



# DECLARACIÓN PRÁCTICAS DE CERTIFICACIÓN

## Control de ediciones

Fecha	Versión	Descripción	Autor
02/09/2016	1.0	Versión Inicial	DIGITEL TS
27/02/2019	2.0	Versión ampliada	DIGITEL TS

### **DERECHOS DE USO:**

*La presente documentación es propiedad de DIGITEL ON TRUSTED SERVICES (Digitel TS) y tiene carácter de confidencial 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

<b>1</b>	<b>INTRODUCCIÓN</b> .....	<b>5</b>
<b>2</b>	<b>IDENTIFICACIÓN DOCUMENTO</b> .....	<b>5</b>
<b>3</b>	<b>ACRÓNIMOS Y DEFINICIONES</b> .....	<b>6</b>
	ACRÓNIMOS .....	6
	DEFINICIONES .....	6
<b>4</b>	<b>NORMAS Y ESTÁNDARES DE APLICACIÓN</b> .....	<b>7</b>
<b>5</b>	<b>DATOS DE IDENTIFICACIÓN Y CONTACTO</b> .....	<b>7</b>
<b>6</b>	<b>DESCRIPCIÓN DEL SERVICIO</b> .....	<b>8</b>
	6.1 PARTES INTERVINIENTES EN LOS SERVICIOS DE DIGITEL TS .....	8
	6.2 CARACTERÍSTICAS PRINCIPALES DE LOS SERVICIOS DE DIGITEL TS .....	9
	6.3 SERVICIO DE NOTIFICACIONES ELECTRÓNICAS CERTIFICADAS Y CUSTODIA .....	10
<b>7</b>	<b>CONTROLES DE SEGURIDAD</b> .....	<b>16</b>
	7.1 SEGURIDAD FÍSICA .....	16
	7.2 SEGURIDAD LÓGICA .....	17
	7.2.1 ACCESO A SISTEMAS .....	18
	7.2.2 REFERENCIA A EVENTOS DEL SISTEMA .....	19
	7.2.3 GESTIÓN DE REGISTROS (PROTECCIÓN, PERIODO DE RETENCIÓN, FUENTES DE TIEMPO, COPIA DE SEGURIDAD...) .....	19
	7.2.3.1 Protección sobre los registros .....	19
	7.2.3.2 Periodo de retención de registros .....	19
	7.2.3.3 Requerimientos para las fuentes de tiempo .....	19
	7.2.3.4 Copia de seguridad de registros .....	20
	7.3 ANÁLISIS DE VULNERABILIDADES .....	20
	7.3.1 Backup remoto .....	21
<b>8</b>	<b>CONTINUIDAD Y PLAN DE CONTINGENCIAS</b> .....	<b>21</b>
	8.1 PLAN DE CONTINUIDAD DE NEGOCIO .....	21
	8.2 PLAN DE CONTINGENCIAS .....	22
<b>9</b>	<b>AUDITORIAS DE CONFORMIDAD</b> .....	<b>22</b>
	9.1 PERFIL AUDITOR .....	22
	9.2 CRITERIOS DE AUDITORIA .....	23
	9.3 FRECUENCIA .....	23
	9.4 PLAN DE ACCION .....	23
	9.5 COMUNICACIÓN RESULTADOS .....	23
<b>10</b>	<b>POLÍTICA DE CONFIDENCIALIDAD</b> .....	<b>24</b>
<b>11</b>	<b>PROTECCIÓN DE DATOS PERSONALES</b> .....	<b>24</b>
	11.1 ENCARGO DE TRATAMIENTO .....	26
<b>12</b>	<b>OBLIGACIONES Y RESPONSABILIDADES</b> .....	<b>28</b>
	12.1 RESPONSABILIDADES .....	28
	12.1.1 RESPONSABILIDADES ESPECÍFICAS .....	28
	12.1.2 Responsabilidades Financieras .....	28
	12.1.3 Comunicación a Autoridades Administrativas / Judiciales .....	28
	12.2 OBLIGACIONES .....	29
	12.2.1 Obligaciones DEL FIRMANTE .....	30

12.2.2 OBLIGACIONES DEL SUJETO/TITULAR .....	30
12.2.3 OBLIGACIONES DE TERCERAS PARTES .....	31
<b>13 NOTIFICACIONES .....</b>	<b>31</b>
<b>14 MODIFICACIONES DEL DOCUMENTO .....</b>	<b>31</b>
14.1 VERSIONES .....	32
14.2 PUBLICACIÓN .....	32
<b>15 FIN PRESTACIÓN DEL SERVICIO .....</b>	<b>32</b>
15.1 PORTABILIDAD .....	32
15.2 CESE ACTIVIDAD DIGITEL TSL – GARANTÍAS .....	33
<b>16 CONDICIONES GENERALES DE USO .....</b>	<b>33</b>
16.1 OBJETO DE LOS SERVICIOS .....	33
16.2 AMBITO TERRITORIAL Y ORGANIZACIÓN DEL SERVICIO .....	33
16.3 MODELO DE PRESTACIÓN DEL SERVICIO .....	34
16.4 CONDICIONES ECONÓMICAS .....	34
16.5 CALIDAD DE LOS TRABAJOS .....	35
16.6 FORMACIÓN DEL PERSONAL .....	35
16.7 CONFIDENCIALIDAD DE LA INFORMACIÓN INTERCAMBIADA .....	35
16.8 TRATAMIENTO DE DATOS PERSONALES .....	36
16.9 RESOLUCIÓN .....	36
16.10 SUBCONTRATACION .....	37
16.11 LEGISLACIÓN Y JURISDICCIÓN APLICABLE .....	37
16.12 RESPONSABILIDAD .....	37
16.13 MODIFICACIONES .....	37
16.14 NULIDAD .....	38
16.15 NOTIFICACIONES .....	38

## 1 INTRODUCCIÓN

---

DIGITEL TS tiene, entre otras, la finalidad de actuar en régimen de libre competencia como **Prestador de Servicios de Certificación** en la categoría de **“Otros servicios relacionados con la firma electrónica”** de conformidad con lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y el Reglamento (UE) N° 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.

A tal efecto, DIGITEL TS ha llevado a cabo el diseño y desarrollo de un sistema tecnológico que, de forma integrada, pone a disposición de sus clientes una herramienta a través de la que poder generar evidencias electrónicas fehacientes, con eficacia jurídica probatoria suficiente para acreditar el consentimiento prestado por parte de los usuarios solicitantes de cualquier tipo de proceso de contratación realizada a distancia o de forma online, así como de almacenamiento de dichas evidencias durante el periodo marcado por la legislación vigente.

## 2 IDENTIFICACIÓN DOCUMENTO

---

La presente Declaración de Políticas de Certificación describe los servicios relacionados con la firma electrónica prestados a través de la plataforma titularidad de DIGITEL TS, incluyendo entre otros aspectos de la descripción y funcionalidad de los servicios prestados los siguientes:

- Las características de cada servicio.
- Los flujos de tratamiento y operación.
- La identificación de todos los intervinientes, desde los propios firmantes, hasta los prestadores de servicios de certificación encargados de la generación de sellos y firmas electrónicas.
- Las condiciones generales de uso y contratación de los servicios.
- Las obligaciones asumidas en la prestación de los servicios.
- Las medidas de seguridad técnicas y organizativas implantadas.

### 3 ACRÓNIMOS Y DEFINICIONES

#### ACRÓNIMOS

ACRÓNIMO	DEFINICIÓN
LFE	Ley 59/2003, de 19 de diciembre, de firma electrónica.
eIDAS	Reglamento (UE) N° 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.
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
RLOPD	Real Decreto 1720/2007, de 21 de diciembre, Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
LSSI	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
PSC	Prestadores de Servicios de Certificación.
TSA	Time Stamp Authority – Autoridad de Sellado de Tiempo.
CPD	Centro de Procesamiento de Datos.
NTP	Network Time Protocol – Protocolo de Internet para sincronizar los relojes de los sistemas informáticos.
PKI	Public Key Infrastructure – Infraestructura de Clave Pública.
WF	Work Flow – Flujos de trabajo de cada proceso.

#### DEFINICIONES

CONCEPTO	DEFINICIÓN
TELECYL	Compañía a la que pertenece DIGITEL TS al 100%, a la que se hará mención a lo largo del documento.
DPC	<b>Declaración de Prácticas de Certificación:</b> Declaración de DIGITEL TS puesta a disposición del público por vía electrónica y de forma gratuita realizada en calidad de Prestador de Servicios de Certificación en cumplimiento de lo dispuesto por la Ley.
CERTIFICADO ELECTRÓNICO	Documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.
CLAVE PÚBLICA (Datos de verificación de firma)	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos.
CLAVE PRIVADA (Datos de creación de firma)	Valor matemático conocido únicamente por el suscriptor y usado para la creación de una firma digital o el descifrado de datos.
ENTIDAD	Empresa u organización de cualquier tipo con la que el solicitante tiene algún tipo de vinculación.
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: <b>Integridad</b> (los datos no han sido modificados), <b>Identificación</b> (la persona que forma los datos es quién dice ser).
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.

<b>HASH O HUELLA DIGITAL</b>	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.
<b>CLAVE</b>	Secuencia de símbolos.
<b>PARTE USUARIA</b>	Persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado.
<b>PIN</b>	Contraseña secreta que se precisa para formalizar operación de identificación y firma por medios electrónicos.
<b>REVOCACIÓN DE CERTIFICADOS</b>	Cambio en el estado del certificado motivado por la pérdida de validez de éste en función de alguna circunstancia distinta a la de su caducidad.
<b>SOLICITANTE</b>	El solicitante podrá ser el mismo Sujeto/titular del certificado o un apersona física apoderada o autorizada para realizar determinados trámites en nombre y representación de la entidad.
<b>SUJETO/FIRMANTE</b>	La persona física cuya clave pública es certificada por la Autoridad de Certificación y dispone de una privada válida para generar firmas digitales.
<b>SUEJETO/CREADOR DEL SELLO</b>	Persona jurídica que crea un sello electrónico.

