

CONFIRMACIÓN DE DATOS DE SOLICITUD DEL CERTIFICADO

CONFIRMACIÓN DE DATOS DE SOLICITUD DEL CERTIFICADO

Tipo de Certificado:

DNI/NIE:

Tipo de Documento:

Nombre:

Primer Apellido:

Segundo Apellido:

Correo Electrónico:

Cargo/Otros:

Tipo de Representación - Referencia Documental:

Seudónimo:

Departamento / Unidad Administrativa:

NIF de la Organización:

Nombre de la Organización:

Denominación de Certificado/Sistema:

Correo Electrónico de la Organización:

Firma el presente documento para dejar constancia de que:

Ha sido informado de las circunstancias relativas al tratamiento de sus datos personales para la correcta prestación del servicio de emisión de certificados contratado y de la relación comercial conforme a lo establecido en la Política de Privacidad disponible en el sitio web siguiente: [DIGITEL T.S.MK - Políticas de Privacidad](#)

Ha sido informado del contenido del certificado y de la posibilidad de acceder a la Declaración de Divulgación de PKI del certificado o PDS en la dirección electrónica: <https://pki.digitelts.es/>

Ha sido informado del régimen de ejercicio de su derecho de desistimiento del servicio, así como del régimen obligatorio de uso del certificado, por medio de unos términos contractuales, los cuales entiende y acepta, y constan a continuación como parte inseparable de este documento.

DIGITELTS

by MADISON®

TÉRMINOS Y CONDICIONES

Servicio de emisión de certificados cualificados

Elaborado por:	Dpto. Seguridad
Revisado por:	CRS
Aprobado por:	CRS Fecha: 23/07/2026
Código:	DIGITEL TS_T&C_Servicio_QCERT-ES
Versión:	1.0
Fecha:	21/05/2026
Clasificación	Público
Estado	Aprobado

Control de ediciones

Fecha	Versión	Descripción	Autor
21/05/2026	1.0	Primera versión del documento aplicable a todos los tipos de certificados cualificados expedidos por DIGITEL TS	DIGITEL TS

DERECHOS DE USO:

La presente documentación es propiedad de DIGITEL ON TRUSTED SERVICES (DIGITEL TS) y no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquiera otro medio/formato. Asimismo, tampoco podrá ser objeto de préstamo, alquiler o cualquier forma de cesión de uso sin el permiso previo y escrito de DIGITEL TS, titular del copyright. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será perseguido conforme a ley.

ÍNDICE

CONFIRMACIÓN DE DATOS DE SOLICITUD DEL CERTIFICADO.....	1
1. DEFINICIONES APLICABLES AL CONTRATO.....	5
2. TIPOS DE CERTIFICADOS BAJO LOS PRESENTES TÉRMINOS Y CONDICIONES GENERALES	7
3. OBJETO	8
4. MARCO LEGAL DE LA PRESTACIÓN DEL SERVICIO	8
5. DURACIÓN DEL CONTRATO	9
6. CONTRAPRESTACIÓN.....	9
7. ACEPTACIÓN DEL CERTIFICADO.....	9
8. OBLIGACIONES DE LA AC.....	9
9. OBLIGACIONES DEL SOLICITANTE Y DEL TITULAR/FIRMANTE DEL CERTIFICADO	11
10. OBLIGACIONES DE LA ENTIDAD SUSCRIPTORA.....	11
11. LIMITES DE USO SEGÚN EL FIN PROPIO DEL CERTIFICADO	11
12. PROHIBICIÓN DE REALIZAR COMERCIO CON EL CERTIFICADO	12
13. DERECHO DE DESISTIMIENTO.....	12
14. RESPONSABILIDADES.....	12
15. MODIFICACIONES	14
16. DISPONIBILIDAD DEL SERVICIO.....	14
17. QUEJAS Y SUGERENCIAS	14
18. INFORMACIÓN PARA PARTES QUE CONFÍAN	14
19. PROTECCIÓN DE DATOS.....	15
20. RESOLUCIÓN DEL CONTRATO	17
21. LEGISLACIÓN Y JURISDICCIÓN.....	18
22. OTRAS OBLIGACIONES DE LA AC	19
23. OTRAS OBLIGACIONES DEL TITULAR/FIRMANTE Y DEL TITULAR/SUSCRIPTOR.....	19
24. TÉRMINOS Y CONDICIONES APLICABLES A VÍDEO-IDENTIFICACIÓN DESASISTIDA	20

1. DEFINICIONES APLICABLES AL CONTRATO

CONTRATO: toda la documentación contractual, los presentes Términos y Condiciones Generales, la Declaración de Prácticas y Políticas de Certificación de los Servicios de Emisión de Certificados Electrónicos de DIGITEL TS y demás documentos que rigen las relaciones entre las Partes.

DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN (en adelante, DPPC): conjunto de prácticas y políticas adoptadas por la Autoridad de Certificación de DIGITEL TS para la emisión de certificados electrónicos donde se encuentra información detallada sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, y sobre la relación de confianza entre las Partes. Se encuentra publicada en la página web de DIGITEL ON TRUSTED SERVICES S.L.U. <https://pki.digitelts.es/>

POLÍTICAS ESPECÍFICAS APLICABLES A LOS CERTIFICADOS: las Políticas específicas de Certificación (CP) aplicables a los certificados electrónicos que emite DIGITEL TS, incluidas en la Declaración de Prácticas y Políticas de Certificación (DPPC) que puede consultarse en la página web: <https://pki.digitelts.es/>. Las Políticas específicas de certificación (CP) se incorporan a estas Condiciones Generales por referencia. En caso de discrepancia, el significado de los términos contenidos en estas condiciones generales prevalecerá respecto de lo que se establece en la DPPC. Los identificadores de política de certificación (OID) aplicables a cada tipo de certificado se incluyen en el propio certificado y se encuentran detallados en la DPPC de DIGITEL TS, conforme a las políticas definidas en ETSI EN 319 411-2 cláusula 5.3: QCP-n, QCP-l, QCP-n-qscd, QCP-l-qscd para certificados cualificados de firma y sello electrónico.

