y la empresa, entidad u organización con la que está vinculada, con independencia de la nacionalidad de la persona física. Ello deriva de la naturaleza corporativa del certificado, del cual es suscriptor la entidad, empresa u organización, y la persona física vinculada la persona autorizada a su uso.

En los certificados emitidos a suscriptores nacionales españoles y extranjeros residentes en España, el campo “número de serie” debe incluir el NIF del firmante, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

3.1.5 Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos, para cada política de certificado.

No se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente, situación que, en principio no se debe producir, gracias a la presencia del número del NIF, o equivalente, en el esquema de nombres.

Un suscriptor puede pedir más de un certificado siempre que la combinación de los siguientes valores existentes en la solicitud fuera diferente de un certificado válido:

- Número de Identificación Fiscal (NIF) u otro identificador legalmente válido de la persona física identificada en el certificado.
- Número de Identificación Fiscal (NIF) u otro identificador legalmente válido del suscriptor corporativo, cuando exista.
- Tipo de Certificado (Campo descripción del certificado).

3.1.6 Resolución de conflictos relativos a nombres

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

La Autoridad de Certificación de DIGITELTS no estará obligada a determinar previamente que un solicitante de certificados tiene derechos de propiedad industrial, de marca o de dominio sobre el nombre que aparece en una solicitud de certificado, sino que en principio procederá a certificarlo.

Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

Sin embargo, en caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación del país del suscriptor, podrá emprender las acciones pertinentes orientadas a revocar el certificado.

En todo caso, el prestador de servicios de certificación se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

Para cuantas dudas o divergencias puedan surgir en la interpretación y/o cumplimiento de este contrato, las Partes, con renuncia expresa a cualquier otro fuero que pudiera corresponderles, pactan sumisión a los Juzgados y Tribunales de Valladolid capital.

3.1.7 Autenticación de la identidad de una persona física

Esta sección describe los métodos de comprobación de la identidad de una persona física identificada en un certificado.

La identidad de las personas físicas identificadas en los certificados cuyo suscriptor sea esta misma persona física, se valida mediante la presentación de su documento oficial de identificación (Documento Nacional de Identidad, tarjeta de identidad, pasaporte u otro medio idóneo reconocido en derecho para su identificación) presencialmente.

La información de identificación de las personas físicas identificadas en los certificados cuyo subscriptor sea una persona jurídica se valida presencialmente y comparando la información de la solicitud con los registros de la entidad, empresa u organización de derecho público o privado a la que está vinculado, asegurando la corrección de la información a certificar.

3.1.7.1 Necesidad de presencia personal

En la solicitud de certificados de persona física individual, se valida esta identidad, personándose la persona física y exhibiendo su documento oficial de identidad o similar ante un operador de una Autoridad de Registro autorizada o de la Autoridad de Certificación de DIGITELTS.

Para la solicitud de los certificados de persona física vinculada no se requiere la presencia física directa debido a la relación ya acreditada entre la persona física y entidad, empresa u organización de derecho público o privado a la que está vinculada.

Sin embargo, antes de la entrega de un certificado, la entidad, empresa u organización de derecho público o privado suscriptora, por medio de su responsable de certificación, de tenerlo, u otro miembro designado, deberá contrastar la identidad de la persona física identificada en el certificado mediante su presencia física, a excepción de que resulte de aplicación lo indicado en el artículo 7.6 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Además, la Autoridad de Registro verificará mediante la exhibición de documentos o a través de sus propias fuentes de información, el resto de los datos y atributos a incluir en el certificado, guardando documentación acreditativa de la validez de estos.

3.1.7.2 Vinculación de la persona física

La justificación documental de la vinculación de una persona física identificada en un certificado con la entidad, empresa u organización de derecho público o privado viene dada por su constancia en los registros internos, administrativos o públicos (contrato de trabajo como empleado, o el contrato mercantil que lo vincula, o el acta donde se indique su cargo, o la solicitud como miembro de la organización…) de cada una de las personas públicas y privadas a las que están vinculadas.

3.1.8 Autenticación de las Autoridades de Registro

La Autoridad de Certificación de DIGITELTS realiza las verificaciones necesarias para confirmar la existencia de la organización que desea convertirse en Autoridad de Registro. La Autoridad de Certificación de DIGITELTS obtiene la documentación de la organización que se presenta, además de utilizar sus propias fuentes de información.

La Autoridad de Certificación de DIGITELTS, en los casos en que la función de registro se delega en un suscriptor, verifica y valida la identidad de los operadores de la Autoridad de Registro con la información que le remite el subscriptor, en la que incluye su autorización para actuar como tal.

La Autoridad de Certificación de DIGITELTS se asegura que los operadores de la Autoridad de Registro reciban la formación suficiente para el desempeño de sus funciones, que verificará en las evaluaciones correspondientes.

Los operadores y responsables de certificación se autentican con certificados digitales o bien con login y password, más un OTP y siempre que ese usuario esté incluido en el LDAP corporativo, para la prestación de sus servicios ante la Autoridad de Registro.

3.2 Validación inicial de la identidad

La identidad de los suscriptores de certificados resulta fijada en el momento de la firma del contrato entre la Autoridad de Certificación de DIGITELTS y dichos suscriptores, momento en el cual se verifica al suscriptor mediante su documento identificativo como el NIF y los poderes de actuación de la persona representante (representante legal o apoderado), y resto de documentación necesaria. Para esta verificación, se podrá emplear documentación pública o notarial, y/o la consulta directa a los registros públicos correspondientes.

En el caso de las **personas físicas individuales**, sus identidades se validan mediante la identificación por un operador autorizado por la Entidad de Registro y la Autoridad de Certificación de DIGITELTS. En relación con dichos datos, la Autoridad de Certificación de DIGITELTS adquiere la condición de responsable del tratamiento de conformidad con lo

indicado en 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

En el caso de las **personas físicas vinculadas** a un suscriptor corporativo, sus identidades se validarán mediante los registros corporativos de la entidad, empresa u organización de derecho público o privado, suscriptoras de los certificados. El suscriptor producirá una certificación de los datos necesarios, y la remitirá a la Autoridad de Certificación de DIGITELTS, por los medios que ésta habilite, para el registro de la identidad de los firmantes.

3.2.1 Prueba de posesión de clave privada

La posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del certificado por el suscriptor, en certificados de sello electrónico o por el firmante en certificados de firma.

3.2.2 Autenticación de la identidad de una organización, empresa o entidad mediante representante

3.2.2.1 Identidad

Las personas físicas con capacidad de actuar en nombre de las personas jurídicas pública o privadas suscriptoras, podrán actuar como representantes de las mismas, siempre y cuando exista una situación previa de representación legal o voluntaria entre la persona física y la persona jurídica, que exige su reconocimiento por la Autoridad de Certificación de DIGITELTS, la cual se realizará mediante el siguiente procedimiento presencial:

- El representante del suscriptor se reunirá presencialmente con un representante autorizado de la Autoridad de Certificación de DIGITELTS, el cual pondrá a su disposición un formulario de autenticación. Alternativamente, el representante del suscriptor podrá

obtener el formulario de la página web de la Autoridad de Certificación de DIGITELTS para su cumplimentación previa.

- El representante cumplimentará el formulario, con las siguientes informaciones y a la que acompañará los siguientes documentos:

  Sus datos de identificación como representante:

  - Nombre y apellidos.
  - Lugar y fecha de nacimiento.
  - Documento: DNI o NIF del representante.

  Los datos de identificación del suscriptor al que representa:
  - Denominación o razón social.
  - Toda información de registro existente, incluyendo los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante.
  - Documento: NIF de la persona jurídica.
  - Documento: Documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

  Los datos relativos a la representación o la capacidad de actuación que ostenta:
  - La vigencia de la representación o la capacidad de actuación (fecha de inicio y fin).
  - La indicación de Representación o capacidad total. Esta comprobación se podrá realizar mediante consulta telemática al registro público donde conste inscrita la representación.

- Cumplimentado y firmado el formulario, se firmará y entregará a la Autoridad de Certificación de DIGITELTS junto con la documentación justificativa indicada.
- El personal de la Autoridad de Certificación de DIGITELTS comprobará la identidad del representante mediante la presentación del DNI o NIF, el contenido de la representación con la documentación.
- Alternativamente, de acuerdo con lo establecido en el artículo 24.1.d) del Reglamento (UE) 910/2014, y en el artículo 7.1 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, se podrá legitimar notarialmente la firma del formulario, y hacerse llegar a la Autoridad de Certificación de

DIGITELTS por correo postal certificado, en cuyo caso los pasos anteriores no serán precisos.

3.2.3 Autenticación de la identidad de una persona física

Esta sección describe los métodos de comprobación de la identidad de una persona física identificada en un certificado.

La información de identificación de las personas físicas identificadas en los certificados cuyo suscriptor sea una persona jurídica se valida presencialmente y comparando la información de la solicitud con los registros de la entidad, empresa u organización de derecho público o privado a la que está vinculado, asegurando la corrección de la información a certificar.

La identidad de las personas físicas identificadas en los certificados cuyo suscriptor sea esta misma persona física, se valida mediante la presentación de su documento oficial de identificación (Documento Nacional de Identidad, tarjeta de identidad, pasaporte u otro medio idóneo reconocido en derecho para su identificación) presencialmente.

3.2.3.1 Necesidad de presencia personal

En la solicitud de certificados de persona física cuyo suscriptor sea esta misma persona física, se valida esta identidad, personándose la persona física y exhibiendo su documento oficial de identidad o similar ante un operador de una Autoridad de Registro autorizada por la Autoridad de Certificación de DIGITELTS. Para la solicitud de los certificados de persona física vinculada no se requiere la presencia física directa debido a la relación ya acreditada entre la persona física y entidad, empresa u organización de derecho público o privado a la que está vinculada.

Sin embargo, antes de la entrega de un certificado, la entidad, empresa u organización de derecho público o privado suscriptora, por medio de su responsable de certificación, de tenerlo, u otro miembro designado, deberá contrastar la identidad de la persona física identificada en el certificado mediante su presencia física, a excepción de que resulte de

aplicación lo indicado en el artículo 7.6 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Además, la Autoridad de Registro verificará mediante la exhibición de documentos o a través de sus propias fuentes de información, el resto de los datos y atributos a incluir en el certificado, guardando documentación acreditativa de la validez de estos.