#### 4 NORMAS Y ESTÁNDARES DE APLICACIÓN

---

- Reglamento (UE) N° 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 59/2003, de 19 de diciembre, de firma electrónica.
- La Orden de 21 de febrero de 2000 por la que se aprueba el reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de forma electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

#### 5 DATOS DE IDENTIFICACIÓN Y CONTACTO

---

- Razón Social: DIGITEL TS ON TRUSTED SERVICES SLU
- Denominación Comercial: DIGITEL TS
- CIF: B47447560
- Domicilio Social: C/ Juan García Hortelano 43, 47014 VALLADOLID, CASTILLA Y LEON
- Servicio de Atención al Cliente (SAC): 902 602 555 – 91 015 05 10
- Correo electrónico: info@digitelts.com
- Web: [www.digitelts.com](http://www.digitelts.com)

## **6 DESCRIPCIÓN DEL SERVICIO**

---

La modalidad del servicio ofrecido por DIGITEL TS se basa en la puesta disposición de una plataforma tecnológica para llevar a cabo procesos de contratación electrónica certificada, notificaciones certificadas y servicios de tercero de confianza. Concretamente, los servicios que serán provistos por parte de DIGITEL TS a través de la plataforma serán los siguientes:

- Servicio de contratación electrónica certificada, mediante Correo electrónico y SMS certificado, que permite la celebración de contratos a distancia con garantías jurídicas, de seguridad y de eficiencia.
- Servicio de notificaciones electrónicas certificadas, mediante Correo electrónico y SMS certificado, que permite a cualquier persona física o jurídica el envío de información relevante con acreditación del envío y recepción de la misma, aportando garantías jurídicas, de seguridad y eficiencia.
- Servicios de Custodia Electrónica Certificada, que consiste en la conservación y custodia de documentos electrónicos con garantías jurídicas y de seguridad, en especial en relación con la integridad de los mismos.
- Servicios de Tercero de Confianza, de conformidad con lo dispuesto en el artículo 25 de la Ley 34/2002 (LSSI)

### **6.1 PARTES INTERVINIENTES EN LOS SERVICIOS DE DIGITEL TS**

Las partes intervinientes de los servicios de DIGITEL TS son:

- **Otros Prestadores de servicios de Certificación.**

DIGITEL TS cuenta con los servicios de otros prestadores de servicios de certificación que intervienen en los servicios prestados a través de los procesos de generación de sellos y firmas electrónicas, así como la TSA encargada de la acreditación del momento exacto en que se producen las operaciones.

La descripción e identificación de las concretas operaciones y procesos en los que intervienen los citados prestadores se incluyen a lo largo de las presentes DPC.

- **Clientes y Usuarios.**

Son usuarios las personas físicas y jurídicas que intervienen en una operación y por tanto aceptan los términos y condiciones en las que se prestan los servicios de certificación.

Los usuarios son los Clientes que solicitan, contratan y/o utilizan los servicios de certificación prestados por DIGITEL TS, así como los destinatarios de las comunicaciones electrónicas y los firmantes de las operaciones de contratación electrónica certificada, y que en todo caso, confían en las evidencias electrónicas generadas como resultado de la utilización de los servicios de certificación de DIGITEL TS, como garantía jurídica y legal a los procesos de negocio de la compañía.



Cada uno de los intervinientes en las operaciones generadas a través de la plataforma de servicios de certificación de DIGITEL TS es responsable de la prestación de servicios que les corresponda, de las obligaciones derivadas de la utilización de los servicios, etc.

## **6.2 CARACTERÍSTICAS PRINCIPALES DE LOS SERVICIOS DE DIGITEL TS**

Los servicios ofrecidos por DIGITEL TS a través de la plataforma tecnológica desde la cual se centralizan y gestionan todos los procesos integrantes de los servicios, tienen las siguientes características:

**1. Garantizan, de forma razonable la identidad** de las partes intervinientes en la comunicación o en el proceso de contratación. En aquellos casos en los que no fuera posible identificar al firmante se podrá realizar una grabación en el sistema donde se solicitarán al usuario los datos de identificación necesarios para poder identificar adecuadamente al firmante:

- Nombre y apellidos del usuario.
- DNI/Pasaporte del usuario.
- Datos de contacto, teléfono móvil, correo electrónico, etc.

En todo momento, el sistema propuesto permite, al menos, garantizar el cumplimiento de las obligaciones en materia de identificación exigidas por parte de la Comisión Nacional de los Mercados y la Competencia (CNMC) en el Acuerdo CNS/DTSA/1743/14/ sobre la obtención del Consentimiento para la Portabilidad numérica.

No obstante, el sistema propuesto no pretende garantizar de forma inequívoca y fehaciente la identidad del usuario que efectivamente acepta la transacción, sin perjuicio de que el mismo permite garantizar de forma indiciaria la misma.

**2. Garantiza el momento exacto de en qué se produjo la puesta a disposición de la información precontractual, y en el que tiene lugar la celebración de la contratación, mediante:**

- La aplicación del correspondiente sellado de tiempo, la fecha y la hora exactas en el que el sistema remite el SMS al usuario con la información precontractual correspondiente.
- La aplicación del correspondiente sellado de tiempo, la fecha y la hora exactas en el que el usuario final remite el SMS con la aceptación de las condiciones contractuales.

La fecha y la hora empleadas para sellar las comunicaciones electrónicas entre las partes es, en todo caso, la hora oficial de España de conformidad con la normativa vigente, en tanto el sellado de tiempo es realizado por un Prestador de Servicios de Confianza Cualificado, emisor de sellados de tiempo.

**3. Garantiza la integridad y no modificación de las comunicaciones intercambiadas entre las partes, mediante;**

- El firmado electrónico del SMS objeto de envío, mediante el cálculo del correspondiente HASH con la aplicación del algoritmo de cifrado correspondiente. En todo caso, el algoritmo para realizar el HASH será al menos SHA-2.
- El sello de tiempo empleado en el proceso, que tiene la consideración de sello cualificado de tiempo electrónico de conformidad con lo dispuesto en la normativa aplicable.
- El soporte electrónico utilizado, que tiene la consideración legal de “soporte duradero” de conformidad con lo dispuesto en la normativa vigente.

**4. Garantiza la prestación del consentimiento expreso e inequívoco de los usuarios intervinientes en el proceso de contratación, a tal efecto;**

- El sistema requiere siempre y, como condición esencial para continuar con el proceso de contratación, la confirmación expresa e inequívoca por parte del usuario final, mediante el envío de un SMS desde el número móvil autorizado.

**5. Garantiza el almacenamiento de una copia íntegra** de las comunicaciones y los documentos aceptados por las partes, durante un plazo de al menos 5 años, sin perjuicio de que este plazo puede ser ampliado en función de las obligaciones legales particulares que pudieran ser aplicables, así como el acuerdo particular al que pudiera llegarse con el cliente final. A tal efecto, el sistema de DIGITEL TS:

- Almacena en formato electrónico todas las comunicaciones intercambiadas entre las partes, que impliquen contratación, o no, garantizándose la integridad de las mismas.
- El plazo de almacenamiento será de cinco años desde el momento de celebración de la comunicación y la contratación. No obstante, este plazo podrá ser ajustado en función de las concretas necesidades de las partes, y la normativa legal de aplicación.
- El soporte utilizado, que tiene la consideración legal de soporte duradero de conformidad con lo dispuesto en la normativa aplicable.

Los documentos electrónicos generados con motivo de la prestación de servicios, las comunicaciones, y en su caso, la contratación efectuada, se encuentran en formatos estándares de uso común, que se encuentran autodocumentados, son autosuficientes e interoperables, garantizando el acceso a los mismos en cualquier momento y desde cualquier plataforma. De este modo, tanto los servicios como la plataforma tecnológica que los soporta cumplen con el principio de neutralidad tecnológica.

**6.3 SERVICIO DE NOTIFICACIONES ELECTRÓNICAS CERTIFICADAS Y CUSTODIA**

La plataforma tecnológica de DIGITEL TS se compone de un sistema de flujos de trabajo (Workflow - WF) que permiten la gestión de los distintos procesos de contratación, y en donde se generan, controlan y se realizan los envíos objeto de la prestación de servicios de comunicaciones electrónicas certificadas, ya se realicen estas vía SMS o CORREO

ELECTRÓNICO, y que permite además la gestión del seguimiento de los envíos realizados, es decir, tener una trazabilidad completa del estado de los envíos realizados.

La plataforma tiene la capacidad de realizar distintos tipos de envíos y acciones relacionadas con los mismos, entre las que cabe destacar:

- Publicación de los documentos con las condiciones contractuales.
- Descarga de dichos documentos.
- Recordatorios.
- Aceptación de respuestas de los usuarios.
- Gestión automática de posibles respuestas.
- Cancelación de los procesos asociados a envíos que se encuentran en curso.
- Comunicación de cambios de estado.
- Manejo de errores y excepciones ocurridas en las comunicaciones.

Las principales etapas del servicio de comunicaciones electrónicas son las siguientes:



### **1. Inicio del proceso de envío de comunicaciones electrónicas y publicación en página web del link de acceso único y temporal.**

Para llevar a cabo el proceso de inicio de una comunicación electrónica certificada o un proceso de contratación por parte del usuario, en primer lugar, con la finalidad de poder identificar al usuario, se realiza una breve grabación con la recogida del número de teléfono al que enviar las comunicaciones, siendo este asociado al documento de certificación que concluye el presente proceso.

El proceso de envío de comunicaciones electrónicas comienza con la generación previa de la documentación necesaria objeto de comunicación (ficheros y contenido de los envíos SMS/correo electrónico), los cuales quedarán específicamente identificados en cada comunicación.

Seguidamente, se inicia la notificación electrónica y/o la solicitud de contratación, la cual contiene al menos:

- Identificación inequívoca del tipo de solicitud.
- Identificación de la documentación referenciada en la solicitud y que han sido puestos a disposición del usuario en repositorio de publicación del servicio.
- Número de teléfono móvil o correo electrónico a utilizar para las comunicaciones.
- Generación de los posibles textos para diferentes casuísticas de SMS (Principal, Confirmación, Respuesta Negativa, Error, Caducado, Cancelación y Recordatorio).
- Fecha límite de vida de la solicitud.

- Otros campos de control.

Si en esta primera fase ocurriera algún tipo de incidencia, fallo o error, se procederá a la eliminación de la solicitud informando expresamente de ello a los distintos intervinientes.

## **2. Publicación de la página Web (link de acceso único y temporal) a la que accede el usuario para ver el detalle y descargar los documentos.**

Realizado el inicio de la solicitud, se procede a la publicación web de la documentación objeto de comunicación / contratación, y cuya URL acortada se incluirá en el medio elegido de comunicación (SMS y/o correo electrónico).