DECLARACIÓN DE DIVULGACIÓN DE PKI o PDS (PKI Disclosure Statement) PARA CERTIFICADOS CUALIFICADOS: resumen y presentación de los puntos principales de la Declaración de Prácticas y Políticas de Certificación para todos los tipos de Certificados cualificados en un formato más legible y comprensible para el beneficio de los suscriptores y partes que confían en la Autoridad de Certificación de DIGITEL TS, conforme a los requisitos del Anexo A de la norma ETSI EN 319 411-1. Se encuentra publicada en la página web de DIGITEL ON TRUSTED SERVICES, S.L.U. <https://pki.digitelts.es/>

DIGITEL ON TRUSTED SERVICES, S.L.U. (en adelante DIGITEL TS): Prestador Cualificado de Servicios de Confianza (Qualified Trust Service Provider o QTSP), de nacionalidad española con sede social en Enrique Cubero 9, Edificio Madison Arena - 47014 Valladolid (España), con NIF B47447560, teléfono +34 91 015 05 10 y correo electrónico de contacto info@digitelts.com, que está sujeto a la supervisión estatutaria del Ministerio para la Transformación Digital y de la Función Pública. DIGITEL TS presta servicios cualificados de confianza conforme al Reglamento (UE) 910/2014 de 23 de julio de 2014, modificado por el Reglamento (UE) 2024/1183 de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital (en adelante, Reglamento eIDAS), y los estándares ETSI EN 319 401; ETSI EN 319 411-1; ETSI EN 319 411-2; ETSI TS 119 431-1 V1.3.1, de acuerdo con sus Informes de evaluación de conformidad elaborados por un Organismo de evaluación de la conformidad acreditado que se puede encontrar en su página: <https://digitelts.es/certificados/>. En la prestación del servicio solicitado, DIGITEL TS actúa como Autoridad de Certificación (en adelante la "AC") relacionando una determinada clave

pública con una persona física o una persona jurídica concreta a través de la emisión de un certificado digital.

AUTORIDAD DE REGISTRO (en adelante, la AR): entidad encargada, entre otras funciones, de verificar la identidad del SOLICITANTE del certificado y en su caso, de las otras circunstancias asociadas al certificado, tal como se regula en la Sección 1.3.2 de la DPPC de DIGITEL TS. Todas o parte de las funciones de AR podrán ser asumidas bien directamente por DIGITEL TS, bien por una AR Delegada. Las funciones de registro de los suscriptores se realizan por delegación y de acuerdo con las instrucciones del Prestador Cualificado de Servicios de Confianza DIGITEL TS, en los términos del artículo 24 apartados 1 y 1 *bis* 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 Cualificado de Servicios de Confianza frente a terceros.

EI SUScriptor: persona física u organización que formaliza una relación contractual con DIGITEL TS para la prestación de servicios de emisión de certificados. En función del tipo de certificado, el suscriptor podrá coincidir con el titular del certificado. En certificados corporativos, el suscriptor podrá ser una organización con o sin personalidad jurídica en cuyo ámbito se emitan certificados a personas físicas vinculadas a las mismas.

EL SOLICITANTE: persona física que solicita la expedición de un certificado para sí misma (con o sin relación de representación o vinculación corporativa a una ENTIDAD) en cuyo caso asumirá la condición de TITULAR/FIRMANTE (certificados de firma electrónica), o para una ENTIDAD en cuyo caso es ésta quien asumirá la condición de TITULAR/SUScriptor (certificados de sello electrónico). En todos los casos, el SOLICITANTE actúa como responsable del certificado.

LA ENTIDAD: es la organización con o sin personalidad jurídica vinculada al TITULAR/FIRMANTE de un certificado por una relación de representación o vinculación corporativa, o es el TITULAR/SUScriptor del certificado en el caso de los certificados de sello electrónico expedidos a organizaciones con personalidad jurídica.

CERTIFICADO CUALIFICADO ó CERTIFICADO: certificado cualificado de firma electrónica, sello electrónico o autenticación de sitio web (según el servicio contratado) expedido por un Prestador Cualificado de Servicios de Confianza de conformidad con los requisitos del Reglamento UE 910/2014 de 23 de julio de 2014 (Reglamento “eIDAS”).

CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA: un certificado de firma electrónica que ha sido expedido por un Prestador Cualificado de Servicios de Confianza y que cumple los requisitos establecidos en el anexo I del Reglamento eIDAS, ofreciendo las máximas garantías legales en cuanto a identificación del firmante y su vinculación con la firma electrónica de manera única, integridad y no repudio de los datos en cuanto están vinculados con la firma electrónica.

CERTIFICADO CUALIFICADO DE SELLO ELECTRÓNICO: certificado de sello electrónico que ha sido expedido por un Prestador Cualificado de Servicios de Confianza y que cumple los requisitos establecidos en el anexo III del Reglamento eIDAS, ofreciendo las máximas garantías legales en cuanto a integridad de los datos y corrección del origen de los datos a los que el sello electrónico esté vinculado.

PARTES QUE CONFÍAN: personas físicas u organizaciones que voluntariamente confían en el certificado emitido por la AC y, por ende, en el servicio de confianza que este respalda.

DISPOSITIVO CUALIFICADO DE CREACIÓN DE FIRMA O SELLO (QSCD): dispositivo cualificado de creación de firma electrónica o de sello electrónico que cumple los requisitos establecidos en el Anexo II del Reglamento eIDAS, certificado por un organismo de certificación designado conforme al artículo 30 del Reglamento eIDAS.

FIRMA REMOTA O SELLO REMOTO: firma electrónica cualificada o sello electrónico cualificado creado mediante un dispositivo cualificado de creación de firma o sello electrónico gestionado a distancia por un Prestador Cualificado de Servicios de Confianza en nombre del firmante o creador del sello, conforme a los artículos 29 bis y 39 bis del Reglamento eIDAS.

DATOS DE ACTIVACIÓN DE FIRMA (SAD): datos necesarios para activar la creación de una firma electrónica o un sello electrónico en el dispositivo cualificado de creación de firma o sello remoto, que están bajo el control exclusivo del firmante o bajo el control del creador del sello.

SERVICIO DE APLICACIÓN DE FIRMA EN SERVIDOR (SSAS): servicio de confianza que consiste en una aplicación de firma en servidor y un QSCD/SCDev para crear un valor de firma digital en nombre del firmante, conforme a ETSI TS 119 431-1.

2. TIPOS DE CERTIFICADOS BAJO LOS PRESENTES TÉRMINOS Y CONDICIONES GENERALES

CERTIFICADO CUALIFICADO DE CIUDADANO: determina la identidad del TITULAR/FIRMANTE únicamente para actuar en su propio nombre. Este tipo de certificados se emite en dispositivo cualificado de creación de firma (QSCD) centralizado, que genera firma cualificada, o bien sin dispositivo QSCD, generando firma avanzada.