La presencia personal en la solicitud de certificados no será necesaria si la firma de la hoja de solicitud o de aceptación del certificado ha sido legitimada ante notario.

3.2.3.2 Vinculación de la persona física

La justificación documental de la vinculación de una persona física identificada en un certificado con la entidad, empresa u organización de derecho público o privado viene dada por su constancia en los registros internos, administrativos o públicos (contrato de trabajo como empleado, o el contrato mercantil que lo vincula, o el acta donde se indique su cargo, o la solicitud como miembro de la organización…) de cada una de las personas públicas y privadas a las que están vinculadas.

3.2.4 Información de suscriptor no verificada

La Autoridad de Certificación de DIGITELTS no incluye ninguna información de suscriptor no verificada en los certificados.

3.2.5 Validación de la autoridad

3.2.5.1 Identificación de la vinculación

Es preciso que exista y se incluya en la solicitud una autorización para dicha expedición del certificado creada por un representante legal de la persona jurídica o entidad sin personalidad jurídica o con poder de representación suficiente del creador de sellos.

La Autoridad de Certificación de DIGITELTS consultará al Registro Mercantil para comprobar que la entidad solicitante está constituida, que dispone de personalidad jurídica, sus datos actuales, así como el nombramiento y vigencia de la persona física autorizada.

Esta validación podrá realizarse por medios electrónicos. En caso que el solicitante aporte documentación en papel se podrá escanear por el operador y firmarla con un sello electrónico.

3.2.6 Criterios de interoperación

La Autoridad de Certificación de DIGITELTS se reserva el derecho de proporcionar servicios de interoperación con otras Autoridades de Certificación. Dichos servicios se establecerán por contrato.

3.3 Identificación y autenticación de solicitudes de renovación

La Autoridad de Certificación de DIGITELTS no realiza renovaciones de certificados.

Antes de la caducidad del certificado se avisa al suscriptor para la emisión de un nuevo certificado, usando para ello las indicaciones del apartado 3.2 de esta DPC.

3.4 Identificación y autenticación de solicitudes de revocación

La Autoridad de Certificación de DIGITELTS o una Autoridad de Registro autentica las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada.

Los métodos aceptables para dicha comprobación son los siguientes:

- El envío de una solicitud de revocación por parte del suscriptor en los certificados corporativos o de la persona física identificada en el certificado, firmada electrónicamente con el certificado a revocar.

- El uso de información que sólo conoce el suscriptor del certificado corporativo o de la persona física identificada en el certificado, y que le permite revocar de forma automática su certificado.
- Ser persona física representante legal del subscriptor del certificado y presentarse ante una Autoridad de Registro o ante la Autoridad de Certificación de DIGITELTS.
- Otros medios de comunicación, como el envío de la solicitud de revocación firmada manuscritamente junto a una fotocopia de su documento oficial de identificación, por medio de envío postal. La Autoridad de Certificación de DIGITELTS realiza las comprobaciones pertinentes para asegurarse de la veracidad de la solicitud.

En los supuestos que se han detallado anteriormente, la Autoridad de Certificación de DIGITEL TS recibirá la petición de revocación y, una vez validada, procederá a la revocación del certificado que viene identificado en dicha petición.

4 Requisitos de operación del ciclo de vida de los certificados

4.1 Solicitud del certificado

4.1.1 Legitimación para solicitar la emisión

El suscriptor del certificado, tanto si es una persona física como jurídica, debe firmar un contrato de prestación de servicios de confianza con la Autoridad de Certificación de DIGITELTS.

Igualmente, con anterioridad a la emisión y entrega de un certificado, existe una previa solicitud de certificados formalizada en documento específico u hoja de solicitud de certificados en formato electrónico.

En el caso de existir una relación previa entre el suscriptor y la Autoridad de Certificación de DIGITELTS, el solicitante dispone de título para realizar la solicitud, que se instrumenta jurídicamente mediante una hoja de solicitud de certificados firmada ya sea en nombre

propio en relación con los certificados en los que el suscriptor sea una persona física, o bien en nombre de la entidad, empresa u organización de derecho público o privado.

4.1.2 Procedimiento de alta y responsabilidades

La Autoridad de Certificación de DIGITELTS puede recibir solicitudes de certificados en nombre de personas físicas o jurídicas.

Las solicitudes se instrumentan mediante un documento cumplimentado por el solicitante en su propio nombre, o en nombre de la persona física o jurídica, documento el cual incluirá los datos de las personas a las que se expedirán los certificados. Estas solicitudes pueden ser tramitadas mediante plataforma electrónica. La solicitud, además, podrá ser realizada por un operador autorizado por el suscriptor (o responsable de certificación), que haya sido designado por el suscriptor en el contrato entre dicho suscriptor y la Autoridad de Certificación de DIGITELTS.

La solicitud deberá acompañarse de toda la documentación justificativa de la identidad y resto de datos necesarios de la persona física identificada en el certificado, de acuerdo con lo establecido en la sección 3.2.3. También se deberán acompañar otros datos, como una dirección de correo electrónico o email que permitan contactar con el responsable de la persona jurídica subscriptora o con la persona física identificada en el certificado.

4.2 Procesamiento de la solicitud de certificados

4.2.1 Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de certificado, la Autoridad de Certificación de DIGITELTS se asegura que las solicitudes sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

En caso afirmativo, la Autoridad de Certificación de DIGITELTS verifica la información proporcionada.

En relación con los certificados cualificados, 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 extinción del certificado o la finalización del servicio prestado, incluso en caso de pérdida anticipada de vigencia por revocación. Esta documentación podrá ser conservada de forma segura por medio de plataforma electrónica.

4.2.2 Aprobación o rechazo de la solicitud

Cuando se verifique la corrección de los datos correspondientes a la solicitud, la Autoridad de Certificación de DIGITELTS aprobará la solicitud del certificado y procederá a su emisión y entrega.

Si de la verificación resulta la certeza que la información no es correcta, o se sospecha incorrecta, o la misma puede afectar a la reputación de la Autoridad de Certificación o de los suscriptores, la Autoridad de Certificación de DIGITELTS denegará la petición, o suspenderá su aprobación hasta que realice las comprobaciones complementarias que considere oportunas. Si dichas comprobaciones no permiten la certeza de la corrección de la información a verificar, la Autoridad de Certificación de DIGITELTS podrá denegará la solicitud definitivamente.

La Autoridad de Certificación de DIGITELTS notifica al solicitante la aprobación o denegación de la solicitud.

La Autoridad de Certificación de DIGITELTS podrá automatizar los procedimientos de verificación de la corrección de la información que será contenida en los certificados, y de aprobación de las solicitudes, por medio de una plataforma electrónica.

4.2.3 Plazo para resolver la solicitud

La Autoridad de Certificación de DIGITELTS atiende las solicitudes de certificados por orden de llegada, en un plazo razonable, pudiendo especificarse una garantía de plazo máximo en el contrato de emisión de certificados. Las solicitudes se mantienen activas hasta su aprobación o rechazo.

4.3 Emisión

4.3.1 Acciones durante el proceso de emisión

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone a disposición del titular para su aceptación.

Los procedimientos establecidos en esta sección también se aplican en caso de *renovación de certificados*, dado que la misma implica la emisión de un nuevo certificado.

Durante el proceso, la Autoridad de Certificación de DIGITELTS:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Se asegura que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
- Incluye en el certificado las informaciones establecidas en el Reglamento (UE) 910/2014, de acuerdo con lo establecido en las secciones 1 y 7.
- Indica la fecha y la hora en que se expidió un certificado.

4.3.2 Notificación de la emisión al suscriptor

La Autoridad de Certificación de DIGITELTS notifica la emisión del certificado:

- a la persona jurídica subscriptora (creador de sellos) identificada en el certificado de sello electrónico

- A la persona física subscriptora identificada en el certificado de firma electrónica para personas físicas individuales.
- A la persona jurídica subscriptora y a la persona física (firmante) identificadas ambas en el certificado de firma electrónica para personas físicas vinculadas o representantes.

4.4 Aceptación

4.4.1 Procedimiento de la aceptación

Durante este proceso, se deben realizar las siguientes actuaciones:

- Cuando no se ha realizado con anterioridad, acreditar definitivamente la identidad de la persona física identificada en el certificado, con la colaboración del subscriptor (empresa, entidad u organización) y/o Autoridad de Registro, de acuerdo con lo establecido en las secciones 2.2 y 3.2.3.
- Entregar a la persona física identificada en el certificado con la colaboración del Operador autorizado de la Autoridad de Registro, en el caso del subscriptor:
  - Las condiciones generales de prestación de servicios de certificación electrónica que incluye aviso legal sobre protección de datos, incluidas en el texto de divulgación o PDS.
  - Las indicaciones exactas para la aceptación del certificado.
  - Información básica acerca del uso del certificado, incluyendo especialmente información acerca del prestador de servicios de certificación y de la Declaración de Prácticas de Confianza aplicable, como sus obligaciones, facultades y responsabilidades.
  - Información acerca del certificado.
  - Reconocimiento, por parte del firmante, apoderado suficiente o persona autorizada, de disponer acceso al certificado.
  - Régimen de obligaciones del uso del certificado.
  - Responsabilidad del titular.

- Método de imputación exclusiva al titular, de su clave privada y de sus datos de activación del certificado.
- La fecha del acto de aceptación.

- Obtener la aceptación del certificado, por medio de firma, escrita o electrónica, de la persona responsable del certificado. En la opción de la firma electrónica de la aceptación, ésta se puede realizar por medio de los servicios de plataforma electrónica o con una firma manuscrita o manuscrita capturada electrónicamente.

El suscriptor o Autoridad de Registro, en su caso, colabora en estos procesos, debiendo registrar documentalmente los anteriores actos y conserva los citados documentos originales (hojas de aceptación), remitiendo copia electrónica a la Autoridad de Certificación de DIGITELTS, así como los originales cuando se precise de acceso a los mismos.

Cuando esta documentación se guarde electrónicamente, o no se realice interviniendo el suscriptor y/o Autoridad de Registro, se podrá utilizar los servicios correspondientes de una plataforma electrónica.