A continuación, se realiza el envío al número de teléfono o correo electrónico indicado como receptor, aplicándose en ese momento un sello de tiempo a través de la petición realizada al servicio publicado por parte de un prestador de servicios cualificado emisora de sellados de tiempo (TSA), que permite la acreditación de la fecha y la hora exactas en el que el sistema remite el SMS o correo electrónico con la documentación correspondiente.

El acceso por parte de los usuarios a la plataforma se realiza de forma única a la documentación asociada a su comunicación, generando la plataforma un registro de los accesos realizados a la base de datos del sistema identificando los siguientes aspectos:

- Fecha.
- Hora.
- Dirección IP.
- Navegador.
- Sistema Operativo.

El link de acceso a la documentación de contratación únicamente será accesible durante un periodo limitado de tiempo limitado desde el momento en que el usuario recibió el SMS, siendo informado el usuario de forma expresa de dicho periodo tiempo en el que el enlace estará vigente en el contenido del SMS. La limitación del periodo de tiempo de la validez del enlace permite minorar el riesgo de que un tercero ajeno a la contratación y al dispositivo móvil pueda enviar el SMS de aceptación y consentimiento.

En este sentido, la plataforma permite configurar el tiempo de vigencia del link en el que son publicadas las condiciones de contratación y por tanto, el tiempo que tiene el usuario para aceptar o rechazar las mismas, siendo en todo caso configurado este plazo de tiempo según las indicaciones del cliente final.

En todo caso, y atendiendo a las recomendaciones establecidas por parte del Internet Engineering Task Force (IETF) en su documento RFC 6238, TOTP: Time-Based One-Time Password Algorithm<sup>1</sup>, la ventana de vigencia de los links o en su caso de las claves en los sistemas One Time Password debe ser la menor posible.

---

<sup>1</sup> Acceso al documento completo: <https://tools.ietf.org/pdf/rfc6238.pdf>

### **3. Gestión y seguimiento de las comunicaciones electrónicas.**

La plataforma de comunicaciones electrónicas certificadas y contratación electrónica de DIGITEL TS permite llevar a cabo una gestión y seguimiento de las comunicaciones efectuadas, en concreto permite llevar a cabo:

- a. Evaluación estados de las comunicaciones electrónicas realizadas.
- b. Comprobación del tiempo de expiración de las comunicaciones electrónicas realizadas, el tiempo de expiración podrá variar por tipo de producto o servicio a contratar.
- c. Cancelación y modificación de procesos de envíos SMS.
- d. Aceptación expresa del usuario final.

El proceso establecido para la gestión y seguimiento de las comunicaciones, es un proceso configurable totalmente automático y que recoge las solicitudes que se encuentran pendientes de resolución, ya sea por falta de aceptación, cambio de estado, envío de recordatorio, o expiración del plazo marcado para la solicitud.

El proceso evalúa cada una de las solicitudes pendientes para determinar alguna actuación para las mismas, para ello:

- Comprueba el tiempo transcurrido desde que se inicia una solicitud. Si transcurrido el tiempo configurado en la plataforma como límite a una determinada solicitud y no se ha obtenido la aceptación por parte del usuario, se envía un SMS recordatorio personalizado. En este caso, la solicitud sigue sin resolverse y continúa a la espera.

Si transcurrido el tiempo establecido de validez de una solicitud no se ha obtenido la correspondiente aceptación por parte del usuario, se procede a expirar dicha solicitud. Se modifica su estado a "RECHAZADO" y se informa al proceso del rechazo de la solicitud. Se envía al usuario el SMS correspondiente que le indique que su solicitud ha expirado.

- Si se recibe la aceptación del usuario, se procede a aceptar la solicitud, y se responde con un SMS indicándole que su aceptación se ha recogido satisfactoriamente. Se modifica su estado a "ACEPTADO" y se informa al proceso de la aceptación de la solicitud.

### **4. Certificación de las comunicaciones realizadas.**

Producido el envío de la comunicación electrónica certificada dirigida al usuario, ya sea vía SMS o correo electrónico, se genera un documento de certificación que incluye el contenido íntegro de dicha comunicación.

Cuando el sistema recibe la aceptación del usuario, se genera otro documento de certificación que recoge el proceso completo de la contratación, es decir, tanto el envío del SMS al usuario, como su respuesta con la aceptación.

En cualquier caso, el documento de certificación incluye la siguiente información:

- El remitente del SMS (entidad que presta el servicio y número de teléfono desde donde se envía el SMS).
- El número de teléfono del destinatario.
- La hora del envío.
- El contenido del SMS.
- Se adjuntan los documentos con los términos de contratación.
- Se adjunta el archivo de audio, en el caso de que hubiese sido necesario realizar la grabación de identificación del usuario y recogida del número de teléfono.
- El Hash del contenido de los SMS, así como de los archivos adjuntos, mediante la aplicación del algoritmo SHA-2.

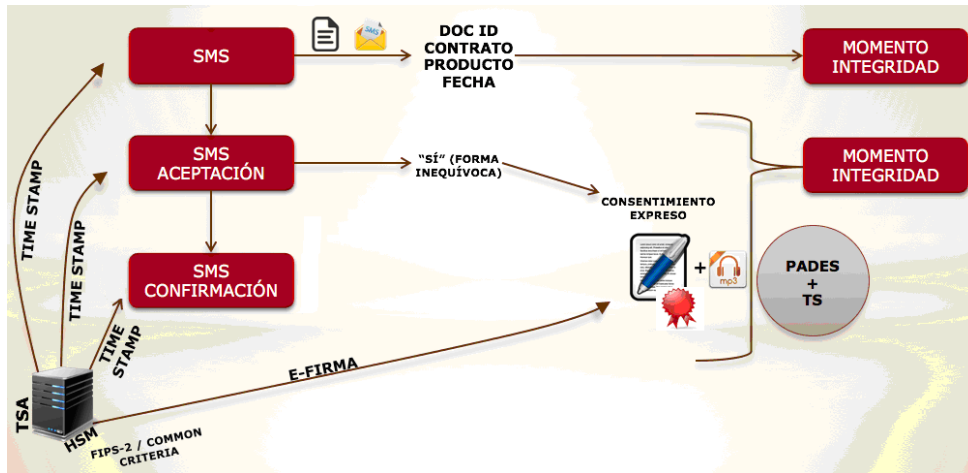
Para finalizar el proceso de contratación, el usuario debe responder al SMS con la palabra "SI" dentro del plazo disponible de aceptación, el sistema remitirá al usuario de forma automática un último SMS confirmándole que la contratación se ha realizado satisfactoriamente. Una vez que el proceso de contratación queda confirmado, se genera un documento de certificación que recoge todas las evidencias generadas durante dicho proceso:

- Identificación tanto del proveedor como del usuario.
- SMS enviado al usuario con la información precontractual.
- SMS de respuesta con la aceptación del usuario.
- Documentación generada con los términos de la contratación (como adjunto).
- Fichero de audio con la grabación de identificación (como adjunto y siempre y cuando existiera).
- El HASH del contenido de los SMS y de los archivos adjuntos, tanto de la documentación, como de la grabación en caso de haberla.

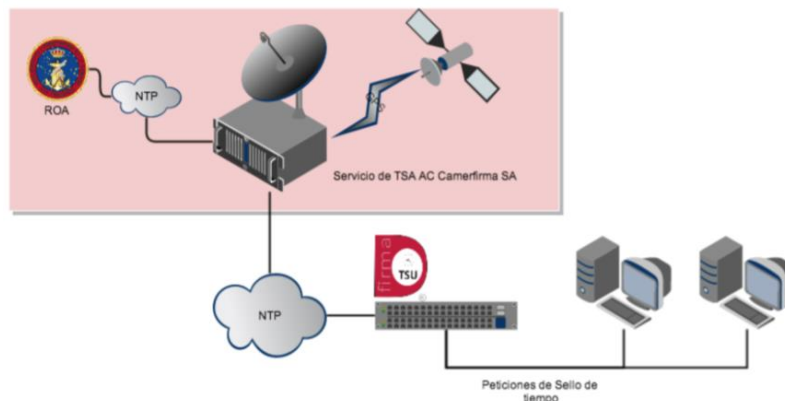
El documento de certificación se firma electrónicamente y se pone un sello de tiempo emitido por una TSA, en concreto en este caso por AC Camerfirma S.A.

Dicho certificado y sello de tiempo se encuentra instalado en un dispositivo seguro de creación de firma HSM (*Hardware Secure Module*) dentro de la plataforma de DIGITEL TS.

El proceso de certificación descrito anteriormente se resume de forma completa en el siguiente diagrama:



El dispositivo HSM implantado en la plataforma de DIGITEL TS se encuentra debidamente certificado bajo las certificaciones *Common Criteria EAL4+* y *FIPS 140-2*, dando de este modo cumplimiento a los requisitos exigidos para los distintos perfiles de protección publicados por parte de la Secretaría de Estado de Telecomunicaciones y sociedad de la información (SETSI), así como los requisitos de los dispositivos cualificados de creación de firma electrónica expresamente dispuestos en el Anexo II del REIDAS.



## 5. Almacenamiento y custodia.

Finalizado el proceso de contratación, y una vez emitido el documento de certificación con todas las evidencias electrónicas generadas a lo largo del proceso, A tal efecto, DIGITEL TS custodia y almacena debidamente dicho documento en sus servidores, garantizando la integridad de la propia base de datos y la trazabilidad de las transacciones realizadas en la misma.

A tal efecto, DIGITEL TS opera como tercero de confianza, de conformidad con lo dispuesto en el artículo 25 LSSI-CE, cuyo sistema garantiza:

- Los documentos acreditativos de la contratación se almacenan durante al menos cinco años.
- Se consigna la fecha y la hora del momento de acuerdo de voluntades.
- Se garantiza la integridad de los documentos almacenados.

## **7 CONTROLES DE SEGURIDAD**

---

DIGITEL TS ha desarrollado e implantado un sistema de gestión de seguridad de la información formado por Políticas, Normas, Estándares, Guías y Procedimientos internos mediante los cuales se define el marco de actuación de la seguridad en los sistemas, servicios y procesos de la compañía, con la finalidad de garantizar que en todos los ámbitos de la entidad se alcanzase el máximo nivel de seguridad.