CERTIFICADO CUALIFICADO DE PERSONA FÍSICA VINCULADA: determina la relación de vinculación (laboral, mercantil, colegial, etc.) entre el TITULAR/FIRMANTE y la ENTIDAD, pero no de representación legal o voluntaria. Este tipo de certificados se emite en dispositivo cualificado de creación de firma (QSCD) centralizado, que generan firma cualificada, o bien sin dispositivo QSCD, generando firma avanzada.

CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD CON O SIN PERSONALIDAD JURÍDICA: Estos certificados son certificados de representante, con poderes totales, administrador único o solidario de la ENTIDAD, o al menos con poderes específicos generales para actuar ante las Administraciones Públicas españolas. Estos certificados garantizan la identidad del SUScriptor y del TITULAR/FIRMANTE, indican una relación de representación legal o apoderamiento general entre el TITULAR/FIRMANTE y la ENTIDAD. Este certificado incluye un campo donde se indica el documento, público si resulta exigible, que acredita de forma fehaciente las facultades del TITULAR/FIRMANTE para actuar en nombre de la ENTIDAD a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales. Este tipo de certificados se emite en dispositivo cualificado de creación de firma (QSCD) centralizado, que generan firma cualificada, o bien sin dispositivo QSCD, generando firma avanzada.

CERTIFICADO CUALIFICADO DE SELLO ELECTRÓNICO PARA PERSONAS JURÍDICAS: Estos certificados garantizan la identidad del TITULAR/SUScriptor, disfrutarán 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. Este tipo de certificados se emite en dispositivo cualificado de creación

de firma (QSCD) centralizado, que generan sello cualificado, o bien sin dispositivo QSCD, generando sello avanzado.

CERTIFICADO CUALIFICADO DE EMPLEADO PÚBLICO: determina la relación de vinculación entre el TITULAR/FIRMANTE Empleado público y la ENTIDAD (Administración Pública), pero no de representación legal o voluntaria. Este tipo de certificados se emite en dispositivo cualificado de creación de firma (QSCD) centralizado, que generan firma cualificada, o bien sin dispositivo QSCD, generando firma avanzada.

CERTIFICADO CUALIFICADO DE EMPLEADO PÚBLICO CON SEUDÓNIMO: determina la relación de vinculación entre el TITULAR/FIRMANTE Empleado público y la ENTIDAD (Administración Pública), pero no de representación legal o voluntaria. Este tipo de certificado no mostrará información personal de ningún tipo tan sólo un seudónimo y la relación como Empleado público con la ENTIDAD (Administración Pública), se emite en dispositivo cualificado de creación de firma (QSCD) centralizado, que generan firma cualificada, o bien sin dispositivo QSCD, generando firma avanzada.

CERTIFICADO CUALIFICADO DE SELLO ELECTRÓNICO PARA AAPP: Estos certificados garantizan la identidad del TITULAR/SUSCRIPTOR (Administración Pública), disfrutarán 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. Este tipo de certificados se emite en dispositivo cualificado de creación de firma (QSCD) centralizado, que generan sello cualificado, o bien sin dispositivo QSCD, generando sello avanzado.

SECCION I

TERMINOS Y CONDICIONES APLICABLES A TODOS LOS TIPOS DE CERTIFICADOS

3. OBJETO

La emisión por parte de la AC a favor del SOLICITANTE de un Certificado del tipo que figura en el formulario de solicitud y las condiciones de utilización por parte del SOLICITANTE del servicio de emisión de certificados, de conformidad con los términos previstos en el presente contrato, las Políticas Específicas, la Declaración de Prácticas de Digitel TS, el Reglamento eIDAS y las leyes locales.

4. MARCO LEGAL DE LA PRESTACIÓN DEL SERVICIO

El SOLICITANTE declara conocer la Declaración de Prácticas y Políticas de Certificación (DPPC) y la Declaración de Divulgación de PKI (PDS) para Certificados Cualificados disponibles en la página web de DIGITEL TS (<https://pki.digitelts.es/>). Los términos y condiciones del presente documento, junto con la DPPC y la PDS constituyen el marco legal que regulará la relación entre las partes, internamente y frente a terceros, sin perjuicio de lo dispuesto en la legislación vigente.

5. DURACIÓN DEL CONTRATO

El presente contrato entrará en vigor y terminará coincidiendo con las fechas de emisión y caducidad indicadas en el Certificado sin perjuicio de las causas de revocación previstas en los PDS y la DPPC, pudiendo ser renovado con arreglo a los términos establecidos en la DPPC.

El periodo de validez del certificado se determinará conforme a las políticas de certificación aplicables y se indicará expresamente en el certificado. La duración máxima de validez de los certificados cualificados será la establecida en la DPPC de DIGITEL TS.

6. CONTRAPRESTACIÓN

El precio del Certificado, que incluirá la contraprestación por los servicios de DIGITEL TS asociados al mismo, viene definido en la oferta que suscribió el SOLICITANTE al realizar la petición del Certificado y en la factura correspondiente.

Dicho precio deberá ser abonado por el SOLICITANTE o la ENTIDAD, a la AC o AR, con carácter previo a la entrega del Certificado salvo acuerdo distinto establecido en la oferta suscrita.

7. ACEPTACIÓN DEL CERTIFICADO

El SOLICITANTE acepta el Certificado de forma expresa, confirmando y asumiendo la exactitud de su contenido, con las consiguientes obligaciones que de ello se deriven frente a la AR, la AC o cualquier tercero que de buena fe confíe en el contenido del Certificado, en virtud de la DPC y/o legislación vigente. En caso de que existiera alguna diferencia entre los datos suministrados a la AC y el contenido del Certificado, o se detecte el defecto, ello deberá ser comunicado de inmediato a la AC o a la AR por el SOLICITANTE o por la ENTIDAD, para que proceda a su revocación.

En el supuesto de que un TITULAR/FIRMANTE a quien se haya emitido un certificado cese en su vinculación con el SUSCRIPTOR, dicho SUSCRIPTOR se obliga a solicitar inmediatamente la revocación del certificado.

8. OBLIGACIONES DE LA AC

- a. Emitir, entregar, administrar, revocar y renovar certificados de acuerdo con lo establecido en su Declaración de Prácticas y Políticas de Certificación.
- b. Comunicar al SOLICITANTE o a la ENTIDAD la revocación de su Certificado o del cual es el responsable, cuando ésta se produzca, explicando los motivos, la fecha y hora en que el certificado quedará sin efecto de acuerdo con los procedimientos definidos en la DPPC. Por motivos de seguridad, la AC podrá realizar la revocación de un certificado de forma unilateral e inmediata sin que el TITULAR/FIRMANTE o la ENTIDAD pueda reclamar ningún tipo de indemnización por este hecho. DIGITEL TS sustituirá el certificado por uno válido siempre y cuando la anomalía haya podido ser corregida.
- c. Mantener actualizadas la base de datos de certificados en vigor y certificados revocados.