4.4.1.1 Conducta que constituye aceptación del certificado

La aceptación del certificado por la persona física identificada en el certificado se produce con cualquiera de las dos opciones:

- Mediante la firma electrónica de una hoja de aceptación.
- Mediante el cambio del PIN del certificado.

4.4.2 Publicación del certificado

Se publica el certificado en el Depósito a que se refiere la sección 2, con los controles de seguridad pertinentes y siempre que se disponga de la autorización de la persona identificada en el certificado.

4.4.3 Notificación de la emisión a terceros

No se produce notificación de emisión a terceras entidades.

4.5 Uso del par de claves y del certificado

4.5.1 Uso por el firmante

Se obliga al firmante a:

- Facilitar a la Autoridad de Certificación de DIGITELTS información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Confianza, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 4.
- Cuando el certificado funcione juntamente con un QSCD, reconocer su capacidad de producción de firmas electrónicas cualificadas; esto es, equivalentes a firmas manuscritas, así como otros tipos de firmas electrónicas y mecanismos de cifrado de información.
- Ser especialmente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 2.2 y 6.4.
- Comunicar a la Autoridad de Certificación de DIGITELTS y a cualquier persona que se crea que pueda confiar en el certificado, sin retrasos injustificables:
  - La pérdida, el robo o el compromiso potencial de su clave privada.
  - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
  - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2.
- Dejar de emplear la clave privada en caso de compromiso de dicha clave, de revocación o de compromiso de las claves de la CA.

4.5.2 Uso por el suscriptor

4.5.2.1 Obligaciones

Se obliga contractualmente al suscriptor a:

- Facilitar a la Autoridad de Certificación información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Confianza, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 4.
- Comunicar a la Autoridad de Certificación de DIGITELTS y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
  - La pérdida, el robo o el compromiso potencial de su clave privada.
  - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
  - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- Trasladar a a las personas físicas identificadas en el certificado y titulares del certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de estas.
- No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de los servicios de la Autoridad de Certificación de DIGITELTS, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de la Autoridad de Certificación de DIGITELTS, sin permiso previo por escrito.

4.5.2.2 Responsabilidad civil del firmante

La Autoridad de Certificación de DIGITELTS obliga al firmante a responsabilizarse de:

- Que todas las informaciones suministradas por el firmante contenidas en el certificado son correctas.

- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Confianza.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de protección del control exclusivo de acceso a la clave privada.
- Que el firmante es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación deCertificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

4.5.2.3 Responsabilidades del suscriptor del certificado

Se obliga contractualmente al suscriptor a responsabilizarse de:

- Que todas las manifestaciones realizadas en la solicitud son correctas.
- Que todas las informaciones suministradas por el suscriptor contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Confianza.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de protección del control exclusivo de acceso a la clave privada.

Que el suscriptor es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

4.5.3 Uso por el tercero que confía en certificados

4.5.3.1 Obligaciones del tercero

Se obliga al tercero que confía en certificados a:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía.
- Reconocer, que para considerarse certificado cualificado debe estar incluido en la Lista de Confianza nacional (Trusted List).
- Reconocer, que si las firmas electrónicas verificadas, son producidas en un dispositivo cualificado de creación de firma (QSCD) tendrán la consideración legal de firmas electrónicas cualificadas; esto es, equivalentes a firmas manuscritas, así como que el certificado permite la creación de otros tipos de firmas electrónicas.
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de los servicios de la Autoridad de Certificación de DIGITELTS, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de la Autoridad de Certificación de DIGITELTS, sin permiso previo por escrito.

4.5.3.2 Responsabilidad civil del tercero

Se obliga contractualmente al tercero a manifestar:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

4.6 Renovación de certificados sin cambio de claves

La Autoridad de Certificación de DIGITELTS no renueva certificados.

4.7 Renovación de certificados con cambio de claves

La Autoridad de Certificación de DIGITELTS no renueva certificados.

4.8 Modificación de certificados

La modificación de certificados, excepto la modificación de la clave pública certificada será tratada como una nueva emisión de certificado.

4.9 Revocación de certificados

4.9.1 Causas de revocación de certificados

La Autoridad de Certificación de DIGITELTS revoca un certificado cuando concurre alguna de las siguientes causas:

- Circunstancias que afectan a la información contenida en el certificado:
  - Modificación de alguno de los datos contenidos en el certificado, después de la correspondiente emisión del certificado que incluye las modificaciones.
  - Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
  - Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.
- Circunstancias que afectan a la seguridad de la clave o del certificado:

- Compromiso de la clave privada, de la infraestructura o de los sistemas del prestador de servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
- Infracción, por la Autoridad de Certificación de DIGITELTS, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas de Confianza.
- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.
- Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.
- El uso irregular del certificado o la falta de diligencia en la custodia de la clave privada.

- Circunstancias que afectan al suscriptor o a la persona física identificada en el certificado:
  - Finalización de la relación jurídica de prestación de servicios entre la Autoridad de Certificación de DIGITELTS y el suscriptor.
  - Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado a la persona física o jurídica identificada en el certificado.
  - Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de este.
  - Infracción por el suscriptor o por la persona física identificada en el certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente.
  - La incapacidad sobrevenida o el fallecimiento de la persona física identificada en el certificado.
  - La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor al firmante o la finalización de la relación entre suscriptor y persona identificada en el certificado.
  - Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 4.
- Circunstancias asociadas al dispositivo de creación de firma cualificado:
  - Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.

- Pérdida o inutilización por daños del dispositivo criptográfico.
- Acceso no autorizado, por un tercero, a los datos de activación del suscriptor.

- Otras circunstancias:
  - La terminación del servicio de certificación de la Autoridad de Certificación de DIGITELTS, de acuerdo con lo establecido en la sección 9.
  - El uso dañino y continuado del certificado para la Autoridad de Certificación de DIGITELTS. En este caso, se considera que un uso es dañino en función de los siguientes criterios:
    - La naturaleza y el número de quejas recibidas.
    - La identidad de las entidades que presentan las quejas.
    - La legislación relevante vigente en cada momento.
    - La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.

4.9.2 Legitimación para solicitar la revocación

Pueden solicitar la revocación de un certificado:

- La persona física identificada en el certificado.
- El suscriptor del certificado.
- La Autoridad de Certificación de DIGITELTS.

4.9.3 Procedimientos de solicitud de revocación

La entidad que precise revocar un certificado debe solicitarlo a la Autoridad de Certificación de DIGITELTS.

La solicitud de revocación puede ser firmada electrónicamente y enviada por email (contacto indicado en el apartado 1.5.1), o acudiendo físicamente a una Autoridad de Registro, a la Autoridad de Certificación de DIGITELTS o al subscriptor corporativo.

La solicitud de revocación comprenderá la siguiente información:

- Fecha de solicitud de la revocación.
- Identidad del suscriptor o persona física identificada en el certificado.
- Razón detallada para la petición de revocación.
- Nombre de la persona física identificada en el certificado o el responsable legal o autorizado que pide la revocación.
- Información de contacto de la persona física o responsable legal o autorizado que pide la revocación.

La solicitud debe ser autenticada, por la Autoridad de Certificación de DIGITELTS, de acuerdo con los requisitos establecidos en la sección 3.4 de esta política, antes de proceder a la revocación.

La Autoridad de Certificación de DIGITELTS podrá incluir cualquier otro requisito para la confirmación de las solicitudes de revocación.

El procedimiento de revocación se puede encontrar en el documento "***DIGITELTS-proc-revoca***".

En caso de que el destinatario de una solicitud de revocación por parte de una persona física identificada en el certificado fuera la entidad suscriptora, una vez autenticada la solicitud debe remitir una solicitud en este sentido a la Autoridad de Certificación de DIGITELTS.

La solicitud de revocación será procesada a su recepción, y se informará al suscriptor en certificados corporativos y a la persona física identificada en el certificado en certificados corporativos o individuales, acerca del cambio de estado del certificado revocado.

La Autoridad de Certificación de DIGITELTS no reactiva el certificado una vez ha sido revocado.

Tanto el servicio de gestión de las revocaciones como el servicio de consulta son considerados servicios críticos y así constan en el ***plan de continuidad de negocio*** de la Autoridad de Certificación de DIGITELTS.

4.9.4 Plazo temporal de solicitud de revocación

Las solicitudes de revocación se remitirán de forma inmediata en cuanto se tenga conocimiento de la causa de revocación, en horario de 24x7 y no será superior a las 24 horas.

4.9.5 Plazo temporal de procesamiento de la solicitud

La revocación se producirá inmediatamente cuando sea recibida, en horario de 24x7. Si la revocación no puede confirmarse en un plazo de 24 horas, se registrarán las medidas adoptadas y su justificación. junto con la justificación.

4.9.6 Obligación de consulta de información de revocación de certificados

Los terceros deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se verifica el estado de los certificados es consultando el servicio OCSP de la Autoridad de Certificación de DIGITELTS en la web siguiente:

http://ocsp.digitelts.es

El servicio OCSP incluye los certificados expirados en sus respuestas.

La Autoridad de Certificación de DIGITELTS valida el estado de todos los certificados antes de la realización de una firma desde sus plataformas de creación de firma.

4.9.7 Frecuencia de emisión de listas de revocación de certificados

Se emite una CRL al menos cada 24 horas.

La CRL indica el momento programado de emisión de una nueva CRL, si bien se puede emitir una antes del plazo indicado en la CRL anterior, para reflejar revocaciones.

La CRL mantiene obligatoriamente el certificado revocado hasta que expira. Las CRL no incluyen los certificados expirados en sus respuestas.

4.9.8 Plazo máximo de publicación de listas de revocación

Las CRL se publican en un periodo inmediato razonable tras su generación, que en ningún caso no supera unos pocos minutos.

4.9.9 Disponibilidad de servicios de comprobación en línea

De forma alternativa, los terceros que confían en certificados podrán consultar el Depósito de certificados de la Autoridad de Certificación de DIGITELTS, que se encuentra disponible las 24 horas de los 7 días de la semana como se describe en el apartado 4.10.

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de la Autoridad de Certificación de DIGITELTS, ésta deberá realizar sus mejores esfuerzos por asegurar que este servicio se mantenga inactivo el mínimo tiempo posible, que no podrá superar un día.

La Autoridad de Certificación de DIGITELTS suministra información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

Los servicios de comprobación de estado de los certificados son de uso gratuito.