### **7.1 SEGURIDAD FÍSICA**

DIGITEL TS cumple la normativa UNE-ISO/IEC 2700, que regula el establecimiento de procesos adecuados para garantizar la correcta gestión de la seguridad de los sistemas de información.

En las instalaciones de DIGITEL TS se han establecido diferentes perímetros de seguridad con barreras de seguridad y controles de entrada adecuados a las actividades que se desarrollan en cada uno de ellos. Todo ello con el fin de reducir el riesgo de accesos no autorizados o de daños a los recursos informáticos.

Los sistemas de información de DIGITEL TS se encuentran ubicados en zonas con acceso restringido que han sido adecuadamente protegidas mediante los mecanismos de control de acceso físico apropiados. Asimismo, estos sistemas han sido protegidos frente a otro tipo de amenazas del entorno como incendios, inundaciones o cortes en el suministro eléctrico.

Dicha protección se extiende a aquellos sistemas cuya securización física está delegada en algún proveedor. Para ello, han sido firmadas las cláusulas oportunas en los contratos y se establecen los mecanismos de seguimiento necesarios por parte de DIGITEL TS. El tratamiento de información fuera de los sistemas de DIGITEL TS es debidamente autorizado, una vez que se garantiza el cumplimiento del nivel de seguridad requerido.

Alguna de las medidas adoptadas por DIGITEL TS son las siguientes:

- Autenticación y Control de Accesos. Control de acceso al edificio 7x24 mediante personal de seguridad privada.
- Control de acceso a centros de proceso de datos (Data Center) basado en identificación biométrica de la huella dactilar y autorización centralizada con registro de accesos, tanto de entrada como de salida.
- Las condiciones de temperatura quedan garantizadas por equipos de refrigeración autónomos ubicados dentro del DataCenter que mantienen la temperatura del mismo dentro de los márgenes establecidos.
- Circuito cerrado de televisión con grabación digital permanente y detección de actividad en las cámaras distribuidas por el edificio.
- Alimentación redundante, dotando de dos líneas de alimentación eléctrica a los racks destinados a albergar los equipos.
- El cableado utilizado en el DataCenter es categoría 5e o 6.
- Detección de incendios, basado en detectores de humo y aspiración.



- Climatización continua y adecuada de las zonas CPD con redundancia n+1 en cada zona.
- Detectores de humedad en las zonas de CPD y sala eléctrica.
- Se cuenta con un acuerdo con un proveedor de servicios especializado (Iron Mountain) para la custodia de soportes magnéticos, contando para ello con una sala acorazada anti-sismos.

## **7.2 SEGURIDAD LÓGICA**

DIGITEL TS utiliza diferentes niveles de seguridad en función de los distintos servicios prestados atendiendo a la naturaleza de estos. Sin embargo, existen medidas de seguridad comunes relativas a la seguridad lógica de todos los sistemas.

Formalmente se han establecido responsabilidades y procedimientos documentados para asegurar la correcta configuración, administración, operación y monitorización de los sistemas de información y comunicaciones de DIGITEL TS.

Se ha establecido y definido un procedimiento de gestión de incidencias con el fin de minimizar el impacto ocasionado debido a incidentes de seguridad o fallos en el funcionamiento de los sistemas, que permite una rápida reacción ante las posibles incidencias producidas, así como el establecimiento de medidas correctivas que eviten su repetición.

Se ha establecido igualmente una adecuada segregación de funciones en la asignación de responsabilidades con el objetivo de prevenir un uso no adecuado de los sistemas de información, estableciendo, en los casos en que dicha segregación no sea factible, otros mecanismos de control adecuados que permitan su seguimiento y control.

Se han establecido los procedimientos y controles que prevengan adecuadamente frente a la introducción de software malicioso, garantizando la integridad del software y de la información de DIGITEL TS.

Se han establecido medidas de salvaguarda, incluyendo las copias de seguridad necesarias, comprobando periódicamente su validez mediante su restauración, junto a la monitorización permanente de los sistemas, lo que permite garantizar la continuidad de los sistemas, servicios e informaciones de DIGITEL TS y los servicios prestados.

La información transmitida por redes de comunicaciones, públicas o privadas, se encuentran adecuadamente protegidas mediante los mecanismos oportunos que garanticen su confidencialidad e integridad. Se han establecido los controles necesarios que impidan la suplantación del emisor, modificación o pérdida de la información transmitida, tanto en las comunicaciones con sistemas situados en las redes internas, como con otros sistemas externos, como aquellas entidades con las que DIGITEL TS cuenta en la prestación de sus servicios como parte interviniente en los mismos.

Se establecen igualmente procedimientos que regulan de forma detallada el almacenamiento, manipulación, transporte y destrucción de la información sensible tanto en

soportes informáticos (cintas, discos, ordenadores portátiles, dispositivos móviles como agendas electrónicas y teléfonos, dispositivos extraíbles, etc.), como residualmente, en soporte papel, todo ello con la finalidad de mitigar el riesgo de acceso no autorizado, pérdida o hurto.

### **7.2.1 ACCESO A SISTEMAS**

El acceso por parte del personal tanto interno como externo a los sistemas de información de DIGITEL TS, así como a la información que tratan y almacenan, se regula sobre la base de las necesidades de información y operación de cada usuario, otorgando acceso exclusivamente a aquellas funciones e información que se requieran para el correcto desempeño de su actividad laboral, acorde con su función y/o perfil operacional.

Los responsables del tratamiento de los activos de información serán los responsables de definir los niveles de acceso a los recursos y autorizar cualquier acceso extraordinario, todo ello de acuerdo con las directrices de los propietarios de la información, o, en su caso, de los propietarios del proceso o negocio.

Sin perjuicio de precisar un mayor detalle en su aplicación, ni de la delegación formal de funciones, se entienden como propietarios del proceso o negocio los responsables de las siguientes posiciones:

- Dirección General
- Subdirección General
- Dirección Financiera
- Dirección de Marketing y Desarrollo de Negocio
- Dirección de Recursos Humanos
- Dirección Jurídica
- Dirección de Calidad
- Dirección de Medios
- Dirección de DIGITEL TS ON TRUSTED SERVICES
- Responsable de Infraestructuras y Telecomunicaciones
- Responsable de Sistemas de la Información

Todos los accesos realizados a los sistemas de información de DIGITEL TS por los usuarios llevarán asociado un proceso de identificación, autenticación y autorización, estableciéndose los controles adecuados para que tales procesos se realicen de forma segura.

A tal efecto, se han diseñado e implantado mecanismos de registro, monitorización de acceso y uso de los sistemas, que permitan conocer la efectividad de las medidas instaladas y detectar posibles incidentes de seguridad.

## **7.2.2 REFERENCIA A EVENTOS DEL SISTEMA**

En relación con los posibles eventos del sistema, teniendo en cuenta la categoría de los servicios prestados, DIGITEL TS ha diseñado un sistema de registros y controles que permiten la inspección reactiva entre otros de los siguientes eventos sobre sus sistemas:

- Intentos exitosos o fracasados de inicio y fin de sesión.
- Intentos exitosos o fracasados de crear, modificar o borrar cuentas del sistema.
- Intentos exitosos o fracasados de crear, modificar o borrar usuarios del sistema autorizados.
- Intentos exitosos o fracasados de creación, modificación o cancelación de peticiones dentro de los diferentes componentes del sistema.
- Intentos exitosos o fracasados de firma de documentos.
- Intentos exitosos o fracasados de documentos de certificación.
- Intentos exitosos o fracasados de intento de envío de comunicaciones.
- Cambios en la configuración del sistema.

## **7.2.3 GESTIÓN DE REGISTROS (PROTECCIÓN, PERIODO DE RETENCIÓN, FUENTES DE TIEMPO, COPIA DE SEGURIDAD...)**

### **7.2.3.1 PROTECCIÓN SOBRE LOS REGISTROS**

El acceso a los sistemas de archivo y custodia de documentación de DIGITEL TS se encuentra restringido exclusivamente al personal autorizado. Así, se ha configurado un sistema de control de accesos, identificación y autenticación de tal manera que se encuentra protegido contra accesos, modificación, borrado u otras manipulaciones no autorizadas, todo ello dentro del sistema de almacenamiento de "Sistema de Confianza".

Los sistemas, soportes y medios que contienen la documentación e información susceptible de archivo y custodia, así como las aplicaciones necesarias para procesar y tratar los datos custodiados son mantenidos y puedan ser accedidos por el período de tiempo establecido en la presente Declaración de Prácticas de Certificación.

### **7.2.3.2 PERIODO DE RETENCIÓN DE REGISTROS**

Los registros anteriormente comentados, incluyendo las evidencias de servicio serán almacenados y retenidos como registros de auditoría generados por el sistema por un periodo mínimo desde la fecha de su creación de un (1) años para los pertenecientes a auditorías diarias, dos (2) años para las mensuales y cuatro (4) años para los de auditorías anuales.

### **7.2.3.3 REQUERIMIENTOS PARA LAS FUENTES DE TIEMPO**

Los certificados, CRLs, y otras entradas de bases de datos de revocación deberán contener información de fecha y hora.

Los sistemas de DIGITEL TS realizan el registro del instante de tiempo exacto en los que se realizan utilizando a tal efecto un sello de tiempo emitido por una TSA para el caso de formar

parte de los procesos integrantes de los servicios de comunicaciones electrónicas certificadas y contratación electrónica prestados por DIGITEL TS

Todos los sistemas de DIGITEL TS sincronizan su instante de tiempo con fuentes fiables de tiempo basadas en el protocolo NTP (Network Time Protocol), auto calibrándose por distintos medios, y utilizando como referencia entre otros la del Real Instituto y Observatorio de la Armada.

#### **7.2.3.4 COPIA DE SEGURIDAD DE REGISTROS**

Se realizan dos copias de seguridad diaria de los ficheros que contienen los registros objeto de retención. Una copia se realiza en local y se almacena en C/ Enrique Cubero 32, 47014 Valladolid, y cada 15 días se deposita una edición de las copias de seguridad en un proveedor externo.

La política de backup actual para este entorno es:

- Servidores de aplicaciones: Full semanal e incremental diario.
- Servidor de BBDD: Full diario
- Documentos: Full cada 8 semanas con incremental diario

Estas copias de seguridad se realizan sobre todos los componentes del servicio.

### **7.3 ANÁLISIS DE VULNERABILIDADES**

DIGITEL TS, o un auditor externo con la certificación y conocimiento suficiente efectuará al menos, un análisis anual de vulnerabilidades.