- d. Tramitar las solicitudes de revocación de certificados lo antes posible.
- e. Proporcionar a través del servicio OCSP la información sobre el estado de revocación de los certificados que han caducado sin límite de tiempo después de su expiración.
- f. En caso de compromiso de la clave privada de la AC, DIGITEL TS proporcionará la información sobre el estado de revocación de los certificados emitidos por la AC por medio del servicio OCSP de una nueva AC, de acuerdo con lo establecido en su Declaración de Prácticas y Políticas de Certificación.
- g. En caso de finalización del servicio prestado por DIGITEL TS con transferencia de gestión de certificados a otro Prestador Cualificado de Servicios de Confianza, DIGITEL TS transferirá también al nuevo Prestador la obligación de proporcionar la información sobre el estado de revocación de los certificados emitidos por la AC por medio del servicio OCSP de una AC del nuevo Prestador, de acuerdo con lo establecido en su Declaración de Prácticas y Políticas de Certificación.
- h. En caso de finalización del servicio prestado por DIGITEL TS sin transferencia de gestión de certificados a otro Prestador Cualificado de Servicios de Confianza, la AC emitirá la última CRL que se mantendrá custodiada y disponible por otra parte confiable a la que DIGITEL TS transfiera esta obligación, para seguir proporcionando a través de ella la información sobre el estado de revocación de los certificados, de acuerdo con lo establecido en su Declaración de Prácticas y Políticas de Certificación.
- i. Identificar, por medio de la AR, correctamente al SOLICITANTE, conforme a los procedimientos que se establecen en la DPPC.
- j. Si procede, comprobar los datos relativos a la constitución y personalidad jurídica de la ENTIDAD y a la relación de representación o de pertenencia corporativa del SOLICITANTE con ésta, conforme a los procedimientos que se establecen en la DPPC.
- k. Archivar y conservar la información relativa a los datos expedidos y recibidos durante 15 años desde la expiración del Certificado o la finalización del servicio prestado. Esta actividad de registro podrá realizarse por medios electrónicos.
- l. Proceder, por medio de la AR, a la entrega del Certificado al SOLICITANTE conforme las condiciones definidas en la DPPC, una vez realizadas las comprobaciones anteriores.
- m. Ejecutar el servicio con los medios técnicos y materiales adecuados, y con personal que cumpla las condiciones de cualificación y experiencia establecidas en la DPPC.
- n. Cumplir los niveles de calidad del servicio, en conformidad con lo que se establece en la DPPC, en los aspectos técnicos, operativos y de seguridad.
- o. Aplicar procedimientos y mecanismos de seguridad apropiados para la gestión de riesgos de ciberseguridad, conforme a la Directiva NIS2 y el Reglamento de Ejecución (UE) 2024/2690.
- p. Notificar al órgano de supervisión cualquier cambio en la prestación de sus servicios cualificados de confianza con al menos un mes de antelación, conforme al artículo 24.2.a) del Reglamento eIDAS, o tres meses en caso de intención de cese de actividad.
- q. Disponer de un plan de terminación actualizado para garantizar la continuidad del servicio, conforme al artículo 24.2.i) del Reglamento eIDAS.
- r. Disponer de canales de comunicación para la atención de clientes y terceros para solicitudes, incidencias, consultas, quejas y reclamaciones y atender a las mismas en un plazo razonable.
- s. Conservar toda la información asociada a la prestación del servicio con los niveles de protección exigibles.
- t. Disponer de un seguro de responsabilidad civil para cubrir los riesgos derivados del servicio conforme al artículo 24.2 c) del Reglamento eIDAS y al artículo 9.3 b) de la Ley 6/2020.

- u. Seleccionar proveedores de servicios y subcontratistas que ofrezcan garantías de ciberseguridad conformes a la legislación aplicable, y exigir que propaguen los requisitos de seguridad de DIGITEL TS a lo largo de su cadena de suministro.
- v. Llevar a cabo las auditorías periódicas necesarias, cada dos años, para asegurar la adecuación y cumplimiento de la normativa aplicable, e informar al organismo de supervisión al menos un mes antes de cualquier auditoría prevista, permitiendo su participación como observador, conforme al artículo 20.1 bis del Reglamento eIDAS.

9. OBLIGACIONES DEL SOLICITANTE Y DEL TITULAR/FIRMANTE DEL CERTIFICADO

- a. Custodiar el Certificado y las claves secretas, Password, pines o datos de activación de firma o sello de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado, manteniendo el control exclusivo sobre los datos de creación de firma electrónica o el control sobre los datos de creación de sello electrónico.
- b. Solicitar la revocación del Certificado cuando se cumpla alguno de los supuestos de revocación de certificados previstos en la DPPC y en la legislación vigente.
- c. No revelar la clave privada.
- d. Suministrar toda la información y documentación exigida, responsabilizándose de su veracidad y corrección.
- e. Notificar inmediatamente a la AC en caso de que detecte que se ha incluido cualquier información incorrecta o inexacta o en caso de que, de forma sobrevenida, la información del Certificado no se corresponda con la realidad.
- f. Informar inmediatamente a la AC acerca de cualquier situación que pueda afectar a la validez del Certificado, o a la seguridad de las claves.
- g. Utilizar el Certificado conforme a la Ley y a los límites fijados por la DPPC y el propio Certificado según su tipo.
- h. Emplear el par de claves únicamente para los fines autorizados por el tipo de certificado (firma electrónica o sello electrónico, según corresponda),
- i. Cualquier otra que se derive del contenido de la DPPC con relación a cada tipo de certificado.

10. OBLIGACIONES DE LA ENTIDAD SUSCRIPTORA

Serán también de aplicación a la ENTIDAD las obligaciones b., d., e., f., g. y h. del SOLICITANTE, que podrá ejercer a través de su representante legal.

11. LIMITES DE USO SEGÚN EL FIN PROPIO DEL CERTIFICADO

Cada tipo de certificado está destinado a una persona concreta (persona física o jurídica) y responde a unas funciones propias que vienen definidas en la DPC de DIGITEL TS. En la medida que los certificados cualificados pueden contener atributos específicos del TITULAR/FIRMANTE o del TITULAR/SUSCRIPTOR, la AR realiza previamente a su emisión, las comprobaciones necesarias que permiten acreditar de forma fehaciente dichos atributos (relación de representación,

pertenencia corporativa, colegiación, etc.). En el caso de los certificados de firma electrónica con atributo de representación de entidad, se consigna en el Certificado las referencias del documento en base al cual se ha acreditado ante la AR que las facultades de representación del TITULAR/FIRMANTE se ajustan al fin del Certificado. Pero es responsabilidad del TITULAR/FIRMANTE el uso adecuado de su certificado conforme a su fin y a las facultades de representación que le han sido otorgadas y es responsabilidad de los terceros que confían comprobar el fin del certificado y sus eventuales limitaciones en su uso.