La Autoridad de Certificación de DIGITELTS mantiene disponible la información del estado de revocación pasado el período de validez del certificado, por medio del servicio OCSP. Esta disponibilidad se mantiene en caso de finalización de los servicios PKI por parte de la Autoridad de Certificación de DIGITELTS, transfiriendo esta obligación a otro prestador.

En el supuesto que la CA emita la última CRL, el campo “nextUpdate” debera ser configurado a “99991231235959Z”, como se define en IETF RFC 5280.

4.9.10 Obligación de consulta de servicios de comprobación de estado de certificados

Resulta obligatorio consultar el estado de los certificados antes de confiar en los mismos.

4.9.11 Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de la Autoridad de Certificación de DIGITELTS es notificado a todos los participantes en los servicios de certificación, en la medida de lo posible, mediante la publicación de este hecho en la página web de la Autoridad de Certificación de DIGITELTS, así como, si se considera necesario, en otros medios de comunicación, incluso en papel. En caso de compromiso de la clave privada, la Autoridad de Certificación de DIGITELTS ejecuta las acciones previstas en el plan de cese del servicio, conforme al escenario de cese no programado.

En caso de compromiso, se procederá a la revocación inmediata de todos los certificados de entidad final, se emitirá una última CRL sin fecha de renovación, que será publicada, y el servicio OCSP, que permanecerá activo, devolverá para todos los certificados que los mismos han sido revocados por compromiso de clave. Esta información de estado se mantendrá accesible durante el plazo de quince años desde la revocación o la expiración de los certificados, según proceda.

4.9.12 Causas de suspensión de certificados

La Autoridad de Certificación de DIGITELTS no realiza suspensión de certificados.

4.9.13 Solicitud de suspensión

La Autoridad de Certificación de DIGITELTS no realiza suspensión de certificados.

4.9.14 Procedimientos para la petición de suspensión

La Autoridad de Certificación de DIGITELTS no realiza suspensión de certificados.

4.9.15 Período máximo de suspensión

La Autoridad de Certificación de DIGITELTS no realiza suspensión de certificados.

4.10 Servicios de comprobación de estado de certificados

4.10.1 Características operativas de los servicios

Los servicios de comprobación de estado de certificados se prestan mediante una interfaz de consulta web, en https://pki.digitelts.es

Cuando se produce una revocación, el sistema de la Autoridad de Certificación de DIGITELTS incluye este hecho en el servicio de validación de certificados por medio del protocolo OCSP, y se generan las correspondientes nuevas CRL.

Si hubiere algún error en la información que se proporcione por estos medios se produce una alarma para subsanarlo.

La información para la verificación del estado de revocación de los certificados electrónicos expedidos por la Autoridad de Certificación de DIGITELTS puede ser consultada mediante el Servicio de Validación mediante el protocolo OCSP y la correspondiente CRL.

Para comprobar la última CRL emitida se deben consultar las siguientes listas:

- La CRL de la CA-ROOT (“*Digitel TS CA ROOT 01*”)
  - http://crl1.pki.digitelts.es/DTSROOTCA01.crl
  - http://crl2.pki.digitelts.es/DTSROOTCA01.crl
- La CRL de la TSA (CA intermedia “*Digitel TS Qualfied CA TSA G1*”)
  - http://crl1.pki.digitelts.es/DTSQualifiedCATSAG1.crl
  - http://crl2.pki.digitelts.es/DTSQualifiedCATSAG1.crl
- La CRL de la SUBCA (CA intermedia “*Digitel TS Qualfied CA G1*”)
  - http://crl1.pki.digitelts.es/DTSQualifiedCAG1.crl
  - http://crl2.pki.digitelts.es/DTSQualifiedCAG1.crl

Los servicios de validación mediante el protocolo OCSP son:

- http://ocsp.digitelts.es

4.10.2 Disponibilidad de los servicios

Los servicios de comprobación de estado de certificados se encuentran disponibles las 24 horasdel día, los 7 días de la semana, durante todo el año, con excepción de las paradas programadas.

4.10.3 Características opcionales

Sin estipulación.

4.11 Finalización de la suscripción

La Autoridad de Certificación de DIGITELTS comercializa certificados a personas individuales o en modalidad de contrato de servicio corporativo.

En el primer caso, el servicio finaliza automáticamente una vez transcurrido el periodo de vigencia del certificado. Como excepción, el suscriptor puede mantener el servicio vigente, solicitando la renovación del certificado, con la antelación que determina esta Declaración de Prácticas de Confianza.

En la modalidad de expedición de certificados corporativos, la suscripción dura tanto tiempo como el contrato de servicio, que al menos cubre la duración de todos los certificados corporativos expedidos en ejecución del mismo.

4.12 Depósito y recuperación de claves

4.12.1 Política y prácticas de depósito y recuperación de claves

No se presta el servicio de depósito y recuperación de claves.

4.12.2 Política y prácticas de encapsulado y recuperación de claves de sesión

Sin estipulación.

5 Controles de seguridad física, de gestión y de operaciones

5.1 Controles de seguridad física

La Autoridad de Certificación de DIGITELTS ha establecido controles de seguridad física y ambiental para 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 y la gestión del hardware criptográfico.

En concreto, la política de seguridad física y ambiental aplicable a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación 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 de certificación.

Estas medidas resultan aplicables a las instalaciones donde se producen los certificados bajo la plena responsabilidad de la Autoridad de Certificación de DIGITELTS, que la presta desde

sus instalaciones de alta seguridad, tanto principales como, en su caso, de operación en contingencia, que son debidamente auditadas de forma periódica.

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.

5.1.1 Localización y construcción de las instalaciones

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 criptográficas 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 Certificación de DIGITELTS dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de estos.

5.1.2 Acceso físico

La Autoridad de Certificación de DIGITELTS 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 de generación de certificados, debiendo accederse desde los niveles inferiores a los niveles superiores.

El acceso físico a las dependencias de la Autoridad de Certificación de DIGITELTS donde se llevan a cabo procesos de certificación 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 Autoridad de Certificación de DIGITELTS 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.

5.1.3 Electricidad y aire acondicionado

Las instalaciones de la Autoridad de Certificación de DIGITELTS 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.

5.1.4 Exposición al agua

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.

5.1.5 Prevención y protección de incendios

Las instalaciones y activos de la Autoridad de Certificación de DIGITELTS cuentan con sistemas automáticos de detección y extinción de incendios.

5.1.6 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.

5.1.7 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.

5.1.8 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.

5.2 Controles de procedimientos

La Autoridad de Certificación de DIGITELTS 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 Autoridad de Certificación de DIGITELTS ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

5.2.1 Funciones fiables

- **Auditor Interno (*System Auditors*[1] en ETSI 310 401):** responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de Sistemas de Información. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.
- **Administrador de Sistemas de certificación (*System administrator*[2] en ETSI 319 401):** responsable del funcionamiento correcto del hardware y software de soporte en la plataforma de certificación
- **Operador del sistema (*System Operator*[3] en ETSI 319 401):** responsables de las operaciones diarias de los sistemas confiables del PSC. Autorizados a realizar copias de seguridad del sistema.

[1] REQ-7.2-15
[2] REQ-7.2-15
[3] REQ-7.2-15

- **Responsable de Seguridad (*Security Officer*[4] en ETSI 319 401):** encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de DIGITEL. Se encarga de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.
- **Operador de Registro (*Registration Officer*[5] en ETSI 319 411-1)**: persona encargada de la verificación y aprobación de las peticiones de certificados.
- **Operador de Revocación (*Revocation Officer*[6] en ETSI 319 411-1)**: Responsable de comprobar y aplicar los cambios en el estado de un certificado.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Estas personas realizarán sus funciones basándose en el principio de menor privilegio.

5.2.2 Numero de personas por tarea

La Autoridad de Certificación de DIGITELTS garantiza al menos dos personas para realizar las tareas que se detallan en el apartado 5.2.4, especialmente en la gestión del dispositivo de custodia de las claves de la Autoridad de Certificación raíz e intermedias.

5.2.3 Identificación y autenticación para cada función

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

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

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

[4] REQ-7.2-15
[5] OVR-6.4.4-02 (with responsibilities as defined in CEN TS 419 261)
[6] OVR-6.4.4-02 (with responsibilities as defined in CEN TS 419 261)

5.2.4 Roles que requieren separación de tareas

Las siguientes tareas son realizadas, al menos, por dos personas:

- Emisión y revocación de certificados, y el acceso al depósito.
- Generación, emisión y destrucción de certificados de la Autoridad de Certificación.
- Puesta en producción de la Autoridad de Certificación.
- Recuperación mediante Backup de la clave privada de las CA's

5.3 Controles de personal

5.3.1 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.

Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

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

La Autoridad de Certificación de DIGITELTS se asegura que el personal de registro es confiable para realizar las tareas de registro. El Operador de Registro ha realizado un curso de preparación para la realización de las tareas de validación de las peticiones.

En general, la Autoridad de Certificación de DIGITELTS 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 Autoridad de Certificación de DIGITELTS no asignará a un sitio confiable 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 puesto. 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.

5.3.2 Procedimientos de investigación de historial

La Autoridad de Certificación de DIGITELTS, 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 Autoridad de Certificación de DIGITELTS 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.

5.3.3 Requisitos de formación

La Autoridad de Certificación de DIGITELTS forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.

Los programas de formación son actualizados y mejorados de forma periódica. 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 DIGITELTS. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- 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.

5.3.4 Requisitos y frecuencia de actualización formativa

La Autoridad de Certificación de DIGITELTS 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.

5.3.5 Secuencia y frecuencia de rotación laboral

Sin estipulación.

5.3.6 Sanciones para acciones no autorizadas

La Autoridad de Certificación de DIGITELTS 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.

5.3.7 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 Autoridad de Certificación de DIGITELTS. 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 de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la DPC, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante, lo cual, la Autoridad de certificación 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 de certificación por tercero distinto a la Autoridad de Certificación de DIGITELTS.

5.3.8 Suministro de documentación al personal

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

5.4 Procedimientos de auditoría de seguridad

La Autoridad de Certificación de DIGITELTS 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. DIGITELTS 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.