Es responsabilidad de los coordinadores de los equipos de análisis el informar a los responsables del servicio de DIGITEL TS, a través del Responsable de Seguridad, de los resultados de los análisis realizados, de cualquier problema que impida la realización de las auditorías, o la entrega de la documentación resultante.

Los análisis de seguridad implican el inicio de las tareas precisas para corregir las vulnerabilidades detectadas y la emisión de un contrainforme.

Las vulnerabilidades encontradas serán detalladas en un documento resultante etiquetado como: "Análisis de vulnerabilidades sobre plataforma DIGITEL TS". Si fuera encontrada alguna vulnerabilidad, el equipo de DIGITEL TS las analizará y las categorizará y ponderará según el grado de afectación procediendo a crear una propuesta con contramedidas.

Las contramedidas serán aplicadas en el menor plazo de tiempo posible, notificando a las partes implicadas si existieran entidades perjudicadas por las vulnerabilidades encontradas.

### 7.3.1 BACKUP REMOTO

Diariamente se realizan copias de backup siendo estas almacenadas en dependencias próximas al Centro de Proceso de Datos en un espacio físico seguro ubicado en la C/ Enrique Cubero 32, 47014 Valladolid.

## 8 CONTINUIDAD Y PLAN DE CONTINGENCIAS

---

DIGITEL TS ha establecido procesos de gestión de continuidad de negocio para minimizar el impacto en las funciones y procesos críticos en caso de desastre, de forma que se reduzca el tiempo de indisponibilidad a niveles establecidos previamente. Dichos procesos cuentan con la adecuada combinación de controles de carácter organizativo, tecnológico y procedimental tanto preventivos como de recuperación.

Estos procesos se apoyan en un Plan de Continuidad de Negocio que es probado de forma periódica, manteniéndose actualizado en todo momento. Para ello se evalúa el riesgo ante amenazas y el impacto asociado ocasionado por la ausencia de continuidad de los activos de información que den soporte o estén implicados en los procesos de negocio de DIGITEL TS.

El CPD de DIGITEL TS dispone de medidas de seguridad contra cortes de electricidad. Todos los equipos ubicados en el CPD disponen de alimentación eléctrica procedente de dos fuentes, una correspondiente al suministrador y otra procedente de un Sistema de Alimentación Ininterrumpida cuya autonomía es de 2 horas al 100% de carga, 4 horas al 50% de carga. Para el caso de los equipos y dispositivos que no cuenten con doble fuente de alimentación, todos los armarios disponen de un switch eléctrico (un STS) cuya función es hacer conmutación entre ambas fuentes de suministros sin provocar cortes en los equipos protegidos por los mismos.

Los sistemas de alimentación ininterrumpida son revisados y mantenidos semestralmente por la empresa fabricante, garantizándose de este modo, que están en óptimas condiciones de funcionamiento en caso de sea necesaria su contribución.

### **8.1 PLAN DE CONTINUIDAD DE NEGOCIO**

En caso de contingencias graves el servicio será suspendido mientras estas duren, notificando a la mayor brevedad posible a los usuarios del sistema.

Las contingencias contempladas que pudieran suponer algún tipo de riesgo para la calidad del servicio son:

- Tiempos de respuesta tan elevados que supusieran una clara violación de la política de calidad de servicio.
- Pérdida de sincronismo con las fuentes de tiempo primaria y secundaria.

Las contingencias que pueden suponer un riesgo para la prestación del servicio son:

- Errores en los sistemas de explotación asociados a la prestación del servicio.

- Errores en los sistemas de comunicación asociados a la prestación del servicio.
- Errores que afecten a la prestación del servicio detectado en el software de alguno de los servicios.

## **8.2 PLAN DE CONTINGENCIAS**

DIGITEL TS cuenta con infraestructuras tecnológicas construidas bajo la premisa de Alta Disponibilidad y Failover, con elementos redundados en activo - activo o activo-pasivo, dependiendo del caso.

En esta premisa se identifican las condiciones para la activación de las operaciones, así como lo que constituye un tiempo aceptable para la interrupción y recuperación del sistema.

Además, se definen los procedimientos para que los equipos reconstituyan las operaciones de DIGITEL TS usando datos de respaldo y las copias de respaldo de las llaves.

Adicionalmente la Premisa de Alta Disponibilidad y Failover incluye:

- La frecuencia para la toma de copias de seguridad de la información y los sistemas esenciales del negocio.
- Procedimientos para asegurar la instalación de los sistemas y ubicaciones necesarios ante la recuperación ante desastres, y durante el periodo mínimo requerido posterior a haberse producido el desastre y previo a la restauración de un entorno seguro, ya sea en el sitio original o uno remoto.

## **9 AUDITORIAS DE CONFORMIDAD**

---

### **9.1 PERFIL AUDITOR**

El auditor externo o equipo de auditores externos será seleccionado en el momento de la planificación de cada auditoría.

Cualquier empresa o persona contratada para realizar una auditoría de seguridad sobre DIGITEL TS o alguno de sus servicios en concreto deberá cumplir con los siguientes requisitos:

- Adecuada y acreditada capacitación y experiencia en seguridad y procesos de auditoría de sistemas de información.
- Independencia a nivel organizativo de la autoridad de DIGITEL TS, para el caso de auditorías externas.

El auditor externo o equipo de auditores externos además no deberán tener ninguna relación, actual o planificada, financiera, legal, o de cualquier otra clase que pueda derivar en un conflicto de intereses con DIGITEL TS. Para poder cumplir con la normativa vigente en materia de tratamiento de datos, y si el proceso de auditoría implicara el acceso a los datos de

carácter personal, el auditor tendrá la consideración de Encargado de Tratamiento, en virtud de lo previsto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre.

## **9.2 CRITERIOS DE AUDITORIA**

Sin perjuicio de verse ampliados por documentos de los servicios particulares ofrecidos por DIGITEL TS, en este apartado definiremos el conjunto de las comprobaciones mínimas de la adecuación de los servicios ofertados respecto a lo definido en esta DECLARACIÓN PRÁCTICAS DE CERTIFICACIÓN. Los aspectos cubiertos por una auditoria incluirán, pero no estará limitada a:

- Política de seguridad.
- Seguridad física de las instalaciones del servicio auditado.
- Seguridad lógica de los sistemas y servicios de DIGITEL TS
- Evaluación tecnológica de los componentes del servicio.
- Administración de los servicios, así como seguridad en la misma.
- DECLARACIÓN PRÁCTICAS DE CERTIFICACIÓN y políticas de servicios vigentes.
- Cumplimiento de las exigencias legales aplicables.

## **9.3 FRECUENCIA**

Las Auditorías de conformidad y cumplimiento son llevadas a cabo al menos con carácter bianual, salvo que se produjesen cambios relevantes o esenciales en los sistemas y servicios de DIGITEL TS, en donde se ejecutarán auditorías de carácter extraordinario.

## **9.4 PLAN DE ACCION**

La identificación de deficiencias en la auditoria dará lugar como medida inmediata a la adopción de medidas correctivas. Las autoridades competentes en la materia según lo definido por la legislación vigente en colaboración con el auditor será la responsable de la determinación de estas.

En caso de encontrarse deficiencias se actuará según lo dispuesto en la Ley 59/2003 de Firma Electrónica, así como en el Reglamento de Identificación Electrónica (UE) 510/2014.

## **9.5 COMUNICACIÓN RESULTADOS**

El auditor externo o auditores externos comunicarán los resultados de la auditoria al Responsable de Seguridad de DIGITEL TS, así como a los responsables de las distintas áreas en las que se detecten no conformidades, así como en su caso a la autoridad competente según lo determinado en la legislación vigente

## **10 POLÍTICA DE CONFIDENCIALIDAD**

---

Existe el deber genérico de confidencialidad respecto a la información que los empleados de DIGITEL TS conozcan por razón de su puesto de trabajo. La información considerada como confidencial facilitada a DIGITEL TS no será en ningún caso divulgada a terceros salvo que se encuentre amparada en los supuestos de requerimiento de colaboración con las instituciones competentes contempladas en la Ley 59/2003 de Firma Electrónica.

En este sentido, se considerará información del tipo "confidencial" (sin perjuicio de que otro tipo de información pueda serlo también):

- Planes de continuidad de negocio y de emergencia.
- Información relativa a la operativa de operaciones y mantenimiento del servicio.
- Toda información relativa a las operaciones que lleve a cabo DIGITEL TS.
- Toda información relativa a los parámetros de seguridad, control y procedimientos de auditoría.
- Toda la información de carácter personal proporcionada a DIGITEL TS durante el proceso de registro de los suscriptores de certificados, con la salvedad de lo especificado por la Política de Certificación aplicable y el contrato de certificación.
- La información de negocio suministrada por sus proveedores y otras personas con las que DIGITEL TS tiene el deber de guardar secreto establecida legal o convencionalmente.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Toda la información clasificada como "CONFIDENCIAL" o "ESTRICTAMENTE CONFIDENCIAL"

Sin embargo, serán considerados como documentos públicos no confidenciales entre otros los siguientes materiales:

- Condiciones generales de uso de DIGITEL TS
- Declaración de Prácticas de Certificación de DIGITEL TS
- Declaración de Prácticas de Validación de Firmas de DIGITEL TS
- Declaración de Prácticas de Sellado de Tiempo de DIGITEL TS
- Declaración de Prácticas de Archivado de Larga Duración de DIGITEL TS
- Toda aquella información que sea considerada como "Pública"

## **11 PROTECCIÓN DE DATOS PERSONALES**

---

DIGITEL TS tratará aquellos datos de carácter personal necesarios para el desarrollo de su actividad obteniendo directamente el consentimiento expreso de los firmantes. Este tratamiento se realizará atendiendo a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y sus normas de desarrollo.

Los datos de carácter personal aportados por los Clientes serán tratados por DIGITEL TS con la máxima confidencialidad y pasarán a formar parte de un fichero de su respectiva titularidad y debidamente inscrito en la Agencia Española de Protección de Datos. En este sentido, DIGITEL TS, como responsables de sus respectivos ficheros, tratará los datos de carácter



personal con la única finalidad de dar cumplimiento al objeto del presente Contrato, garantizando la plena observancia a la normativa vigente en materia de protección de datos.