12. PROHIBICIÓN DE REALIZAR COMERCIO CON EL CERTIFICADO

La contratación del servicio de emisión de certificados con DIGITEL TS admite solamente el uso del Certificado en el ámbito de actividad del SOLICITANTE o de la ENTIDAD, de acuerdo con la finalidad del tipo de certificado solicitado. Una vez emitido el Certificado, el SOLICITANTE o la ENTIDAD no podrán, salvo acuerdo específico entre las partes, hacer un uso con fines comerciales del Certificado. Se entiende por uso comercial del Certificado, cualquier actuación mediante la cual el SOLICITANTE o la ENTIDAD ofrece a terceras personas ajenas al presente contrato, a título oneroso o gratuito, servicios que requieren el uso del Certificado expedido.

El servicio de emisión de certificados de Digitel TS no ha sido diseñado ni permite su utilización como equipos de control de situaciones peligrosas, o para usos que requieran actuaciones a prueba de errores, como por ejemplo la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tránsito aéreo o sistemas de control de armamento, donde un error pudiera directamente causar la muerte, daños físicos o daños medioambientales graves.

El incumplimiento de la presente cláusula facultará a la AC a revocar el Certificado y a reclamar la indemnización de los daños y perjuicios que se le hubieren causado por el incumplimiento, incluyendo lucro cesante y daños indirectos.

La AC no acepta responsabilidad por daños derivados del uso del servicio que excedan las limitaciones indicadas en estos términos y condiciones, conforme al artículo 13.2 del Reglamento eIDAS y ETSI EN 319 401 REQ-6.2-02 b).

13. DERECHO DE DESISTIMIENTO

El suministro del Certificado al SOLICITANTE o a la ENTIDAD bien mediante su entrega para descargar en soporte software, bien mediante su entrega en soporte dispositivo cualificado de creación de firma (QSCD) centralizado, supone el comienzo de la ejecución del contrato, con lo que, conforme lo permite la Ley General para la Defensa de los Consumidores y Usuarios (RDL 1/2007) en dichos casos, el SOLICITANTE y la ENTIDAD pierden su derecho de desistimiento.

14. RESPONSABILIDADES

La AC y, en su caso, la AR responderán de las funciones que les correspondan conforme a la DPPC y, en especial, asumirán toda la responsabilidad por la correcta comprobación de la identidad del SOLICITANTE, y en su caso de la ENTIDAD y otras circunstancias procedentes.

DIGITEL TS mantiene recursos financieros suficientes y/o un seguro de responsabilidad civil apropiado, de conformidad con la legislación aplicable, para cubrir las responsabilidades derivadas de sus operaciones y actividades. La cobertura mínima asegurada es de 3.000.000 de euros.

La AC y la AR no serán responsables de los daños derivados de o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del SOLICITANTE, de la ENTIDAD y/o Terceros usuarios, ni de la incorrecta utilización de los Certificados y las claves, ni de cualquier daño indirecto que pueda resultar de la utilización del Certificado o de la información suministrada por la AC, en particular, el lucro cesante, la pérdida de ingresos o pedidos o pérdida de datos, no dando lugar a ningún tipo de derecho indemnizatorio.

Ni la AC ni la AR serán responsables ante el TITULAR/FIRMANTE o TITULAR/SUSCRIPTOR ni ante terceros del uso inadecuado o fraudulento del Certificado en caso de que el TITULAR/FIRMANTE o TITULAR/SUSCRIPTOR lo haya cedido o haya autorizado su uso a favor de una tercera persona, siendo exclusiva responsabilidad del TITULAR/FIRMANTE o TITULAR/SUSCRIPTOR el control de las claves asociadas a su certificado.

Ni la AC ni la AR serán responsables de las eventuales inexactitudes en el Certificado que resulten de la información facilitada por el SOLICITANTE, a condición de haber actuado siempre con la máxima diligencia exigible.

Ni la AC, ni la AR, asumirán responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones en virtud de la DPPC si tal falta de ejecución o retraso resultara o fuera consecuencia de un supuesto de fuerza mayor, caso fortuito o, en general, cualquier circunstancia sobre la que la AC no pueda tener un control razonable y entre otros: los desastres naturales, la guerra, el estado de sitio, las alteraciones de orden público, la huelga en los transportes, el corte de suministro eléctrico y/o telefónico, los virus informáticos, deficiencias en los servicios de telecomunicaciones, violaciones de seguridad del sistema de certificación o cualquier perjuicio que se derive de un hecho causado por un avance imprevisible de la técnica.

Ni la AC ni la AR, serán responsables del contenido de aquellos documentos firmados o cifrados digitalmente.

La AC y la AR, no se responsabilizarán por el correcto funcionamiento con aplicaciones que no estén aprobadas, y por daños generados por la imposibilidad del uso con dichas aplicaciones.

Tampoco serán responsables ni la AC ni la AR por deterioros o averías en los equipos informáticos o en los datos por causas no imputables directamente a la utilización de los Certificados o a la instalación del certificado, y siempre que el SOLICITANTE no actúe con la diligencia necesaria.

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 DIGITEL TS responderá en el supuesto de actuación negligente en el cumplimiento de las obligaciones asumidas será de SEIS MIL EUROS (6.000€) por certificado, salvo que se hubiera acordado expresamente un límite superior.

15. MODIFICACIONES

La AC podrá modificar el presente contrato, así como la DPPC o cualquiera de sus cláusulas en los términos previstos en la misma, comunicándolo al SOLICITANTE o al SUSCRIPTOR, cuando el cambio incida directamente en sus derechos y obligaciones, con 15 días de antelación, debiendo explicar, en todo caso, los motivos de tal decisión. El SOLICITANTE o el SUSCRIPTOR podrá optar entre la resolución del contrato o la novación de este conforme a los nuevos términos. El SOLICITANTE o el SUSCRIPTOR dispondrá de un máximo de 15 días a partir de la fecha de dicha comunicación para comunicar a la AC la aceptación de la subrogación o de las modificaciones efectuadas. No obstante, si pasado ese período la AC no ha recibido por parte del SOLICITANTE o del SUSCRIPTOR comunicación escrita de lo contrario, se entenderán como aceptadas la subrogación y las modificaciones efectuadas.