5.4.1 Tipos de eventos registrados

La Autoridad de Certificación de DIGITELTS 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 PKI.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de este.
- Las actividades de los cortafuegos y enrutadores
- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación oinformación personal del suscriptor, en caso de certificados corporativos, o de la persona física identificada en el certificado.
- Posesión de datos de activación, para operaciones con la clave privada de la Autoridad de Certificación.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan

soporte a la emisión y gestión de certificados.

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.

5.4.2 Frecuencia de tratamiento de registros de auditoría

La Autoridad de Certificación de DIGITELTS revisa sus logs 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 Autoridad de Certificación de DIGITELTS mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

5.4.3 Período de conservación de registros

La Autoridad de Certificación de DIGITELTS almacena la información de los logs al menos durante 15 años.

5.4.4 Protección de los registros de auditoría

Los logs de los sistemas:

- Están protegidos de manipulación, borrado o eliminación mediante la firma de los ficheros que los contienen.
- Son almacenados en dispositivos ignífugos.
- Se protege su disponibilidad mediante el almacén en instalaciones externas al centro donde se ubica la AC.

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

5.4.5 Procedimientos de copia de seguridad

La Autoridad de Certificación de DIGITELTS 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 Autoridad de Certificación de DIGITELTS tiene implementado un procedimiento de copia de seguridad seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs.

5.4.6 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 certificados, 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.

5.4.7 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.

5.4.8 Análisis de vulnerabilidades

Toda la infraestructura 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.

5.5 Archivos de informaciones

5.5.1 Tipos de registros archivados

La Autoridad de Certificación de DIGITELTS, garantiza que toda la información relativa a los certificados se conserva durante un período de tiempo apropiado, según lo establecido en la sección 5.7.1 de esta política.

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por la Autoridad de Certificación de DIGITELTS (o por las entidades de registro):

- Todos los datos de auditoría de sistema (PKI, TSA y OCSP).

- Todos los datos relativos a los certificados, incluyendo los contratos con los titulares y los datos relativos a su identificación y su ubicación.
- Solicitudes de emisión y revocación de certificados, incluidos todos los informes relativos al proceso de revocación.
- Todas aquellas elecciones específicas que el subscriptor disponga durante el acuerdo de subscripción.
- El documento presentado en la solicitud del certificado.
- La Identidad de la Autoridad de Registro que acepta la solicitud de certificado, en caso de existir.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos de la PKI.
- Las Prácticas de Certificación
- Todos los datos de auditoría identificados en la sección 4
- Información de solicitudes de certificación.
- Documentación aportada para justificar las solicitudes de certificación.
- Información del ciclo de vida del certificado.

La Autoridad de Certificación de DIGITELTS es responsable del correcto archivo de todo este material.

5.5.2 Período de conservación de registros

La Autoridad de Certificación de DIGITELTS archiva los registros especificados anteriormente durante 15 años tras la finalización de la vigencia del certificado al que están asociadas.

5.5.3 Protección del archivo

La Autoridad de Certificación de DIGITELTS 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 Autoridad de Certificación de DIGITELTS asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas.

5.5.4 Procedimientos de copia de seguridad

La Autoridad de Certificación de DIGITELTS 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.

Además, La Autoridad de Certificación de DIGITELTS (o las organizaciones que realizan la función de registro) guarda copia de los documentos en papel en un lugar seguro diferente de las instalaciones de la propia Autoridad de certificación.

5.5.5 Requisitos de sellado de tiempo electrónico

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

Los servidores de la Autoridad de Certificación de DIGITELTS están conectados a las fuentes primarias Equinix Precision Time NTP, con un nivel Stratum 1, desde Frankfurt 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.

No es necesario que esta información se encuentre firmada digitalmente.

5.5.6 El sistema de archivo

La Autoridad de Certificación de DIGITELTS dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

5.5.7 Procedimientos de obtención y verificación de información de archivo

Estos sistemas disponen de un alto nivel de integridad, confidencialidad y disponibilidad para evitar intentos de manipulación.

5.6 Renovación de claves

Con anterioridad a que el uso de la clave privada de la autoridad de certificación caduque, será realizado un cambio de claves. La antigua autoridad de certificación y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por dicha autoridad de certificación. Se generará una nueva autoridad de certificación con una clave privada nueva y un nuevo DN.

El cambio de claves del suscriptor es realizado mediante un nuevo proceso de emisión.

5.7 Compromiso de claves y recuperación de desastre

5.7.1 Procedimientos de gestión de incidencias y compromisos

Son almacenadas copias de seguridad de la siguiente información, que se ponen a disposición en caso de compromiso o desastre: datos técnicos de solicitud de certificados, datos de auditoría y registros de base de datos de todos los certificados emitidos.

Las copias de seguridad de las claves privadas de la Autoridad de Certificación de DIGITELTS son generadas y mantenidas de acuerdo con lo establecido en la sección 6.2.4

5.7.2 Corrupción de recursos, aplicaciones o datos

Cuando ocurra un evento de corrupción de recursos, aplicaciones o datos, se comunicará la incidencia a seguridad, y se iniciarán los procedimientos de gestión oportunos, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres de la Autoridad de Certificación de DIGITELTS.

5.7.3 Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso de la Autoridad de Certificación de DIGITELTS, se activarán los procedimientos de compromiso de claves, documentados como parte de los planes de contingencia de la organización: Tratamiento del compromiso de clave privada de la autoridad de certificación. Dicho procedimiento contempla:

- Notificación de la incidencia al órgano de supervisión.
- Emisión inmediata de una CRL nueva y publicarla.
- Recomendación a los usuarios de los servicios de certificación que incorporen sellos de tiempo de archivo a todas las firmas o sellos, por defecto.
- Sin perjuicio de lo anterior, se procede a las actuaciones referidas a la información de revocación previstas para el cese de la autoridad de certificación, antes de la revocación del certificado de la CA Subordinada.
- Advertencia a todos los suscriptores, de forma individualizada, y a las terceras partes interesadas, mediante publicación en la página web de la Autoridad de Certificación de DIGITELTS y, en su caso, a través de algún medio de comunicación pública.

5.7.4 Continuidad del negocio después de un desastre

La Autoridad de Certificación de DIGITELTS 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 Autoridad de Certificación de DIGITELTS.

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.

La Autoridad de Certificación de DIGITELTS 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, ha 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.

5.8 Terminación del servicio

En caso de cese de los servicios, la Autoridad de Certificación de DIGITELTS 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 y para garantizar la continuidad del servicio. Para dar satisfacción a esta responsabilidad, se ha desarrollado un plan de cese que ordena las medidas a tomar en caso del cese de la empresa como prestadora de servicios de confianza, y también en caso de cierre de alguno de los servicios de confianza que presta. Este plan cubre:

- Se provisionará la cantidad necesaria, mediante seguro de responsabilidad civil, para cubrir los costes a efectos de contingencia de cierre.
- Informará a todos Firmantes/Suscriptores, Tercero que confían y otras AC's con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 2 meses.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.
- En caso de cese de la figura jurídica, transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios.
- Destruirá o deshabilitará para su uso las claves privadas de la AC.
- Comunicará al Ministerio de Industria, Energía y Turismo, con una antelación mínima de 2 meses, el cese de su actividad.
- Comunicará, también al supervisor nacional, la apertura de cualquier proceso concursal que se siga contra la Autoridad de Certificación de DIGITELTS, así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

6 Controles de seguridad técnica

La Autoridad de Certificación de DIGITELTS emplea sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

El par de claves de las entidades de certificación intermedias “DIGITEL TS QUALIFIED CA TSA G1” y “DIGITEL TS QUALIFIED CA G1” son creadas por la entidad de certificación raíz “DIGITEL TS CA ROOT 01” de acuerdo con los procedimientos de ceremonia de la Autoridad de Certificación de DIGITELTS, dentro del perímetro de alta seguridad destinado a esta tarea.

Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma, con la presencia de un Auditor externo. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por la Autoridad de Certificación de DIGITELTS.

Para la generación de la clave de las entidades de certificación raíz e intermedias se han utilizado dispositivos con las certificaciones FIPS 140-2 nivel 3.

Descripción de la autoridad de certificación raíz creada:

DIGITEL TS CA ROOT 01	4.096 bits (RSA)	25 años

Descripción de las CA’s intermedias creadas:

DIGITEL TS QUALIFIED CA TSA G1	4.096 bits (RSA)	25 años
DIGITEL TS QUALIFIED CA G1	4.096 bits (RSA)	13 años

Descripción de las correspondientes TSU:

DIGITEL TS QUALIFIED TSU 01 G1	4.096 bits (RSA)	5 años
DIGITEL TS QUALIFIED TSU 01 G2	4.096 bits (RSA)	5 años
DIGITEL TS QUALIFIED TSU 01 G3 EDCSA	EDCSA 256	5 años
DIGITEL TS QUALIFIED TSU 01 G4 EDCSA	EDCSA 256	5 años
DIGITEL TS QUALIFIED TSU 01 G5 EDCSA	EDCSA 256	5 años
DIGITEL TS QUALIFIED TSU 01 G6 EDCSA	EDCSA 256	5 años
DIGITEL TS QUALIFIED TSU RSA2048 01 G7	2048 bits (RSA)	3 años
DIGITEL TS QUALIFIED TSU RSA2048 01 G8	2048 bits (RSA)	3 años

Más información en la dirección:

https://pki.digitelts.es

Las claves del firmante son creadas por él mismo mediante software autorizado por la Autoridad de Certificación de DIGITELTS.

Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

6.1.2 Envío de la clave privada al titular

En la emisión de certificados de sellos electrónicos de TSU las claves se gestionan internamente en los equipos existentes.

En certificados en software, el envío de la clave privada al firmante tras la generación de las claves en el sistema PKI de la Autoridad de Certificación de DIGITELTS se realiza de forma segura al firmante, en un fichero "*.p12*".No aplica en los certificados en los que la clave privada reside en un HSM centralizado, para los que el firmante es el único que tiene control exclusivo de dicha clave.

6.1.3 Envío de la clave pública al emisor del certificado

El método de remisión de la clave pública al prestador de servicios de certificación es PKCS#10, otra prueba criptográfica equivalente o cualquier otro método aprobado.

Cuando las claves se generan en un QSCD, la Autoridad de Certificación de DIGITELTS se asegura que la clave pública que se remite proviene de un par de claves generadas por dicho QSCD.

No aplica para la emisión de sellos electrónicos de TSU.