Asimismo, los Clientes podrán ejercer en todo momento los derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Estos derechos podrán ejercerlos dirigiéndose:

- Mediante correo postal: C/ Juan García Hortelano, 43, 47014 Valladolid.
- Forma electrónica: [lop@digitelts.com](mailto:lop@digitelts.com)

El contenido de la solicitud debe incluir:

- Nombre y apellidos del interesado
- Fotocopia de su documento nacional de identidad, pasaporte u otro documento válido que lo identifique y, si fuera necesario, de la persona que lo represente, así como el documento o instrumento electrónico acreditativo de tal representación
- Detalle de la petición que se realiza.
- Dirección a efectos de notificaciones.
- Fecha y firma del solicitante.
- Documentos acreditativos de la petición que formula si fuera necesario.

El tiempo de respuesta es, tal y como marca la normativa, de 30 días para el Acceso y de 10 días para la Ratificación, Cancelación y Oposición.

La información personal que no haya de ser empleada para la prestación del servicio será considerada información personal de carácter privado, de conformidad con lo establecido en el artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se consideran datos de carácter personal cualquier información relativa a personas físicas identificadas o identificables.

En cualquier caso, los siguientes datos son considerados como información privada y tendrán la consideración legal de datos de nivel básico:

- Los datos necesarios para la prestación de (i) servicios de contratación electrónica certificada mediante SMS; (ii) servicios de notificaciones electrónicas certificadas mediante Correo electrónico y SMS certificado; (iii) servicios de custodia electrónica certificada y; (iv) servicios de terceros de confianza.
- Claves privadas generadas y/o almacenadas por DIGITEL TS necesarias para garantizar la seguridad y la correcta prestación del servicio.
- Toda otra información identificada como "Información privada" de conformidad con lo establecidos la normativa vigente.

En este sentido, DIGITEL TS se compromete a no realizar ningún otro tratamiento sobre los datos personales, ni a aplicar o utilizar los datos con una finalidad distinta a la prestación de los Servicios a los que se hace referencia en el presente documento.

De conformidad con la Ley Orgánica 15/99 la información confidencial está protegida frente a su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos.

En caso de que se realizaran servicios de certificación a clientes que utilicen un seudónimo en el certificado electrónico, DIGITEL TS constatará su identidad y conservará la documentación que la acredite la misma. En caso de solicitud por parte de órganos judiciales en desarrollo de las funciones que tienen atribuidas, así como en los supuestos del artículo 11.2 de la Ley Orgánica de Protección de Datos de Carácter Personal, DIGITEL TS revelará la identidad del cliente identificado mediante seudónimo.

En ningún caso DIGITEL TS recogerá ni tratará datos especialmente protegidos, entendiéndolos como tales; la ideología, religión y creencias con base en el artículo 7 de la Ley Orgánica de Protección de Datos.

En caso de violación de la seguridad o pérdida de la integridad que suponga un impacto significativo en el servicio prestado o en los datos de carácter personal tratados, DIGITEL TS lo notificará en el plazo máximo de 24 horas desde que se tuviera conocimiento de tal incidente al organismo de supervisión y en caso necesario a la Agencia Española de Protección de datos en cumplimiento del artículo 19.2 del Reglamento 910/2014 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.

### **11.1 ENCARGO DE TRATAMIENTO**

En el caso en que DIGITEL TS preste los servicios de Custodia Electrónica Certificada, actuará como Encargado de Tratamiento de los datos responsabilidad de terceros en los términos y condiciones previstos en el artículo 12 de la Ley Orgánica de Protección de Datos. En este sentido, DIGITEL TS se compromete a cumplir las siguientes condiciones:

- El tratamiento de datos que DIGITEL TS realizará se limitará a las actuaciones que resulten necesarias para prestar al RESPONSABLE DEL FICHERO los Servicios contratados.
- En concreto, DIGITEL TS se compromete a realizar el tratamiento de los Datos Personales ajustándose a las instrucciones que, en cada momento, le indique el RESPONSABLE DEL FICHERO, así como a lo dispuesto en la normativa que le resulte aplicable en materia de protección de datos personales.
- Asimismo, DIGITEL TS se compromete a no realizar ningún otro tratamiento sobre los Datos Personales, ni a aplicar o utilizar los datos con una finalidad distinta a la prestación del Servicio.
- DIGITEL TS declara conocer que el Fichero contiene datos personales y que, como Encargado de Tratamiento, en el caso de que tuviera que trasladar la información contenida en el Fichero, estará obligado a adoptar las medidas del nivel de seguridad que correspondan a la situación que resulten necesarias conforme a las exigidas para

el nivel de seguridad, a los efectos de garantizar la confidencialidad e integridad en función de la naturaleza de los datos, de conformidad con lo establecido en el Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD.

A los efectos de lo previsto en el presente apartado, DIGITEL TS, deberá informar a sus empleados de la obligación de secreto y confidencialidad, así como las consecuencias de su incumplimiento, respecto del tratamiento de datos de carácter personal.

DIGITEL TS se compromete a guardar bajo su control y custodia el Fichero y/o los Datos Personales suministrados por el RESPONSABLE DEL FICHERO a los que acceda con motivo de la prestación del Servicio y a no divulgarlos, transferirlos, o de cualquier otra forma comunicarlos, ni siquiera para su conservación a otras personas.

Una vez cumplida la prestación del servicio objeto del Contrato, el DIGITEL TS se compromete a destruir o devolver aquella información que contenga datos de carácter personal que haya sido transmitida por el RESPONSABLE DEL FICHERO al DIGITEL TS con motivo de la prestación del Servicio

En el caso de que los afectados, cuyos datos se encuentren en ficheros titularidad del RESPONSABLE DEL FICHERO, ejercitasen sus derechos ante el DIGITEL TS, éste deberá dar traslado de la solicitud de forma inmediata al RESPONSABLE DEL FICHERO y, a no más tardar, dentro del plazo de tres (3) días naturales a contar desde su recepción, para que el RESPONSABLE DEL FICHERO resuelva debidamente dicha solicitud.

El Documento de Seguridad de DIGITEL TS deberá contener la identificación de los ficheros que se traten en concepto de encargo del tratamiento. Asimismo, en el Documento de Seguridad del DIGITEL TS se identificará al RESPONSABLE DEL FICHERO y se indicará el período de vigencia del encargo.

En el caso de que los datos de los ficheros se incorporen y traten de modo exclusivo en los sistemas de información de DIGITEL TS, el RESPONSABLE DEL FICHERO deberá anotarlo en su Documento de Seguridad.

DIGITEL TS garantiza el cumplimiento de las obligaciones que le correspondan como DIGITEL TS en virtud de la normativa que le resulte de aplicación en materia de protección de datos personales.

DIGITEL TS garantiza el cumplimiento de las obligaciones derivadas de la normativa aplicable a los PSC con el fin de proporcionar un servicio de calidad. En particular, DIGITEL TS cumplirá con lo dispuesto en la LFE y el EIDAS asumiendo la responsabilidad que pudiese surgir durante el desarrollo de su actividad.

## **12 OBLIGACIONES Y RESPONSABILIDADES**

---

### **12.1 RESPONSABILIDADES**

DIGITEL TS como Prestador de Servicios de Certificación se encuentra sujeto al régimen de responsabilidad recogido en los artículos 22.1 LFE (Ley de Firma Electrónica) y 13 del eIDAS, por lo que asumirá las responsabilidades por los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en los términos previstos en la legislación vigente y en las Políticas de Certificación.

Quedan excluidas de las responsabilidades todos los supuestos contemplados por la ley como Limitaciones a la responsabilidad del PSC.

#### **12.1.1 RESPONSABILIDADES ESPECÍFICAS**

En concreto DIGITEL TS se hace responsable de:

- Exactitud de toda la información contenida en el certificado en la fecha de su emisión.
- Garantizar de que, en el momento de entrega del certificado, obra en poder del Firmante la clave privada correspondiente a la clave pública dada, identificada con el proceso correspondiente.
- Garantizar que la clave pública y privada funcionan conjunta y complementariamente.
- Correspondencia entre certificado solicitado y el entregado.

En cumplimiento con la legislación vigente, DIGITEL TS dispone de un seguro de responsabilidad civil, al que se hace referencia a continuación. (ap.12.1.2)

#### **12.1.2 RESPONSABILIDADES FINANCIERAS**

De conformidad con lo dispuesto en el artículo 20.2 LFE, los prestadores de servicios de certificación que expidan certificados reconocidos deberán constituir un seguro de responsabilidad civil por importe de al menos 3.000.000 de euros para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan, pudiendo ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea al menos de 3.000.000 de euros.

#### **12.1.3 COMUNICACIÓN A AUTORIDADES ADMINISTRATIVAS / JUDICIALES**

DIGITEL TS comunicará a la Autoridad Pública correspondiente aquella información confidencial o que contenga datos de carácter personal cuando haya sido requerida por la misma y en los supuestos previstos legalmente.

En concreto, DIGITEL TS está obligada a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tengan atribuidas, y en el resto de los supuestos previstos en el artículo 11.2 de la LOPD donde así se requiera.

## **12.2 OBLIGACIONES**

DIGITEL TS como Prestador de Servicios de Certificación está obligado según lo dispuesto en las Políticas de Certificación implicadas a:

- Respetar lo dispuesto en el alcance de las Políticas de Certificación correspondientes.
- Proteger de forma segura sus claves privadas.
- Emitir los certificados de acuerdo con las Políticas de Certificación y a los estándares técnicos correspondientes.
- Emitir certificados según la información que tenga en su poder y libres de errores de entrada de datos.
- Emitir certificados cuyo contenido como mínimo sea el especificado en la normativa vigente para los certificados cualificados.
- Publicar los certificados emitidos en un directorio, respetando en todo momento lo dispuesto en cuanto a protección de datos.
- Suspender y/o revocar los certificados según lo dispuesto en la normativa, publicando estas revocaciones.
- Informar a los Firmantes de las revocaciones o suspensión de sus certificados, en tiempo y forma según la legislación vigente.
- No almacenar ni copiar los datos del Firmante excepto certificados de cifrado y para los casos en los que legalmente se prevea o permita dicho almacenaje.
- Proteger los datos de creación de firmas mientras estén bajo su custodia.
- Establecer los mecanismos de generación y custodia de la información de todas las actividades descritas, protegiéndolas ante pérdidas, destrucción o falsificación.
- Conservar la información sobre el certificado emitido por el periodo mínimo exigido por la normativa vigente.