16. DISPONIBILIDAD DEL SERVICIO

La solicitud y/o la consulta del estado del Certificado están disponibles las 24 horas del día, los 7 días de la semana y 365 días al año conforme se indica en las secciones 2.1 y 4.9.9 y 4.10.2 de la DPPC.

DIGITEL TS garantiza una disponibilidad del servicio de consulta del estado de los certificados (OCSP y CRL) de al menos el 99% del tiempo, conforme a los niveles de servicio establecidos en la DPPC. El periodo durante el cual DIGITEL TS retiene los registros de eventos del servicio se establece conforme a la DPPC y la legislación aplicable, siendo de al menos 15 años.

No obstante, podrá interrumpirse de manera temporal por razones de mantenimiento, actualización o mejora del sistema, previa comunicación al SUSCRIPTOR con una antelación razonable. En casos de emergencia o incidente de seguridad, DIGITEL TS se reserva el derecho de interrumpir el servicio de manera inmediata para proteger la integridad de las evidencias y la seguridad de los usuarios.

17. QUEJAS Y SUGERENCIAS

Cualquier parte interesada en realizar una sugerencia, queja o reclamación referente al servicio de emisión de certificados de DIGITEL TS, podrá hacerlo a través de la cuenta de correo electrónico info@digitelts.com o a través de la siguiente url: <https://digitelts.es/contacto/>

En todo caso, DIGITEL TS dispone de un plazo máximo de 30 días para atender la queja o reclamación formulada.

18. INFORMACIÓN PARA PARTES QUE CONFÍAN

Las partes que confían en los certificados emitidos por DIGITEL TS deben verificar la validez del Certificado consultando los servicios de comprobación de estado (OCSP o CRL) antes de confiar en el mismo. La información de estado de los certificados está disponible en los puntos de distribución indicados en el propio certificado y en <https://pki.digitelts.es/>. Las partes que confían

deben verificar toda la cadena de certificados antes de confiar en una firma digital o en alguno de los certificados de la jerarquía.

Las partes que confían deben tener en cuenta cualquier limitación de uso del Certificado, independientemente de que se encuentre en el propio Certificado o en los presentes términos y condiciones, así como el periodo de validez asociado al Certificado.

19. PROTECCIÓN DE DATOS

De conformidad con lo establecido en el Reglamento UE 2016/679 de 27 de abril de 2016 General de Protección de Datos, y la Ley Orgánica 3/2018, le facilitamos la siguiente información relativa al tratamiento de sus datos personales en el marco de la prestación del servicio de emisión de certificados:

Responsable del tratamiento:

DIGITEL ON TRUSTED SERVICES, S.L.U.

NIF: B47447560

Dirección postal: C/ Enrique Cubero 9, Edificio Madison Arena - 47014 – Valladolid (España)

Teléfono: +34 91 015 05 10

Mail: dpo@madisonmk.com

Finalidad del tratamiento:

El tratamiento de sus datos personales servirá a los usos previstos propios de la prestación del servicio de confianza contratado, lo cual incluye la identificación fehaciente del SOLICITANTE del Certificado, la emisión del Certificado solicitado y la conservación de las evidencias generadas por el servicio durante el período legalmente exigido. Asimismo, se utilizarán para la gestión administrativa, técnica y contractual del servicio, incluida su facturación.

DIGITEL TS obtiene los datos personales que figuran en los ficheros por varios procedimientos:

- Por cesión de los datos por parte del SUSCRIPTOR a través del SOLICITANTE, que debe haberlos obtenido legalmente, en las condiciones previstas en la normativa sobre firma electrónica y sobre protección de datos de carácter personal.
- Directamente del TITULAR/FIRMANTE, cuando el registro de sus datos es efectuado por la AC de DIGITEL TS o por sus intermediarios autorizados.

Para el servicio de emisión de certificados, los datos personales serán incluidos en el directorio de claves públicas de firma electrónica necesario para comprobar la validez del certificado electrónico así como en el directorio de certificados revocados, de forma que tendrán un tratamiento automatizado para poder ser accesibles para su consulta por todos los usuarios del sistema, es decir las personas que voluntariamente confían y hacen uso de los certificados, siempre de acuerdo con lo establecido en la PDS y la DPPC de DIGITEL TS.

Conforme a la regulación aplicable en materia de certificación electrónica, la mecánica del sistema de certificación y de internet, obligan a que los usuarios del sistema puedan acceder a sus datos personales desde cualquier lugar del mundo, por lo que se le informa que, si contrata el servicio, sus datos estarán disponibles para su consulta por los usuarios del sistema, quedando

DIGITEL TS exonerada de cualquier responsabilidad derivada de un uso indebido de los mismos por parte de terceros.

No se elaborarán perfiles en base a la información facilitada ni se tomarán decisiones automatizadas.

En el marco de procesos de verificación de identidad a distancia de SOLICITANTES de certificados, DIGITEL TS podrá utilizar vídeo-identificación desasistida. En consecuencia, requerirá tratar otros datos personales del usuario, concretamente datos biométricos. Previo a la verificación de identidad por esta modalidad del servicio DIGITEL TS pondrá a disposición del SOLICITANTE del certificado la información de protección de datos personales y recabará su consentimiento para el tratamiento de los citados datos.

Plazos de Conservación:

Los datos proporcionados se conservarán en formato electrónico y/o en formato papel, mientras se mantenga la relación comercial y durante los años necesarios para cumplir con las obligaciones legales de registro y acceso, en particular las definidas en el artículo 9.3 de la Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza (15 años) y del Reglamento UE N°910/2014.

En el marco de la identificación a distancia por vídeo-identificación DIGITEL TS conservará por 15 años las evidencias de procesos de identificación exitosos y por 5 años las evidencias de aquellos procesos de identificación por vídeo que hayan resultado fallidos conforme a lo establecido en la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados, modificada por la Orden ETD/743/2022, de 26 de julio.

Legitimación del tratamiento:

La base jurídica para el tratamiento de sus datos personales se encuentra bien en:

- i. la relación contractual establecida en virtud de los servicios contratados a DIGITEL TS según las condiciones de uso que constan con la suscripción de los servicios,
- ii. el objeto mismo de la prestación de expedición de certificados electrónicos que requiere vincular datos de validación de firma con una persona física,
- iii. la obligación legal que se impone a los Prestadores Cualificados de Servicios de Confianza que expiden certificados cualificados de servicios de confianza de verificar la identidad y otros atributos de la persona física a la que se le expide un certificado cualificado (Ley 06/2020 y Reglamento UE N°910/2014) y de registrar y mantener accesible dichos datos durante el plazo legal estipulado (15 años).
- iv. El consentimiento del SOLICITANTE para que sus datos personales biométricos sean tratados en el marco de procesos de verificación de identidad a distancia mediante vídeo-identificación.