6.1.4 Distribución de la clave pública del prestador

Las claves de la Autoridad de Certificación de DIGITELTS son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el Depósito.

Los usuarios pueden acceder al Depósito para obtener las claves públicas, y adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

El certificado de las CA raíz y subordinadas estarán a disposición de los usuarios en la página Web de la Autoridad de Certificación de DIGITELTS.

6.1.5 Tamaños de claves

La longitud de las claves de la Autoridad de Certificación raíz o subordinadas es de 4096 bits como mínimo.

Las claves de los certificados de TSU serán de 2048 bits como mínimo.

6.1.6 Generación de parámetros de clave pública

La clave pública de la CA raíz, de las CA intermedias y de los certificados de los suscriptores están codificadas de acuerdo con la RFC 5280.

6.1.7 Comprobación de calidad de parámetros de clave pública

Las CA emplean los siguientes parámetros criptográficos:

- Cuando se usa el algoritmo RSA
  - Longitud del Módulo = 4096.
  - Funciones criptográficas de Resumen: SHA512WithRSA.

6.1.8 Propósitos de uso de claves

Los usos de las claves para los certificados de las CA son exclusivamente para la firma de certificados y de CRLs.

Los usos de las claves para los certificados de entidad final de firma electrónica y de sellos electrónicos son exclusivamente para la firma digital y el no repudio recogidos en el apartado 1.4 de este documento.

6.2 Protección de la clave privada y controles de los módulos criptográficos

6.2.1 Estándares de módulos criptográficos

En relación con los módulos que gestionan claves de la Autoridad de Certificación de DIGITELTS y de las unidades de tiempo electrónico se asegura el nivel exigido por los estándares indicados en las secciones anteriores.

Los módulos criptográficos se someten a los controles de ingeniería previstos en las normas indicadas a lo largo de esta sección.

Los algoritmos de generación de claves empleados se aceptan comúnmente para el uso de la clave a que están destinados.

Todas las operaciones criptográficas de la Autoridad de Certificación son realizadas en módulos con las certificaciones FIPS 140-2 level 3.

6.2.2 Control por más de una persona (n de m) sobre clave privada

Se requiere un control multi-persona para la activación de la clave privada de la AC. En el caso de esta DPC, en concreto existe una política de **2 de 3** personas para la activación de las claves.

Los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

Las instalaciones de la Autoridad de Certificación están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular.

6.2.3 Depósito de la clave privada

La Autoridad de Certificación de DIGITELTS no almacena copias de las claves privadas de los suscriptores.

6.2.4 Copia de respaldo de la clave privada

La Autoridad de Certificación de DIGITELTS realiza copia de seguridad de las claves privadas de las autoridades de certificación que hacen posible su recuperación en caso de desastre, pérdida o deterioro de estas. Tanto la generación de la copia como la recuperación de ésta necesitan al menos de la participación de dos personas.

Estos ficheros de recuperación se almacenan en armarios ignífugos. Las claves del suscriptor en software pueden ser almacenadas para su posible recuperación en caso de contingencia, en un dispositivo de almacenamiento externo separado de la clave de instalación.

El firmante puede realizar copias de seguridad de sus claves en software, ya que estas se ubican en los sistemas del firmante.

El firmante no puede realizar copias de seguridad de sus claves en hardware, ya que estas no pueden salir del dispositivo criptográfico.

6.2.5 Archivo de la clave privada

Las claves privadas de las autoridades de certificación son archivadas por un periodo de 10 años después de la emisión del último certificado. Se almacenarán en archivos ignífugos seguros. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de las autoridades de certificación en el dispositivo criptográfico inicial.

6.2.6 Introducción de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos de producción de la Autoridad de Certificación de DIGITELTS. No es posible la transferencia de claves, aunque como se indica en el apartado 6.2.4 existe la opción de recuperación como medida de contingencia para su copia de seguridad.

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

Las claves privadas de la Autoridad de Certificación de DIGITELTS se almacenan cifradas en sus módulos criptográficos de producción.

6.2.8 Método de activación de la clave privada

La clave privada de la Autoridad de Certificación de DIGITELTS se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.2.2.

Las claves de la autoridad de certificación raíz se activan por un proceso de *m de n* (2 de 3).

La activación de las claves privadas de las autoridades de certificación Intermedias es gestionada con el mismo proceso de *m de n* que las claves de la autoridad de certificación raíz.

6.2.9 Método de desactivación de la clave privada

Para la desactivación de la clave privada de Autoridad de Certificación de DIGITELTS se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente, así como en el plan de cese.

6.2.10 Método de destrucción de la clave privada

Con anterioridad a la destrucción de las claves, se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de la Autoridad de Certificación de DIGITELTS que deban ser objeto de destrucción. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico, así como en el plan de cese.

Finalmente se destruirán de forma segura las copias de seguridad.

Las claves del firmante o del creador de sellos en software se podrán destruir mediante el borrado de estas, siguiendo las instrucciones de la aplicación que las alberga.

Las claves del firmante o del creador de sellos en HSM podrán ser destruidas mediante una aplicación informática especial en las dependencias de la Autoridad de Certificación de DIGITELTS.

6.2.11 Clasificación de módulos criptográficos

Ver la sección 6.2.1.

6.3 Otros aspectos de gestión del par de claves

6.3.1 Archivo de la clave pública

La Autoridad de Certificación de DIGITELTS archiva sus claves públicas de forma rutinaria, de acuerdo con lo establecido en la sección 5.5 de este documento.

6.3.2 Períodos de utilización de las claves

Los periodos de utilización de las claves son los determinados por la duración del certificado, transcurrido el cual no pueden continuar utilizándose.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas son generados de acuerdo con lo establecido en la sección 6.2.2 y los procedimientos de ceremonia de claves.

La creación y distribución de dichos dispositivos es registrada. Asimismo, la Autoridad de Certificación de DIGITELTS genera de forma segura los datos de activación.

6.4.2 Protección de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de las Autoridades de certificación raíz e intermedias, son protegidos por los poseedores de las tarjetas de administradores de los módulos criptográficos, según consta en el documento de ceremonia de claves.

El firmante del certificado es el responsable de la protección de su clave privada, con una contraseña lo más completa posible. El firmante debe recordar dicha contraseña.

6.5 Controles de seguridad informática

6.5.1 Requisitos técnicos específicos de seguridad informática

La Autoridad de Certificación de DIGITELTS emplea sistemas fiables para ofrecer sus servicios de certificación. 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 la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información, la Autoridad de Certificación de DIGITELTS 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 Autoridad de Certificación de DIGITELTS, 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 Autoridad de Certificación de DIGITELTS incluye las siguientes funcionalidades:

- Control de acceso a los servicios de la CA intermedia 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 y la CA intermedia y datos de auditoría.
- Auditoría de eventos relativos a la seguridad.
- Autodiagnóstico de seguridad relacionado con los servicios de la CA intermedia.
- Mecanismos de recuperación de claves y del sistema de la CA intermedia.

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

6.5.2 Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas por la Autoridad de Certificación de DIGITELTS son fiables.

6.6 Controles de seguridad del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por la Autoridad de Certificación de DIGITELTS 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.

6.6.2 Controles de gestión de seguridad

La Autoridad de Certificación de DIGITELTS desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. 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 Autoridad de Certificación de DIGITELTS exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

6.6.2.1 Clasificación y gestión de información y bienes

La Autoridad de Certificación de DIGITELTS 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 Autoridad de Certificación de DIGITELTS 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.

6.6.2.2 Operaciones de gestión

La Autoridad de Certificación de DIGITELTS 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 Autoridad de Certificación de DIGITELTS se desarrolla en detalle el proceso de gestión de incidencias.

La Autoridad de Certificación de DIGITELTS 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.

6.6.2.3 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.

6.6.2.4 Planificación del sistema

El departamento de Sistemas de la Autoridad de Certificación de DIGITELTS 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.

6.6.2.5 Reportes de incidencias y respuesta

La Autoridad de Certificación de DIGITELTS 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.

6.6.2.6 Procedimientos operacionales y responsabilidades

La Autoridad de Certificación de DIGITELTS 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.

6.6.2.7 Gestión del sistema de acceso

La Autoridad de Certificación de DIGITELTS 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 Autoridad de Certificación de DIGITELTS dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- La Autoridad de Certificación de DIGITELTS 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 Autoridad de Certificación de DIGITELTS 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.

6.6.2.8 Generación del certificado

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

6.6.2.9 Gestión de la revocación.

La revocación se realizará 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 DIGITELTS.

6.6.2.10 Estado de la revocación

La aplicación del estado de la revocación 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.

6.6.2.11 Gestión del ciclo de vida del hardware criptográfico

La Autoridad de Certificación de DIGITELTS se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.

La Autoridad de Certificación de DIGITELTS registra toda la información pertinente del dispositivo para añadir al catálogo de activos. El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

La Autoridad de Certificación de DIGITELTS realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

La clave privada de firma de La Autoridad de Certificación de DIGITELTS almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema de la Autoridad de Certificación de DIGITELTS, así como sus modificaciones y actualizaciones son documentadas y controladas.

La Autoridad de Certificación de DIGITELTS posee un contrato de mantenimiento del dispositivo. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.7 Controles de seguridad de red

La Autoridad de Certificación de DIGITELTS 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.

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.

6.8 Fuentes de tiempo

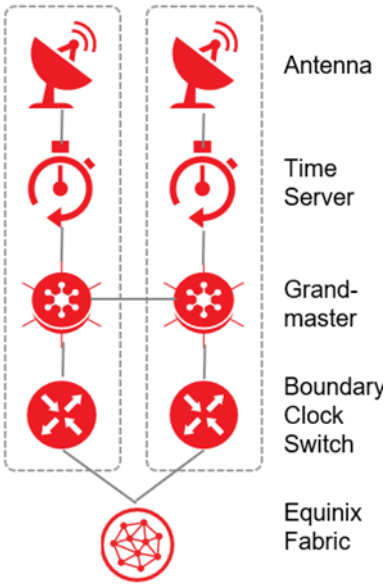
La Autoridad de Certificación de DIGITELTS tiene un procedimiento de sincronización de tiempo coordinado mediante **Equinix Precision Time**[7], dicho servicio basado en suscripción provee una sincronización de tiempo preciso, seguro y confiable para aplicaciones empresariales.