### - Obligaciones previas a la expedición de un certificado:

- Informar adecuadamente a los solicitantes de la firma de sus obligaciones y responsabilidades.
- Proporcionar una adecuada identificación de los solicitantes, que deben de ser personas capacitadas y/o autorizadas para solicitar un certificado digital.
- Correcta comprobación de la validez y vigencia de esos datos de las solicitudes y de la Entidad, en el caso de que exista vinculación.

### - Obligaciones una vez expedido el certificado:

- Suscribir los contratos de Prestación de Servicios de Certificación Digital con los solicitantes, no pudiéndose realizar la emisión sin antes no haber aceptado las condiciones de uso.
- El mantenimiento de los certificados durante su vigencia (extinción, suspensión, revocación)

- Archivar las copias de la documentación presentada y los contratos debidamente firmados por los solicitantes en conformidad con la legislación vigente.

### **12.2.1 OBLIGACIONES DEL FIRMANTE**

El Firmante (Creador del Sello), está obligado a cumplir con lo dispuesto en la normativa, y además a:

- Aceptar los términos y condiciones impuestas por DIGITEL TS.
- Usar la información del firmante bajo las leyes de protección de datos.
- Permitir la publicación de los certificados digitales en un repositorio público.
  
- Garantizar la exactitud y veracidad de la información suministrada.
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- Custodiar los datos de activación de su clave privada, siendo el único responsable de las consecuencias que un uso indebido pueda generar.

### **12.2.2 OBLIGACIONES DEL SUJETO/TITULAR**

El sujeto está obligado a cumplir con la normativa vigente además de:

- Usar el certificado según las Políticas de Certificación.
- Respetar lo dispuesto en los documentos firmados con DIGITEL TS.
- Informar lo más breve posible de alguna pausa/revocación.
- Notificar cualquier inexactitud o cambio.
- No utilizar la clave privada o el certificado una vez expirado el plazo de validez de éste.
- Hacer uso del certificado de forma personal e intransferible y custodiar los datos de activación. Esto es, asumir la responsabilidad de cualquier actuación en la que tenga lugar el uso del certificado. Un uso indebido del mismo puede declararle responsable frente a terceros o la entidad que representa.
- Autorizar a DIGITEL TS a proceder a tratar los datos personales contenidos en los certificados, en conexión con finalidades de la relación electrónica, y verificación de certificados.
- Responsabilizarse de que toda la información incluida, por cualquier medio, en la solicitud del certificado y en el mismo certificado sea exacta, completa y esté actualizada.
- Informar inmediatamente a DIGITEL TS de cualquier inexactitud en el certificado detectada según se haya emitido, así como de los cambios que se produzcan en la información aportada por la emisión del certificado.
- No utilizar la clave privada, el certificado electrónico o cualquier otro soporte técnico entregado por DIGITEL TS, para realizar ninguna transacción prohibida por ley.
- En el caso de certificados cualificados, el Firmante debe utilizar el par de claves exclusivamente para la creación de firmas o sellos electrónicos y de acuerdo con cualesquiera otras limitaciones que le sean notificadas.

Si el firmante genera sus propias claves se obliga a:

- Generar sus claves de Firmante utilizando un algoritmo reconocido como aceptable para la firma electrónica o el sello electrónico, ambos cualificados.
- Crear las claves dentro del dispositivo de creación de firma o de sello, utilizando un dispositivo cualificado en el caso de ser necesario.

### **12.2.3 OBLIGACIONES DE TERCERAS PARTES**

Será obligación de la Parte Usuaría cumplir con lo dispuesto en la normativa vigente, y además:

- Verificar la validez de los certificados antes de realizar cualquier operación basada en ellos.
- Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía y aceptar o sujetarse a las mismas.
- Comprobar que la validez de la cualificación de una firma asociada a un certificado emitido por DIGITEL TS comprobando que la autoridad de certificación que ha emitido el certificado se encuentra publicada en la lista de confianza del supervisor nacional correspondiente.

## **13 NOTIFICACIONES**

---

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las prácticas descritas en esta Declaración de Prácticas de Certificación se realizará mediante documento o mensaje electrónico firmado digitalmente o por escrito mediante correo certificado dirigido a cualquiera de las direcciones contenidas en el punto relativo a Datos de contacto. Las comunicaciones electrónicas se harán efectivas una vez que las reciba el destinatario al que van dirigidas.

## **14 MODIFICACIONES DEL DOCUMENTO**

---

DIGITEL TS se reserva el derecho de modificar unilateralmente este documento siempre y cuando:

- La modificación esté justificada desde el punto de vista técnico y legal.
- Se notifiquen a los usuarios de todas las afectaciones derivadas de estas modificaciones y estos acepten las mismas previo uso del servicio
- Se ofrezca un mecanismo de control de cambios y de ediciones.

En este sentido, en DIGITEL TS, una vez decidida la conveniencia de realizar una revisión, el responsable de la elaboración del documento efectuará las modificaciones oportunas, quedando identificadas en la nueva edición mediante sombreado del texto modificado. Este método puede coexistir o ser sustituido por un listado de control de cambios en el que se relacionen los cambios introducidos en cada una de las ediciones o versiones del documento.

Si las modificaciones efectuadas sobre el documento producen una alteración que afecte al servicio prestado a los usuarios estas serán consideradas un “*major reléase*”. De otro modo serán consideradas un “*minor reléase*”.

Los usuarios serán informados en caso de producirse un “*major reléase*” quedando modificada la relación contractual entre DIGITEL TS y éstos. De este modo los clientes deberán adherirse a las nuevas condiciones de uso previa prestación de nuevos servicios o abrirse un proceso de baja en el servicio.

#### **14.1 VERSIONES**

Esta Declaración de Prácticas de Certificación y las Políticas de Certificación puede sufrir cambios en el transcurso del tiempo. Cuando se produzca un cambio “*major release*” supondrá aumentar en uno las versiones del documento. Sin embargo, cuando se produzca un cambio “*minor reléase*” modificará el número de subversión.

#### **14.2 PUBLICACIÓN**

Es obligación de DIGITEL TS publicar la información relativa a sus prácticas, sus certificados y el estado en que se encuentran dichos certificados. Todo el histórico de esta documentación deberá ser conservado y accesible al menos por un periodo de 15 años.

Toda publicación se llevará a cabo en el sitio web de DIGITEL TS o en sitios web bajo el control de DIGITEL TS y con una vinculación directa o indirecta a la razón social y/o marca de DIGITEL TS. También se publicará mediante el envío de correo electrónico certificado y en la página de la Autoridad competente.

La publicación se realizará en el momento de su creación y los certificados emitidos se publicarán de manera inmediata a su emisión.

### **15 FIN PRESTACIÓN DEL SERVICIO**

---

#### **15.1 PORTABILIDAD**

DIGITEL TS efectuará la transmisión de la documentación que evidencie todo el registro y otro material en su poder que pudiera ser necesario a quien se considere para poder demostrar la correcta operación del servicio durante un periodo de tiempo razonable según lo dispuesto en el apartado correspondiente a fin de la actividad de la ley 59/2003.

Los procesos de destrucción de material o traspasos concretos de cada servicio, si estos existieran quedarían definidos en sus definiciones de políticas concretas.



## **15.2 CESE ACTIVIDAD DIGITEL TSL – GARANTÍAS**

En caso de cese de su actividad como Prestador de Servicios de Certificación, DIGITEL TS realizará, con una antelación mínima de dos meses, las siguientes acciones:

- Informar a todos los suscriptores de sus certificados y extinguir la vigencia de los mismos revocándolos.
- Informar a todas las terceras partes con las que tenga que haya firmado un convenio de certificación.
- Comunicar al Ministerio competente en materia de Sociedad de la Información y firma electrónica el cese de su actividad y el destino que va a dar a los certificados, así como cualquier otra circunstancia relevante relacionada con el cese de actividad.
- Remitir al Ministerio competente en materia de Sociedad de la Información y firma electrónica toda la información relativa a los certificados electrónicos revocados así como información de eventos y evidencias generadas durante el proceso para que éste se haga cargo de su custodia durante el resto del periodo comprometido.
- Revocar las autorizaciones para poder ejecutar el proceso de emisión de certificados a todo subcontratado.
- Destrucción de las claves privadas.
- DIGITEL TS no contempla la transferencia de la gestión de los certificados que todavía pudieran estar vigentes en el momento del cese de la CA, por lo que extinguirá la vigencia de todos los certificados en los términos establecidos en la Ley 59/2003.

## **16 CONDICIONES GENERALES DE USO**

---

Las Condiciones Generales de la Contratación de los servicios prestados por DIGITEL TS se detallan a continuación:

### **16.1 OBJETO DE LOS SERVICIOS**

DIGITEL TS a través de las presentes Condiciones Generales de Uso regula la prestación de los servicios prestados, que podrán ser completadas, en su caso, por Condiciones Particulares.

### **16.2 AMBITO TERRITORIAL Y ORGANIZACIÓN DEL SERVICIO**

Los Servicios prestados por DIGITEL TS se limitarán al territorio europeo, así como en su caso, a territorio de Latinoamérica.

DIGITEL TS determinará cuál es el equipo humano y técnico necesario para la prestación de los servicios asegurando las condiciones de calidad y operación requeridas y garantizando el nivel de servicio acordado.

DIGITEL TS utilizará todos los medios técnicos y humanos necesarios para la ejecución de los servicios, con la capacidad, cualificación y experiencia adecuada para la prestación de los mismos.

DIGITEL TS se reserva la capacidad de realizar los cambios técnicos y humanos que estime adecuados para mantener la calidad del servicio prestado, sin perjuicio de lo cual, se intentará que los cambios en la prestación del Servicio sean los menores posibles.

### **16.3 MODELO DE PRESTACIÓN DEL SERVICIO**

DIGITEL TS ha implantado un modelo de prestación de los servicios de conformidad con lo descrito en la presente Declaración de Prácticas de Certificación, que permiten dar cumplimiento a las obligaciones establecidas en las presentes Condiciones de Uso.