Les avisamos que la contratación de nuestros servicios obliga al cliente a facilitar sus datos personales, incluso en caso de uso de seudónimo, por lo que, si no consiente al tratamiento de sus datos personales, no se le podrá prestar el servicio.

Destinatarios (cesiones y transferencias):

Para prestar sus servicios de emisión de certificados, DIGITEL TS podrá delegar a una tercera entidad las labores de registro. Dicha entidad en su condición de Autoridad de Registro dentro del sistema de certificación de DIGITEL TS, tendrá la consideración de Encargada del tratamiento al tener acceso a los datos que ha facilitado a DIGITEL TS, para el cumplimiento único y exclusivo de sus labores de registro cuando éstas sean necesarias para prestar el servicio contratado.

No se cederán sus datos personales a terceros salvo obligación legal, ni se transferirán a terceros países u organización internacional.

Derechos de las personas interesadas:

Las personas que hayan facilitados sus datos tienen derecho a:

- Conocer si sus datos personales están siendo tratados por DIGITEL TS.
- Acceder a sus datos personales y solicitar su rectificación o supresión, por ejemplo, si los datos ya no son necesarios para los fines por los que fueron recogidos.
En caso de solicitar la rectificación o supresión de sus datos personales de nuestras bases de datos, se le informa que los certificados electrónicos emitidos a su nombre y vigentes en aquel momento deberán ser revocados por DIGITEL TS. DIGITEL TS conservará copia de dichos datos únicamente con el fin de dar cumplimiento a las obligaciones legales sobre plazos de conservación y para el ejercicio o defensa de reclamaciones.
- Solicitar la limitación del tratamiento de sus datos a la finalidad principal por la que fueron cedidos a DIGITEL TS, retirando su consentimiento a su tratamiento para fines informativos o de prospección comercial. Dicha solicitud no afectará a la licitud del tratamiento previo basado en la necesidad contractual de tratar sus datos.
- Solicitar la portabilidad de sus datos personales a favor de otro responsable.

Para ejercer sus derechos, podrá utilizar alguna de las dos opciones:

- De forma telemática enviando un email a dpo@madisonmk.com con el asunto "Protección de Datos".
- Mediante correo postal enviando un escrito a "DPO" C/ Enrique Cubero 9, Edificio Madison Arena - 47014 Valladolid (España), con la Referencia "Protección de Datos".

En caso de no haber obtenido satisfacción a la solicitud de ejercicio de sus derechos, podrán presentar una reclamación ante la Autoridad de Control en materia de Protección de Datos, dirigiéndose a la Sede Electrónica de la Agencia Española de Protección de Datos.

Pueden consultarse otros detalles sobre como se tratan sus datos personales en la Política de privacidad de DIGITEL TS disponible en el sitio web siguiente: [DIGITEL T.S.MK - Políticas de Privacidad](#)

20.RESOLUCIÓN DEL CONTRATO

El incumplimiento de las estipulaciones contenidas en el presente contrato y/o en la DPPC por cualquiera de las partes será causa de resolución del presente contrato. En tal caso, la parte no incumplidora tendrá derecho a resolver el contrato con efecto inmediato. El incumplimiento por

parte del SOLICITANTE o de la ENTIDAD dará derecho a la AC a revocar el Certificado, con independencia de los daños y perjuicios que pudiera reclamar.

La AC tendrá derecho a revocar y no renovar el Certificado con anterioridad al plazo previsto de vigencia en los casos previstos en la DPPC. Cuando la revocación sea injustificada, la AC podrá indemnizar a aquellos SOLICITANTES o ENTIDADES que lo soliciten por escrito dentro de los tres meses siguientes a la fecha de revocación. Esta indemnización no podrá ser superior a lo pagado por el propio SOLICITANTE por la obtención del referido Certificado.

EL SOLICITANTE o la ENTIDAD podrá resolver libremente el presente contrato en cualquier momento mediante la notificación por escrito con una antelación de 30 días. En ningún caso, dicha resolución dará derecho a la devolución de las cantidades abonadas por la obtención del Certificado.

Si el ejercicio de los derechos de oposición o cancelación de los datos personales dificultase la prestación de servicios objeto de este contrato, DIGITEL TS quedará facultada para resolver el presente contrato.

21. LEGISLACIÓN Y JURISDICCIÓN

El presente contrato y la DPPC se regirán por la Ley española y europea en materia de emisión de certificados cualificados aplicable en cada momento y, con arreglo a la cual deberá ser interpretado su contenido.

Para la resolución de cualquier conflicto que pudiera surgir en relación con este contrato, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a la jurisdicción de los Tribunales de la ciudad de Valladolid (España).

SECCION II

TÉRMINOS Y CONDICIONES APLICABLES A LOS CERTIFICADOS DE FIRMA Y SELLO ELECTRÓNICOS REMOTOS

El Reglamento eIDAS regula la posibilidad de confiar a un tercero los dispositivos cualificados de creación de firmas y sellos electrónicos, a condición de que se apliquen los procedimientos y mecanismos adecuados para garantizar que el firmante tiene el control exclusivo del uso de sus datos de creación de firma electrónica, que el creador del sello tiene el control del uso de sus datos de creación de sello electrónico, y que la utilización de los dispositivos cumple los requisitos de la firma electrónica cualificada y del sello electrónico cualificado. Así posibilita la creación de firmas y sellos electrónicos a distancia en un entorno de creación de firma y sello electrónico gestionado por un Prestador Cualificado de Servicios de Confianza en nombre del firmante o del creador del sello, para el cual se aplica procedimientos de seguridad de la gestión y administrativos específicos y se utilizan sistemas y productos fiables, incluidos canales de comunicación electrónica seguros para garantizar que el entorno de creación de firmas y sellos electrónicos es fiable y se utiliza bajo el control exclusivo del firmante o bajo el control del creador del sello (artículos 29 *bis* y 39 *bis* del Reglamento eIDAS).

El servicio de creación de firmas y sellos electrónicos remotos de DIGITEL TS opera conforme a la política EUSPv2 (EU SSAS Policy v2) definida en ETSI TS 119 431-1, que incluye los requisitos específicos del Reglamento (UE) 2024/1183 relativos a la gestión de QSCD remotos. El OID de esta política es: 0.4.0.19431.1.1.4.