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.

[7] https://docs.equinix.com/en-us/Content/Edge-Services/EPT/EPT.htm

- 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**[8].
- Soporte para hasta 1000 clientes NTP.



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

7 Perfiles de certificados, CRL y OCSP

7.1 Perfil de certificado

Todos los certificados emitidos bajo esta DPC cumplen el estándar X.509 versión 3, RFC 5280 y las siguientes normas:

- ETSI EN 319 422 para la definición de los perfiles de los sellos de tiempo.
- ETSI EN 319 412-5 para la definición de los QCStatements de los certificados cualificados de acuerdo con el RD (EU) 910/2014
- ETSI EN 319 412-2 para certificados emitidos a personas físicas
- ETSI EN 319 412-3 para certificados emitidos a personas jurídicas/ESPJ

7.1.1 Número de versión

La Autoridad de Certificación de DIGITELTS emite certificados X.509 Versión 3

7.1.2 Extensiones del certificado

Las extensiones de los certificados se encuentran detalladas en los documentos de perfiles que son accesibles desde la página web de la Autoridad de Certificación de DIGITELTS en la dirección web: https://pki.digitelts.es

7.1.3 Identificadores de objeto de los algoritmos

Los identificadores de objeto del algoritmo de firma son:

- 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
- 1.2.840.113549.1.1.12 (sha384WithRSAEncryption)
- 1.2.840.113549.1.1.13 (sha512WithRSAEncryption)

7.1.4 Formato de nombres

Los certificados deberán contener las informaciones que resulten necesarias para su uso. La codificación de los certificados sigue las recomendaciones de la RFC 5280 de la forma que se describe en el punto 3.1 de este documento.

7.1.5 Restricción de los nombres

Los nombres contenidos en los certificados están restringidos a "Distinguished Names" X.500, que son únicos y no ambiguos. Adicionalmente se pueden establecer restricciones de nombres en relación con los certificados para la autenticación, firma electrónica, cifrado o evidencia electrónica, siempre que las mismas resulten objetivas, proporcionadas, transparentes y no discriminatorias.

7.1.6 Identificador de objecto de los tipos de certificados

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos, de acuerdo con la estructura indicada en el punto 1.2.1.

7.1.7 Uso de la extensión "Policy Constraints"

La extensión "Policy Constraints" no se utiliza en los certificados raíz.

7.1.8 Sintaxis y semántica de los calificadores de política

Se incluyen dos campos:

- CPS Pointer: la URL donde se encuentra el documento de prácticas de confianza.
- User notice: Texto para que el usuario pueda visualizar la información del certificado.

7.1.9 Tratamiento semántico para la extensión crítica "certificate policy"

Se identifica la política asociada al certificado por parte de la jerarquía de la Autoridad de Certificación de DIGITELTS y los campos indicados en el apartado anterior.

7.2 Perfil de la lista de revocación de certificados

Las CRL emitidas por la Autoridad de Certificación de DIGITELTS son de la versión 2.

7.3 Perfil de OCSP

Según el estándar IETF RFC 6960.

8 Auditoría de conformidad

La Autoridad de Certificación de DIGITELTS 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 Autoridad de Certificación de DIGITELTS realiza auditorías de conformidad del Reglamento eIDAS por medio de evaluaciones de conformidad anuales sobre los siguientes servicios:

- Servicio de expedición de sellos electrónicos cualificados de tiempo
- Servicio de expedición de certificados electrónicos cualificados de firma electrónica
- Servicio de expedición de certificados electrónicos cualificados de sello electrónico

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 Time-Stamps.
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI).
- Time-stamping protocol and time-stamp token profiles

- ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates: Requirements for trust service providers issuing EU qualified certificates.

La Autoridad de Certificación de DIGITELTS realiza las pertinentes auditorías sobre protección de datos con periodicidad bienal.

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 de certificación de clave pública, y los elementos relacionados.

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

Para la evaluación de conformidad eIDAS la Autoridad de Certificación de DIGITELTS ha usado los servicios de AENOR (https://www.aenor.com/).

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 DPC y otra documentación vinculada con la emisión de los distintos certificados digitales, bajo el marco del Reglamento (UE) 910/2014 del parlamento europeo y del consejo de 23 de julio de 2014.
- Que la DPC y demás documentación jurídica vinculada, se ajusta a lo acordado por la Autoridad de Certificación de DIGITELTS y con lo establecido en la normativa vigente.
- Que la entidad gestiona de forma adecuada sus sistemas de información

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

- Procesos de la AC, ARs y elementos relacionados.
- Sistemas de información.
- Protección del centro de proceso de datos.
- Documentación asociada.

8.5 Acciones que emprender como resultado de una falta de conformidad

Una vez recibido por la dirección 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 Autoridad de Certificación de DIGITELTS 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 Seguridad de la Información de DIGITEL que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar la clave de la AC y regenerar la infraestructura.
- Terminar el servicio de la AC.
- 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 Seguridad de la Información de DIGITEL en un plazo máximo de 15 días tras la ejecución de la auditoría, para su análisis y tratamiento.

Si a causa de la auditoría realizada fuera necesaria la revocación de certificados, este informe servirá como justificante de dicha revocación.

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 emisión o por la renovación de los certificados, de la que, en su caso, se informará oportunamente a los suscriptores.

9.1.2 Tarifa de acceso a certificados

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

9.1.3 Tarifa de acceso a información de estado de certificado

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

9.1.4 Tarifas de otros servicios

Sin estipulación

9.1.5 Política de reintegro

Sin estipulación

9.2 Responsabilidad financiera

La Autoridad de Certificación de DIGITELTS 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, según lo establecido en la ETSI EN 319 411-1, en relación con la gestión de la finalización de los servicios y plan de cese.

9.2.1 Cobertura de seguro

La Autoridad de Certificación de DIGITELTS 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.

9.2.3 Cobertura de seguro para suscriptores y terceros que confían

La Autoridad de Certificación de DIGITELTS 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.

9.3 Confidencialidad de la información

9.3.1 Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.
- Claves privadas generadas y/o almacenadas por el prestador de servicios de certificación.
- 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 la Autoridad de Certificación 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 siguiente información se considera no confidencial:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por la Autoridad de Certificación.
- El nombre y los apellidos de la persona física identificada en el certificado, así como cualquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico de la persona física identificada en el certificado o la asignada por el suscriptor, en el supuesto de que sea significativa en función de la finalidad del certificado.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (LRCs), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Cualquier otra información que no esté indicada en la sección anterior.

Las siguientes informaciones serán públicas:

- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (CRLs), así como las restantes informaciones de estado de revocación.

9.3.3 Divulgación de información de revocación

Ver sección anterior.

9.3.4 Divulgación legal de información

La Autoridad de Certificación de DIGITELTS divulga la información confidencial únicamente en los casos legalmente previstos.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado, 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 certificación en un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

La Autoridad de Certificación indicará estas circunstancias en la política de privacidad prevista en la sección 9.4.

9.3.5 Divulgación de información por petición de su titular

La Autoridad de Certificación de DIGITELTS 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.

9.3.6 Otras circunstancias de divulgación de información

Sin estipulación.

9.4 Protección de la información personal

Para la prestación del servicio de confianza de expedición de certificados cualificados y sellos electrónicos cualificados 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 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 Autoridad de Certificación de DIGITELTS 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). Específicamente, la base legal para el tratamiento de los datos mínimos que se deben contener dentro del certificado cualificado a expedir es el cumplimiento de una obligación legal aplicable al responsable del tratamiento (artículo 6.1.c) del RGPD). Asimismo, la base legal para el mantenimiento de relaciones comerciales es el interés legítimo (artículo 6.1.f) del RGPD).

Los datos que se solicitan a los interesados son estrictamente los necesarios para la suscripción del contrato y la prestación del servicio de expedición del certificado. La no comunicación de los datos supone la imposibilidad de prestación del servicio, por exigencia legal.

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 Autoridad de Certificación de DIGITELTS. 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 Autoridad de Certificación de DIGITELTS en las direcciones indicadas en el apartado 1.5 de este documento.

La autoridad de certificación de DIGITELTS no adopta decisiones automatizadas, ni siquiera la elaboración de perfiles.

La autoridad de certificación de DIGITELTS no realiza transferencias de datos personales a terceros países.

9.5 Derechos de propiedad intelectual

9.5.1 Propiedad de los certificados e información de revocación

Únicamente la Autoridad de Certificación de DIGITELTS goza de derechos de propiedad intelectual sobre los certificados que emita, sin perjuicio de los derechos de los suscriptores y terceros, a los que conceda licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de uso del certificado, y de acuerdo con la documentación que los vincula.

Adicionalmente, los certificados emitidos por la Autoridad de Certificación de DIGITELTS contienen un aviso legal relativo a la propiedad de estos.

Las mismas reglas resultan de aplicación al uso de la información de revocación de los certificados.

9.5.2 Propiedad de la Declaración de Prácticas de Confianza

Únicamente la Autoridad de Certificación de DIGITELTS goza de derechos de propiedad intelectual sobre esta Declaración de Prácticas de Confianza.

9.5.3 Propiedad de la información relativa a nombres

El suscriptor y, en su caso, la persona física identificada en el certificado conserva la totalidad de derechos, de existir los mismos, sobre la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3.1 del presente documento.

9.5.4 Propiedad de claves

Los pares de claves son propiedad de los subscriptores, las personas jurídicas que poseen de forma exclusiva las claves de firma digital de los certificados de sello electrónico.

Cuando una clave se encuentra fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.6 Obligaciones y responsabilidad civil

9.6.1 Obligaciones de la Autoridad de Certificación

La Autoridad de Certificación de DIGITELTS garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la DPC, siendo el único responsable

del cumplimiento de los procedimientos descritos, incluso si una parte o la totalidad de las operaciones se subcontratan externamente.

La Autoridad de Certificación de DIGITELTS presta los servicios de certificación conforme con esta Declaración de Prácticas de Confianza.

Con anterioridad de la emisión y entrega del certificado al suscriptor, la Autoridad de Certificación de DIGITELTS informa al suscriptor de los términos y condiciones relativos al uso del certificado, de su precio y de sus limitaciones de uso, mediante un contrato de suscriptor.

Este requisito de información también se cumple mediante un documento PDS, también denominado texto de divulgación, que incorpora el contenido del anexo A de la norma técnica ETSI EN 319 411-1, documento que puede ser transmitido por medios electrónicos, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

La Autoridad de Certificación de DIGITELTS 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, poseedores de claves y terceros que confían en certificados 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 contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para la publicación del certificado en el depósito y acceso por terceros al mismo.
- 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 Entidad de Certificación sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 4.2

- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial de la Autoridad de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Autoridad de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Si la Autoridad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

9.6.2 Garantías ofrecidas a suscriptores y terceros que confían en certificados

La Autoridad de Certificación de DIGITELTS realiza las verificaciones necesarias para confirmar la existencia de la organización que desea convertirse en Autoridad de Registro. Se obtiene la documentación de la organización que se presenta, además de utilizar sus propias fuentes de información.

Autoridad de Certificación de DIGITELTS, en los casos en que la función de registro se delega en un suscriptor, verifica y valida la identidad de los operadores de la Autoridad de Registro con la información que le remite el subscriptor, en la que incluye su autorización para actuar como tal.

Autoridad de Certificación de DIGITELTS se asegura que los operadores de la Autoridad de Registro reciban la formación suficiente para el desempeño de sus funciones, que verificará en las evaluaciones correspondientes.

Garantías ofrecidas a suscriptores que confían:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Autoridad de Certificación.
- 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 del mismo.
- Que los certificados cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Confianza.
- Que los servicios de revocación y el empleo del Depósito cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Confianza.

Garantías ofrecidas 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 identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 4
- 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 Declaración de Prácticas de Confianza.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y Depósito.

Finalmente la Autoridad de Certificación de DIGITELTS garantiza al suscriptor y al tercero que confían en el certificado:

- 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 certificado de sello electrónico de persona jurídica contiene las informaciones que debe contener un certificado cualificado, de acuerdo con el Anexo III del Reglamento (UE) 910/2014.
- Que el certificado de firma electrónica de persona física contiene las informaciones que debe contener un certificado cualificado, de acuerdo con el Anexo I del Reglamento (UE) 910/2014.La responsabilidad de la Entidad de Certificación, con los límites que se establezcan.

9.7 Exención de garantía

La Autoridad de Certificación de DIGITELTS 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

9.8.1 Responsabilidades de la Autoridad de Certificación

La Autoridad de Certificación de DIGITELTS en su actividad de prestación de servicios de certificación, responderá por el incumplimiento de lo establecido en la DPC, 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.

Sin perjuicio de lo anterior, la Autoridad de Certificación de DIGITELTS 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 DPC, 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 Autoridad de Certificación de DIGITELTS será responsable del daño causado ante el Suscriptor y/o firmante o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

- La exactitud de la información contenida en el certificado en la fecha de su emisión, siempre que ésta corresponda a información autenticada.
- La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
- La correspondencia entre el certificado solicitado y el certificado entregado.
- Cualquier responsabilidad que se establezca por la legislación vigente aplicable.

En ningún caso será responsable de las acciones u omisiones de terceros distintos de la Autoridad de Certificación de DIGITELTS 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 Autoridad de Certificación de DIGITELTS en los referidos procedimientos de expedición y/o de gestión de los certificados.

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 los certificados, así como de la cuantía de los perjuicios que se pudieran causar, la cantidad máxima por la que la Autoridad de Certificación de DIGITELTS 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 de emisión y gestión de los certificados de clave pública, la Autoridad de Certificación de DIGITELTS se atendrá a la normativa de firma electrónica vigente en cada momento, informando en todo caso con suficiente antelación a los titulares de los certificados, así como a los usuarios de los servicios afectados y transferirá a otro Prestador de Servicios de Certificación que los asuma, con expreso consentimiento de sus titulares, aquellos certificados que sigan siendo válidos en la fecha efectiva de cese de actividad.

En el supuesto de que esta transferencia de los certificados no fuera posible por cualquier motivo, se procederá, previo aviso a los titulares de los certificados afectados, a la revocación de la validez de estos.

9.8.2 Responsabilidades de la Autoridad de Registro

La RA asumirá toda la responsabilidad en el procedimiento de identificación de los suscriptores y en la verificación de la identidad. Deberá seguir lo estipulado en la presente DPC o según otro procedimiento aprobado por la Autoridad de Certificación de DIGITELTS.

9.8.3 Responsabilidades del suscriptor

El suscriptor es responsable de cumplir con las obligaciones estipuladas en esta DPC, y en el contrato que le vincule.

9.8.4 Delimitación de responsabilidades

La Autoridad de Certificación de DIGITELTS no será responsable en ningún caso ante las siguientes circunstancias:

- Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el Suscriptor o por los Terceros, o cualquier otro caso de fuerza mayor.
- Por el uso indebido o fraudulento del directorio de certificados y CRL's (Lista de Certificados
  - Revocados) emitidos por la Autoridad de Certificación.
  - Por el uso indebido de la información contenida en el Certificado o en la CRL.
  - Por el contenido de los mensajes o documentos firmados o encriptados mediante los certificados.
  - En relación con las siguientes acciones u omisiones del Solicitante y Suscriptor:
    - Falta de veracidad de la información suministrada para emitir el certificado.
    - Retraso en la comunicación de las causas de suspensión o revocación del certificado.

- Ausencia de solicitud de suspensión o revocación del certificado cuando proceda.
  - Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
  - Uso del certificado fuera de su periodo de vigencia, o cuando la Autoridad de Certificación de DIGITELTS o la RA le notifique la revocación o suspensión de este.
  - Extralimitación en el uso del certificado, según lo dispuesto en la normativa vigente y en la presente DPC, en particular, superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al titular por la Autoridad de Certificación de DIGITELTS.
- En relación con acciones u omisiones del tercero que confía en el certificado:
  - Falta de comprobación de las restricciones que figuren en el certificado electrónico o en la presente DPC en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.
  - Falta de comprobación de la suspensión o pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados o falta de verificación de la firma electrónica.

9.8.5 Cláusula de indemnidad de suscriptor

La Autoridad de Certificación de DIGITELTS incluye en el contrato con el suscriptor o (en los textos de divulgación – PDS), una cláusula por la cual el suscriptor se compromete a mantener indemne a la Autoridad de Certificación 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:

- Falsedad o manifestación errónea realizada por el usuario del certificado.
- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión ha mediado dolo o negligencia con respecto a la Autoridad de Certificación o a cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de domino), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

9.8.6 Cláusula de indemnidad de tercero que confía

La Autoridad de Certificación de DIGITELTS incluye en la PDS, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne a la Autoridad de Certificación 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.

9.8.7 Caso fortuito y fuerza mayor

La Autoridad de Certificación de DIGITELTS incluye en la PDS cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

9.9 Indemnizaciones

9.9.1 Alcance de la cobertura

La Autoridad de Certificación de DIGITELTS dispone de un seguro que responde de las cantidades que le resulte legalmente obligado a pagar, hasta el límite de cobertura contratado, como resultado de cualquier procedimiento judicial en el que pueda declararse su responsabilidad, derivada de cualquier acto negligente, error u incumplimiento no intencionado de la legislación vigente entre otros, en los términos expresamente pactados con la compañía aseguradora.

9.9.2 Limitaciones de pérdidas

La Autoridad de Certificación de DIGITELTS limita su responsabilidad mediante la inclusión de los límites de uso del certificado con la extensión *qcStatements* en los perfiles de los certificados.

El suscriptor podrá, si lo desea, solicitar y en su caso contratar un límite superior al indicado, asumiendo los costes adicionales que en su caso se establezcan. Además, el suscriptor y terceras partes podrán acordar bilateralmente pactos o coberturas específicas para transacciones de valor superior, manteniéndose en este caso el límite de responsabilidad de la CA citado en los párrafos anteriores.

9.10 Periodo de validez

9.10.1 Plazo

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

9.10.2 Sustitución y derogación de la DPC

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

9.10.3 Efectos de la finalización

Para los certificados vigentes emitidos bajo una DPC anterior, la nueva versión prevalecerá a la anterior en todo lo que no se oponga a ésta.

9.11 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.

9.12 Enmiendas

9.12.1 Procedimiento para los cambios

Elementos que pueden cambiar sin necesidad de notificación

Los únicos cambios que pueden realizarse a esta política 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 DPC pueden ser cambiados unilateralmente por la Autoridad de Certificación de DIGITELTS sin preaviso. Las modificaciones pueden traer causa justificativa en motivos legales, técnicos o comerciales.

Cuando corresponda, dichas modificaciones serán notificadas al Organismo de Supervisión correspondiente, 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.

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 Autoridad de Certificación de DIGITELTS.

Las RA podrán ser notificadas directamente mediante correo electrónico o telefónicamente en función de la naturaleza de los cambios realizados.

9.12.2 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.

9.12.3 Circunstancias en las que el OID debe ser cambiado

Se procederá al cambio de OID en aquellas circunstancias que se altere alguno de los procedimientos descritos en el presente documento, y que afecte directamente al modo operativo de alguna de las entidades participantes.

9.13 Reclamaciones y resolución de conflictos

La Autoridad de Certificación de DIGITELTS establece, en el contrato de suscriptor, y en la PDS, los procedimientos de mediación y resolución de conflictos aplicables.

9.14 Normativa aplicable

La Autoridad de Certificación de DIGITELTS establece, en el contrato de suscriptor y en la PDS, que la legislación aplicable a la prestación de los servicios, incluyendo las prácticas de

certificación, 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.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
- 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.

Añadir que las prácticas de los servicios de confianza de la Autoridad de Certificación de DIGITELTS siguen las directrices de los siguientes estándares:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles.
- ETSI EN 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles
- 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 Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev

9.15 Cumplimiento de la normativa aplicable

La Autoridad de Certificación de DIGITELTS 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 Autoridad de Certificación de DIGITELTS 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.

9.16 Otras disposiciones

9.16.1 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

La Autoridad de Certificación de DIGITELTS establece, en el contrato de suscriptor, y en la PDS, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la Autoridad de Certificación vela porque, al menos los requisitos contenidos en las secciones 12.1 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 8.9 (Confidencialidad), continúen vigentes tras la terminación del servicio y de las condiciones generales de emisión/uso.

- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

9.17 Otras provisiones

Sin estipulación