El modelo de prestación de servicios irá acompañado de un acuerdo de nivel de servicio para medir su realización, así como de un servicio de soporte, que incorporará en términos generales:

- Los criterios que se van a utilizar para la atención de las peticiones.
- El nivel de soporte funcional que se va a proporcionar y disponibilidad de este.
- El nivel de soporte técnico que se va a proporcionar y disponibilidad del mismo.
- El proceso de escalado que se va a seguir a la hora de notificar la ocurrencia de una incidencia.
- El sistema de gestión de peticiones para la resolución de incidencias que se va a utilizar.
- Los mecanismos de comunicación que se van a emplear para proporcionar el soporte.
- Los idiomas disponibles en los que se va a proporcionar el soporte.
- El Acuerdo de Nivel de Servicio (ANS) asociado al servicio contendrá:
  - ANS relativos a tiempos de atención y resolución a la hora de resolver las incidencias
  - ANS relativos a la calidad general con la cual se prestan los servicios
  - ANS relativos a la disponibilidad de los servicios
  - ANS relativos al tiempo de aprovisionamiento de servicios nuevo y/o escalables
  - ANS relativos al rendimiento de volúmenes de información.
- Cuadro de Mando para la gestión, control y gobierno del servicio.
- Informes estadísticos, operativos y de cumplimiento de ANS.

### **16.4 CONDICIONES ECONÓMICAS**

Las tarifas y condiciones económicas de los diferentes servicios se encuentran disponibles en el documento de "Condiciones Generales de Contratación de DIGITEL TS".

No obstante, DIGITEL TS puede establecer marcos contractuales con clientes puntuales que particularicen estas condiciones para el escenario de colaboración establecido entre ambas partes.

Las tarifas establecidas por DIGITEL TS para el pago por la prestación del servicio se mantendrán en base a los siguientes conceptos:

- Cuota mensual por la utilización del Servicio
- Coste por operación de certificación gestionada por la Plataforma: el importe de cada solicitud de operación a la Plataforma.
- Coste por operación de comunicación gestionada por la Plataforma.

En el momento de la contratación, así como previamente o en cualquier otro momento que se precise, si se solicitan a DIGITEL TS estos datos, puede accederse a esta información económica actualizada.

Cabe señalar que, independientemente de que el Destinatario Final de una comunicación acepte o no la operación, la misma se considera como procesada, y por tanto, a efectos de cómputo de uso en la Plataforma, la operación se entiende como solicitada por parte de la aplicación de negocio gestionada por la Plataforma.

### **16.5 CALIDAD DE LOS TRABAJOS**

DIGITEL TS se compromete al desarrollo de su actividad utilizando la diligencia y calidad idónea con el respeto absoluto a las condiciones de confidencialidad y privacidad.

### **16.6 FORMACIÓN DEL PERSONAL**

DIGITEL TS garantiza poner a disposición de su personal los cursos de formación que resultaren necesarios para que la prestación de servicios realice de manera diligente y con el nivel de cualificación adecuado para el desarrollo óptimo del servicio.

Igualmente, serán a cuenta de DIGITEL TS la formación que resultare necesaria para que el personal del Cliente que utilice el servicio contratado. La duración y el número de asistentes serán acordados con el CLIENTE.

### **16.7 CONFIDENCIALIDAD DE LA INFORMACIÓN INTERCAMBIADA**

Todos los datos, programas, aplicaciones y en general la información y utilización de medios aportados permanecerán únicamente en el ámbito de la prestación del servicio, con la obligación de mantener el régimen de confidencialidad de tales medios e información por plazo indefinido.

La información aportada se utilizará única y exclusivamente para los fines determinados en la prestación del servicio y DIGITEL TS velará por la seguridad y confidencialidad de la misma y adoptará todos los medios a su alcance para evitar que sea divulgada a terceros no autorizados, así como evitar que pueda ser transmitida, almacenada o reproducida por cualquier medio. DIGITEL TS tomará así mismo todas las medidas necesarias para evitar que la información sea sustraída o publicada en cualquier forma, excepto por normativa legal o mandato judicial.

Una vez finaliza la prestación del servicio, ambas partes se comprometen a devolver la información considerada como confidencial por escrito o cualquier otro medio sin guardar copia de ningún tipo. En caso de que esta información confidencial no pudiera ser devuelta, a petición del titular de la información, todos los documentos y copias referentes a la misma, serán destruidas o extraídas de los soportes que contuvieran dicha información.

En particular, y por imperativo legal, el PROVEEDOR archivará en soporte informático las declaraciones que hubieran tenido lugar por vía telemática entre las Partes, por un periodo

de 5 años, tras los cuales serán entregados al CLIENTE en un medio duradero de almacenamiento y eliminado de los sistemas informáticos del PROVEEDOR.

Las Partes no estarán sujetas a la obligación de confidencialidad regulada en la presente Cláusula cuando la información confidencial deba ser revelada por imperativo legal o para dar cumplimiento a una orden de naturaleza judicial o administrativa, siempre que notifiquen dicha circunstancia a la Parte a quien pertenece la información confidencial en cuestión.

### **16.8 TRATAMIENTO DE DATOS PERSONALES**

DIGITEL TS se compromete al tratamiento de datos personales en las condiciones y en los términos previstos en el apartado 11 de la Declaración de Prácticas de Certificación.

Así mismo, ambas partes se comprometerán a respetar las obligaciones que, en materia de protección de datos de carácter personal, y en relación con las presentes Condiciones, se deriven del cumplimiento de la normativa vigente, así como a colaborar con la otra Parte en el cumplimiento de dicha normativa

Además, el Cliente empresa jurídica, deberá garantizar en relación con los ficheros que contengan datos de carácter personal de Destinatarios Finales (en adelante, los Ficheros) a los cuales DIGITEL TS tenga acceso exclusivamente para el cumplimiento de los servicios objeto del presente Contrato, de conformidad con lo previsto en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal:

- Que los datos personales de los usuarios Finales de la documentación objeto de revisión y firma que serán procesados por el servicio prestado por DIGITEL TS, han sido facilitados por los propios Destinatarios u obtenidos con su consentimiento.
- Que ha informado a dichos Destinatarios de que sus datos personales están incluidos en los Ficheros de su titularidad, de conformidad con la vigente normativa de protección de datos, y de que el Destinatario tiene derecho de acceso, rectificación, cancelación y oposición a dicho tratamiento, así como cualquier otra obligación de información que exija la ley.
- Que ha recabado cuantos consentimientos de los Destinatarios exija la ley

### **16.9 RESOLUCIÓN**

Sin perjuicio de las causas descritas en la normativa española, DIGITEL TS considerará como causa de resolución anticipada de la prestación de los servicios, las siguientes:

- El incumplimiento por las partes de cualquier obligación de las previstas en las presentes Condiciones Generales de Uso, requerida la Parte incumplidora, ésta no procede a la subsanación del incumplimiento en un plazo de 30 días.
- Por decisión judicial o administrativa, que implique la imposibilidad para cualquiera de las partes de ejecutar las condiciones pactadas del servicio.
- El simple incumplimiento y/o retraso en el pago de cualquiera de las obligaciones de abono que se relacionan en las condiciones de contratación, se entenderá como motivo suficiente para que DIGITEL TS de por resuelto de manera unilateral el contrato

de prestación de servicio, sin perjuicio de reclamar las obligaciones pendientes de abono o pagos si las hubiere.

DIGITEL TS se reserva la facultad de resolución del contrato en caso de que existieran circunstancias sobrevenidas, derivadas en un cambio de las condiciones de mercado, por vicios o deficiencias en los datos o informaciones recibidas para la elaboración de la Propuesta Económica, o cualquier otra circunstancia ajena a su voluntad, incluida la producción de un desajuste entre los precios pactados y el coste de ejecución del Servicio, derivado de circunstancias del mercado resultare un déficit económico por la ejecución del Servicio y en general por cualquier causa ajena a la voluntad de DIGITEL TS, que produzca la ruptura del equilibrio económico del mismo.

#### **16.10 SUBCONTRATACION**

DIGITEL TS podrá subcontratar los servicios que estime necesarios para el aprovisionamiento y explotación del Servicio de acuerdo a las necesidades que surgieran.

#### **16.11 LEGISLACIÓN Y JURISDICCIÓN APLICABLE**

Las presentes condiciones generales de contratación se regirán por la normativa española.

Las partes, con expresa renuncia a cualquier fuero propio que pudiera corresponderles, se someten a la Jurisdicción y Competencia de los Juzgados y Tribunales de Valladolid para cualquier cuestión relativa a la interpretación, cumplimiento o ejecución del presente Contrato.

#### **16.12 RESPONSABILIDAD**

DIGITEL TS no será responsable de los actos u omisiones realizados por el Cliente, siendo éste quien asumirá todos los daños y perjuicios, directos e indirectos, que se pudieren ocasionar a cualquier persona, propiedad, empresa, servicio público o privado, concretamente por las pérdidas de beneficios, pérdida de información y datos, o los correspondientes daños, como consecuencia de los actos, omisiones o negligencias del Cliente así como de terceros a él ligados, por uso inadecuado, siendo de exclusivo riesgo del Cliente.

Tampoco se responsabilizará DIGITEL TS de las pérdidas de negocio, perjuicios patrimoniales o de cualquier otro daño causado al Cliente o a terceros, derivado de cualquier circunstancia fuera del control del DIGITEL TS.

DIGITEL TS no será responsable en ningún caso, de consecuencias dañosas que tengan su origen en causas de fuerza mayor. A tales efectos, se entiende por "fuerza mayor", un acontecimiento extraño a la voluntad del individuo que sin culpa le impide cumplir una obligación contractual y por ello se le exime de responsabilidad en ese incumplimiento que le sería exigible en condiciones normales.

#### **16.13 MODIFICACIONES**

Las partes podrán modificar las presentes condiciones generales de uso, así como establecer cláusulas particulares siempre que se realice por escrito.

#### **16.14 NULIDAD**

Si cualquiera de las Condiciones Generales de Uso fuese declarada total o parcialmente nula o ineficaz, tal nulidad o ineficacia afectará únicamente a dicha disposición o parte de la misma que resulte ineficaz o nula, y el resto de las cláusulas continuarán vigentes, teniéndose tal condición o la parte de la misma que resulte afectada por no puesta.

#### **16.15 NOTIFICACIONES**

Las notificaciones, comunicaciones o requerimientos entre las partes en desarrollo de la prestación de servicios acordada, deberán realizarlas mediante cualquier medio que permita tener fehaciente constancia de su envío, recepción y contenido de la comunicación.

A los efectos las partes designarán expresamente los domicilios para la práctica de comunicaciones. En caso de modificación del domicilio, las partes se obligarán a notificar a la otra la modificación en la forma establecida en el párrafo primero.