22. OTRAS OBLIGACIONES DE LA AC

- a. La AC deberá aplicar procedimientos de seguridad de la gestión y administrativos específicos y utilizar sistemas y productos fiables, incluidos canales de comunicación electrónica seguros para garantizar que el entorno de creación de firmas y sellos electrónicos es fiable y se utiliza bajo el control exclusivo del firmante o bajo el control del creador del sello. El QSCD deberá operarse en su configuración conforme a la documentación de certificación correspondiente o en una configuración equivalente que alcance el mismo objetivo de seguridad. En cualquier caso, la garantía de la AC al respecto se limita al correcto funcionamiento del procedimiento de firma remota p sello remoto de acuerdo con el nivel de servicio contratado.
- b. La AC deberá custodiar los datos de creación de firma electrónica o sello electrónico en nombre del firmante o creador del sello y protegerlos frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad para el firmante o creador del sello. Las claves de firma del firmante o del creador del sello se generarán y utilizarán únicamente dentro de un QSCD.
- c. Por sus características técnicas y de usabilidad, el certificado remoto requiere el uso de servicios APIRest y/o aplicaciones específicas para su uso. Dichos complementos se proporcionarán al usuario durante el proceso de emisión del Certificado y son por tanto parte del servicio.

La AC solo podrá duplicar los datos de creación de firma electrónica o sello electrónico con fines de copia de seguridad, siempre que: (i) la seguridad de los conjuntos de datos duplicados sea del mismo nivel que la de los conjuntos de datos originales; y (ii) el número de conjuntos de datos duplicados no supere el mínimo necesario para garantizar la continuidad del servicio, conforme al artículo 29 bis 1.b) del Reglamento eIDAS.

La AC cumplirá con cualquier requisito identificado en el informe de certificación del dispositivo cualificado de creación de firma o sello remoto específico utilizado.

23. OTRAS OBLIGACIONES DEL TITULAR/FIRMANTE Y DEL TITULAR/SUSCRIPTOR

- a. El TITULAR deberá custodiar sus datos de activación de firma (SAD) de manera diligente y aplicar todas las medidas apropiadas destinadas a evitar daños a terceros como resultado del uso de firmas electrónicas o sellos electrónicos o procesos de autenticación. Las herramientas de autenticación para la activación del procedimiento de firma remota o sello remoto son estrictamente personales, por lo que se requiere que el TITULAR protejan el secreto de tales herramientas al no divulgarlas a terceros en su totalidad o en parte y al almacenarlas de manera segura, manteniendo el control exclusivo (en el caso de certificados de firma electrónica) o el control (en el caso de certificados de sello electrónico) sobre los datos de activación de firma.

- b. En caso de que el TITULAR cediera el uso de su certificado a favor de otra persona en base a las normas generales del negocio jurídico del mandato o las normas reguladoras del apoderamiento y de las delegaciones de funciones, el TITULAR será el único responsable frente a terceros o frente a la ENTIDAD que representa si no está debidamente autorizado para ello, de las consecuencias que un uso indebido del Certificado pueda generar, ello sin perjuicio de las acciones contra la persona que haya podido extralimitarse de los límites de uso autorizados.
- c. El TITULAR deberá actualizar sus sistemas de hardware y software para cumplir con los requisitos de seguridad exigidos por las leyes aplicables.
- d. El TITULAR/FIRMANTE reconoce que la firma electrónica cualificada generada mediante el servicio de firma remota tiene efectos jurídicos equivalentes a una firma manuscrita, conforme al artículo 25.2 del Reglamento eIDAS, siempre que se haya utilizado un QSCD certificado y se cumplan los requisitos establecidos.
- e. El TITULAR autoriza expresamente a DIGITEL TS a generar y gestionar los datos de creación de firma electrónica o de sello electrónico en su nombre, así como a duplicar dichos datos únicamente con fines de copia de seguridad en los términos establecidos en estos términos y condiciones, conforme al artículo 29 bis del Reglamento eIDAS.

SECCION III

TERMINOS Y CONDICIONES APLICABLES A

VÍDEO-IDENTIFICACIÓN PARA LA EMISIÓN DE CERTIFICADOS CUALIFICADOS DE FIRMA

24.TÉRMINOS Y CONDICIONES APLICABLES A VÍDEO-IDENTIFICACIÓN DESASISTIDA

El SOLICITANTE manifiesta que acepta la realización del proceso de vídeo-identificación desasistida para la emisión de certificados cualificados de la Autoridad de Certificación de DIGITEL TS y utilizará el Servicio de vídeo-identificación desasistida de conformidad con las condiciones adjuntas y la Declaración de Prácticas y Políticas de Certificación de la Autoridad de Certificación de DIGITEL TS y con arreglo a la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados y normas concordantes, consintiendo la grabación íntegra de su imagen y voz y la obtención de otras evidencias durante el proceso de registro, así como el tratamiento y conservación de categorías especiales de datos personales (datos biométricos) y la no aplicación de derecho de desistimiento una vez el servicio haya sido completamente ejecutado, de acuerdo con lo dispuesto en el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

Estos términos y condiciones se establecen con el fin de proporcionar información clara y comprensible a los SOLICITANTES sobre el servicio de vídeo-identificación desasistida, de las recomendaciones de seguridad aplicables y de la información sobre privacidad, según se establece en las normas de aplicación. El SOLICITANTE, mediante la aceptación de las presentes condiciones, otorga consentimiento expreso para la grabación íntegra del vídeo y para el

tratamiento y conservación de categorías especiales de datos. Al pulsar la opción de Aceptar, para realizar el proceso de verificación de identidad mediante vídeo-identificación desasistida para la obtención de un certificado cualificado de firma electrónica, está aceptando también la política de privacidad, de información sobre protección de datos y las presentes condiciones de uso. La no aceptación de estas condiciones supone que no podrá tener acceso al servicio de vídeo-identificación.

DIGITEL TS, como Prestador Cualificado de Servicios de Confianza, le informa de que existen otras alternativas para la identificación que no requieren el tratamiento y la conservación de su imagen y sus datos biométricos, mediante la presencia física ante una Oficina de Registro de DIGITEL TS.

Estando DIGITEL ON TRUSTED SERVICES S.L.U. y, en su caso, la AUTORIDAD DE REGISTRO conformes con los extremos anteriormente consignados, el SOLICITANTE o el SUSCRIPTOR lee, por sí, la totalidad del presente documento y manifiesta que adhiere íntegramente a su contenido, lo cual formaliza mediante la aceptación del contrato de forma electrónica, conforme a la normativa en vigor sobre contratación a distancia.

Firmado por el SOLICITANTE:

Firmado por el SUSCRIPTOR: