PÚBLICO

POLÍTICA DE CERTIFICACIÓN - DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN PARA LAS AUTORIDADES DE CERTIFICACIÓN EN LÍNEA

AUTOR(ES)	:	F. Da Silva
NÚMERO DE DOCUMENTO	:	WLM-OTU-F002
VERSIÓN	:	4.0
ESTADO	:	Final
ORIGEN	:	Worldline
FECHA DEL DOCUMENTO	:	23 de abril de 2019
NÚMERO DE PÁGINAS	:	97

TSP MediaCert

Digitally signed by TSP MediaCert
DN: CN=TSP MediaCert, O=Worldline, E=dl-mediacert-tsp@worldline.com, C=FR
Reason: I am approving this document
Location:
Date: 2019-05-14 15:38:19

Función	Nombre	Firma	Fecha
Corrector 1 - Asistente Resp.	Fanny Lesecq	Fanny Lesecq	23/04/2019
Revisor 2 - CISO *(Director de seguridad de la información)*	Didier Sobkowiak	Didier Sobkowiak	23/04/2019
Función de aseguramiento de la calidad	Fanny Lesecq	Fanny Lesecq	23/04/2019
Propietario del documento	Comité MediaCert	Guillaume Bailleul	23/04/2019
Autorizador - TSP Resp.	Guillaume Bailleul	Guillaume Bailleul	23/04/2019

Tabla de Contenido

Tabla de Contenido 2

Lista de cambios 4

1 Introducción 7

1.1 Presentación general 7
1.2 Identificación 8
1.3 Entidades implicadas en la Infraestructura de Gestión de Claves 10
1.4 Categorías de Certificados 15
1.5 Uso de los Certificados 17
1.6 Gestión de la PC 18
1.7 Definiciones y acrónimos 18

2 Responsabilidades en materia de suministro de la información que debe publicarse 24

2.1 Entidades responsables de la puesta a disposición de la información 24
2.2 Información que se publicará 24
2.3 Plazos de publicación y periodicidad 24
2.4 Control de acceso a la información publicada 25

3 Identificación y autenticación 26

3.1 Nombramiento 26
3.2 Validación inicial de identidad 27
3.3 Identificación y validación de una solicitud de renovación de claves 35
3.4 Identificación y validación de una solicitud de revocación 35

4 Requisitos operativos a lo largo del ciclo de vida de los Certificados 37

4.1 Solicitud de creación de un Certificado 37
4.2 Procesamiento de una solicitud para crear un Certificado 38
4.3 Emisión del Certificado 40
4.4 Aceptación del Certificado 41
4.5 Usos de la Pareja de claves y del Certificado 41
4.6 Renovación de un Certificado 42
4.7 Emisión de un nuevo Certificado tras el cambio de la Pareja de claves 43
4.8 Modificación de un Certificado 43
4.9 Revocación y suspensión de un Certificado 44
4.10 Funciones de información sobre el estado de los Certificados 49
4.11 Fin de la relación entre el Suscriptor y la AC 50
4.12 Secuestrador de claves y recuperación 50

5 Medidas de seguridad no técnicas 52

5.1 Medidas de seguridad física 52
5.2 Medidas de seguridad de procedimiento 52
5.3 Medidas de seguridad para el personal 53
5.4 Procedimientos para la compilación de datos de auditoría 54
5.5 Archivo de datos 55
5.6 Cambio de Pareja de claves de AC 57
5.7 Recuperación del compromiso y del desastre 58

5.8 Fin del ciclo de vida de la IGC 58

6 Medidas técnicas de seguridad 60

6.1 Generación e instalación de Parejas de claves 60
6.2 Medidas de seguridad para la protección de la clave privada y los módulos criptográficos 62
6.3 Otros aspectos de la gestión de Parejas de claves 65
6.4 Datos de activación 66
6.5 Medidas de seguridad de los sistemas informáticos 66
6.6 Medidas de seguridad para los sistemas durante su ciclo de vida 67
6.7 Medidas de seguridad de la red 67
6.8 Sistema de registro de fecha y hora 67

7 Modelo de los Certificados y LCR 68

7.1 Modelo de los certificados 68
7.2 Perfil LCR 81
7.3 Perfil de OCSP 82

8 Auditoría de cumplimiento y otras evaluaciones 85

8.1 Frecuencia y/o circunstancias de las evaluaciones 85
8.2 Identidades / cualificaciones de los evaluadores 85
8.3 Relaciones entre los evaluadores y las entidades evaluadas 85
8.4 Temas cubiertos por las evaluaciones 85
8.5 Medidas adoptadas en respuesta a las conclusiones de la evaluación 85
8.6 Comunicación de resultados 85

9 Otros asuntos comerciales y legales 86

9.1 Tarifas 86
9.2 Seguros 86
9.3 Confidencialidad de los datos profesionales 86
9.4 Protección de datos de carácter personal 90
9.5 Derechos de propiedad intelectual e industrial 90
9.6 Interpretaciones y garantías contractuales 90
9.7 Límite de garantía 94
9.8 Limitación de responsabilidad 94
9.9 Indemnizaciones 95
9.10 Duración y terminación anticipada de la validez de la PC 95
9.11 Notificaciones individuales y comunicaciones entre participantes 95
9.12 Enmiendas a la PC 96
9.13 Disposiciones relativas a la resolución de conflictos 96
9.14 Jurisdicciones competentes 96
9.15 Cumplimiento de las leyes y reglamentos 96
9.16 Disposiciones diversas 96
9.17 Otras provisiones 97

Lista de cambios

Versión	Fecha	Descripción	Autor(es)
1.0	24/12/2012	Versión pública inicial.	C. Brunet
1.1	08/04/2013	Evolución tras la observación durante la auditoría inicial ETSI 102 042: • 4.9.2.1: reformulación de los orígenes de la revocación • 5.8.2: aclaración sobre la LCR ampliado en caso de cese de actividad	C. Brunet
1.2	22/11/2013	Evolución tras el ajuste del contrato: • 3.2.3.1: explicaciones adicionales sobre la conservación de los datos no utilizados en el Certificado • 5.5.2: modificación de los plazos de conservación de los expedientes de registro. • 9.6.4: el término "inmediatamente" se sustituye por "lo antes posible". • 9.9, 9.13, 9.14, 9.16.5: modificación de la referencia a los contratos Cliente/AWL	C. Brunet
1.3	01/02/2015	Evolución tras el cambio de denominación social y la modificación del modelo de Certificado: • Todo el documento: Atos Worldline se sustituye por Worldline (tenga en cuenta que es la misma empresa con el mismo Siret[1]). • 7.1.2.3: modificación de los valores indicados en los campos DN y Subject alt y key usage	C. Brunet
2.0	07/11/2016	Evolución tras la retroalimentación de la auditoría: • Modificación del §3.2.3.1 para la Validación de la identidad de un titular de un Certificado de un solo uso mediante identificación externa y, en el caso del titular perteneciente a la Organización del Suscriptor, reformulación del requisito de control de la identidad del Titular. • Adición de procedimientos y razones para destruir las Parejas de llaves AC en §6.3.4 • Cambiar "operador" por "piloto". • Homogeneización de los límites de cobertura con respecto a la GCU (§9.7) • Modificación del §4.9.3.2 para describir el procedimiento de revocación de un Certificado de Organización. • Añadidos métodos para asegurar que el periodo de revocación sea monitoreado (§4.9.3.2 y §5.7.3). • Adición de los §5.2.5 y §5.2.6 y modificación del §5.3.6 para el cumplimiento de AC con los requisitos del 7.4.3 • Adición de §5.4.6 sobre los procedimientos para la restitución y control de la restitución de los registros de eventos. • Modificación del §5.2.4 sobre las funciones que requieren la separación de asignaciones • Añadir OIDs a los certificados de ensayo (§1.2.2) y añadir descripciones (§7.1.2.4 y	V. Dumond C. Lootvoet A. Brugnot J.J. Milhem

[1] Siret: Número de identificación de una empresa francesa

Versión	Fecha	Descripción	Autor(es)
		§7.1.2.5) • Adición del OID de la PC OTU a las plantillas de todos los Certificados • Adición de §4.9.10 sobre el archivo de las LCR • Añadida la descripción de la monitorización de la página de MediaCert (§2.4.2) • Adición de una referencia a la firma de los documentos de la Autoridad de Certificación para garantizar el control de la autenticidad (§2.4.3). • Revisión del §5.3.2 sobre la comprobación de los antecedentes penales • Modificación de plantillas y OIDs para seguir el cambio de versión de PC (§1.2.2, §7.1.2.2, §7.1.2.3, §7.1.2.4, §7.1.2.5) • Adición de una mención de la no verificación del correo electrónico al solicitar un Certificado en §3.2.4. • Corrección del § 7.1.5 Limitaciones de los nombres que afectan al atributo CN y también a las GN y SN, si procede, a los Certificados de la Organización. • Modificación del §9.12.2 sobre las circunstancias bajo las cuales se debe cambiar el OID • Adición de las definiciones que faltan • Reformulaciones y aclaraciones sobre el contrato, el expediente de suscripción, las obligaciones del Suscriptor, la identificación del Titular, la validación de una Organización. • Adición de un paso de aceptación del Certificado por parte del Titular de un Certificado OTU • Adición de un compromiso práctico no discriminatorio al §9.6	
2.1	02/02/2017	• Modificación de la información del Titular que debe ser recogida, verificada y almacenada por la AC (§3.2.3.1) • Revisión de los perfiles de LCR (§7.2) • Revisión de las plantillas de Certificados (§7.1) • Modificación de la duración del plazo de preaviso en caso de cambio en la PC (§9.11)	C. Lootvoet
3.0	09/06/2017	Reescritura para tener en cuenta las limitaciones reglamentarias de eIDAS.	F. Lesecq V. Dumond
3.1	21/07/2017	Teniendo en cuenta las observaciones de la auditoría de eIDAS.	F. Lesecq F. Da Silva
3.2	18/09/2018	Integración del documento en la estructura documental del TSP MediaCert, es decir, coherencia con el PG. Añadir causas de revocación de acuerdo con la actualización de ETSI EN 319 411-1 (v1.2.2). Supresión de la obligación de publicar en línea: • versiones anteriores de PC-DPC	F. Da Silva

Versión	Fecha	Descripción	Autor(es)
		• versiones en inglés de las políticas Adición de una especificación relacionada con el RGPD[2] y la conservación de la información de identificación de un Titular de un Certificado OTU. Excepcionalmente, esta versión no se publicará porque no introduce nuevos elementos y se publicará una nueva versión (con la integración de una nueva AC en este documento) dentro del mismo plazo (más información en el informe de validación de la reunión de seguridad).	
3.3	18/09/2018	Adición de una AC al alcance de este documento. El impacto es sólo la adición de dos rangos y la especificación del nivel de identificación asociado con ellos. Este PC-DPC se convierte en la PC-DPC de las "AC en línea". Teniendo en cuenta las observaciones/desviaciones detectadas durante la auditoría de vigilancia de 2018 de la AC OTU. Revisión de la coherencia con la RGPD.	F. Da Silva V. Dumond
3.4	12/10/2018	Consideración de las observaciones/desviaciones detectadas durante la auditoría de certificación 2018 de la AC OTU LCP: • cambio de la descripción del contenido de una LCR • aclaración de la lista de medios de validación de los consentimientos • revisión de las condiciones de revocación de los Certificados de un solo uso	F. Da Silva
3.5	23/04/2019	Revisión de las condiciones para la revocación de los Certificados de Uso Único (extensión de la enmienda realizada en la v3.4) Modificación de la descripción del contenido de una LCR (cancela la modificación realizada en la v3.4) Supresión de la referencia al artículo 40 (derechos humanos) Evolución de las versiones estándar en el repositorio	F. Da Silva
4.0	23/04/2019	Nueva estructura: en el marco del DRP, el AC OTU se divide en dos AC (AC OTU y AC ORG).	F. Da Silva J. Steux

[2] RGPD = Reglamento General de Protección de Datos

1 Introducción

1.1 Presentación general

El *Proveedor de Servicios Fiduciarios*[3] MediaCert, establecido por Worldline, proporciona un conjunto de servicios fiduciarios y, por lo tanto, está sujeto al Reglamento eIDAS nº 910/2014 del Parlamento Europeo y del Consejo Europeo sobre identificación electrónica y servicios fiduciarios para transacciones electrónicas en el mercado interior.

Este documento describe la Política de Certificación de varias Autoridades de Certificación denominadas "en línea", no cualificadas, operadas por TSP MediaCert para regir todo el ciclo de vida (creación, emisión, uso,...) de los Certificados de firma de *un solo uso*[4] *(*también llamados "One Time Usage") implementados en el contexto de la suscripción en línea, pero también por los Certificados de Sello Electrónico utilizados para sellar los datos electrónicos para garantizar su origen e integridad:

- la Autoridad de Certificación llamada "AC OTU LCP";
- la Autoridad de Certificación llamada "AC OTU".
- La Autoridad de Certificación llamada "AC ORG"

Estas AC funcionan exactamente de la misma manera (organizativa, técnica, infraestructura, etc.), y tienen el mismo hardware y software.

Sin embargo, difieren en diferentes temas :

Diferencias	AC OTU	AC ORG	AC OTU LCP
Uso de la clave / certificado	Certificado de firma electrónica (véase el capítulo 1.5.1.1)	Certificado de sellado electrónico (véase el capítulo 1.5.1.1)	Certificado de firma electónica (véase el capítulo 1.5.1.1)
Identificación del futuro titular del certificado de uso único	exige un nivel de identificación más estricto para la expedición de los certificados de uso único que el definido por el nivel LCP, pero menos estricto que el definido por el nivel NCP, de ahí su denominada gama "mejorada". (véase el capítulo 1.2.1);	X	exige un nivel de identificación para la provisión de Certificados de Uso Único de acuerdo con el nivel LCP, de ahí su llamado rango "estándar". (véase el capítulo 1.2.1).

Este documento se presenta en este contexto:

- los requisitos a los que están sujetas cada una de estas AC en línea operadas por TSP MediaCert;
- los usos para los que se expiden los Certificados;
- la gestión de estos Certificados en su ciclo de vida;

[3] Proveedor de Servicios Fiduciarios= Trust Service Provider

[4] Un solo uso = One Time Usage (OTU)

- medidas de seguridad entorno a la Infraestructura de Gestión de Claves;
- obligaciones y requisitos relativos a los distintos actores.

Además de describir la Política de Certificación, este documento describe la Declaración de Prácticas de Certificación. Esta es la declaración de prácticas que las Autoridades de Certificación en línea utilizan en la gestión de los Certificados que emiten.

Además, como Servicio de Confianza proporcionado por TSP MediaCert, todos los requisitos y prácticas de la [PG] son, a menos que se indique lo contrario, aplicables al alcance de estas AC en línea.

1.2 Identificación

1.2.1 Identificación del documento

Elementos	Valor
Título	Política de certificación - Declaración de prácticas de certificación para las autoridades de certificación en línea
Referencia del documento	WLM-OTU-F002
OID	1.2.250.1.111.20.5.4
Versión	4.0
Autor	F. Da Silva

El OID de este documento se basa en el OID "**1.2.250.1.111.20.5**": 1.2.250.1.111.20.5.**z**.**w** donde:

- z : versión principal de esta política (por ejemplo, la versión 3.1 → 3);
- w : tipo de Certificado utilizado por las Autoridades de Certificación (AC) en línea.

Como se desprende de la descripción anterior, las Autoridades de Certificación en línea han definido un OID para cada uno de los tipos de Certificados que emiten de la siguiente manera:

Ámbito de aplicación	Gama de certificado	Cumplimiento y nivel de seguridad específico	OID
AC OTU	Certificados de un solo uso *"reforzado"*	[ETSI EN 319 411-1] Nivel LCP *(no calificado)*	1.2.250.1.111.20.5.4.1
	Certificados de pruebas "reforzados" de un solo uso	[ETSI EN 319 411-1] Nivel LCP *(no calificado)*	1.2.250.1.111.20.5.4.3
AC ORG	Certificados de Organización	[ETSI EN 319 411-1] Nivel LCP *(no calificado)*	1.2.250.1.111.20.5.4.2
	Certificados de Organización de pruebas	[ETSI EN 319 411-1] Nivel LCP *(no calificado)*	1.2.250.1.111.20.5.4.4
AC OTU LCP	Certificados de un solo uso	[ETSI EN 319 411-1]	1.2.250.1.111.20.5.4.5

Ámbito de aplicación	Gama de certificado	Cumplimiento y nivel de seguridad específico	OID
	"estándar"	Nivel LCP *(no calificado)*	
	Certificados de un solo uso de pruebas *"estándar"*	[ETSI EN 319 411-1] Nivel LCP *(no calificado)*	1.2.250.1.111.20.5.4.6

Puede obtenerse más información en la Política General [PG].

Este documento se denominará "PC-DPC" en todo el documento.

1.2.2 Identificación de las Autoridades de Certificación

A menos que se especifique lo contrario, los requisitos de este documento son aplicables a las AC definidas en el capítulo **Erreur ! Source du renvoi introuvable.** este documento. Los requisitos aplicables a una única AC van precedidos de la declaración:

- [AC OTU LCP] para la AC OTU LCP;
- [AC OTU] para la AC OTU;
- [AC ORG] para la AC ORG.

Estos están enlazados a las Autoridades de Certificación Raíz de Worldline, cuya información necesaria es la siguiente:

Ámbito de aplicación	Elementos	Valor
AC OTU y AC ORG	*OID* de la PC-DPC	1.2.250.1.111.20.3.1
	OID de la AC emisora	1.2.250.1.111.20.3.1.3
	Distinguished Name (DN)[5] de la AC Raíz	C = FR O = Worldline OU = 0002 378901946 CN = MediaCert Trust CA - 2019
AC OTU LCP	*OID* de la PC-DPC	1.2.250.1.111.20.3.1
	OID de la AC emisora	1.2.250.1.111.20.3.1.1
	Distinguished Name (DN)[6] de la AC Raíz	C = FR O = Worldline OU = 0002 378901946 CN = MediaCert Root CA 2018

La estructura de las cadenas de certificación AC en línea es la siguiente :

[5] DN por "Distinguished Name" = Nombre Distinguido
[6] DN por "Distinguished Name" = Nombre Distinguido

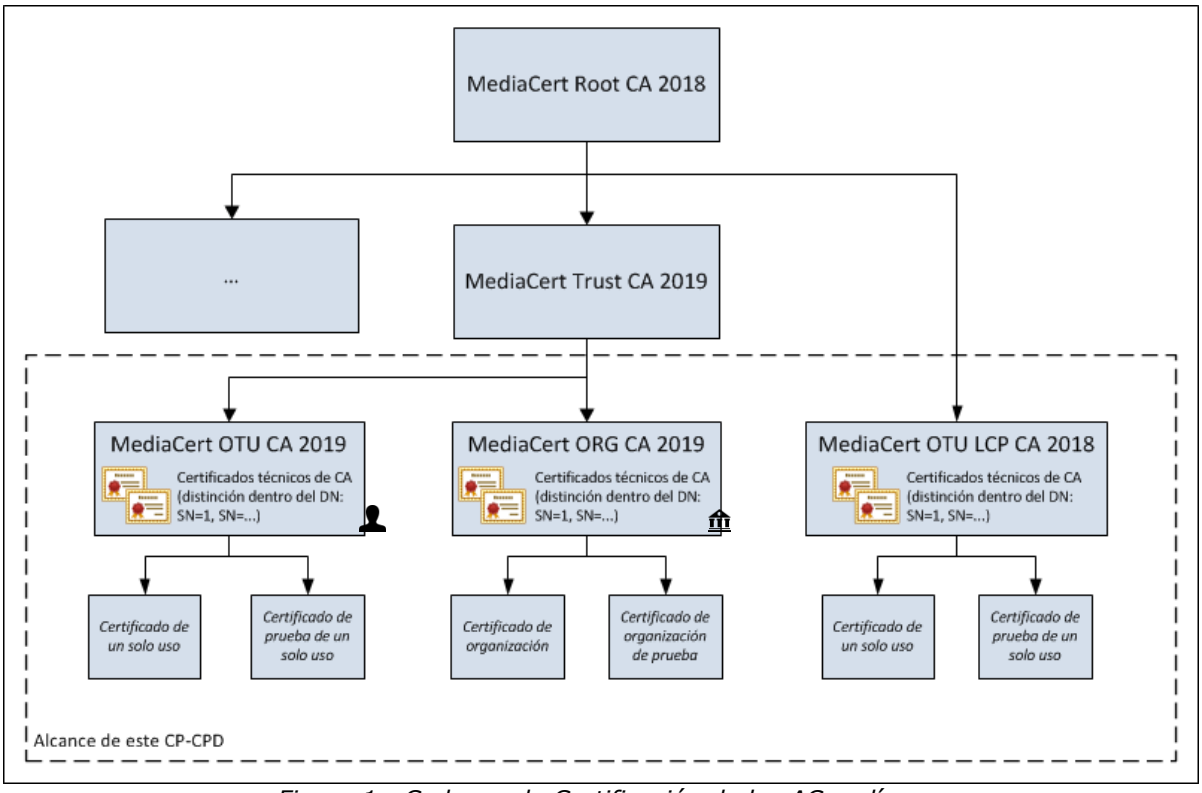

Figura 1 - Cadenas de Certificación de las AC en línea

1.3 Entidades implicadas en la Infraestructura de Gestión de Claves

La Infraestructura de Gestión de Claves (IGC) consiste en un conjunto de recursos técnicos, humanos, documentales y contractuales, dedicados a gestionar el ciclo de vida de los Certificados electrónicos emitidos por la Autoridad de Certificación. Proporciona, mediante sistemas criptográficos asimétricos, un entorno seguro para los intercambios electrónicos.

Las AC confían en esta infraestructura técnica. Los servicios de las IGC son el resultado de diferentes servicios que corresponden a las diferentes etapas del ciclo de vida de los Pares de Claves y Certificados. Con este fin, las IGC en cuestión están formadas por una serie de entidades, como se muestra en el diagrama de bloques de la figura 2.

El desglose funcional de las IGC afectadas por esta PC-DPC es el siguiente:

- Servicio de registro;
- Servicio de generación de Certificados;
- Servicio de entrega de Certificados;
- Servicio de revocación de Certificados;
- Servicio de información sobre el estado de los Certificados.

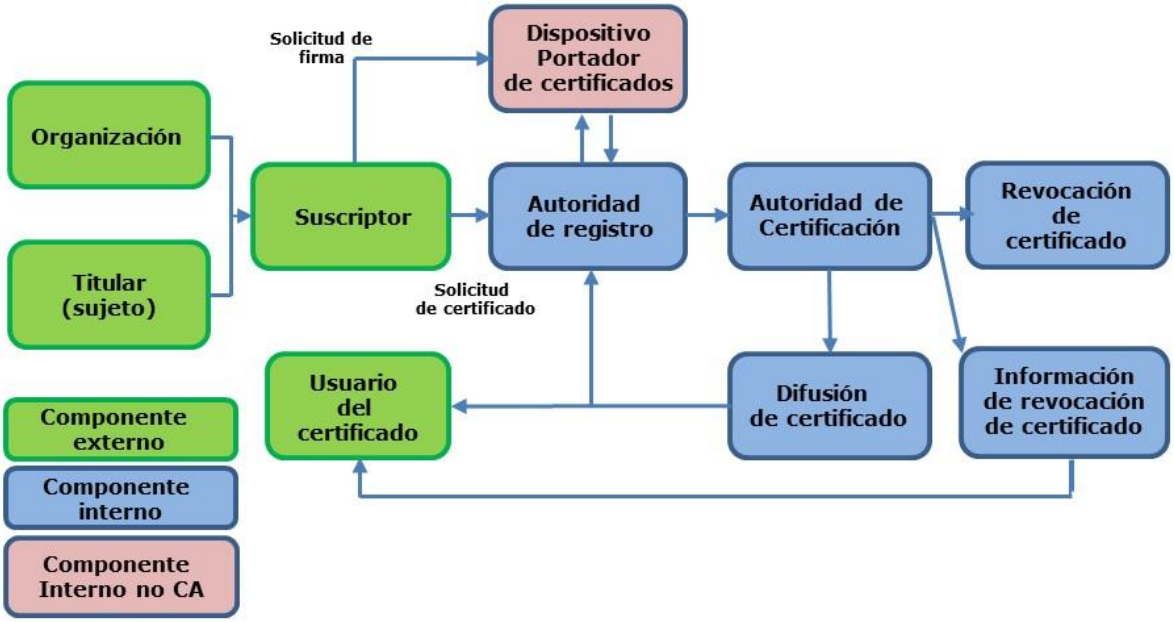

Figura 4- Diagrama de bloques de las IGC que operan ACs en línea

1.3.1 Autoridad de Certificación

Una Autoridad de Certificación se refiere a una entidad capaz de producir Certificados a petición del Servicio de registro. Esta entidad se encarga de todo el ciclo de vida de los Certificados (creación, publicación,...).

Las Autoridades de Certificación en línea están representadas por un Gerente de Autoridad designado dentro de Worldline. Este Gerente de Autoridad tiene subordinados, es decir, Gerentes de Autoridades adjuntos, nombrados por el Gerente de Autoridad él mismo.

1.3.1.1 Servicio de generación

Este servicio genera Certificados a partir:

- de la información transmitida por la Autoridad de Registro; y
- de la clave pública del Certificado desde la función de generación de elementos secretos.

Estos Certificados se firman electrónicamente con la clave privada de la AC de destino y sólo pueden utilizarse para los fines descritos en el capítulo 1.5.1.1 de este documento.

1.3.1.2 Servicio de difusión

Una vez generados los Certificados, se envían a la Autoridad de Registro, que a su vez los envía al Dispositivo Portador del Certificado.

1.3.1.3 Servicio de revocación

Este servicio revoca los Certificados basados en una solicitud de revocación previamente proporcionada. Los resultados se difunden a través de los servicios de información sobre el estado de los Certificados.

1.3.1.4 Servicio de información sobre el estado de los Certificados

Este servicio proporciona a los usuarios de Certificados información sobre el estado de los Certificados (revocados, suspendidos,...). Esta función se implementa a través de modos de publicación actualizados regularmente: Listas de Certificados Revocados (LCR), Lista de Autoridades Revocadas (LAR), contestador automático OCSP.

1.3.2 Autoridad de Registro

La Autoridad de Registro es el interlocutor de las unidades cliente (Suscriptores) que le transmiten las solicitudes de creación o revocación de Certificados. Por lo tanto, soporta las siguientes operaciones:

- autenticación del Suscriptor que solicita la creación de un Certificado;
- verificación del contenido de las solicitudes de creación de Certificados;
- [AC OTU][AC OTU LCP] verificación de la correcta aplicación de la política de identificación, por parte de los Suscriptores, en el contexto de la emisión de Certificados de un solo uso;
- [AC ORG] verificación de la identidad del futuro Titular del Certificado de Organización;
- registro de las solicitudes de creación y revocación de Certificados;
- aceptación o denegación de solicitudes de creación y revocación de Certificados;
- suministro de Certificados al Dispositivo Portador de Certificados;
- archivo de solicitudes para crear y revocar Certificados.

Para la prestación de estos servicios, las AC disponen de una Autoridad de Registro propia (además, es la misma) que cuenta con un servicio que cuenta con los medios técnicos y humanos para asegurar la gestión del ciclo de vida de los Certificados que emiten y que, por tanto, constituye un único punto de acceso a dichas Autoridades de Certificación (servidores que permiten la transmisión de solicitudes y la entrega de Certificados).

1.3.3 Dispositivo Portador de Certificados

A los efectos de este PC-DPC, el Dispositivo Portador de Certificados no se considera el Titular del Certificado.

De hecho, el Dispositivo Portador de Certificados se refiere aquí a una entidad de software y hardware alojada por Worldline, que almacena el Certificado y la clave privada del Titular o de una Organización.

Para cada Certificado generado por las Autoridades de Certificación (AC), el Dispositivo Portador de Certificado(s) es responsable de las siguientes funciones:

- generación del Par de claves;

- almacenamiento seguro del Par de claves;
- generación de la solicitud de Certificación (CSR), que contiene la información del usuario previamente transmitida por el Suscriptor;
- uso de la clave privada y del Certificado en los casos de uso descritos en el capítulo 1.5;
- destrucción de la clave privada tal como se describe en el capítulo 6.2.10.2 presente documento;

El Dispositivo Portador de Certificados proporciona almacenamiento seguro y control exclusivo en nombre del Titular u Organización de los elementos secretos.

El control exclusivo de los Certificados está garantizado:

- por los elementos de seguridad de la caja criptográfica (protección de los secretos almacenados);
- por un aislamiento de red que impide que cualquier servidor no autorizado se conecte a estas cajas.

El dispositivo portador del Certificado puede tener dos (2) tipos de Certificados:

- Certificado de un solo uso: véase el capítulo 1.4.1;
- Certificado de Organización: véase el capítulo 1.4.2.

1.3.4 Destinatario de los Certificados

La provisión de Certificados por parte de las Autoridades de Certificación (AC) en línea requiere la suscripción previa a los servicios de estas Autoridades de Certificación. Esto requiere la firma de un Contrato de Suscripción con TSP[7] MediaCert. Este contrato especifica el tipo de Certificado que el Suscriptor desea implementar:

- [AC OTU][AC OTU LCP] Certificado de firma de *One Time Usage*[8] expedido a nombre de una persona física (Titular) para poder firmar Documentos (véase el capítulo 1.5.1.1); y/o
- [AC ORG] Certificado de Organización expedido a nombre de una Organización para poder sellar Documentos a nombre de su Organización o de su Organización principal (véase el capítulo 1.5.1.1).

1.3.4.1 [AC OTU][AC OTU LCP] Servicio de firma electrónica

Si se trata de firmar datos electrónicos, las dos (2) AC en línea producen Certificados de un solo uso (ver Capítulo 1.4.1).
En el caso de los Certificados de un solo uso, el Suscriptor solicita la creación de un Certificado a la Autoridad de Registro mediante un proceso técnico descrito en el capítulo 3.2.5.1. El Suscriptor, en este caso:

- debe identificarse ante la Autoridad de Registro (véase el capítulo 3.2.2.1);

[7] TSP = Trust Service Provider = Proveedor de Servicios Fiduciarios
[8] One Time Usage = OTU = Un solo uso

- debe, previo a la solicitud de creación del Certificado para el Titular, haberle identificado de manera que el Certificado expedido pueda basarse en una identidad fiable y verificada (véase el capítulo 3.2.3.1);

- debe haber obtenido del Titular los consentimientos necesarios para solicitar a la Autoridad de Registro la generación de un Certificado de un solo uso (véase el capítulo 3.2.3.1).

1.3.4.2 [AC ORG] Servicio de sellado electrónico

Si se trata de sellar datos electrónicos en nombre de Organizaciones vinculadas al Suscriptor, legalmente o por convenio, el AC produce Certificados de Organización (véase el capítulo 1.4.2). De hecho, la Organización, a través del Suscriptor, utilizará un Certificado operado por Worldline, para garantizar la integridad de los documentos y autenticar su origen.

Un Certificado de Organización puede referirse a la persona que lo representa legal, estatutariamente o por acuerdo. Cualquiera de los dos:

- el representante legal que figura en el extracto Kbis[9] de la Organización;

- una persona debidamente autorizada, ya sea por acuerdo o por ley, para representar a la Organización y para figurar en el Certificado.

En todos los casos, la persona designada deberá estar debidamente autorizada por los órganos competentes de la Organización para ser incluida en el Certificado.

La persona que tenga derecho a incluir su identidad en el Certificado deberá aportar pruebas de ello a la autoridad de registro para poder actuar como representante de la Organización. Si la Organización no es el Suscriptor y autoriza al Suscriptor a actuar en su nombre, el Suscriptor deberá justificar ante la Autoridad de Registro sus derechos para actuar en nombre de esta Organización, así como los derechos de la persona designada para incluir su identidad en el Certificado para representar a la Organización.

El representante del Suscriptor es la única persona autorizada para presentar solicitudes de Certificados a la Autoridad de Registro.

Por consiguiente, debe designarse por escrito a la Autoridad de Registro un representante del Suscriptor. Este representante del Suscriptor puede ser:

- el representante legal del Suscriptor (tal como aparece en un extracto Kbis[10] del Suscriptor con menos de tres (3) meses de antigüedad);

- su representante convencional (como aparece, por ejemplo, en los estatutos);

- un representante autorizado por el representante legal para representar al Suscriptor en la ejecución del Contrato de Suscripción.

Aunque el Suscriptor y la Organización son en la mayoría de los casos una misma entidad, es posible diferenciarlas. Por ejemplo, un Suscriptor puede querer utilizar una marca en lugar del nombre de la empresa suscriptora. Además, en el caso de múltiples filiales de un grupo, el Suscriptor y la Organización pueden no tener el mismo nombre.

[9] Kbis = Documento oficial que certifica la existencia legal de una empresa en Francia.
[10] Kbis = Documento oficial que certifica la existencia legal de una empresa en Francia.

En todos los casos, el Suscriptor deberá demostrar el derecho que le asiste (propiedad del nombre, documento Kbis, mandato, etc.) a indicar un nombre de Organización diferente al suyo propio.

El Suscriptor, a través de su representante legal o estatutario, podrá designar formalmente por escrito a uno o varios representantes adjuntos del Suscriptor que también estén autorizados para representarlo. Para ello, el Suscriptor debe informar a la Autoridad de Registro y otorgarle las facultades necesarias.

1.3.5 Usuarios de Certificados

El usuario de un Certificado es la persona física o jurídica que utiliza la información contenida en un Certificado que recibe para los fines descritos en el capítulo 1.5.1.1.

Es responsabilidad de los usuarios verificar la validez del Certificado, al menos antes de su uso, mediante el uso de:

- la información contenida en el Certificado (fecha de validez,...);
- información adicional proporcionada por la Autoridad de Certificación (AC), como el estado de revocación del Certificado (véase el capítulo 4.10).

Cabe señalar que la firma de un Documento es utilizada principalmente por los productos proporcionados por la empresa ADOBE™, como Acrobat Reader©. Estos productos tienen funciones de visualización de firmas de documentos.

No todos los productos de visualización de Documentos tienen funciones de visor de firmas.

1.3.6 Otros participantes

Los recursos humanos completan el sistema:

- operadores de sistemas informáticos (mantenimiento de condiciones operativas);
- equipos encargados de mantener el cumplimiento.

1.4 Categorías de Certificados

Las Autoridades de Certificación (AC) en línea emiten una serie de Certificados:

- [AC OTU LCP] La AC produce dos (2) tipos de Certificados;
- [AC OTU] La AC produce dos (2) tipos de Certificados;
- [AC ORG] La AC produce dos (2) tipos de certificados.

Cada tipo de Certificado se distingue por su OID (véase el capítulo 1.2.1).

1.4.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

Un Certificado de un solo uso es producido dinámicamente por las Autoridades de Certificación durante el proceso de firma electrónica iniciado por el Suscriptor a petición de una persona física (Titular).

Este Titular podrá ser una persona física que actúe por sus propias necesidades o por las necesidades de su Organización y para la que esté debidamente autorizado a firmar.

Este Certificado se utiliza durante una única sesión de firma (firma de los distintos Documentos de un contrato para el Titular) por el Dispositivo Portador del Certificado. Tiene una vida útil muy corta, como se describe en el capítulo 6.3.2.

El Suscriptor transmite la solicitud de un Certificado de un solo uso a la Autoridad de Registro mediante un mensaje firmado electrónicamente por el Suscriptor. Este mensaje contiene:

- los datos de identificación del Titular;
- un Sello electrónico para garantizar la integridad de los datos de identificación, así como la identidad del Suscriptor.

Una vez que la aplicación del Certificado de un solo uso del Suscriptor ha sido controlada y validada por la Autoridad de Registro, el Certificado es emitido por la AC de destino que firma el Certificado que contiene la identidad del Titular que aparece en el Certificado, verificado por el Suscriptor.

En efecto, el Suscriptor es responsable de los datos de identificación transmitidos en la solicitud a la Autoridad de Registro y que permite crear un Certificado con datos verificados del Titular.

La clave privada del Titular se genera en un equipo seguro y dedicado, de acuerdo con la información proporcionada en el capítulo 6.2.1.1 este documento.

Una vez que el Certificado de un solo uso ha sido utilizado por el Titular a petición del Suscriptor, la clave privada correspondiente se destruye en el HSM[11] como se describe en el capítulo 6.2.10.2. Sin embargo, el Certificado sigue siendo accesible en el documento firmado.

1.4.2 [AC ORG] Certificados de Organización

El Certificado de Organización se emite a petición del Suscriptor a Worldline, en nombre de la Organización u Organizaciones para las que el Suscriptor está autorizado a solicitar un sello de Documento (de acuerdo con el uso definido en el capítulo 1.5.1.1). Este servicio es operado por Worldline en sus propias instalaciones.

La solicitud de este tipo de Certificado se realiza según un procedimiento entre un representante autorizado del Suscriptor y el Operador de Registro de Worldline. La información que debe facilitarse para la solicitud se detalla en el capítulo 4.1.2.2 presente documento.

Este PC-DPC no establece ningún requisito presencial, pero se reserva el derecho de llevar a cabo comprobaciones adicionales del tipo de contra-llamada.

La clave privada de una Organización se genera en un equipo seguro y dedicado de conformidad con la información que figura en el capítulo 6.2.1.1.

[11] HSM = Hardware Security Module = Módulo de Seguridad Hardware

1.4.3 Certificados de prueba

A efectos técnicos (prueba de presencia y funcionamiento del servicio), demostración y aceptación de las modificaciones introducidas en el sistema de información de la producción, está permitido expedir Certificados de prueba en el marco de las AC de producción.

El Suscriptor podrá, en efecto, solicitar la creación de un Certificado de prueba a la Autoridad de Registro, para su propio uso o para el de un Titular.

Bajo ninguna circunstancia se pueden utilizar Certificados de prueba para vincular al Titular, Suscriptor o Worldline como un Certificado de producción. Sin embargo, las obligaciones de protección y uso del Certificado para el Titular, el Suscriptor y las AC son idénticas a las definidas para los Certificados de producción.

Para estos Certificados de prueba, el atributo "*CommonName*"[12] en el campo "*Subject*"[13] debe ir precedido del valor "TEST" (véanse los capítulos 7.1.8, 7.1.9 y 7.1.10). Estos Certificados deben ser revocados tan pronto como su uso ya no sea necesario.

Las limitaciones de uso y responsabilidad aplicables a los Certificados de producción también se aplican a los Certificados de prueba.

1.5 Uso de los Certificados

1.5.1 Ámbitos de aplicación aplicables

1.5.1.1 Par de claves y Certificados Portador

Esta PC-DPC se ocupa de los Pares de claves y de los Certificados electrónicos asociados a estos Pares de claves, gestionados por el Dispositivo Portador de Certificados (definido en el capítulo 1.3.3 anterior), de modo que los Titulares de Certificados electrónicos puedan, como parte del procedimiento de suscripción o de transmisión desmaterializada:

- [AC OTU][AC OTU LCP] firmar electrónicamente un Documento con un Certificado de un solo uso;
- [AC ORG] sellar electrónicamente un Documento con un Certificado de Organización.

1.5.1.2 Parejas de claves y Certificados de AC y de componentes

Las Parejas de claves de AC se utilizan exclusivamente para firmar certificados y LCRs cuyas plantillas se definen en el capítulo 7 este documento.
Su Certificado está firmado por la Autoridad de Certificación de nivel superior según la descripción en el capítulo 1.2.2 este documento.

1.5.2 Áreas de uso prohibidas

Cualquier uso distinto al definido en el párrafo anterior está prohibido por esta PC-DPC. Además, el Certificado debe utilizarse dentro de los límites de las leyes y reglamentos en vigor (véase el capítulo 9.15).
TSP MediaCert no se hace responsable de cualquier uso indebido según lo especificado.

[12] CommonName = Nombre común
[13] Subject = Sujeto

1.6 Gestión de la PC

1.6.1 Entidad que gestiona la PC

La entidad que gestiona esta política se indica en la [PG].

1.6.2 Punto de contacto

El punto de contacto se indica en la [PG].

1.6.3 Entidad que determina la conformidad de una DPC con esta PC

Esta entidad se describe en la [PG].

1.6.4 Procedimiento para aprobar el cumplimiento de la DPC

El procedimiento para aprobar esta PC-DPC se describe en la [PG].

1.7 Definiciones y acrónimos

1.7.1 Principales definiciones

A continuación se presenta una lista de las principales definiciones de los términos técnicos utilizados en esta PC.

Suscriptor: entidad que firma el contrato de suscripción con el TSP MediaCert para su entrega por parte de las Autoridades de Certificación (AC) en línea:

- [AC ORG] de Certificados de Organización a solicitud de personas debidamente autorizadas dentro del Suscriptor que se encuentren vinculadas legal y/o convencionalmente a él;
- [AC OTU][AC OTU LCP] de Certificados de un solo uso a nombre de los Titulares, tal como se definen en la presente PC-DPC, que el Suscriptor haya identificado previamente o que hayan sido identificados bajo su responsabilidad por personas debidamente autorizadas que estén convencionalmente vinculadas a él.

El Suscriptor está en contacto directo con la AR y realiza una serie de verificaciones de la misma, en particular en lo que se refiere a la identidad y, posiblemente, a los atributos de los Titulares de Certificados.
En el caso de los Certificados de un solo uso, el Suscriptor está autorizado por los Titulares a presentar una solicitud de Certificado en su nombre.

Autenticación: proceso electrónico que permite confirmar la identificación electrónica de una persona física o jurídica, o el origen y la integridad de los datos en formato electrónico.

Autoridad de Certificación (AC): La autoridad responsable de la aplicación de esta PC-DPC, también se refiere a la entidad técnica que produce los Certificados a petición del Servicio de Registro y, de forma más general, los gestiona (fabricación, entrega, revocación, publicación, registro, archivo) de acuerdo con esta PC-DPC. Para más información, véase el capítulo 1.3.1.

Autoridad de Certificación Técnica (ACT): Una Autoridad de Certificación que actúa bajo el nombre de la Autoridad de Certificación OTU, de la autoridad de Certificado ORG o la Autoridad de Certificación OTU LCP.

Autoridad de Registro (AR): Autoridad encargada de recibir las solicitudes de Certificados del Suscriptor, verificarlas, archivarlas y enviarlas a la Autoridad de Certificación. El término también se refiere a la entidad técnica encargada de implementar el Servicio de Registro. Para más información, véase el capítulo 1.3.2.

Pareja de claves: Pareja compuesto por una clave privada (a mantener en secreto) y una clave pública, necesarias para la implementación de un servicio de criptografía basado en algoritmos asimétricos (RSA por ejemplo).

Sello electrónico: datos en formato electrónico, que se adjuntan o se asocian lógicamente con otros datos en formato electrónico para garantizar el origen y la integridad de estos últimos. Esto también se conoce como "Certificado de Organización".

Certificado: Elemento de datos estándar X509 utilizado para asociar una clave pública a su titular. Un Certificado contiene datos como la identidad del titular, su clave pública, la identidad de la organización que emitió el Certificado, el período de validez, un número de serie, una huella dactilar (*digest*) o los criterios de uso. Está firmada por la clave privada de la AC que emitió el Certificado.

Certificado de AC hija: Categoría de Certificados expedidos por la AC Raíz para firmar los certificados de AC hijas y las listas de revocación de las AC hijas.

Certificado ORG: o Certificado de Organización o Sello Electrónico; véase el capítulo 1.4.2.

Certificado OTU (One Time Usage): o Certificado de un solo uso; consulte el capítulo 1.4.1.

Certificado Portador: Categoría de Certificados expedidos por una CA hija a Titulares u Organizaciones. El Certificado de un solo uso y el Certificado de Organización son Certificados Portadores.

Cadena de Certificación: Todos los Certificados requeridos para validar la filiación de un Certificado emitido a una entidad.

Componente de la IGC: Plataformas de hardware (ordenadores, HSM, lector de tarjetas inteligentes) y productos de software que desempeñan una función específica en la IGC.

Contrato de Suscripción: Contrato firmado entre la AC y el Suscriptor y que consiste en los documentos a los que se refiere.

Declaración de Prácticas de Certificación (DPC): Identifica las prácticas (Organización, procedimientos operativos, recursos técnicos y humanos) que la AC aplica en la prestación de sus servicios de Certificación electrónica a los usuarios y de acuerdo con la(s) política(s) de Certificación a la(s) que se ha(n) comprometido.

Solicitud de Certificado: Solicitud realizada por el Suscriptor a la Autoridad de Registro para obtener un Certificado para una persona física o jurídica relacionada con el Suscriptor. Esta persona física o jurídica es identificada y autentificada previamente por el Suscriptor o por las personas debidamente autorizadas a tal efecto bajo la responsabilidad de este último. Incluye un conjunto de información que debe proporcionar el Suscriptor al Servicio de Registro junto con la solicitud del Certificado.

Dispositivo Portador de Certificado: Un componente de software que obtiene un (o más) Certificado(s) de la AC. Estos Certificados se utilizan de acuerdo con las solicitudes y los tipos de Certificados para los usos definidos en el capítulo 1.5.1.
El Dispositivo Portador de Certificados está compuesto por servidores y cajas criptográficas operadas conjuntamente con la AC. Garantiza el control exclusivo de los Pares de claves y los Certificados a los Portadores.

Documento: Documento electrónico estático en formato PDF.

Expediente de registro electrónico: Contenedor de datos en formato electrónico, destinado a contener todos los datos transmitidos por un Suscriptor durante una solicitud de creación de un Certificado (información sobre el Certificado, datos de identificación del Titular, etc.). Estos datos se archivan en un sistema de archivo con vocación probatoria, que puede ser consultado en cualquier momento por la AC.

Plantilla de Certificado: Datos informáticos resultantes de la escritura de registro de un Suscriptor que solicita un Certificado al Departamento de Registro y que luego se transmite a la Autoridad de Certificación para ser firmado.

Hash o huella dactilar digital: se refiere al resultado de una función de cálculo realizada sobre el contenido digital de tal manera que incluso un ligero cambio en el contenido da lugar a la modificación de la huella dactilar. El hash se utiliza para identificar los datos y verificar su integridad a lo largo del tiempo.

Identificación electrónica: El proceso de utilización de datos de identificación personal en forma electrónica que representa de manera exclusiva a una persona física, a una persona jurídica o a una persona física que representa a una persona jurídica.

Lightweight Certificate Policy (LCP): Política de certificación definida por [ETSI EN 319 411-1] que ofrece una calidad de servicio menos costosa que la del NCP (es decir requisitos de política menos estrictos) y que debe utilizarse cuando una evaluación de riesgos no justifica la carga adicional de cumplir todos los requisitos del NPC (por ejemplo, la identificación cara a cara).

Normalized Certificate Policy (NCP): Política de certificación definida por [ETSI EN 319 411-1] que cumple con las mejores prácticas generalmente reconocidas por los TSPs que emiten Certificados.

Organización: Entidad que representa en particular a una empresa, una administración pública, etc., o que puede referirse a una marca o nombre de empresa para la que se emitirá un Certificado de Organización o Sello Electrónico a petición de un Suscriptor.

Dispositivo de identificación electrónica: Elemento tangible y/o intangible que contiene datos de identificación personal y que se utiliza para autenticarse en un servicio en línea.

Interesado: En el contexto de esta PC-DPC, el interesado es la entidad que utiliza el Certificado que recibe (aquí a través de una firma electrónica. Esta firma está asociada a un Documento).

PDF: Formato de un fichero informático creado por ADOBE Systems® y cuya especificidad es preservar el formato definido por su autor.

Política de Certificación (PC): documento publicado que describe todas las reglas y requisitos que la AC cumple en el establecimiento y prestación de servicios de confianza. En particular, indica la aplicabilidad de un Certificado a una comunidad y/o clase particular de aplicaciones con requisitos de seguridad comunes. También identifica las obligaciones y requisitos relativos a los distintos actores, así como los que pesan sobre todos los componentes que intervienen en la gestión del ciclo de vida de las Certificados.

La Política de Certificación se identifica mediante un OID.

Servicio de registro: véase Autoridad de Registro.

Servicio de gestión de revocaciones: véase el capítulo 1.3.1.3.

Servicio de información sobre el estado de los Certificados: véase el capítulo 1.3.1.4.

Sesión de firma: Operación entre la solicitud de firma y la devolución del documento o documentos firmados por la persona física o jurídica designada en la solicitud. Se pueden hacer varias firmas sucesivas con el mismo Certificado en una Sesión de firma.

Signatario: Una persona física identificada en uno o más documentos electrónicos y que crea una firma electrónica para ese o esos documentos.

Firma electrónica: Según el Reglamento Europeo eIDAS, se trata de datos en formato electrónico, que se adjuntan o se asocian lógicamente con otros datos en formato electrónico y que el firmante utiliza para firmar.
Según el Código Civil francés, la firma se utiliza para identificar a la persona que la pone, para expresar su consentimiento y para garantizar la integridad del documento al que se adjunta.

Se recuerda que la firma electrónica implementada en esta PC-DPC no se ajusta a la definición de firma cualificada. Según el Reglamento Europeo eIDAS, el efecto jurídico y la admisibilidad de una firma electrónica como prueba ante un tribunal no pueden rechazarse por el mero hecho de que esté en forma electrónica o de que no cumpla los requisitos de una firma electrónica reconocida.

Titular: Persona física identificada en el Certificado como Titular del mismo. La generación y uso exclusivo de la clave privada asociada a la clave pública especificada en el Certificado se confía al Dispositivo Portador de Certificado.

Usuario: ver Interesado.

1.7.2 Acrónimos

Los acrónimos utilizados en este CP-CDP son las siguientes:

- **AC:** Autoridad de Certificación;
- **AC OTU:** Autoridad de Certificación que expide los Certificados descritos en este PC-DPC;
- **ACR:** Autoridad de Certificación Raíz;
- **AR:** Autoridad de Registro;
- **AH:** Autoridad de sellado de tiempo;
- **CC :** Criterios comunes *(Common Criteria)*;
- **CN:** Nombre común *(Common Name)*;
- **CSR:** Solicitud de firma de Certificado *(Certificate Signing Request)*;
- **DN:** Nombre Distinguido *(Distinguished Name)*;
- **DPC:** Declaración de Prácticas de Certificación;
- **ETSI:** Instituto Europeo de Normas de Telecomunicaciones *(European Telecommunications Standards Institute)*;
- **HSM :** Módulo hardware de seguridad *(Hardware Security Module);*
- **KC :** Ceremonia Clave (*Key Ceremony*);
- **IGC (PKI):** Infraestructura de Gestión de Claves *(Public Key Infrastructure);*
- **LAR:** Lista de Certificados Revocados de las Autoridades de Certificación;
- **LCR:** Lista de Certificados Revocados;
- **OCSP:** Protocolo de estado de Certificados en línea; *(Online Certificate Status Protocol)*
- **OR**: Operador de Registro;
- **OID:** Identificador de objeto (*Object Identifier*);

- **PC:** Política de Certificación;
- **PSI:** Política de Seguridad de la Información;
- **CISSO:** Responsable de Seguridad de los Sistemas de Información;
- **RFC:** Solicitud de Comentarios *(Request for Comment)*;
- **RSA:** *Rivest Shamir Adelman*;
- **SHA:** Algoritmo Hash Seguro (*Secure Hash Algorithm)*;
- **URL** Localizador Uniforme de Recursos *(Uniform Resource Locator)*;
- **UTC:** Tiempo Universal Coordinado *(Universal Time Coordinated).*

1.7.3 Referencias

1.7.3.1 Reglamento

Referencia	Descripción
[CNIL]	Ley n°78-17 del 6 de enero de 1978 relativa a la informática, a los ficheros y a las libertades, en su versión modificada.
[EIDAS]	REGLAMENTO (UE) No 910 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 sobre identificación electrónica y servicios fiables en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
[RGPD]	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

1.7.3.2 3. Reglamentos técnicos

Referencia	Descripción
[RFC 3647]	Network Working Group – November 2003 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practises Framework
[RFC 5280]	Network Working Group - May 2008 Internet X.509 Public Key Infrastructure and Certificate Revocation List (CRL) Profile
[RFC 6960]	IETF - June 2013 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP
[ETSI TS 119,312]	ETSI TS 119 312 v1.2.1 (2017-05) Electronic Signature and Infrastructures (ESI); Cryptographic Suites
[ETSI EN 319.401]	ETSI EN 319 401 v2.2.1 (2018-04) Electronic Signature and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (TSP).
[ETSI EN 319 411-1]	ETSI EN 319 411-1 v1.2.2 (2018-04) Electronic Signature and Infrastructures (ESI); Policy and security requirements for for Trust Service Providers issuing Certificates; Part 1: General requirements
[ETSI EN 319 412-2]	ETSI EN 319 412-2 v2.1.1 (2016-02) Electronic Signature and Infrastructures (ESI); Certificates Profiles; Part 2: Certificate Profiles for Certificates issued to natural persons
[ETSI EN 319 412-3]	ETSI EN 319 412-3 v1.1.1 (2016-02)

Referencia	Descripción
	Electronic Signature and Infrastructures (ESI); Certificates Profiles; Part 3: Certificate profile for Certificates issued to legal persons

1.7.3.3 Documentación interna

Referencia	Descripción
[DTPC]	Documentación Técnica de Prácticas de Certificación Autoridades de Certificación en línea Referencia: WLS-OTU-F003
[CGA]	Condiciones Generales de Suscripción al servicio de firma electrónica OTU y/o sello electrónico Autoridades de Certificación en línea Referencia: WLS-OTU-F008
[CGS]	Términos y Condiciones Generales de Servicio Autoridades de Certificación en línea Referencia: WLS-OTU-F022
[PCA]	Plan de Cierre de Negocios Autoridades de Certificación en línea Referencia: WLS-OTU-F028
[PCRA]	Plan de Continuidad y Reanudación de Negocio Autoridades de Certificación en línea Referencia: WLS-OTU-F029
[PESV]	Protocolo de externalización de copias de seguridad de Vendôme Worldline Referencia: Protocolo de externalización de copias de seguridad de Vendôme
[PG]	Política General del TSP MediaCert TSP MediaCert Referencia: WLM-TSP-F094 OID: 1.2.250.1.111.20.1.1
[PGI]	Política de Gestión de Incidentes Worldline Referencia: WLM-SEC-0008
[PTVDP]	Procedimiento para el Tratamiento de las Violaciones de Datos Personales Worldline Referencia: WLP-DPO-F017

1.7.3.4 Documentación externa

Referencia	Descripción
[Notificación ANSSI]	Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI) Formulario de declaración de un incidente de seguridad relacionado con un producto o servicio cualificado.

2 Responsabilidades en materia de suministro de la información que debe publicarse

2.1 Entidades responsables de la puesta a disposición de la información

La entidad descrita en el documento de la [PG] en el capítulo correspondiente es la entidad responsable de poner a disposición la información a publicar descrita en el capítulo 2.2 de este documento. El sitio de publicación se describe en la [PG].

2.2 Información que se publicará

La información publicada por las Autoridades de Certificación (AC) en línea en el sitio web de TSP MediaCert es la siguiente:

- esta PC-DPC;
- las presentes Condiciones Generales de Servicios (CGS);
- las presentes Condiciones Generales de Suscripción (CGA[14]);
- las presentes Condiciones Generales de Venta (CGV);
- listas de Certificados Revocados (LCR);
- el Certificado de las AC válido en línea;
- Los Certificados del rango de pruebas.

Esta PC-DPC se publica en formato PDF/A.

Las URL para acceder a este PC-DPC, y LCR, así como al contestador automático OCSP, están disponibles en las extensiones de los Certificados emitidos de acuerdo con el capítulo 7.1 este documento.

La Política de Gestión de Pruebas (PGP) se pone a disposición del Suscriptor previa solicitud electrónica (por correo electrónico) en el punto de contacto definido en el capítulo 1.6.2 de este documento.

2.3 Plazos de publicación y periodicidad

Se aplican todos los requisitos y prácticas descritos en la [PG] en el capítulo correspondiente.

Además, las políticas de certificación se actualizan y publican regularmente, especialmente en caso de cambios importantes (véanse los capítulos 9.11 y 9.12).

El plazo y la frecuencia de publicación de la información sobre la situación de los Certificados se indican en los capítulos 4.9.8 y 4.9.7 del presente documento, respectivamente. Además, los Certificados de las AC se publican después de su generación y antes de cualquier Certificación.

[14] CGA : Por su acrónimo en francés « Conditions Générales de Abonnement » = Condiciones Generales de Suscripción

2.4 Control de acceso a la información publicada

Se aplican todos los requisitos y prácticas descritos en la [PG] en el capítulo correspondiente.

3 Identificación y autenticación

3.1 Nombramiento

3.1.1 Tipos de nombres

Los nombres utilizados cumplen con las especificaciones de la norma X.500.

En cada Certificado conforme con X509, los campos "*Issuer*" (emisor AC) y "*Subject*" (sujeto) se identifican con un "*Distinguished Name* "(DN, Nombre distintivo) del tipo X.501 en forma de "*Printable String*" (Cadena imprimible).

3.1.2 Necesidad de usar nombres explícitos

3.1.2.1 [AC OTU][AC OTU LCP Certificados de un solo uso

En el caso de los Certificados de un solo uso, los Certificados expedidos a nombre del Titular en virtud de esta PC-DPC contienen el nombre y los apellidos que figuran en los documentos de identidad válidos, presentados por el Titular.

3.1.2.2 [AC ORG] Certificados de Organización

En el caso de un Certificado de Organización, los Certificados emitidos contienen:

- el nombre del Suscriptor; y
- el nombre de la Organización; y
- el nombre y apellidos que figuren en la prueba de identidad válida presentada por la persona autorizada por el Suscriptor para representar a esta Organización; o
- el nombre de la unidad de la Organización a la que se destina el Certificado.

3.1.3 Anonimización o seudonimización de los Portadores

Los Certificados cubiertos por esta PC-DPC no pueden en ningún caso ser anónimos.
Los nombres previstos para la emisión de un Certificado no podrán en ningún caso ser seudónimos.

3.1.4 Normas para la interpretación de las diferentes formas de nombres

La interpretación de información como el campo "*Distinguished Name*" (Nombre Distinguido) se indica en cada plantilla de Certificado en el capítulo 7 esta PC-DPC.

3.1.5 Unicidad de los nombres

El "*Distinguished Name*" (DN, Nombre Distinguido) es único para cada Titular u Organización. Cualquier solicitud del Suscriptor que no cumpla con esta regla será rechazada por la Autoridad de Registro (véase el capítulo 4.2.1). A lo largo del ciclo de vida de las AC y después de que dejen de funcionar, un "*Distinguished Name"* (DN, Nombre Distinguido) asignado a un Titular u Organización por estas AC no puede, por lo tanto, ser asignado a otro Titular u Organización.

Las reglas que se aplican para obtener esta singularidad en DN son las siguientes:

- [AC OTU][AC OTU LCP] en el caso de los Certificados de un solo uso, se garantiza la unicidad mediante:
    - el identificador del contenedor de trazas en el campo "*Common Name*" (Nombre común) del DN; y
    - el campo "*SERIALNUMBER*" (número de serie) del DN ;
- [AC ORG] para los Certificados de Organización, la unicidad está garantizada por:
    - el campo "*Organization ID*" (ID de organización) del DN, que debe ser único para cada Organización. Esto es verificado por la AR al aceptar la solicitud de creación; y
    - el campo "*SERIALNUMBER*" (número de serie) del DN.

Más información sobre la construcción de algunos de estos campos está disponible en el capítulo 7.1 este documento.

3.1.6 Identificación, autenticación y función de las marcas de fábrica o de comercio

La información está disponible en el capítulo 3.2.2.2 esta PC-DPC.

3.2 Validación inicial de identidad

3.2.1 Método para probar la posesión de la clave privada

3.2.1.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

En el caso de uso a corto plazo (véase el capítulo 6.3.2), el control de la posesión de la clave privada se realiza mediante una verificación criptográfica de bajo nivel de una primera firma producida mediante la clave privada.

Si la verificación falla, entonces:

- el Documento no está firmado;
- se destruye la clave privada (véase el capítulo 6.2.10.2);
- el Suscriptor que ha realizado la solicitud recibe un mensaje de error informándole del fallo de la solicitud.

El Titular del Certificado no está sujeto a esta prueba de posesión.

3.2.1.2 [AC ORG] Certificado de Organización

La prueba de posesión de la clave privada proporcionada por el Dispositivo Portador de Certificado se garantiza durante la generación de la solicitud mediante la firma del mensaje con la clave privada que corresponde a la clave pública contenida en el mensaje PKCS#10 (CSR) enviado a la Autoridad de Registro.

Estos formatos de consulta incluyen la firma de la clave privada correspondiente para garantizar la integridad y la prueba de posesión de la clave privada.

La persona autorizada en el Certificado no está sujeta a esta prueba de posesión.

3.2.2 Validación de la identidad de las organizaciones

3.2.2.1 Validación de un Suscriptor

La validación de la identidad de un Suscriptor requiere seguir los pasos que se describen a continuación y recopilar toda la información necesaria. La Autoridad de Registro conserva todos los documentos enviados cuando el Suscriptor se suscribe al Servicio.

Firma del Contrato de Suscripción

La condición de Suscriptor está sujeta al establecimiento previo de una relación contractual entre el Suscriptor y TSP MediaCert. Este es el Contrato de Suscripción para el servicio de firma electrónica de un solo uso y/o Sello Electrónico. La firma del presente Contrato de Suscripción certifica, en particular, la aceptación de las obligaciones del Suscriptor descritas en el presente documento en el capítulo 9.6.3.1 Condiciones Generales de Suscripción [CGA][15] (documentos adjuntos al Contrato de Suscripción).

Nombramiento o designación de representantes dentro del Suscriptor

A continuación, debe designarse un representante del Suscriptor en la Autoridad de Registro para que pueda convertirse en la persona de contacto para las solicitudes de Certificados de Organización. Este representante del Suscriptor puede ser:

- el representante legal del Suscriptor (tal como aparece en un extracto Kbis[16] del Suscriptor con menos de tres meses de antigüedad);
- su representante convencional (como aparece, por ejemplo, en los estatutos);
- un representante autorizado (delegación, poder o mandato) por el representante legal para representar al Suscriptor en la ejecución del Contrato de Suscripción.

El Suscriptor, a través de su representante legal o estatutario, podrá designar formalmente por escrito (a través de la hoja de información del representante adjunto del Suscriptor a las AC en línea proporcionada por la Autoridad de Registro) a uno o más representantes adjuntos del Suscriptor que también estén autorizados para representarlo. Para ello, debe informar a la Autoridad de Registro y otorgarle las facultades necesarias.

Suministro de la documentación necesaria para la suscripción del Contrato de Suscripción

Además, al firmar el Contrato de Suscripción, el representante del Suscriptor designado debe proporcionar:

- las Condiciones Generales de Suscripción [CGA] que haya rubricado o que haya rubricado el representante legal de la Organización;

[15] CGA : Por su acrónimo en francés « Conditions Générales de Abonnement » = Condiciones Generales de Suscripción

[16] Kbis = Documento oficial que certifica la existencia legal de una empresa en Francia.

la ficha de información del representante del Suscriptor ante las AC en línea, facilitada por la Autoridad de Registro, debidamente cumplimentada y firmada por el representante del Suscriptor. Este formulario contiene, entre otras cosas, la dirección física del Suscriptor y una dirección de correo electrónico válida de su representante, lo que le permite ser contactado. Esta dirección de correo electrónico se utilizará, entre otras cosas, para transmitir información al crear Certificados de Organización; y

- la política de identificación que aplica, de conformidad con las prescripciones y recomendaciones que le haga la Autoridad de Registro, sólo en el caso de que desee suscribirse al servicio de Certificado de un solo uso. Esto debe ser validado por la AR y puede ser controlado por la AR, como se indica en el Capítulo 3.2.3.1;

- una copia de un documento oficial de identidad válido en el momento de la contractualización que contenga una fotografía de identidad de entre los documentos que se definen a continuación: documento nacional de identidad, pasaporte o permiso de residencia; y

- un extracto de Kbis17 de menos de tres (3) meses antes de la contratación, o de los estatutos publicados en vigor de la Organización a la que pertenece, incluyendo su nombre y capacidad y los documentos válidos necesarios para justificar sus poderes;

- Si no figura en el extracto del Kbis de menos de tres (3) meses de antigüedad, o en los estatutos publicados de esta Organización en vigor, deberá estar debidamente autorizado por el representante legal del Suscriptor en el marco de un poder escrito para representarle con el carácter exhaustivo de las facultades que se le otorguen.

Todos estos elementos también se mencionan en una notificación que se entrega al Suscriptor con el Contrato de Suscripción.

3.2.2.2 [AC ORG] Validación de una Organización

La validación de una Organización como beneficiario de los servicios se basa en la validación previa de la identidad del Suscriptor (véase el capítulo 3.2.2.1). Se realiza tras la recepción de una solicitud de creación de un Certificado, siendo la persona de contacto de la AC únicamente el Suscriptor.

Como se describe en el capítulo 1.3.4.2, una Organización está representada por una persona autorizada: el representante de la Organización. La información relativa a la Organización que el Suscriptor debe enviar a la Autoridad de Registro cuando solicite la creación de un Certificado es la siguiente:

En el caso de que la Organización y el Suscriptor sean dos entidades diferentes

- cualquier documento, válido en el momento de la solicitud de creación del Certificado, que demuestre el derecho y la autoridad del Suscriptor para incluir el nombre de la Organización en el Certificado.

En todos los casos

- si las Condiciones Generales de Suscripción [CGA][18] han cambiado desde la contractualización o desde la última solicitud de creación de un Certificado, dicho documento actualizado deberá ser devuelto rubricado por el representante legal o por el representante del Suscriptor autorizado;

[17] Kbis = Documento oficial que certifica la existencia legal de una empresa en Francia.

[18] CGA : Por su acrónimo en francés « Conditions Générales de Abonnement » = Condiciones Generales de Suscripción

- una solicitud de creación de un Certificado, firmado y fechado por un representante legal, por el representante del Suscriptor o uno de sus suplentes, especificando:
    - el nombre del Suscriptor que se incluirá en el Certificado electrónico; y
    - el nombre de la Organización que se incluirá en el Certificado electrónico; y
    - el nombre completo (nombre y apellidos) de la persona autorizada para representar a la Organización e identificada en el Certificado; o
    - el nombre de la unidad de la Organización a la que se destina el Certificado.

El derecho de este Suscriptor a incluir el nombre de la Organización en el Certificado se basa en todos los elementos siguientes:

- cualquier documento, válido en el momento de la solicitud de creación del Certificado, que acredite la existencia de la Organización (extracto de Kbis[19] con fecha de menos de tres (3) meses o, original o copia de cualquier documento oficial o extracto del registro oficial con fecha de menos de tres (3) meses que acredite el nombre, la forma jurídica, el domicilio social y la identidad de los socios y administradores mencionados en los apartados 1 y 2 del artículo R. 123-54 del Código de Comercio, o sus equivalentes en virtud de la legislación extranjera,...);
- De hecho, cuando la identidad de una persona llega a ser incluida en el Certificado, el Suscriptor debe transmitir a la Autoridad de Registro:
    - cualquier documento, válido en el momento de la solicitud de creación de un Certificado, que demuestre la pertenencia de la persona autorizada a la Organización;
    - una copia de un documento oficial de identidad válido de la persona autorizada a partir de los siguientes documentos:
        - documento nacional de identidad;
        - pasaporte
        - permiso de residencia.

      La Autoridad de Registro conserva esta copia.
    - la dirección postal, una dirección de correo electrónico y un número de teléfono que permitan a la Autoridad de Registro ponerse en contacto con esta persona autorizada.

Esta PC-DPC no establece ningún requisito para la identificación cara a cara. No obstante, la autoridad de registro podrá llevar a cabo verificaciones adicionales.

[19] Kbis = Documento oficial que certifica la existencia legal de una empresa en Francia.

3.2.3 Validación de la identidad de una persona

3.2.3.1 [AC OTU][AC OTU LCP] Certificado de un solo uso

La solicitud de crear un Certificado a nombre de un Titular la realiza el Suscriptor a la Autoridad de Registro.
Esta solicitud se hace en formato electrónico porque debe estar firmada por el solicitante mediante una firma electrónica (véase el capítulo 3.2.5.1). Contiene al menos los siguientes datos del Titular:

- su nombre y apellidos;
- su fecha y lugar de nacimiento.

El Suscriptor también puede especificar para el archivo de registro:

- el título de cortesía del Titular;
- la dirección postal del Titular;
- el número de teléfono del Titular;
- la dirección de correo electrónico del Titular.

El Suscriptor podrá complementar la información proporcionada anteriormente con información conocida de antemano y específica del futuro Titular, permitiendo su identificación dentro de una base de datos preestablecida.

En los Certificados expedidos por las Autoridades de Certificación (AC) sólo se incluye la información relativa al "nombre y apellidos" del titular. No obstante, la Autoridad de Registro conservará toda la información antes mencionada en el expediente de registro en formato electrónico asociado con la emisión del Certificado, de conformidad con el capítulo 5.4 presente documento, con el fin de apoyar la prueba de identificación.

La conservación de estos datos es necesaria porque están previstos para la constitución del expediente de registro asociado a cada emisión de un Certificado. Este expediente de registro recoge los datos mencionados anteriormente, describiendo los procesos y datos de identificación del cliente final (Titular).

El capítulo 3.1.5 este documento también define cómo se garantiza la unicidad del "*Distinguished Name*" (*Nombre Distinguido)* en los Certificados de un solo uso.

Política de identificación
El Suscriptor debe especificar por escrito a la AR, al contratar con la TSP MediaCert para la emisión de Certificados de un solo uso, la política de identificación que ha establecido (ver Capítulo 3.2.2.1, sección *"Suministro de la documentación necesaria en el momento de la suscripción al Contrato de Suscriptor"*) a fin de verificar la identidad civil declarada por el futuro Titular.

Los procedimientos de identificación contenidos en esta política deben basarse al menos en la verificación de un documento oficial válido que lleve una fotografía del Titular (documento nacional de identidad, pasaporte o permiso de residencia) o en cualquier otro procedimiento oficial válido que permita o haya permitido, antes de la emisión de un Certificado, verificar la identidad declarada de un Titular. Más específicamente:

- [AC OTU LCP] la identidad del futuro Titular podrá ser comprobada automáticamente para verificar la identidad declarada del Titular;

- [AC OTU] los controles de identidad del futuro Titular deben ser realizados por los operadores para poder verificar la identidad del Titular de forma física.

En cualquier caso, durante el proceso de identificación, la comprobación de la identidad del futuro Titular debe basarse en documentos de identidad legalmente válidos, que pueden presentarse en algunos países en formato electrónico. De hecho, en algunos Estados, la etapa de identificación puede llevarse a cabo sobre la base de un documento de identidad electrónico o puede basarse en otros medios electrónicos de identificación jurídicamente válidos para lograr una identificación fiable. En este contexto, el Suscriptor verifica que el Titular es efectivamente el Titular de un documento de identidad electrónico válido o que posee otros medios electrónicos de identificación legalmente válidos para lograr una identificación fiable.

Estos documentos de identidad en forma física o electrónica se utilizan para respaldar los datos de identificación que el Suscriptor ha recogido previamente del Titular, con la emisión de un Certificado de un solo uso como parte del proceso de firma electrónica.

Los datos que deben registrarse, verificarse y conservarse incluyen los nombres, apellidos, fecha y lugar de nacimiento de la persona, así como la naturaleza y fecha de expedición del documento.

La Autoridad de Registro se reserva el derecho de evaluar la fiabilidad del proceso de identificación establecido y de no emitir un Certificado si se considera que la política de identificación del Suscriptor no proporciona un nivel suficiente de fiabilidad. En particular, la AR supervisará periódicamente esta política mediante muestreo de acuerdo con el procedimiento de muestreo de la AR. En caso de desviaciones de dicho procedimiento, el Suscriptor se compromete a establecer un plan de acción con TSP MediaCert para resolver dichas desviaciones. La no aplicación de este plan de acción o la observación de discrepancias durante la próxima campaña de muestreo puede dar lugar a la desactivación del servicio de Firma electrónica mediante Certificados de un solo uso.

La mencionada política de identificación se complementa con una descripción del proceso que utilizará el Titular para consentir en proceder con una firma electrónica utilizando el Certificado de un solo uso (Política de Recogida del Consentimiento).
Esta política de recogida del consentimiento detalla, para cada uno de los consentimientos que se obtengan en el contexto de la implementación de esta firma electrónica, la identificación de los medios a través de los cuales el Titular expresará su consentimiento. Antes de poder firmar electrónicamente, el Titular deberá, de hecho:

- conocer las condiciones de uso de la firma electrónica y sus obligaciones descritas por el Suscriptor en un soporte duradero puesto a su disposición de forma legible y explícita;

- consentir la firma, en formato electrónico, en el contexto de la transacción de la que es parte, aceptando los términos y condiciones relativos al uso del Certificado de un solo uso;

- aceptar el mantenimiento de un registro por parte de la Autoridad de Registro que le permita procesar y conservar la información de identidad utilizada necesaria para la generación del certificado de un solo uso, durante el período fijado por el ejercicio de su misión y las auditorías correspondientes;

- en el contexto de los controles de identidad automatizados, dar su consentimiento para la automatización de dichos controles;

- confirmar la validez de la información contenida en el Certificado;

- como consecuencia de lo anterior, otorgar al Suscriptor un mandato expreso para que proceda a la Autoridad de Registro con la solicitud de un Certificado de un solo uso para que pueda firmarlo. Se especifica que en este contexto, los consentimientos dados por el Titular inician una solicitud automatizada a nombre del Suscriptor de una firma electrónica por parte de la Autoridad de Registro.

Los procedimientos para validar la expresión y obtención del consentimiento del Titular elegido por el Suscriptor pueden ser los siguientes:

- una captura electrónica de la firma manuscrita del Titular;
- enviar un código OTP recibido por SMS al teléfono móvil personal del Titular.

La lista anterior tiene un carácter meramente ilustrativo y no exhaustivo.

Como el proceso de identificación es descrito por el Suscriptor, depende de él/ella:

- ejecutarlo o hacer que se ejecute bajo su responsabilidad. Si el Suscriptor designa y autoriza a personas para realizar esta identificación bajo su responsabilidad, el Suscriptor deberá estipularlo en la política de identificación que proporciona a la Autoridad de Registro;
- transmitir a la AR, en un expediente de registro electrónico, los datos de identificación capturados y la prueba de identidad que le hayan facilitado durante la implementación del proceso de firma electrónica.

Excepciones al principio de transmisión de los elementos que justifican la identidad de los titulares a la AR

Por lo tanto, el Suscriptor transmite a la Autoridad de Registro copias digitales de todos los elementos utilizados para verificar la identidad del futuro Titular, excepto en los siguientes casos:

- el Titular pertenece a la Organización del Suscriptor. En efecto, no es necesario que el Suscriptor realice una comprobación de identidad adicional si el Suscriptor ha facilitado al futuro Titular un medio de autenticación fiable aceptado por la AR, en particular para acceder a su buzón de correo electrónico profesional o para conectarse a la aplicación que requiere la firma de este último.

  En este contexto, el Suscriptor debe pedir al futuro Titular que garantice la seguridad de su ordenador, de su buzón profesional y de sus identificadores.

  La AR debe asegurarse de que el Titular era miembro de la Organización del Suscriptor en el momento de la firma mediante la realización de comprobaciones por muestreo, tal como se menciona anteriormente en este capítulo.

- el Suscriptor conserva los elementos de verificación de identidad del futuro Titular de la identidad en nombre de la AR. En este contexto, el Suscriptor debe mantener estos elementos de forma segura. La AR hará entonces las declaraciones necesarias a la CNIL[20] para poder cumplir las obligaciones impuestas a las Autoridades de Certificación con respecto a sus auditores.

  La AR debe garantizar que el Suscriptor ha implementado realmente la verificación de la identidad del futuro Titular mediante la realización de comprobaciones por muestreo, tal y como se ha mencionado anteriormente en este capítulo.

[20] CNIL = Commission Nationale de l'Informatique et des Libertés = Comisión Nacional de Informática y Libertades, en Francia.

3.2.3.2 [AC OTU] Certificado de Organización

La información está disponible en el capítulo 3.2.2.2, sección *"Sobre el derecho del Suscriptor a incluir el nombre de la Organización en el Certificado"*.

3.2.4 Información no verificada

Los Certificados expedidos por las Autoridades de Certificación de conformidad con este PC-DPC no contienen ninguna información no verificada, excepto el correo electrónico y el campo *Organization Unit* (OU, Unidad organizativa) correspondiente al nombre de la unidad de la organización dentro del *Distinguished Name* (DN, nombre distinguido) del *Subject* (asunto).

3.2.5 Validación de la autoridad del solicitante

Tanto si se trata de un Certificado de un solo uso como de un Certificado de Organización, la solicitud la realiza el Suscriptor, que debe ser identificado antes de realizar cualquier solicitud de creación de un Certificado, la validación inicial de un Suscriptor se describe en el capítulo 3.2.2.1.

En el momento de cada solicitud de creación de un Certificado, el Suscriptor se autentica ante la Autoridad de Registro y el Dispositivo Portador de Certificados. La autenticación se realiza de forma diferente según el tipo de Certificado solicitado.

3.2.5.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

Al solicitar la creación de un Certificado de un solo uso y la firma de la Autoridad de Registro (que a continuación se pone en contacto con el Dispositivo Portador de Certificados), el Suscriptor debe autenticarse y firmar la solicitud electrónicamente.

La autenticación del Suscriptor se realiza mediante un Certificado. Este Certificado debe ser emitido por una Autoridad de Certificación aprobada por el TSP MediaCert como se describe en el documento [DTPC].

3.2.5.2 [AC ORG] Certificado de Organización

Cuando el representante del Suscriptor solicita a la Autoridad de Registro la creación de un Certificado de Organización, el representante del Suscriptor es autenticado por la Autoridad de Registro.

La autenticación del Suscriptor se realiza mediante una solicitud manuscrita y firmada. La autenticidad de esta solicitud es verificada por la AR utilizando la firma en la copia de la prueba de identidad, conservada por la AR, así como un conjunto de elementos relacionados con la relación comercial que Worldline tiene con el Suscriptor.

3.2.6 Criterios de interoperabilidad

Esta PC-DCP no hace ningún requerimiento al respecto.

3.3 Identificación y validación de una solicitud de renovación de claves

3.3.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

A los efectos de esta PC-DPC, no existe una función de renovación de claves para esta categoría de Certificado. De hecho, como su nombre indica, este tipo de Certificado es para un solo uso.

3.3.1.1 Identificación y validación de una renovación actual

No se aplica.

3.3.1.2 Identificación y validación para la renovación tras la revocación

No se aplica.

3.3.2 [AC ORG] Certificados de Organización

Para esta categoría de Certificado, una solicitud de renovación de claves se trata como una solicitud de creación inicial. Por lo tanto, no se puede proporcionar un nuevo Certificado de Organización sin la renovación del correspondiente Pareja de claves (véase el capítulo 4.6).

3.3.2.1 Identificación y validación de una renovación actual

No se aplica.

3.3.2.2 Identificación y validación para la renovación tras revocación

No se aplica.

3.4 Identificación y validación de una solicitud de revocación

3.4.1 [AC OTU][AC OTU LCP] Certificado de un solo uso

Cuando se utiliza un Certificado con una vida útil tan corta (véase el capítulo 6.3.2), la revocación sólo puede producirse cuando se utiliza durante una sesión de firma. Por lo tanto, el Certificado del Titular sólo puede revocarse a petición del Dispositivo Portador de Certificados (véase el capítulo 4.9.2.1).

Por lo tanto, esta solicitud es transmitida por el Dispositivo Portador de Certificados a la Autoridad de Registro, que a su vez redirecciona la solicitud a la Autoridad de Certificación emisora del Certificado afectado por la revocación. Este último valida automáticamente la solicitud y, a continuación, lleva a cabo la revocación directamente.

Cualquier solicitud de revocación de un Certificado de un solo uso del Dispositivo Portador de Certificados se considera válida.

3.4.2 [AC ORG] Certificado de Organización

Un Certificado de Organización puede ser revocado por:

- la persona autorizada y designada en el Certificado en cuestión, o una persona explícitamente autorizada y designada por ella. La solicitud se envía a la Autoridad de Registro, que la redirecciona a la Autoridad de Certificación para su validación y ejecución si la solicitud está en orden;

- la Autoridad de Certificación que expide el Certificado.

La identificación se lleva a cabo tal como se define en el capítulo 4.9.3.2.

4 Requisitos operativos a lo largo del ciclo de vida de los Certificados

4.1 Solicitud de creación de un Certificado

4.1.1 Origen de una solicitud

4.1.1.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

La creación de un Certificado de un solo uso sólo puede ser solicitada por un Suscriptor identificado por la Autoridad de Registro (véase el capítulo 3.2.2.1). Antes de realizar cualquier solicitud a la Autoridad de Registro, el Suscriptor se compromete a identificar, o hacer identificar al futuro Titular bajo su responsabilidad, y a obtener el consentimiento del Titular tal y como se describe en el Capítulo 3.2.3.1 que pueda beneficiarse de este servicio.

4.1.1.2 [AC ORG] Certificados de Organización

La creación de un Certificado de Organización sólo puede ser solicitada por un Suscriptor identificado por la Autoridad de Registro a través de su representante o representante adjunto, de conformidad con el capítulo 3.2.2.1.

4.1.2 Proceso y responsabilidades para preparar una solicitud

4.1.2.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

Toda la información que debe incluirse como mínimo en la solicitud se especifica en el Capítulo 3.2.3.1 esta PC-DPC.

La solicitud es establecida por el Suscriptor sobre la base de la información recogida de fuentes fiables y de documentos justificativos válidos del Titular (véase el Capítulo 4.1.1.1).

El Suscriptor se compromete con Worldline a través del Contrato de Suscripción a:

- informar a la Autoridad de Registro, por escrito, de sus procedimientos para identificar a los futuros Titulares que desea implementar mediante la provisión de su Política de Identificación;
- aplicar dichos procedimientos de identificación del futuro Titular, definidos en su política de identificación de acuerdo con el capítulo 3.2.3.1 y aplicarlos antes de proceder a cualquier solicitud de creación de un Certificado en nombre del futuro Titular;
- informar al futuro Titular de las distintas gestiones que deberá realizar para expedir un Certificado en su nombre a fin de poder firmar electrónicamente el documento o documentos que le presente el Suscriptor y, a tal fin, obtener el consentimiento previo del futuro Titular para la elección de la firma electrónica para la firma de dichos documentos y de las obligaciones que se deriven de dicha elección, tal como se especifica en el capítulo 3.2.3.1, incluida la facultad de otorgar al Suscriptor la facultad de solicitar a la Autoridad de Registro un Certificado de un solo uso en beneficio del Titular y de aceptar el tratamiento de sus datos personales por parte de la Autoridad de Registro y la Autoridad de Certificación;
- como consecuencia de lo anterior, informar al futuro Titular del tratamiento de sus datos personales por parte de la Autoridad de Registro y de la Autoridad de Certificación y, a tal

fin, obtener del mismo los consentimientos previos necesarios para el tratamiento y almacenamiento de sus datos en el marco de la generación del Certificado de un solo uso y de la gestión de las pruebas;

- proporcionar toda la información necesaria para la emisión del Certificado.

Una vez que la solicitud ha sido enviada a la Autoridad de Registro y validada, se envía a la Autoridad de Certificación para la generación del Certificado de un solo uso en nombre del Titular.

TSP MediaCert no podrá ser considerada responsable si el Suscriptor y/o el Titular no respetan los compromisos que han aceptado para beneficiarse del servicio de firma electrónica.

TSP MediaCert se reserva el derecho de negarse a emitir un Certificado de un solo uso si se descubre que las obligaciones del Titular, relacionadas con el Suscriptor, y/o las obligaciones del Suscriptor no son respetadas.

4.1.2.2 [AC ORG] Certificados de Organización

Toda la información que debe incluirse como mínimo en la solicitud se especifica en el capítulo 3.2.3.2 esta PC-DPC.

La solicitud es establecida por el representante del Suscriptor a través de un expediente de solicitud para la creación de un Certificado de Organización. El representante autorizado de la Organización cumplimenta este expediente y lo envía a la Autoridad de Registro, que tramita la solicitud tal como se define en el capítulo 4.2.1.2 presente documento.

TSP MediaCert no podrá ser considerada responsable si el Suscriptor no respeta los compromisos que ha aceptado en virtud del Contrato de Suscripción.

TSP MediaCert se reserva el derecho de negarse a emitir un Certificado de Organización si parece que no se respetan las obligaciones del Suscriptor.

4.2 Procesamiento de una solicitud para crear un Certificado

4.2.1 Ejecución de los procesos de identificación y validación de la solicitud

4.2.1.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

Una vez que la solicitud del Suscriptor ha sido recibida por la Autoridad de Registro, ésta realiza las siguientes operaciones:

- verificación de la identidad del Suscriptor (véase el capítulo 3.2.2.1): la Autoridad de Registro verifica la información transmitida por el Suscriptor y comprueba que la Autoridad de Registro conoce realmente el Suscriptor;

- Verificación de la solicitud: La Autoridad de Registro verifica que la solicitud del Suscriptor está firmada electrónicamente en su nombre;

- Validación de los consentimientos y de los datos de identidad del Titular: la Autoridad de Registro valida la presencia de la información necesaria (véase el capítulo 3.2.3.1). La firma de la solicitud, hecha por el Suscriptor, atestigua la validez de la información proporcionada para su inclusión en el Certificado.

Una vez realizadas estas operaciones, si todo es correcto, la Autoridad de Registro emite la solicitud de generación de Certificado a la Autoridad de Certificación de destino y mantiene un registro de la solicitud del Suscriptor archivada en formato digital.

[AC OTU LCP] La Autoridad de Certificación generará entonces un Certificado que contendrá los datos de identidad del Titular, tal como se definen en el capítulo 7.1.5 este documento.

[AC OTU] La Autoridad de Certificación generará entonces un Certificado que contendrá los datos de identidad del Titular, tal como se definen en el capítulo 7.1.6 este documento.

De lo contrario, se rechaza la solicitud (véase el capítulo 4.2.2.1).

4.2.1.2 [AC ORG] Certificados de Organización

Una vez que la solicitud del representante del Suscriptor ha sido recibida por la Autoridad de Registro, ésta realiza las siguientes operaciones:

- validación de los datos de identificación de la Organización y de la persona que la representa dentro de la Organización (véase el capítulo 3.2.2.2): cumplimentación, carácter único y exactitud de la información;
- verificación de la integridad del expediente de solicitud para la creación de un Certificado de Organización: la Autoridad de Registro garantiza, en particular, que dispone de información que le permite ponerse en contacto con el futuro Titular del Certificado.

Una vez realizadas estas operaciones, si todo es correcto, la Autoridad de Registro emite la solicitud de generación de Certificado a la Autoridad de Certificación OTU y mantiene un registro de la solicitud del representante del Suscriptor, archivada en formato digital.

De lo contrario, se rechaza la solicitud (véase el capítulo 4.2.2.2).

4.2.2 Aceptación o rechazo de la solicitud

4.2.2.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

La aceptación o rechazo se realiza automáticamente.

En caso de que se rechace la solicitud, la Autoridad de Registro informará al Suscriptor mediante una notificación técnica a petición de éste. La notificación incluirá la justificación del rechazo. Se debe hacer una nueva solicitud.

4.2.2.2 [AC ORG] Certificados de Organización

La aceptación o rechazo se realiza manualmente.

En caso de que se rechace la solicitud, la Autoridad de Registro informará al punto de contacto identificado en la solicitud, justificando el rechazo. La Autoridad de Registro podrá entonces solicitar los documentos que falten para completar el expediente de registro, pero en ningún caso podrá modificar los datos firmados. Se debe hacer una nueva solicitud.

4.2.3 Plazo de expedición del Certificado

4.2.3.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

Una vez validada la solicitud de creación de un Certificado de un solo uso, la generación del Certificado es inmediata.

4.2.3.2 [AC ORG] Certificados de Organización

Una vez validada la solicitud de creación de un Certificado de Organización, se realiza la generación del Certificado lo antes posible.
Se crea un documento técnico específico que traza la generación del Certificado, así como los participantes técnicos, y se mantiene como un registro de ejecución.

4.3 Emisión del Certificado

4.3.1 Acciones de la AC en relación con la emisión del Certificado

Después de autenticar el origen y verificar la integridad de la solicitud de la Autoridad de Registro, la Autoridad de Certificación inicia el proceso de generación del Certificado. Las condiciones para la generación de claves y Certificados y las medidas de seguridad a seguir se especifican en los Capítulos 5 y 6 esta PC-DPC. Una vez generado, la Autoridad de Certificación transmite el Certificado producido al Dispositivo Portador de Certificado a través de la Autoridad de Registro. El Dispositivo Portador de Certificados garantiza la seguridad de las Parejas de claves tal y como se define en el Capítulo 6.1.1.4.

4.3.1.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

En el caso de los Certificados de un solo uso, el Certificado producido es accesible al Titular en la firma del documento o documentos para los que se expidió el Certificado.

4.3.1.2 [AC ORG] Certificados de Organización

En el caso de los Certificados de Organización, el Certificado producido también se envía al representante del Suscriptor para validar la información contenida en el Certificado antes de que pueda utilizarse (véase el capítulo 4.4.1.2).

4.3.2 Notificación por parte de la AC de la emisión del Certificado

La Autoridad de Certificación transmite el Certificado producido al Dispositivo Portador de Certificado a través de la Autoridad de Registro en respuesta al procesamiento de la solicitud de creación de Certificado (véase el capítulo 4.3.1). La operación se registra en los registros de la Autoridad de Registro. Dicha transmisión constituirá una notificación.

4.3.2.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

No se aplica.

4.3.2.2 [AC ORG] Certificados de Organización

En el caso de la emisión de Certificados de Organización, el Certificado también se envía al representante del Suscriptor (véase el capítulo 4.3.1.2), lo que equivale a un acuerdo de notificación expresa.

4.4 Aceptación del Certificado

4.4.1 Proceso de Aceptación del Certificado

4.4.1.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

Los datos de identificación del Titular y el resultado de su procesamiento para formar los datos del Certificado son validados explícitamente por el Titular antes de la emisión del Certificado. Esta validación se almacena en el expediente de registro correspondiente.

En efecto, dado el carácter atómico de la operación de firma en el contexto de la utilización de un certificado de un solo uso, la validación de los datos contenidos en el certificado se lleva a cabo antes de su expedición.

Además de esta validación, el Dispositivo Portador de Certificado realiza comprobaciones automáticas para detectar cualquier incumplimiento antes de que se expida el Certificado.

4.4.1.2 [AC ORG] Certificados de Organización

El Certificado de Organización producido por la Autoridad de Certificación OTU se envía al Suscriptor para su validación antes de su uso, tal y como se define en el capítulo 4.3.1 este documento.

La aceptación explícita de la información contenida en el Certificado por parte del representante legal o estatutario del Suscriptor que hizo la solicitud o de la persona autorizada identificada en el Certificado es requerida por esta PC-DPC dentro de los diez (10) días hábiles siguientes a la generación del Certificado (período llamado la "fase de aceptación"). Se considera suficiente la aceptación explícita por correo electrónico, cuya dirección se comunica en el momento de la elaboración del fichero de suscripción. De hecho, la dirección de correo electrónico del emisor que estaba inscrito cuando se creó el expediente de suscripción se considera la autenticación del origen de la aceptación del Certificado.

Sin esta fase de aceptación, no es posible el uso de Certificados de Organización por parte del Dispositivo Portador del Certificado.

Una vez que esta fase de aceptación ha expirado, un Certificado de Organización emitido se considera aceptado y ahora puede ser utilizado por el Dispositivo Portador de Certificado.

4.4.2 Publicación del Certificado

No hay servicio de publicación de Certificados emitidos por las Autoridades de Certificación. Sólo se publican los Certificados de estas Autoridades de Certificación (véase el capítulo 2.2).

4.4.3 Notificación por parte de la AC a otras entidades de la emisión del Certificado

No se aplica.

4.5 Usos de la Pareja de claves y del Certificado

4.5.1 Uso de la clave privada y del Certificado por parte del Dispositivo Portador de Certificados

El uso de la clave privada por el Dispositivo Portador de Certificado y el Certificado asociado se limita estrictamente al servicio de firma/sello electrónico descrito en el capítulo 1.5.1.1 este documento. De lo contrario, TSP MediaCert no podrá ser considerada responsable.

El uso autorizado de la Pareja de claves y del Certificado asociado también se indica en el Certificado a través de las extensiones relativas al uso de las claves.

4.5.2 Uso de la clave pública y el Certificado por las partes interesadas

Los Suscriptores deberán respetar y garantizar que sus personas vinculadas que soliciten Certificados respeten el uso estipulado en los Certificados producidos a su solicitud por las Autoridades de Certificación, tal como se explica en el capítulo 4.5.1 anterior. Por lo tanto, deben rechazar cualquier otro uso del Certificado. En caso contrario, se puede comprometer la responsabilidad de los Suscriptores y de las personas relacionadas con ellos que hayan solicitado un Certificado.

4.6 Renovación de un Certificado

La renovación del Certificado (nuevo Certificado sin cambio de clave) no está permitida bajo esta PC-DPC.

4.6.1 Posibles causas para la renovación de un Certificado

No se aplica.

4.6.2 Origen de una solicitud de renovación

No se aplica.

4.6.3 Procedimiento para tramitar una solicitud de renovación

No se aplica.

4.6.4 Notificación del establecimiento de un nuevo Certificado

No se aplica.

4.6.5 Proceso de aceptación del nuevo Certificado

No se aplica.

4.6.6 Publicación del nuevo Certificado

No se aplica.

4.6.7 Notificación por parte de la AC a otras entidades de la emisión del nuevo Certificado

No se aplica.

4.7 Emisión de un nuevo Certificado tras el cambio de la Pareja de claves

La emisión de un nuevo Certificado relacionado con la generación de una nueva Pareja de claves se trata como una solicitud inicial para crear un Certificado.

Está prohibido utilizar una Pareja de claves existente asociado con una CSR antigua.

4.7.1 Posibles razones para cambiar una Pareja de claves

No se aplica.

4.7.2 Origen de la solicitud de un nuevo Certificado

No se aplica.

4.7.3 Procedimiento de tramitación de la solicitud de un nuevo Certificado

No se aplica.

4.7.4 Notificación del establecimiento de un nuevo Certificado

No se aplica.

4.7.5 Proceso de aceptación del nuevo Certificado

No se aplica.

4.7.6 Publicación del nuevo Certificado

No se aplica.

4.7.7 Notificación por parte de la AC a otras entidades de la emisión del nuevo Certificado

No se aplica.

4.8 Modificación de un Certificado

La modificación del Certificado no está autorizada por este PC-DPC.

[AC ORG] Sin embargo, la modificación de un Certificado de Organización equivale a revocar el Certificado en cuestión y luego proceder a una nueva solicitud de Certificado de acuerdo con el procedimiento descrito en el capítulo 4.1.1.2.

4.8.1 Posibles razones para modificar un Certificado

No se aplica.

4.8.2 Origen de una solicitud de cambio

No se aplica.

4.8.3 Procedimiento para procesar una solicitud de cambio

No se aplica.

4.8.4 Procedimiento de aceptación del Certificado modificado

No se aplica.

4.8.5 Publicación del Certificado modificado

No se aplica.

4.8.6 Notificación por parte de la AC a otras entidades de la emisión del Certificado modificado

No se aplica.

4.9 Revocación y suspensión de un Certificado

Esta PC-DPC no autoriza la suspensión del Certificado.

Además, cualquier información relacionada con la revocación de un Certificado de una Autoridad de Certificación está disponible dentro de la Política de Certificación - Declaración de Prácticas de Certificación que rige su Autoridad de Certificación emisora.

4.9.1 Posibles razones para revocar un Certificado

4.9.1.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

Las siguientes circunstancias pueden llevar a la revocación del Certificado de un solo uso del Titular:

- el Certificado ya no cumple con la PC-DPC al que está sujeto;
- la criptografía utilizada ya no garantiza la conexión entre el sujeto y la clave pública;
- en caso de que se produzca un cambio importante, después de la evaluación de impacto, que afecte a la validez del Certificado;
- se ha producido un incidente cuando el Dispositivo Portador de Certificado ha utilizado el Certificado del Titular para una firma como parte del uso normal, tal como se define en el capítulo 1.5.1.1;
- las claves privadas o públicas no coinciden o el Dispositivo Portador de Certificados no puede utilizarlas para el uso normal definido en el capítulo 1.5.1.1

Cuando se produzca una de las circunstancias mencionadas y la Autoridad de Certificación tenga conocimiento de ella, el Certificado en cuestión deberá ser revocado sin demora. Sin embargo, dado el uso de los Certificados de un solo uso producidos bajo esta PC-DPC y la corta vida útil de estos Certificados, es importante notar que la revocación es aquí principalmente un instrumento para proporcionar una LCR[21] para los componentes técnicos que se requieren para disponer de ellos.

Para esta categoría de Certificados, no se publica el motivo de la revocación.

4.9.1.2 [AC ORG] Certificados de Organización

Las siguientes circunstancias pueden llevar a la revocación del Certificado de Organización:

- el Certificado ya no cumple con el PC-DPC al que está sujeto;
- la criptografía utilizada ya no garantiza la conexión entre el sujeto y la clave pública;
- la información de la Organización contenida en el Certificado expedido a su nombre no se ajusta a la identidad de la Organización ni al uso previsto en el Certificado;
- se detecta un error (intencional o no intencional) en la solicitud de registro de la Organización;
- se sospecha que se ha perdido el control sobre el uso de la clave privada del Titular o se sospecha que se ha perdido la clave privada del Titular:
    - sospecha de estar comprometida;
    - comprometida;
    - perdida;
    - descargada;
    - destruida;
    - alterada.
- el representante autorizado (véase el capítulo 3.4.2) solicita la revocación del Certificado;
- cese de la actividad de la Autoridad de Certificación, de la Organización o del Suscriptor;
- fin de la relación contractual entre el Suscriptor y la Autoridad de Certificación;
- cambio en las regulaciones técnicas o legales, o cambio en la recomendación aplicable a la Autoridad de Certificación o a la Organización, que requiera la finalización del uso del Certificado.

Cuando se produzca una de las circunstancias mencionadas y la Autoridad de Certificación tenga conocimiento de ella, el Certificado en cuestión deberá ser revocado sin demora.

Además, la Autoridad de Certificación puede revocar automáticamente un Certificado de Organización en las siguientes circunstancias:

[21] LCR = Lista de Certificados Revocados

- incumplimiento de esta PC-DPC;
- incumplimiento de cualquiera de las obligaciones derivadas del contrato de Suscriptor o de cualquier otro documento del expediente de suscripción (como este PC-DPC y su capítulo 9.6) por parte de un Titular o de un Suscriptor, en particular en lo que se refiere a la utilización del Certificado en condiciones distintas de las previstas en el presente documento (véase el capítulo 1.5.1.1).

Para esta categoría de Certificado, se publica el motivo de la revocación. Esta es una forma de identificar el tipo de certificado en la LCR.

4.9.2 Origen de una solicitud de revocación

4.9.2.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

Sólo el Dispositivo Portador de Certificados está autorizado a solicitar la revocación de este tipo de Certificado después de encontrarse con una de las circunstancias mencionadas en el capítulo 4.9.1.1 este documento.

4.9.2.2 [AC ORG] Certificados de Organización

Las personas y entidades habilitadas para solicitar la revocación de este tipo de Certificado, tras el encuentro de una de las circunstancias mencionadas en el capítulo 4.9.1.2 este documento, son:

- el representante del Suscriptor o uno de sus representantes adjuntos, que disponga de los datos de identificación y autenticación que le permitan acceder a esta función;
- la Autoridad de Certificación.

4.9.3 Procedimiento para procesar una solicitud de revocación

4.9.3.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

Esta PC-DPC no requiere la identificación de la solicitud de revocación. De hecho, sólo el Dispositivo Portador del Certificado, tal como se describe en el capítulo 1.3.3 puede solicitar una revocación sobre la base de una de las posibles causas de revocación que ha detectado (véase el capítulo 4.9.1.1).

Por lo tanto, la solicitud se autoriza automáticamente. A continuación, la Autoridad de Certificación procede a la revocación. La operación es instantánea y se registra en los registros de eventos (véase el capítulo 5.4.1).

Una vez que se revoca el Certificado, no se puede restablecer. Se informa al interesado del cambio de estado mediante la publicación del Certificado revocado en una de las Listas de Certificados Revocados publicadas en la dirección definida en el capítulo 2.2 este documento.

4.9.3.2 [AC ORG] Certificados de Organización

La solicitud de revocación de este tipo de Certificado no se autoriza automáticamente. De hecho, la solicitud de la persona o entidad autorizada (ver Capítulo 4.9.1.2) debe ser validada por personal autorizado de Worldline (llamado "Piloto"). A tal efecto, la persona o entidad autorizada para realizar la solicitud se pone en contacto con un número de teléfono que le fue facilitado en el momento de la creación del Certificado susceptible de revocación. Este número está disponible los

7 días de la semana, las 24 horas del día. La información que debe proporcionarse al Piloto para la autorización de la revocación es:

- datos de identificación: nombre de la Organización e identidad del representante autorizado;
- elemento de autenticación: código secreto que se proporciona al crear el Certificado.

Una vez que estos elementos han sido validados por el sistema, se autoriza la solicitud de revocación. La operación es llevada a cabo en varios pasos por el Piloto. Algunos pasos también requieren la intervención del solicitante, por teléfono, quien debe dar la información que el Piloto debe ingresar o verificar para que el solicitante pueda mantener el control sobre la operación. La operación se registra en los registros de eventos (véase el capítulo 5.4.1).

Una vez que se revoca el Certificado, no se puede restablecer. Se informa al interesado del cambio de situación mediante una notificación enviada por la Autoridad de Registro y mediante la publicación del Certificado revocado en una de las Listas de Certificados Revocados publicadas en la dirección definida en el capítulo 2.2 presente documento.

La solicitud de revocación de este tipo de Certificado es rastreada para cumplir con el plazo de revocación establecido por la Autoridad de Certificación (ver capítulo 4.9.5.2).

Sin embargo, la Autoridad de Certificación puede revocar un Certificado (véase el capítulo 4.9.2.2) si los eventos así lo requieren. La [DTPC][22] proporciona más información sobre este tema.

4.9.4 Plazo para presentar la solicitud de revocación

4.9.4.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

Dada la naturaleza atómica de la operación en términos de firma electrónica cuando se utiliza un Certificado de un solo uso, la solicitud presentada por el solicitante (véase el capítulo 4.9.2.1) es inmediata cuando se encuentra una de las causas mencionadas en el capítulo 4.9.1.1

4.9.4.2 [AC ORG] Certificados de Organización

Tan pronto como el representante autorizado tenga conocimiento de una de las posibles causas de revocación definidas en el capítulo 4.9.1.2 este documento, deberá presentar su solicitud de revocación sin demora.

4.9.5 Tiempo para que la AC procese una solicitud de revocación

El tiempo máximo entre la recepción de la solicitud de revocación y la consideración de la solicitud de revocación es de veinticuatro (24) horas, con la función de gestión de revocación disponible los 7 días de la semana, las 24 horas del día.

4.9.5.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

[22] DTPC = Documentación Técnica de Prácticas de Certificación (ver capítulo 1.7.3.3)

La solicitud de revocación de un Certificado de un solo uso se procesa inmediatamente después de que la Autoridad de Certificación la recibe. La revocación es efectiva cuando el Certificado en cuestión se introduce en la LCR generado.

La operación se realiza de forma inmediata y automática tras la recepción y validación de la solicitud.

4.9.5.2 [AC ORG] Certificados de Organización

La solicitud de revocación de un Certificado de organización se procesa inmediatamente después de que la Autoridad de Certificación la recibe. La revocación es efectiva cuando el Certificado en cuestión se introduce en la LCR generado.

Una solicitud de revocación de un Certificado de Organización se define por su número de seguimiento y por su fecha de revocación, su seguimiento y trazabilidad están claramente definidos y son alcanzables. Esto permite comprobar si se ha respetado o no el plazo de revocación.

4.9.6 Requisitos para la verificación de la revocación por parte de los usuarios de Certificados

4.9.6.1 [AC OTU][AC OTU LCP] Certificados de un solo uso

Cuando se utiliza un Certificado de un solo uso proporcionado por una Autoridad de Certificación en línea, esta PC-DPC no formula, dado el carácter atómico de la operación de firma, ningún requisito para la verificación de la revocación del Certificado.

4.9.6.2 [AC ORG] Certificados de Organización

Cuando se utiliza un Certificado de Organización proporcionado por la Autoridad de Certificación, el usuario debe comprobar el estado del Certificado en el que desea confiar antes de utilizarlo. Para ello, puede consultar las LCR publicadas o hacer una solicitud al contestador automático del OCSP[23] (véase el capítulo 4.10).

Además del estado, el usuario debe comprobar la validez del Certificado en cuestión y la correspondiente Cadena de Certificación.

4.9.7 Frecuencia de establecimiento de las LCR

La frecuencia de establecimiento de las LCR es de veinticuatro (24) horas. Sin embargo, una nueva LCR puede publicarse en cualquier momento, por ejemplo, tras una revocación. Tienen una validez de siete (7) días.

4.9.8 Plazo máximo de publicación de una LCR

Una LCR se publicará en un plazo máximo de sesenta (60) minutos a partir de su generación.

[23] OCSP = "*Online Certificate Status Protocol*" = Protocolo de Estado de Certificados en Línea

4.9.9 Disponibilidad de un sistema en línea para comprobar la revocación y el estado de los Certificados.

Un contestador automático OCSP está disponible en línea y es accesible como se describe en el capítulo 2.2, lo que permite al usuario comprobar la revocación y el estado de los Certificados en línea (véase el capítulo 4.10).

La información de revocación disponible es consistente entre los diferentes servicios de información de revocación (LCR y contestador automático OCSP).

4.9.10 Requisitos de verificación en línea para la revocación de Certificados por parte de los usuarios

Los requisitos de verificación en línea para la revocación de los Certificados por parte de los usuarios se detallan en el capítulo 4.9.6 esta PC-DPC.

4.9.11 Otros medios de información disponibles sobre las revocaciones

No se aplica.

4.9.12 Requisitos específicos en caso de compromiso de la clave privada

Las entidades autorizadas a presentar una solicitud de revocación están obligadas a hacerlo lo antes posible tras conocer el compromiso de la clave privada (véase el capítulo 4.9.4).

En el caso de los Certificados de las Autoridades de Certificación, la revocación por compromiso de la clave privada se notificará al organismo de control [Notificación ANSSI] en un plazo de veinticuatro (24) horas de acuerdo con los requisitos de [eIDAS].

4.9.13 Posibles causas de una suspensión

Bajo esta PC-DPC, no se permite la suspensión de los Certificados.

4.9.14 Origen de una solicitud de suspensión

No se aplica.

4.9.15 Procedimiento para tramitar una solicitud de suspensión

No se aplica.

4.9.16 Límites al período de suspensión de un Certificado

No se aplica.

4.10 Funciones de información sobre el estado de los Certificados

4.10.1 Características de funcionamiento

Las Autoridades de Certificación proporcionan a los usuarios dos mecanismos para la consulta pública de la situación del certificado: las LCR y el contestador automático del OCSP.
Las LCR se publican en formato v2 en Internet, accesibles en los protocolos HTTP(s):

- especificados en el capítulo 2.2 esta PC-DPC;
- especificados en el Certificado expedido por la Autoridad de Certificación, tal como se especifica en el capítulo 7.1a presente PC-DPC.

Una LCR contiene una lista de Certificados emitidos por una de las Autoridades de Certificación en línea que están revocados y no han expirado (no se ha alcanzado la fecha y hora de expiración del Certificado). De hecho, un certificado revocado y caducado ya no aparece en el LCR.
Incluirá, en particular, la fecha de su publicación y la fecha de la siguiente publicación.
Las LCR también están firmadas por la Autoridad de Certificación de destino para asegurar su origen e integridad.
El enlace al contestador automático OCSP se especifica en Internet, accesible en el (los) protocolo(s) HTTP en la dirección:

- especificados en el capítulo 2.2 esta PC-DPC;
- especificados en el Certificado expedido por la Autoridad de Certificación, tal como se especifica en el capítulo 7.1a presente PC-DPC.

Las Autoridades de Certificación garantizan el origen y la integridad de las respuestas proporcionadas por el contestador automático OCSP que pone a disposición de los usuarios.

4.10.2 Disponibilidad de la función

La función de información sobre el estado de los Certificados está disponible los 7 días de la semana, las 24 horas del día. El tiempo máximo de inactividad de la plataforma es de ocho (8) horas al mes.

4.10.3 Dispositivos opcionales

No se aplica.

4.11 Fin de la relación entre el Suscriptor y la AC

La terminación de la relación entre el Suscriptor y TSP MediaCert como parte de los servicios presentados en el capítulo 1.5.1.1 terminación o no renovación del Contrato de Suscripción o de los contratos de servicios expresamente vinculados al mismo.

La Autoridad de Registro ya no reconoce las solicitudes transmitidas y firmadas por el Suscriptor, su representante o los suplentes de su representante.

A continuación, se pide al Suscriptor que presente una o más solicitudes (teniendo en cuenta el número de Certificados de que se trate) para que revoque su(s) Certificado(s) de la Organización sin demora si siguen siendo válidos.

4.12 Secuestrador de claves y recuperación

Esta PC-DPC prohíbe el secuestro de las claves privadas de las Autoridades de Certificación, y los Certificados de portador.

4.12.1 Política y prácticas de secuestro de claves

No se aplica.

4.12.2 Política y prácticas de recuperación al encapsular claves de sesión

No se aplica.

5 Medidas de seguridad no técnicas

5.1 Medidas de seguridad física

5.1.1 Ubicación geográfica y construcción de los sitios

Se aplican todos los requisitos y prácticas descritos en la [PG][24].

En particular, todos los sistemas de alojamiento de las instalaciones que intervienen en la generación y revocación de Certificados funcionan en un entorno que protege físicamente los servicios de las amenazas de riesgo debidas al acceso no autorizado a los sistemas o datos. El perímetro del área segura está claramente identificado y no puede ser accedido por personal no autorizado u organizaciones de terceros.

5.1.2 Acceso físico

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.1.3 Suministro de energía y aire acondicionado

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.1.4 Vulnerabilidad a los daños causados por el agua

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.1.5 Prevención y protección contra incendios

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.1.6 Conservación de los soportes

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.1.7 Desmantelamiento de los soportes

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.1.8 Copias de seguridad externas

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.2 Medidas de seguridad de procedimiento

5.2.1 Funciones de confianza

[24] PG = Política General del TSP MediaCert (ver capítulo 1.7.3.3)

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.2.2 Número de personas necesarias

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.2.3 Identificación y autenticación para cada función

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.2.4 Roles que requieren segregación de funciones

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.3 Medidas de seguridad para el personal

5.3.1 Calificaciones, habilidades y autorizaciones requeridas

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.3.2 Procedimientos de verificación de antecedentes

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.3.3 Requisitos de formación inicial

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.3.4 Requisitos y frecuencia de la formación continua

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.3.5 Frecuencia y secuencia de rotación entre las distintas atribuciones

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.3.6 Sanciones en caso de acciones no autorizadas

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.3.7 Requisitos para el personal de los proveedores de servicios externos

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.3.8 Documentación proporcionada al personal

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.4 Procedimientos para la compilación de datos de auditoría

5.4.1 Tipo de eventos registrados

Se aplican todos los requisitos y prácticas descritos en la [PG].

Además de los eventos descritos en la |PG], esta política requiere que las Autoridades de Certificación dentro de su alcance recopilen los siguientes datos de auditoría:

- todos los eventos relacionados con la seguridad, en particular:
    - acceso físico a los locales que albergan los sistemas;
    - cambios en la política de seguridad de los sistemas;
    - cambios en el personal que trabaja en nombre de las Autoridades de Certificación;
    - Arranques y paradas de los sistemas;
    - Arranques y paradas de los parámetros de la función de registro de eventos;
    - fallos de hardware y software;
    - modificaciones (cambio, corrección o evolución) de los distintos componentes;
    - intentos de acceso a los sistemas;
    - conexiones y desconexiones a los sistemas de los usuarios autorizados.
- todos los eventos relacionados con el registro de titulares, en particular:
    - recepción de una solicitud de Certificado (inicial y de renovación);
    - validación / rechazo de una solicitud de Certificado;
    - eventos relacionados con claves de firma y Certificados de la Autoridad de Certificación (generación (ceremonia de claves), backup/recuperación, revocación, renovación, destrucción, etc.);
    - generación de Certificados de titulares;
    - publicación y actualización de información relacionada con las Autoridades de Certificación (PC-DPC, Certificados de AC, condiciones generales de uso, etc.);
    - recepción de una solicitud de revocación;
    - validación / rechazo de una solicitud de revocación;
    - generación y publicación de las LAR y LCR.

En cuanto al procedimiento de registro, las Autoridades de Certificación también mantienen:

- la identidad de la persona que solicitó el Certificado;
- el original del formulario de solicitud de Certificado;

- la identidad de la persona como rol de confianza que realizó el registro.

Dado que el expediente de registro contiene los datos personales del titular, el almacenamiento está sujeto a medidas de seguridad, de acuerdo con el capítulo 9.4 este documento.

5.4.2 Frecuencia de procesamiento del registro de eventos

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.4.3 Período de retención del registro de eventos

Se archivan los registros de eventos que se pretende mantener. El período de archivo de esta información se especifica en el capítulo 5.5.2 este documento.

5.4.4 Protección de registros de eventos

Los registros de eventos están protegidos bajo las mismas condiciones que las definidas en el capítulo 5.5.3 este documento.

5.4.5 Procedimiento para realizar copias de seguridad de los registros de eventos

El procedimiento para realizar copias de seguridad de los registros de eventos de la IGC[25] es interno y se especifica en el documento [DTPC][26].

5.4.6 Sistema de recogida de datos de registro de eventos

El sistema de recopilación de registros de eventos de las IGC es interno y se especifica en el documento [DTPC].

5.4.7 Notificación de la inscripción de un evento al gestor de eventos

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.4.8 Evaluación de las vulnerabilidades

Las vulnerabilidades se evalúan durante un análisis de riesgos (véase el capítulo sobre análisis de riesgos en la [PG]). El control de los registros de eventos funcionales se lleva a cabo bajo demanda en caso de litigio o para el análisis del comportamiento de las IGC.

5.5 Archivo de datos

TSP MediaCert se encarga de organizar el archivo. Este archivo garantiza la durabilidad de los registros de eventos constituidos por los distintos componentes de las IGC.

[25] IGC = Infraestructura de Gestión de Claves *("PKI")*

[26] DTPC = Documentación Técnica de Prácticas de Certificación (ver capítulo 1.7.3.3)

5.5.1 Clases de datos que se deben archivar

Los datos que deben archivarse son los siguientes:

- software (ejecutable) y archivos de configuración de los equipos informáticos;
- las PC-DPCs;
- las DTPCs;
- los expedientes de registro;
- los Certificados expedidos;
- las LAR y LCR emitidas o publicadas;
- los distintos compromisos firmados por el Comité MediaCert;
- los registros de eventos de las diferentes entidades de la IGC (véase el capítulo 5.4.1).

5.5.2 Período de conservación de archivos

Los períodos mínimos de retención son los siguientes:

Versión	Autor(es)
3 años después del final de la vida de la AC	• software (ejecutable) y archivos de configuración de los equipos informáticos; • las PC-DPCs; • las DTPCs; • los Certificados expedidos; • las LAR y LCR emitidas o publicadas; • los distintos compromisos firmados por el Comité MediaCert.
7 años después de la expiración del Certificado asociado	• los expedientes de registro; Nota: Especificidad para los expedientes de registro relacionadas con los certificados de un solo uso, el período de retención del archivo es de ocho (8) años, debido a la naturaleza especial de la vida útil de esta gama de Certificados. • los elementos del ciclo de vida del Certificado (generación, revocación, etc.).
10 años después de su generación	Otros datos de auditoría (p. ej., arranque y parada de los sistemas)

Sin embargo, el período de almacenamiento de los expedientes de registro podrá ser modificado a petición del Suscriptor, quien podrá solicitar una prórroga más allá del período definido anteriormente a Worldline, mediante acuerdo expreso en las condiciones específicas del Contrato

de Suscripción. Esta extensión debe estar justificada por obligación reglamentaria o legal y acompañada de la obligación de información, asumida por el Suscriptor, de las personas afectadas por el procesamiento de los datos personales contenidos en el expediente de registro.

5.5.3 Protección de los archivos

Se aplican todos los requisitos y prácticas descritos en la [PG].

Los medios de protección de archivos implementados por TSP MediaCert en el contexto de las Autoridades de Certificación en línea difieren según el tipo de datos. Típicamente:

- los archivos documentales digitales están protegidos por una caja fuerte digital cuyo acceso está controlado por TSP MediaCert.
- los archivos manuscritos están protegidos por sistemas físicos seguros, como cajas fuertes o armarios, cuyo acceso está controlado por TSP MediaCert.

5.5.4 Procedimiento de copia de seguridad de archivo

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.5.5 Requisitos de estampación de la hora de los datos

En el capítulo 6.8 este documento se especifican los requisitos para la datación y la estampación de fecha y hora.

5.5.6 Sistema de recogida de archivos

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.5.7 Procedimiento de recuperación y verificación de archivos

El procedimiento para recuperar los archivos de las Autoridades de Certificación es interno y se especifica en la [DTPC]. El acceso a los archivos está sujeto a restricciones.

Los archivos estarán disponibles en caso de requerimiento judicial.

5.6 Cambio de Pareja de claves de AC

Las Autoridades de Certificación no pueden generar un Certificado con una fecha final posterior a la fecha de expiración del Certificado de la Autoridad de Certificación. A tal fin, el período de validez del certificado de la Autoridad de Certificación deberá ser superior al de los Certificados que firme.

Respecto a la fecha de caducidad de este Certificado, se solicitará su renovación en un plazo al menos igual a la vigencia de los Certificados firmados por la clave privada correspondiente.

En cuanto se genere una nueva pareja de claves AC, sólo se utilizará la nueva clave privada para firmar los Certificados.

El Certificado anterior sigue siendo utilizable para validar los Certificados emitidos con esta clave hasta que hayan expirado todos los Certificados firmados con la clave privada correspondiente.

5.7 Recuperación del compromiso y del desastre

5.7.1 Procedimientos para reportar y manejar incidentes y compromisos

Se aplican todos los requisitos y prácticas descritos en la [PG].

En el caso de un incidente importante, como la pérdida, la sospecha de compromiso, el compromiso, el robo de la clave privada de una AC, el acontecimiento desencadenante es el reconocimiento de este incidente a nivel de la IGC. El responsable del TSP MediaCert debe ser informado inmediatamente. Entonces tendrá que asegurarse de que la anomalía sea tratada. Si considera que el incidente es grave, solicitará la revocación inmediata del Certificado. Si esto ocurre, publicará la información de revocación del Certificado con la mayor urgencia, o incluso inmediatamente. Lo hará a través del sitio web público de TSP MediaCert y/o mediante notificación por correo electrónico a todos los clientes. Si alguno de los algoritmos, o parámetros asociados, utilizados por la AC o sus titulares se vuelven insuficientes para el uso restante previsto, entonces el administrador de TSP MediaCert publicará la información a través del sitio público y notificará a todos sus clientes afectados por correo electrónico. Todos los Certificados relevantes serán revocados.

5.7.2 Procedimientos de recuperación en caso de corrupción de los recursos informáticos (hardware, software y/o datos)

TSP MediaCert tiene un plan de continuidad de negocio (véase el capítulo 5.7.4) para satisfacer los requisitos de disponibilidad de las diversas funciones de las IGC derivadas de esta PC-DPC, los compromisos en línea de las Autoridades de Certificación en esta PC-DPC, en particular en lo que se refiere a las funciones relacionadas con la publicación y/o revocación de certificados. Este plan se prueba regularmente.

5.7.3 Procedimientos de recuperación en caso de comprometer la clave privada de un componente

El compromiso de una infraestructura o clave de control de un componente se aborda en el plan de continuidad y recuperación de desastres del componente (véase el capítulo 5.7.4) como un desastre.

En caso de que la clave privada de la Autoridad de Certificación se vea comprometida, el MediaCert TSP indicará públicamente que los certificados y la información de revocación emitida con dicha clave pueden dejar de ser válidos. El Certificado correspondiente será revocado inmediatamente.

5.7.4 Capacidades de continuidad después de un desastre

Se aplican todos los requisitos y prácticas descritos en la [PG].

5.8 Fin del ciclo de vida de la IGC

El cese de actividad puede ser total o parcial (por ejemplo: cese de actividad sólo para una determinada familia de Certificados).

El cese parcial de la actividad será gradual, de forma que sólo las obligaciones a las que se hace referencia a continuación serán cumplidas por la IGC, o por una entidad tercera que se haga cargo de las actividades, al expirar el último Certificado expedido.

En caso de cese total de actividad, la IGC o, en caso de imposibilidad, cualquier entidad que la sustituya en virtud de una ley, reglamento, decisión judicial o acuerdo previamente celebrado con esta entidad, deberá garantizar la revocación de los Certificados y la publicación de las LAR/LCR de acuerdo con los compromisos adquiridos en su PC-DPC. A continuación, la IGC aplica un plan de cese de actividad. Este plan se actualiza periódicamente e incluye las acciones que se enumeran a continuación.

La IGC tomará las siguientes disposiciones en caso de separación:

- notificación de las entidades afectadas;
- transferencia de sus obligaciones a Worldline;
- gestión del estado de revocación de los Certificados que han sido emitidos y que aún no han caducado.

Cuando se interrumpa el servicio, la IGC tomará las siguientes medidas:

- informar (por ejemplo, mediante recibo) a todos los titulares de Certificados revocados o que vayan a ser revocados, así como a sus entidades de conexión, si procede;
- abstenerse de transmitir la clave privada que le permitió emitir Certificados;
- revocar todos los Certificados que haya firmado y que sigan siendo válidos;
- revocar su Certificado;
- tomar todas las medidas necesarias para destruirlo o inutilizarlo (la clave nominal y las posibles copias de seguridad).

6 Medidas técnicas de seguridad

6.1 Generación e instalación de Parejas de claves

6.1.1 Generación de Parejas de claves

6.1.1.1 Parejas de claves AC

Se aplican todos los requisitos y prácticas descritos en la [PG].

Las claves de firma de AC en línea se generan e implementan en un módulo criptográfico que ha sido sometido a una evaluación de seguridad según se define en el Capítulo 6.2.11.1 este documento.
Estas claves de firma tienen un identificador único que se especifica necesariamente al configurar las aplicaciones para no comprometer su uso.

6.1.1.2 Claves de autenticación de un componente de la IGC

Se aplican todos los requisitos y prácticas descritos en la [PG].

6.1.1.3 Claves de autenticación del Suscriptor

La autenticación del Suscriptor se describe en el Capítulo 3.2.5 esta PC-DPC.

Las AC en línea no producen los Certificados de autenticación adjuntos a la clave privada de un Suscriptor y no son responsables de la emisión de estos Certificados. En efecto, se informa al Suscriptor de las normas que deben respetarse para autenticarse ante la Autoridad de Registro (véase el capítulo 3.2.5) y le corresponde a él obtener el o los Certificados que le permitan autenticarse ante la Autoridad de Registro.

6.1.1.4 Parejas de claves de Certificados portadores generados por la AC

Las Autoridades de Certificación en línea no generan las claves de los Certificados portadores.

6.1.1.5 Parejas de claves de Certificados portadores generados para la parte interesada

Las Parejas de claves son generadas por el Dispositivo Portador de Certificados, que conserva el uso exclusivo de las mismas, bajo las siguientes condiciones:

Certificado de un solo uso	Certificado de Organización
Dentro de un módulo criptográfico aislado físicamente que cumpla los requisitos definidos en el capítulo 6.2.11.2 presente documento.	
Copiado en otros módulos criptográficos dedicados para el mismo uso, cumpliendo los mismos requisitos que los anteriores, de acuerdo con los procesos de clonación recomendados por el proveedor.	

Certificado de un solo uso	Certificado de Organización
En los locales seguros de TSP MediaCert (véase el capítulo 5.1)	
Bajo el control del Dispositivo Portador del Certificado	Bajo la supervisión de dos (2) personas en un puesto de confianza dentro del TSP MediaCert
Según un script previamente definido por el TSP MediaCert	Según un documento de la Organización y un documento técnico, ambos firmados por todos los participantes, en particular por el maestro de ceremonias.

El TSP MediaCert implementa medidas de control y protección a nivel de Dispositivo Portador de Certificados para proteger el uso de claves privadas.

Esta PC-DPC también prohíbe utilizar una Pareja de claves existente asociada con una CSR anterior (véase el capítulo 4.7).

6.1.2 Transmisión de la clave privada al beneficiario

No se aplica.

6.1.3 Transmisión de la clave pública a la AC

La clave pública es transmitida por el Dispositivo Portador del Certificado a la Autoridad de Registro, que la transmite a la AC de destino dentro de una plantilla en formato PKCS#10 (CSR) para la generación del Certificado de un solo uso/de Organización.

6.1.4 Transmisión de la clave pública de la AC a los usuarios de Certificados

Los Certificados que contienen claves públicas de las Autoridades de Certificación se publican en su sitio web, cuya dirección se define en el capítulo 2.2 este documento.

6.1.5 Tamaño de las Parejas de claves

Se aplican todos los requisitos y prácticas descritos en la [PG].

También se aplican los requisitos y prácticas adicionales específicos que se definen a continuación.

Parejas de claves	Algoritmo	Función Hash	Tamaño (bits)
Certificados de la AC OTU	RSA	SHA-2	4096
Certificados de la AC OTU LCP	RSA	SHA-2	4096
Certificados de la AC ORG	RSA	SHA-2	4096
Certificados de un solo uso "estándar"	RSA	SHA-2	2048

Parejas de claves	Algoritmo	Función Hash	Tamaño (bits)
Certificados de un solo uso "reforzados"	RSA	SHA-2	2048
Certificados de Organización	RSA	SHA-2	2048
Certificados de un solo uso de pruebas "estándar"	RSA	SHA-2	2048
Certificados de un solo uso de pruebas "reforzados"	RSA	SHA-2	2048
Certificados de Organización de pruebas	RSA	SHA-2	2048

6.1.6 Verificación de la generación de los parámetros de las Parejas de claves y de su calidad

El equipo de generación de Parejas de claves utilizado para la generación de los parámetros de las Parejas de claves de las Autoridades de Certificación son módulos criptográficos configurados para cumplir estos requisitos (véase el capítulo 6.1.1.1). Las Parejas de claves sólo pueden generarse en un módulo que cumpla este requisito, o a un nivel criptográfico y de seguridad superior.

Lo mismo se aplica a las Parejas de claves portador (véase el capítulo 6.1.1.5).

6.1.7 Objetivos del uso de las claves

Los usos de las claves se definen en el capítulo 1.5 y más concretamente en los Certificados según la extensión "*Key Usage*" (véase el capítulo 7.1).

6.2 Medidas de seguridad para la protección de la clave privada y los módulos criptográficos

6.2.1 Estándares y medidas de seguridad para los módulos criptográficos

6.2.1.1 Módulos criptográficos de la AC

Se aplican todos los requisitos y prácticas descritos en la [PG].

Las claves de firma de las Autoridades de Certificación se generan e implementan en un módulo criptográfico que ha sido sometido a una evaluación de seguridad según se define en el capítulo 6.2.11.1 este documento.
Sin embargo, las claves de firma de estas Autoridades de Certificación operan en componentes de software separados para asegurar el control durante el uso.

6.2.1.2 Dispositivos criptográficos de los beneficiarios

No se aplica.

6.2.2 Comprobación de la clave privada

6.2.2.1 Claves privadas de AC

Se aplican todos los requisitos y prácticas descritos en la [PG].

Además, el control de las claves privadas de firma de las AC se lleva a cabo por personal de

confianza (Titulares de secretos) y a través de una herramienta que implementa la compartición de secretos.

6.2.2.2 Claves privadas de los Certificados de Portadores

El control de las claves privadas correspondientes a los diferentes Certificados emitidos por las Autoridades de Certificación está garantizado por el Dispositivo Portador de Certificados, que tiene el control exclusivo sobre las mismas. Sin embargo, este control exclusivo sigue estando sujeto a la activación descrita en el capítulo 6.4.1.2 este documento.

6.2.3 Depósito de la clave privada

Se aplican todos los requisitos y prácticas descritos en la [PG].

6.2.4 Copia de seguridad de la clave privada

Se aplican todos los requisitos y prácticas descritos en la [PG].

Además, como las claves privadas de las AC gobernadas por esta PC-DPC no están permanentemente activadas dentro del módulo criptográfico, estas claves privadas son respaldadas fuera de un módulo criptográfico. Esta copia de seguridad se realiza de forma encriptada y con un mecanismo de control de integridad. El cifrado utilizado proporciona un nivel de seguridad equivalente o superior al del almacenamiento dentro del módulo criptográfico y, en particular, se basa en un algoritmo, una longitud de clave y un modo de funcionamiento capaces de resistir los ataques criptoanalíticos durante al menos la vida útil de la clave así protegida. Las operaciones de cifrado y descifrado se realizan dentro del módulo criptográfico de tal forma que las claves privadas de AC no se encuentran en ningún momento en texto claro fuera del módulo criptográfico. Los medios de almacenamiento para las copias de seguridad se almacenan en una caja fuerte. El control de las operaciones de cifrado/descifrado cumple los requisitos del capítulo 6.2.2.

6.2.5 Archivo de la clave privada

Se aplican todos los requisitos y prácticas descritos en la [PG].

6.2.6 Transferencia de la clave privada desde/hacia el módulo criptográfico

6.2.6.1 Claves privadas de AC

La transferencia hacia/desde el módulo criptográfico sólo se realiza para la generación de copias de seguridad. Esto se hace en forma numérica, de acuerdo con los requisitos del capítulo 6.2.4.

6.2.6.2 Claves privadas de los Certificados portadores

No se aplica.

6.2.7 Almacenamiento de la clave privada en un módulo criptográfico

Se aplican todos los requisitos y prácticas descritos en la [PG].

6.2.8 Método de activación de la clave privada

6.2.8.1 Claves de AC privadas

Se aplican todos los requisitos y prácticas descritos en la [PG].

6.2.8.2 Claves privadas de los Certificados portadores

[AC OTU][AC OTU LCP] Certificados de un solo uso

Las claves privadas de los Certificados de un solo uso son activadas por el Dispositivo Portador de Certificado con uno de los módulos criptográficos previstos a tal efecto, tras la recepción del Certificado de un solo uso emitido por la AC de destino durante la sesión de firma.

[AC ORG] Certificados de Organización

Las claves privadas de los Certificados de Organización son activadas por el Dispositivo Portador de Certificados con uno de los módulos criptográficos previstos a tal efecto, previa recepción de una solicitud debidamente validada y autenticada.

6.2.9 Método de desactivación de la clave privada

6.2.9.1 Claves privadas de AC

Se aplican todos los requisitos y prácticas descritos en la [PG].

6.2.9.2 Claves privadas de los Certificados portadores

[AC OTU][AC OTU LCP] Certificados de un solo uso

La clave privada de un Certificado de un solo uso se destruye después de su uso.

[AC ORG] Certificados de Organización

La desactivación de la clave privada de un Certificado de Organización en el módulo criptográfico es automática tan pronto como finaliza la sesión de sellado o tan pronto como el módulo se detiene o desconecta.

6.2.10 Método de destrucción de la clave privada

6.2.10.1 Claves de AC privadas

Se aplican todos los requisitos y prácticas descritos en la [PG].

Además, la destrucción permanente de una clave privada de AC se consigue destruyendo los medios de restauración de la clave privada:

- la destrucción de la clave privada y de todas las copias de seguridad, y
- la destrucción de los medios de activación de la clave privada, si procede.

6.2.10.2 Claves privadas de los certificados portadores

[AC OTU][AC OTU LCP] Certificados de un solo uso

Las claves privadas de los Certificados de un solo uso se destruyen después de su uso por el Dispositivo Portador de Certificado, que realiza un seguimiento del evento.

[AC ORG] Certificados de Organización

No se aplica.

6.2.11 Nivel de cualificación del módulo criptográfico

6.2.11.1 Módulos criptográficos asociados a los Certificados de AC

El módulo criptográfico de hardware utilizado para alojar las claves privadas de las AC se evalúa en el siguiente nivel de certificación: Criterios comunes EAL4+.

6.2.11.2 Módulos criptográficos asociados a los Certificados portadores

El módulo criptográfico de hardware utilizado para alojar las claves privadas de los Certificados portadores generados por las Autoridades de Certificación se evalúa en el siguiente nivel de certificación: FIPS 140-2 nivel 3.

6.3 Otros aspectos de la gestión de Parejas de claves

6.3.1 Archivo de las claves públicas

Las claves públicas de las AC se archivan de acuerdo con el capítulo 5.5.2 este documento.

6.3.2 Vida útil de las Parejas de claves y los Certificados

La vida útil de las Parejas de claves y los Certificados varía según el tipo de Certificado. El tamaño de las Parejas de claves se ha tenido en cuenta al momento de definir estas vidas útiles, de acuerdo con los requisitos criptográficos [ETSI TS 119 312].

Las AC no pueden emitir Certificados portadores cuya vida útil exceda la del Certificado de la AC utilizado para la emisión.

Parejas de claves	Vida útil
Certificados de la AC OTU	10 años
Certificados de la AC OTU LCP	10 años
Certificados de la AC ORG	10 años
Certificados de un solo uso "estándar"	15 minutos
Certificados de un solo uso "reforzados"	15 minutos
Certificados de Organización	3 años
Certificados de un solo uso de ensayo "estándar"	15 minutos
Certificados de un solo uso de ensayo	15 minutos

Parejas de claves	Vida útil
"reforzados"	
Certificados de Organización de ensayo	3 años

6.3.3 Inventario de las Parejas de claves

6.3.3.1 Parejas de claves y Certificados de AC

TSP MediaCert mantiene un inventario actualizado regularmente de secretos y Parejas de claves.

6.3.3.2 Parejas de claves y Certificados portadores

Se realiza un inventario para verificar que todas las claves privadas producidas por las Autoridades de Certificación para el Dispositivo Portador de Certificado se han solicitado correctamente.

6.4 Datos de activación

6.4.1 Generación e instalación de los datos de activación

6.4.1.1 Generación e instalación de los datos de activación correspondientes a la clave privada de una AC

Se aplican todos los requisitos y prácticas descritos en la [PG].

6.4.1.2 Generación e instalación de los datos de activación correspondientes a la clave privada de un Certificado portador

No hay datos de activación correspondientes a la clave privada de un Certificado portador. Sin embargo, el Dispositivo Portador de Certificado no podrá utilizar la clave privada de un Certificado portador sin haber recibido una solicitud del Suscriptor.

6.4.2 Protección de datos de activación

6.4.2.1 Protección de los datos de activación correspondientes a la clave privada de una AC

Se aplican todos los requisitos y prácticas descritos en la [PG].

6.4.2.2 Protección de los datos de activación correspondientes a la clave privada de un Certificado portador

Se implementa una protección del mecanismo de autenticación del Dispositivo Portador de Certificados para la activación y el uso de claves privadas.

6.5 Medidas de seguridad de los sistemas informáticos

6.5.1 Requisitos técnicos de seguridad específicos de los sistemas informáticos

Se aplican todos los requisitos y prácticas descritos en la [PG].

6.5.2 Nivel de cualificación de los sistemas informáticos

No se aplica.

6.6 Medidas de seguridad para los sistemas durante su ciclo de vida

6.6.1 Medidas de seguridad relacionadas con el desarrollo de los sistemas

Todos los desarrollos realizados por el TSP MediaCert y que impactan en la IGC son documentados y llevados a cabo a través de un proceso con el fin de asegurar su calidad. La configuración del sistema de los componentes de la IGC, así como las modificaciones y actualizaciones, están documentadas y controladas. Además, TSP MediaCert opera una división entre los entornos de desarrollo, pruebas, preproducción y producción. Esto asegura un comienzo de producción de calidad.

6.6.2 Medidas relacionadas con la gestión de la seguridad

Cualquier evolución del sistema de un componente de las IGC se documenta y se hace un seguimiento. Aparece en los procedimientos operativos internos del componente.

6.6.3 Nivel de evaluación de la seguridad del ciclo de vida de los sistemas

Cualquier evolución significativa del sistema de un componente de las IGC se prueba y valida antes de su despliegue. Estas operaciones son llevadas a cabo por personal de confianza.

6.7 Medidas de seguridad de la red

Se aplican todos los requisitos y prácticas descritos en la [PG].

6.8 Sistema de registro de fecha y hora

Se aplican todos los requisitos y prácticas descritos en la [PG].

Además, los servidores de TSP MediaCert sincronizan sus relojes internos como máximo cada 24 horas en los servidores de referencia para garantizar la consistencia de la hora (UTC) indicada en los distintos registros electrónicos.

7 Modelo de los Certificados y LCR

7.1 Modelo de los certificados

7.1.1 Definiciones

Los Certificados emitidos por las Autoridades de Certificación en línea, incluidos los suyos propios, cumplen con las normas X.509.

Campos	Descripción
Version	Versión del Certificado X.509
Serial number	Número de serie único del Certificado
Signature	OID del algoritmo utilizado por la Autoridad de Certificación emisora para firmar el Certificado expedido
Issuer	Valor del DN (X.500) de la AC emisora del Certificado
Validity	Fecha de activación y expiración del Certificado
Subject	Valor del DN (X.500) del sujeto
Subject Public Key Info	Algoritmo OID y valor de la clave pública
Extensions	Lista de extensiones. Una extensión puede ser crítica o no crítica: • si es crítica, la aplicación de usuario a la que se presenta el Certificado debe ser capaz de procesarlo de acuerdo con su uso. Si la aplicación no sabe cómo manejar la extensión o si la extensión no está de acuerdo con su uso previsto, debe rechazar el Certificado; • si no es crítica, no hay rechazo de Certificado y la solicitud puede ignorar la extensión en cuestión.

7.1.2 Certificado de la AC OTU

Los Certificados AC OTU, llamados Certificados Técnicos AC (ACT), se diferencian por el campo *Serial Number*[27] (SERIALNUMBER) del *Distinguished Name*[28] (DN) del *Sujeto*.

Campos de DN	Obligatorio	Descripción
C	Sí	País de la Organización que rige la AC: FR
O	Sí	Nombre legal de la Organización que rige la AC: Worldline
OU	Sí	Identificador de la Organización que rige la AC: 0002 378901946
SERIALNUMBER	Sí	Número de serie único del DN[29]
CN	Sí	Identidad del Titular: MediaCert OTU CA 2019

7.1.2.1 Campos básicos

Campos	Valor
Version	2 (para la versión 3)
Serial Number	Generado automáticamente durante la Ceremonia Clave
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	DN de la AC emisora (ver capítulo 1.2.2)
Validity	10 años
Subject	DN de la AC Técnica (ver capítulo 7.1.2)
Subject Public Key Info	RSA 4096 bits

7.1.2.2 Extensiones

Campos	Crítica	Valor
Authority Key Identifier	No	[RFC 5280] método[0]: identificador de clave pública de la AC emisora
Subject Key Identifier	No	[RFC 5280] método[1]: identificador de clave pública contenido en el Certificado
Key Usage	Sí	keyCertSign, CRLSign
Certificate Policies	No	• Policy Identifier: anyPolicy (2.5.29.32.0) • Policy Qualifier Id: 1.3.6.1.5.5.7.2.1 • Qualifier: https://www.mediacert.com
Basic Constraint	No	• CA: verdadero • Maximum Path Length: 0
CRL Distribution	No	• fullName:

[27] *Número de Serie*

[28] *Nombre Distinguido*

[29] Este SERIALNUMBER se utiliza para diferenciar entre los diferentes ACTs. Se trata de un contador incrementado cada vez que se emite un nuevo ACT. Se construye de la siguiente manera:
SERIALNUMBER =
- 1: representa a la Autoridad de Certificación Técnica 1;
- 2: representa a la Autoridad de Certificación Técnica 2;
- …

Campos	Crítica	Valor
Points		http://www.mediacert.com/trustCA2019/trustCA2019.crl[30] • reason: Ausente • cRLIssuer: Ausente
Authority Information Access	No	• accessMethod : id-ad-caIssuers • accessLocation: http://www.mediacert.com/trustCA2019/trustCA2019.crt [2]

7.1.3 Certificado de la AC OTU LCP

Los certificados de la AC OTU LCP, llamados Certificados Técnicos AC (ACT), se diferencian por el campo *Serial Number*[31] (SERIALNUMBER) del *Distinguished Name*[32] (DN) del *Subject*[33].

Campos de DN	Obligatorio	Descripción
C	Sí	País de la Organización que rige la AC: FR
O	Sí	Nombre legal de la Organización que rige la AC: Worldline
OU	Sí	Identificador de la Organización que rige la AC: 0002 378901946
SERIALNUMBER	Sí	Número de serie único del DN[34]
CN	Sí	Identidad del Titular: MediaCert OTU LCP CA 2018

7.1.3.1 Campos básicos

Campos	Valor
Version	2 (para la versión 3)
Serial number	Generado automáticamente durante la Ceremonia Clave
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	DN de la AC emisora (ver capítulo 1.2.2)
Validity	10 años
Subject	DN de la AC Técnica
Subject Public Key Info	RSA 4096 bits

7.1.3.2 Extensiones

[30] Esta URL se da sólo a título informativo. La URL auténtica es la que aparece en el Certificado.

31 *Número de Serie*

32 "*Distinguished Name*" = Nombre Distinguido

33 "*Subject*" = Sujeto

34 Este SERIALNUMBER se utiliza para diferenciar entre los diferentes ACTs. Se trata de un contador incrementado cada vez que se emite un nuevo ACT. Se construye de la siguiente manera:

SERIALNUMBER =

- *1:* representa a la Autoridad de Certificación Técnica 1;
- *2:* representa a la Autoridad de Certificación Técnica 2;
- …

Campos	Crítica	Valor
Authorithy Key Identifier	No	[RFC 5280] método[0]: identificador de clave pública de la AC emisora
Subject Key Identifier	No	[RFC 5280] método[1]: identificador de clave pública contenido en el Certificado
Key Usage	Sí	keyCertSign, CRLSign
Certificate Policies	No	• Policy Identifier: anyPolicy (2.5.29.32.0) • Policy Qualifier Id: de calificador de política: 1.3.6.1.5.5.7.2.1 • Qualifier: https://www.mediacert.com
Basic Constraint	No	• CA: verdadero • Maximum path length[35]: 0
CRL Distribution Points	No	• fullName: http://www.mediacert.com/rootCA2018/rootCA2018.crl[36] • reason: Ausente • cRLIssuer: Ausente
Authorithy Information Access	No	• accessMethod : id-ad-caIssuers • accessLocation: http://www.mediacert.com/rootCA2018/rootCA2018.crt[37]

7.1.4 Certificado de la AC ORG

Los certificados de la AC ORG, llamados Certificados de la AC tecnica (ACT), se differencian por el campo Serial Number (SERIALNUMBER) del Nombre Distinguido (DN) del sujeto.

Campos del DN	Obligatorio	Descripción
C	Sí	País de la Organización que gobierna la AC: FR
O	Sí	Denominación jurídica de la Organización que gobierna la AC : Worldline
OU	Sí	Identificador de organización que gobierna la AC : 0002 378901946
SERIALNUMBER	Sí	Número de serie único del DN [38]
CN	Sí	Identidad del titular : MediaCert ORG CA 2018

7.1.4.1 Campos bàsicos

[35] Longitud máxima del trayecto

[36] Esta URL se da sólo a título informativo. La URL auténtica es la que aparece en el Certificado.

[37] Esta URL se da sólo a título informativo. La URL auténtica es la que aparece en el Certificado.

[38] Este SERIALNUMBER se utiliza para diferenciar entre los diferentes ACTs. Se trata de un contador incrementado cada vez que se emite un nuevo ACT. Se construye de la siguiente manera:

SERIALNUMBER =

- *1 :* representa la Autoridad Técnica de Certificación 1;
- *2 :* representa la Autoridad Técnica de 2 ;
- …

Campos	Valor
Versión	2 (para la versión 3)
Número de serie	Generado automáticamente durante la ceremonia de entrega de llaves
Firma	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Emisor	DN de la AC emisora (ver capítulo 1.2.2)
Validez	10 años
Sujeto	DN de la AC Tecnicà
Subject Public Key Info	RSA 4096 bits

7.1.4.2 Extensiones

Campos	Crítica	Valor
Authority Key Identifier	No	[RFC 5280] método [0] : identificador de clave pública de la autoridad de certificación emisora
Subject Key Identifier	No	[RFC 5280] método [1] : identificador de la clave pública contenida en el certificado
Key Usage	Sí	keyCertSign, CRLSign
Certificate Policies	No	• Policy Identifier : anyPolicy (2.5.29.32.0) • Policy Qualifier Id : 1.3.6.1.5.5.7.2.1 • Qualifier : https://www.mediacert.com
Basic Constraint	No	• CA : vrai • Maximum Path Length : 0
CRL Distribution Points	No	• fullName : http://www.mediacert.com/trustCA2019/trustCA2019.crl [39] • reason : ausente • cRLIssuer : ausente
Authority Information Access	No	• accessMethod : id-ad-caIssuers • accessLocation: http://www.mediacert.com/trustCA2019/trustCA2019.crt [6]

7.1.5 Certificado de un solo uso "estándar"

7.1.5.1 Campos básicos

Campos		Valor
Version		2 (para la versión 3)
Serial Number		Definido por la AC Técnica emisora
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN de la AC Técnica emisora
Validity		15 minutos
Subject	C	Nacionalidad del Titular
	SN	Apellidos del Titular

[39] Esta URL se da sólo a título informativo. La URL auténtica es la que aparece en el certificado.

	GN	Nombre del Titular
	OU	Nombre del Suscriptor
	SERIALNUMBER[40]	Número de serie único DN
	CN	Identidad del Titular formado de esta manera: Nombre del Titular [espacio] Apellidos del Titular[espacio][TraceID][41]
Subject Public Key Info		RSA 2048 bits

7.1.5.2 Extensiones

Campos		**Crítica**	**Valor**
Authority Key Identifier		No	[RFC 5280] método[0]: identificador de clave pública de la AC emisora
Subject Key Identifier		No	[RFC 5280] método[1]: identificador de clave pública contenido en el Certificado
Key Usage		Sí	nonRepudiation
Basic Constraint	Certificate Authorithy	No	Falso
Certificate Policies	policyIdentifier	No	1.2.250.1.111.20.5.3.5
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
CRL Distribution Points		No	http://pki-otu-lcp-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl[42]
Authorithy Information Access	OCSP	No	http://pki-otu-lcp-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp[42]
	CaIssuers		http://pki-otu-lcp-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate[42]

7.1.6 Certificado de un solo uso "Reforzado"

7.1.6.1 Campos básicos

Campos		**Valor**
Version		2 (para la versión 3)
Serial number		Definido por la AC Técnica emisora
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN de la AC Técnica emisora
Validity		15 minutos
Subject	C	Nacionalidad del Titular

[40] Según[RFC 3739], el campo SERIALNUMBER se utiliza para eliminar el riesgo de homonimia en los campos restantes del DN. Se construye de la siguiente manera:

SERIALNUMBER = *ReqTime:DocRef:ClientId*

- *ReqTime:* representa el tiempo de solicitud del Certificado;
- *DocRef:* representa la identificación del documento a firmar (en caso de multi-firma, es el primer documento al que se hace referencia en la solicitud de firma que aparece);
- *ClientId*: representa la identificación única del cliente.

El valor *ReqTime se utiliza para* proteger contra un caso de firmas conjuntas de dos (2) personas con el mismo nombre. La concatenación de las tres (3) informaciones garantiza un valor único entre todos los usuarios.

[41] Representa la identificación única del contenedor de trazas para la firma

[42] Esta URL se da sólo a título informativo. La URL auténtica es la que aparece en el Certificado.

	SN	Apellidos del Titular
	GN	Nombre del Titular
	OU	Nombre del Suscriptor
	SERIALNUMBER[43]	Número de serie único DN
	CN	Identidad del Titular formado de esta manera: Nombre del Titular [espacio] Apellidos del Titular [espacio] [TraceID][44]
Subject Public Key Info		RSA 2048 bits

7.1.6.2 Extensiones

Campos		Crítica	Valor
Authorithy Key Identifier		No	[RFC 5280] método[0]: identificador de clave pública de la AC emisora
Subject Key Identifier		No	[RFC 5280] método[1]: identificador de clave pública contenido en el Certificado
Key Usage		Sí	nonRepudiation
Basic Contraint	Certificate Authorithy	No	Falso
Certificate Policies	policyIdentifier	No	1.2.250.1.111.20.5.3.1
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
CRL Distribution Points		No	http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl[45]
Authorithy Information Access	OCSP	No	http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp[45]
	CaIssuers		http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificat[45]

7.1.7 Certificado de Organización

7.1.7.1 Campos básicos

Campos		Valor
Version		2 (para la versión 3)
Serial number		Definido por la AC Técnica emisora
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN del ACT emisora
Validity		3 años
Subject	C	País de la Organización

[43] Según[RFC 3739], el campo SERIALNUMBER se utiliza para eliminar el riesgo de homonimia en los campos restantes del DN. Se construye de la siguiente manera:
SERIALNUMBER = ReqTime:DocRef:ClientId
- ReqTime: representa el tiempo de solicitud del Certificado;
- DocRef: representa la identificación del documento a firmar (en caso de multi-firma, es el primer documento al que se hace referencia en la solicitud de firma que aparece);
- ClientId: representa la identificación única del cliente.

El valor ReqTime se utiliza para proteger contra un caso de firmas conjuntas de dos (2) personas con el mismo nombre y apellido. La concatenación de las tres (3) informaciones garantiza un valor único entre todos los usuarios.

[44] Representa la identificación única del contenedor de rastreo para la firma.

[45] Esta URL se da sólo a título informativo. La URL auténtica es la que aparece en el Certificado.

	OI[46]	Identificador de la Organización formado de esta manera: ICD [espacio] Identificador de la Organización
	SN[47]	Apellidos de la persona autorizada en la Organización
	GN[48]	Nombre de la persona autorizada en la Organización
	OU[49]	Nombre de la unidad de la Organización
	O	Nombre del Suscriptor
	SERIALNUMBER[50]	Número de serie único DN
	CN	Identidad de la Organización
Subject Public Key Info		RSA 2048 bits

7.1.7.2 Extensiones

Campos		Crítica	Valor
Authorithy Key Identifier		No	[RFC 5280] método[0]: Identificador de la clave pública de la AC emisora
Subject Key Identifier		No	[RFC 5280] método[1]: identificador de clave pública contenido en el Certificado
Key Usage		Sí	nonRepudiation
Basic Constraint	Certificate Authorithy	No	Falso
Certificate Policies	policyIdentifier	No	1.2.250.1.111.20.5.3.2
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Subject Alternative Name		No	[RFC 822]: correo electrónico del Titular del Certificado
CRL Distribution Points		No	http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl[51]
Authorithy Information Access	OCSP	No	http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp[57]
	CaIssuers		http://pki-org-ac[SERIALNUMBER ACT

[46] El ICD (*International Code Designator*) tiene un código único de 4 caracteres y el ID de la organización tiene un máximo de 35 caracteres.
Para las organizaciones de derecho francés, el ICD es 0002 y el ID de organización aceptado es el número de SIREN.

[47] Al menos uno de los dos datos debe estar presente en el DN: el nombre de la unidad de la Organización o el nombre completo (Nombre, Apellido) de la persona autorizada para representar a la Organización.

[48] Al menos uno de los dos datos debe estar presente en el DN: el nombre de la unidad de la Organización o el nombre completo (Nombre, Apellido) de la persona autorizada para representar a la Organización.

[49] Al menos uno de los dos datos debe estar presente en el DN: el nombre de la unidad de la Organización o el nombre completo (Nombre, Apellido) de la persona autorizada para representar a la Organización.

[50] Según[RFC 3739], el campo SERIALNUMBER se utiliza para eliminar el riesgo de homonimia en los campos restantes del DN. 50Se construye de la siguiente manera:
NÚMERO DE SERIE = *Fecha de creación*
- *CreationDate:* representa la fecha y hora (arbitraria) en el momento de retirar el Certificado: en el formato *aaaammddhhmmss*

El valor *CreationDate se utiliza para* proteger contra un caso de firmas conjuntas de dos (2) personas con el mismo nombre. La concatenación de las dos (2) informaciones garantiza un valor único entre todos los usuarios.

[51] Esta URL se da sólo a título informativo. La URL auténtica es la que aparece en el Certificado.

Campos		Crítica	Valor
			émettrice].mediacert.com/certificate[57]

7.1.8 Certificado de un solo uso de pruebas "estándar"

7.1.8.1 Campos básicos

Campos		Valor
Version		2 (para la versión 3)
Serial number		Definido por la AC Técnica emisora
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN del ACT emisora
Validity		15 minutos
Subject	C	Nacionalidad del Titular
	SN	Apellidos del Titular
	GN	Nombre del Titular
	OU	Nombre del Suscriptor
	SERIALNUMBER[52]	Número de serie único DN
	CN	Identidad del titular del pruebas formado de esta manera: TEST [espacio] Nombre del Titular [espacio] Apellidos del Titular [espacio] [TraceID][53]
Subject Public Key Info		RSA 2048 bits

7.1.8.2 Extensiones

Campos		Crítica	Valor
Authorithy Key Identifier		No	[RFC 5280] método[0]: identificador de clave pública de la AC emisora
Subject Key Identifier		No	[RFC 5280] método[1]: identificador de clave pública contenido en el Certificado
Key Usage		Sí	nonRepudiation
Basic Constraint	Certificate Authorithy	No	Falso
Certificate Policies	policyIdentifier	No	1.2.250.1.111.20.5.3.6
	policyQualifierID		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
CRL Distribution Points		No	http://pki-otu-lcp-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl[54]
Authorithy Information Access	OCSP	No	http://pki-otu-lcp-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp[58]
	CaIssuers		https://pki-otu-lcp-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate[58]

[52] Según[RFC 3739], el campo SERIALNUMBER se utiliza para eliminar el riesgo de homonimia en los campos restantes del DN. 52Se construye de la siguiente manera:

SERIALNUMBER = *ReqTime:DocRef:ClientId*

- *ReqTime:* representa el tiempo de solicitud del Certificado;
- *DocRef:* representa la identificación del documento a firmar (en caso de multi-firma, es el primer documento al que se hace referencia en la solicitud de firma que aparece);
- *ClientId*: representa la identificación única del cliente.

El valor *ReqTime se utiliza para* proteger contra un caso de firmas conjuntas de dos (2) personas con el mismo nombre. La concatenación de las tres (3) informaciones garantiza un valor único entre todos los usuarios.

[53] Representa la identificación única del contenedor de trazas para la firma.

[54] Esta URL se da sólo a título informativo.[54]La URL auténtica es la que aparece en el certificado.

7.1.9 Certificado de un solo uso de pruebas "reforzado"

7.1.9.1 Campos básicos

Campos		Valor
Version		2 (para la versión 3)
Serial number		Definido por la AC Técnica emisora
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN del ACT emisora
Validity		15 minutos
Subject	C	Nacionalidad del Titular
	SN	Apellidos del Titular
	GN	Nombre del Titular
	OU	Nombre del Suscriptor
	SERIALNUMBER[55]	Número de serie único DN
	NC	Identidad del Titular del ensayo formado de esta manera: TEST [espacio] Nombre del Titular [espacio] Apellidos del Titular [espacio] [TraceID][56]
Subject Public Key Info		RSA 2048 bits

7.1.9.2 Extensiones

Campos		Crítica	Valor
Authorithy Key Identifier		No	[RFC 5280] método[0]: identificador de clave pública de la AC emisora
Subject Key Identifier		No	[RFC 5280] método[1]: identificador de clave pública contenido en el Certificado
Key Usage		Sí	nonRepudiation
Basic Constraint	Certificate Authorithy	No	Falso
Certificate Policies	policyIdentifier	No	1.2.250.1.111.20.5.3.3
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
CRL Distribution Points		No	http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl[57]
Authorithy Information Access	OCSP	No	http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp[63]
	CaIssuers		https://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate[63]

[55] Según[RFC 3739], el campo SERIALNUMBER se utiliza para eliminar el riesgo de homonimia en los campos restantes del DN. Se construye de la siguiente manera:
SERIALNUMBER = ReqTime:DocRef:ClientId
- ReqTime: representa el tiempo de solicitud del Certificado;
- DocRef: representa la identificación del documento a firmar (en caso de multi-firma, es el primer documento al que se hace referencia en la solicitud de firma que aparece);
- ClientId: representa la identificación única del cliente.

El valor ReqTime se utiliza para proteger contra un caso de firmas conjuntas de dos (2) personas con el mismo nombre. La concatenación de las tres (3) informaciones garantiza un valor único entre todos los usuarios.

[56] Representa la identificación única del contenedor de trazas para la firma.

[57] Esta URL se da sólo a título informativo. La URL auténtica es la que aparece en el Certificado.

7.1.10 Certificado de Organización de pruebas

7.1.10.1 Campos básicos

Campos		Valor
Version		2 (para la versión 3)
Serial number		Definido por la AC Técnica emisora
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN del ACT emisora
Validity		3 años
Subject	C	País de la Organización
	OI[58]	Identificador de la Organización formado de esta manera: ICD [espacio] Identificador de la Organización
	SN[59]	Apellidos de la persona autorizada en la Organización
	GN[60]	Nombre de la persona autorizada en la Organización
	OU[61]	Nombre de la unidad de la Organización
	O	Identidad del Suscriptor
	SERIALNUMBER[62]	Número de serie único DN
	NC	TEST Identidad de la Organización[63]
Subject Public Key Info		RSA 2048 bits

7.1.10.2 Extensiones

Campos		Crítica	Valor
Authorithy Key Identifier		No	[RFC 5280] método[0]: identificador de clave pública de la AC emisora
Subject Key Identifier		No	[RFC 5280] método[1]: identificador de clave pública contenido en el Certificado
Key Usage		Sí	nonRepudiation
Basic Constraint	Certificate Authorithy	No	Falso
Certificate Policies	policyIdentifier	No	1.2.250.1.111.20.5.3.4
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com

[58] El ICD (*International Code Designator*) tiene un código único de 4 caracteres y el ID de la organización tiene un máximo de 35 caracteres.
Para las organizaciones de derecho francés, el ICD es 0002 y el ID de organización aceptado es el número SIREN.

[59] Al menos uno de los dos datos debe estar presente en el DN: el nombre de la unidad de la Organización o el nombre completo (nombre, apellido) de la persona autorizada para representar a la Organización.

[60] Al menos uno de los dos datos debe estar presente en el DN: el nombre de la unidad de la Organización o el nombre completo (nombre, apellido) de la persona autorizada para representar a la Organización.

[61] Al menos uno de los dos datos debe estar presente en el DN: el nombre de la unidad de la Organización o el nombre completo (nombre, apellido) de la persona autorizada para representar a la Organización.

[62] Según[RFC 3739], el campo SERIALNUMBER se utiliza para eliminar el riesgo de homonimia en los campos restantes del DN. 62Se construye de la siguiente manera:

NÚMERO DE SERIE = *Fecha de creación*

- *CreationDate:* representa la fecha y hora (arbitraria) en el momento de retirar el Certificado: en el formato *aaaammddhhmmss*

El valor *CreationDate se utiliza para* proteger contra un caso de firmas conjuntas de dos (2) personas con el mismo nombre. La concatenación de las dos (2) informaciones garantiza un valor único entre todos los usuarios.

[63] La palabra "TEST" y la identidad de la Organización no están separadas por un espacio.

Campos		Crítica	Valor
Subject Alternative Name		No	[RFC 822]: correo electrónico del Titular del Certificado
CRL Distribution Points		No	http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl[64]
Authorithy information	OCSP	No	http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp[65]
	CaIssuers		http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate[74]

[64] Esta URL se da sólo a título informativo. La URL auténtica es la que aparece en el Certificado.
[65] La palabra "TEST" y la identidad de la Organización no están separadas por un espacio.

7.2 Perfil LCR

7.2.1 Campos básicos

Campos		Valor
Version		1 (para la versión 2)
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN del ACT emisora
This Update		Fecha de emisión de la LCR
Next Update		Fecha de expedición de la LCR + 7 días[66]
Revoked Certificates	userCertificate	Número de serie único del Certificado revocado
	revocationDate	Fecha de revocación
	crlEntryExtensions	Información adicional que se puede proporcionar en las extensiones de entrada de LCR

7.2.2 Extensiones

Campos	Crítica	Valor
Authorithy Key Identifier	No	[RFC 5280] método[0]: identificador de la clave pública del ACT emisora
CRL Number	No	Número de LCR definido por la AC Técnica emisora

7.2.3 Extensiones de entrada

Campos	Crítica	Valor
Reason Code	No	[RFC 5280]: código correspondiente al motivo de revocación correcto

[66] En caso de que la AC deje de funcionar, la última LCR publicado será válido durante tres (3) años o más.

7.3 Perfil de OCSP

De acuerdo con el capítulo 4.10 este documento, TSP MediaCert proporciona a los usuarios un contestador OCSP para que puedan comprobar en tiempo real el estado de los certificados emitidos por las Autoridades de Certificación en línea. Este servicio cumple con [RFC 6960].

7.3.1 AC OTU

En este contexto, el contestador automático OCSP dispone de un Certificado emitido por la AC OTU, cuyo modelo se detalla a continuación.

7.3.1.1 Campos básicos

Campos		Valor
Version		2 (para la versión 3)
Serial number		Definido por la AC Técnica emisora
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN del ACT emisora
Validity		3 años
Subject	C	FR
	IO	0002 378901946
	OU	AC OTU
	O	Worldline
	SERIALNUMBER[67]	Número de serie único DN
	CN	Servicio OCSP PKI OTU
Subject Public Key Info		RSA 2048 bits

7.3.1.2 Extensiones

Campos		Crítica	Valor
Authorithy Key Identifier		No	[RFC 5280] método[0]: identificador de clave pública de la AC emisora
Subject Key Identifier		No	[RFC 5280] método[1]: identificador de clave pública contenido en el Certificado
Key Usage		Sí	Firma Digital
Basic constraint	Certificate Authorithy	No	Falso
Certificate policies	policyIdentifier	No	1.2.250.1.111.20.5.3
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Extended Key Usage		No	ocspSigning (1.3.6.1.5.5.7.3.9)
CRL Distribution Points		No	http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl[68]
Authorithy	OCSP	No	http://pki-otu-ac[SERIALNUMBER ACT

[67] Según[RFC 3739], el campo SERIALNUMBER se utiliza para eliminar el riesgo de homonimia en los campos restantes del DN. Se construye de la siguiente manera:
SERIALNUMBER = número incrementado cada vez que se emite un certificado OCSP para la AC Técnica Emisora en cuestión.

[68] Esta URL se da sólo a título informativo. La URL auténtica es la que aparece en el Certificado.

Campos		Crítica	Valor
Information Access			émettrice].mediacert.com/ocsp[81]
	CaIssuers		http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate[81]

7.3.2 AC OTU LCP

En este contexto, el contestador automático OCSP dispone de un Certificado emitido por el AC OTU LCP y cuyo perfil se detalla a continuación.

7.3.2.1 Campos básicos

Campos		Valor
Version		2 (para la versión 3)
Serial number		Definido por la AC Técnica emisora
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN del ACT emisora
Validity		3 años
Subject	C	FR
	IO	0002 378901946
	OU	AC OTU LCP
	O	Worldline
	SERIALNUMBER[69]	Número de serie único DN
	CN	Servicio OCSP PKI OTU LCP
Subject Public Key Info		RSA 2048 bits

7.3.2.2 Extensiones

Campos		Crítica	Valor
Authorithy Key Identifier		No	[RFC 5280] método[0]: identificador de clave pública de la AC emisora
Subject Key Identifier		No	[RFC 5280] método[1]: identificador de clave pública contenido en el Certificado
Key Usage		Sí	Firma Digital
Basic Constraint	Certificate Authorithy	No	Falso
Certificate Policies	policyIdentifier	No	1.2.250.1.111.20.5.3
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Extended Key Usage		No	ocspSigning (1.3.6.1.5.5.7.3.9)
CRL Distribution Points		No	http://pki-otu-lcp-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl[70]
Authorithy Information	OCSP	No	http://pki-otu-lcp -ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp[81]

[69] Según[RFC 3739], el campo SERIALNUMBER se utiliza para eliminar el riesgo de homonimia en los campos restantes del DN. Se construye de la siguiente manera:69

SERIALNUMBER = número incrementado cada vez que se emite un certificado OCSP para la CA técnica emisora en cuestión.

[70] Esta URL se da sólo a título informativo. La URL auténtica es la que aparece en el Certificado.

Campos		Crítica	Valor
Access	CaIssuers		http://pki-otu-lcp -ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate[81]

7.3.3 AC ORG

En este contexto, el contestador OCSP dispone de un Certificado emitido por la AC ORG y cuyo modelo se detalla a continuación.

7.3.3.1 Campos básicos

Campos		Valor
Version		2 (para la versión 3)
Serial number		Definido por la AC Técnica emisora
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN del ACT emisora
Validity		3 años
Subject	C	FR
	OI	0002 378901946
	OU	AC ORG
	O	Worldline
	SERIALNUMBER [71]	Número de serie único DN
	CN	Servicio OCSP PKI ORG
Subject Public Key Info		RSA 2048 bits

7.3.3.2 Extensions

Campos		Crítica	Valor
Authority Key Identifier		No	[RFC 5280] método[0]: identificador de clave pública de la AC emisora
Subject Key Identifier		No	[RFC 5280] método[1]: identificador de clave pública contenido en el Certificado
Key Usage		Si	Firma Digital
Basic Constraint	Certificate Authority	No	Falso
Certificate Policies	policyIdentifier	No	1.2.250.1.111.20.5.3
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Extended Key Usage		No	ocspSigning (1.3.6.1.5.5.7.3.9)
CRL Distribution Points		No	http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl [72]
Authority Information Access	ocsp	No	http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp [85]
	caIssuers		http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate [85]

[71]Según[RFC 3739], el campo SERIALNUMBER se utiliza para eliminar el riesgo de homonimia en los campos restantes del DN. Se construye de la siguiente manera:
SERIALNUMBER = número incrementado cada vez que se emite un certificado OCSP para la CA técnica emisora en cuestión.

[72] Esta URL se da sólo a título informativo. La URL auténtica es la que aparece en el Certificado.

8 Auditoría de cumplimiento y otras evaluaciones

8.1 Frecuencia y/o circunstancias de las evaluaciones

Worldline, como parte de la evaluación de este servicio de certificación, lleva a cabo una auditoría de certificación externa de la norma [ETSI 319 411-1] de las IGC presentada dentro de esta PC-DPC cada dos (2) años por una organización acreditada.

Además, Worldline lleva a cabo una auditoría de vigilancia (interna o externa) entre dos (2) auditorías externas de Certificación de la norma [ETSI 319 411-1].

8.2 Identidades / cualificaciones de los evaluadores

Se aplican todos los requisitos y prácticas descritos en la [PG].

8.3 Relaciones entre los evaluadores y las entidades evaluadas

Se aplican todos los requisitos y prácticas descritos en la [PG].

8.4 Temas cubiertos por las evaluaciones

Se aplican todos los requisitos y prácticas descritos en la [PG].

8.5 Medidas adoptadas en respuesta a las conclusiones de la evaluación

Se aplican todos los requisitos y prácticas descritos en la [PG].

8.6 Comunicación de resultados

Se aplican todos los requisitos y prácticas descritos en la [PG].

9 Otros asuntos comerciales y legales

9.1 Tarifas

Worldline no comercializa sus Certificados por sí sola, sino sólo a través de servicios de alto nivel.

9.1.1 Tarifas por la expedición o renovación de un Certificado

Esto se trata en el contexto del acuerdo de servicio de nivel superior entre Worldline y el Suscriptor.

9.1.2 Tarifas de acceso a los Certificados

Esto se trata en el contexto del acuerdo de servicio de nivel superior entre Worldline y el Suscriptor.

9.1.3 Tarifas de acceso a la información de estado y revocación de los Certificados

No se aplica.

9.1.4 Tarifas para otros servicios

No se aplica.

9.1.5 Política de reembolso

No se aplica.

9.2 Seguros

9.2.1 Cobertura de seguro

Se aplican todos los requisitos y prácticas descritos en la [PG].

9.2.2 Otros recursos

Se aplican todos los requisitos y prácticas descritos en la [PG].

9.2.3 Cobertura y garantía para las entidades usuarias

No se aplica.

9.3 Confidencialidad de los datos profesionales

9.3.1 Alcance de la información confidencial

Se aplican todos los requisitos y prácticas descritos en la [PG].

En particular, dentro del alcance de esta PC-DPC, la siguiente información se considera confidencial:

- la DTPC;
- las claves privadas de la AC;
- los datos de activación asociados a las claves privadas de la AC;
- todos los secretos de la IGC;
- los registros de eventos de los componentes de la IGC;
- los expedientes de registro de los titulares;
- los informes de auditoría.

9.3.2 Información fuera del ámbito de la información confidencial

Se aplican todos los requisitos y prácticas descritos en la [PG].

9.3.3 Responsabilidades en cuanto a la protección de la información confidencial

Se aplican todos los requisitos y prácticas descritos en la [PG].

También se aplican los requisitos y prácticas adicionales específicos que se definen a continuación.

9.3.3.1 Legislación aplicable

La Ley n° 2018-493 de 20 de junio de 2018, promulgada el 21 de junio de 2018, modificó la Ley de protección de datos para adaptar la legislación nacional al marco jurídico europeo.
Worldline procesa los datos personales de acuerdo con la legislación francesa en vigor en el territorio francés, que cumple con la vigente en el territorio europeo, en lo que respecta a la protección de datos personales. Worldline toma todas las medidas apropiadas y necesarias de acuerdo con estas regulaciones para asegurar que los datos personales que se requieren para almacenar a través de las IGC estén protegidos de cualquier compromiso, violación de la seguridad o pérdida de integridad que pueda tener un impacto en el servicio de confianza proporcionado y en los datos personales almacenados en el mismo.

Para ello, TSP MediaCert pone en marcha medidas de seguridad en los locales y sistemas de información para evitar que los ficheros almacenados sean distorsionados, dañados o accedidos por terceros no autorizados.

9.3.3.2 Consentimiento previo del Titular, de los representantes de la Organización y de los representantes del Suscriptor al tratamiento de sus datos por parte de la IGC

Al crear los archivos de registro, se requiere un conjunto de datos personales. Los Suscriptores o su representante los transmiten a la Autoridad de Registro.

[AC OTU][AC OTU LCP] Certificados de un solo uso

En el contexto de los Certificados de un solo uso, se recuerda que el Suscriptor se asegurará de obtener el consentimiento expreso de los futuros Titulares para el tratamiento y almacenamiento de sus datos por parte de la IGC, antes de transmitir sus datos personales, para el tratamiento de las solicitudes de creación de este tipo de Certificados.
A tal fin, el futuro Titular de Registro deberá aceptar antes de cualquier solicitud iniciada en su nombre por el Suscriptor que los datos personales que le conciernen, transmitidos por el Suscriptor a la Autoridad de Registro, sean procesados electrónicamente con el único propósito de:

- constituyen su identificación y permiten su autenticación para generar un Certificado en su nombre;
- ser capaz de proporcionarle los datos de activación de su clave privada;
- permitir acreditar la identidad indicada en el Certificado aportando la prueba necesaria, en su caso, conservando los elementos en el expediente de registro.

Además, estos justificantes podrán ser objeto, en su caso, de un control automatizado para comprobar la coherencia de los campos. En caso de que los controles sean negativos o infructuosos, los controles manuales serán realizados por la Organización con la que el Titular esté en contacto.

El consentimiento del futuro Titular del tratamiento para estos tratamientos, en el marco de la implementación de la firma electrónica, debe expresarse mediante una acción positiva por su parte, la cual debe ser informada con antelación de las consecuencias de su elección y poder disponer de los medios para ejercerla.

A este respecto, se especifica que cualquier oposición a la retención de datos personales impedirá la emisión de este tipo de Certificado. En efecto, al aceptar la disposición del Certificado para proceder a la firma electrónica, el Titular acepta que la AC a través de la AR, a petición de la AR conserve, los datos personales durante el tiempo necesario para cumplir los fines de las operaciones de tratamiento llevadas a cabo en el contexto de la entrega y gestión del Certificado de un solo uso. En efecto, la IGC debe poder cumplir las obligaciones a las que está sujeta en el marco de las auditorías que debe superar, justificar el cumplimiento del nivel o niveles de certificación elegidos, las funciones de identificación asignadas a la firma electrónica, las reglas de la técnica y las normas aplicables.

El Suscriptor se asegurará de que el Titular esté plenamente informado y de que el proveedor de servicios designado cumpla con las disposiciones legales aplicables en materia de protección de datos personales.

[AC ORG] Certificados de Organización

Como parte de la preparación del expediente de registro, el Suscriptor, a través de sus representantes, proporciona a la Autoridad de Registro un conjunto de datos personales necesarios para la preparación del expediente. Esta transmisión por parte del representante del Suscriptor se realiza con conocimiento de los fines de esta colección. A tal fin, los representantes del Suscriptor y los representantes de la Organización deberán aceptar que los datos personales que les conciernen puedan ser tratados electrónicamente con la única finalidad de:

- constituyen su identificación y, en el caso de que el Suscriptor y la Organización sean la misma entidad, permiten su autenticación, con el fin de generar un Certificado que contenga su información;

- apoyar la identidad, si la hubiere, contenida en el certificado y las facultades conferidas aportando las pruebas necesarias, en caso necesario, mediante la conservación de los elementos en el expediente de pruebas.

Por consiguiente, al aceptar representar al Suscriptor, los representantes del Suscriptor habrán aceptado previamente que sus datos personales puedan ser procesados y almacenados durante el tiempo que sea necesario para los fines de las operaciones de procesamiento llevadas a cabo en el contexto de la provisión y gestión de los Certificados de Organización.

9.3.3.3 Derechos del interesado a los datos

De conformidad con el artículo 39 de la Ley de protección de datos, modificada por la Ley nº 2018-493 de 20 de junio de 2018, y el artículo 14 de la RGPD, toda persona física que pueda acreditar su identidad tiene derecho a solicitar el acceso a sus datos personales en las condiciones previstas en estos artículos.

Cualquier persona física que acredite su identidad podrá solicitar la rectificación, actualización o supresión de sus datos personales.
En el caso de los Certificados de un solo uso, los datos personales utilizados para apoyar la identificación del Titular para la elaboración del Certificado con el que ha firmado sólo podrán rectificarse, bloquearse o borrarse una vez que se haya completado la finalidad para la que fueron recogidos dichos datos personales y se haya completado el tratamiento.
Lo mismo se aplica a los datos personales recogidos para la emisión de Certificados de Organización.
Los datos personales utilizados para identificar y autenticar al futuro titular del Certificado comunicados durante el proceso de firma electrónica o la constitución del fichero de registro permanecen en la historia de los rastros de la transacción y de la firma electrónica realizada hasta que se haya completado la finalidad para la que fueron recogidos los datos personales y el tratamiento realizado.
Lo mismo se aplica a los datos personales proporcionados al solicitar la creación de un Certificado de Organización.

Como resultado de las disposiciones anteriores, las personas que hayan dado su consentimiento previo al tratamiento de sus datos personales por parte de la IGC, tal como se establece en el presente documento, podrán, de conformidad con la ley, acceder y obtener una copia de toda la información que les concierna que obre en poder de la IGC.

Ninguno de los datos personales comunicados en el momento de la inscripción del Titular o en la preparación del expediente de inscripción de los Suscriptores y de las Organizaciones podrá ser utilizado por la IGC para fines distintos de los definidos en la PC-DPC.

El derecho de acceso puede ejercerse por escrito: por correo postal al punto de contacto de TSP MediaCert, en la dirección indicada en el capítulo 1.6.2 este documento o en el sitio web de TSP MediaCert (véase el capítulo 2.2), acompañado de una copia de un documento de identidad. Idealmente, por correo certificado con acuse de recibo.

9.3.3.4 Condiciones para la divulgación de información personal a las autoridades judiciales o administrativas

Worldline puede tener que poner los registros almacenados del registro de Titulares, Suscriptores y Organizaciones a disposición de terceros autorizados en procedimientos legales o auditorías para verificar la emisión de Certificados. La IGC cuenta con procedimientos seguros para permitir este acceso, que se rastrean por nombre y se almacenan.

9.4 Protección de datos de carácter personal

9.4.1 Política de protección de datos personales

Se aplican todos los requisitos y prácticas descritos en la [PG].

Con este fin, la Autoridad de Registro recoge y procesa los datos de identificación de los futuros Titulares de registro, Suscriptores o representantes, Organizaciones o representantes que figuran en los expedientes de registro (expediente de pruebas).

9.4.2 Datos personales

Los datos de registro del Titular o de las Personas Autorizadas, tal y como han sido proporcionados por el Suscriptor, son información considerada personal. El acceso a los datos personales se facilitará de conformidad con la [PG].

9.4.3 Información no personal

No se aplica.

9.4.4 Responsabilidad de la protección de datos personales

Se aplican todos los requisitos y prácticas descritos en la [PG].

9.4.5 Notificación y consentimiento para el uso de datos personales

De conformidad con la legislación vigente en Francia, los datos personales facilitados por los titulares a la IGC no se revelan ni se transfieren a terceros, salvo en los siguientes casos: consentimiento previo del Titular, decisión judicial u otra autorización legal.

9.4.6 Condiciones para la divulgación de información personal a las autoridades judiciales o administrativas

Se aplican todos los requisitos y prácticas descritos en la [PG].

9.4.7 Otras circunstancias para revelar información personal

No se aplica.

9.5 Derechos de propiedad intelectual e industrial

Se aplican todos los requisitos y prácticas descritos en la [PG].

9.6 Interpretaciones y garantías contractuales

Las obligaciones comunes a los componentes de la IGC son las siguientes:

- proteger y garantizar la integridad y confidencialidad de sus claves secretas y/o privadas;

- utilizar sus claves criptográficas (públicas, privadas o secretas) únicamente para los fines previstos en el momento de su expedición y con las herramientas especificadas en las condiciones establecidas en la PC-DPC de la AC y en los documentos relacionados (véase el capítulo 1.5);
- respetar y aplicar la parte de la [DTPC] de la que son responsables (esta parte debe ser comunicada al componente correspondiente);
- someterse a los controles de conformidad realizados por el equipo de auditoría autorizado por la AC (véase el capítulo 7.3.3);
- respetar los acuerdos o contratos que los vinculan entre ellos o con los titulares;
- documentar sus procedimientos operativos internos, implementar los recursos (técnicos y humanos) necesarios para llevar a cabo los servicios a los que se comprometen en condiciones que garanticen la calidad y la seguridad;
- tener prácticas no discriminatorias en sus políticas y procedimientos.

9.6.1 Autoridad de Certificación

La obligación de las Autoridades de Certificación es:

- asegurarse de que la Autoridad de Registro que actúa en nombre de la AC OTU cumple con la presente PC-DPC;
- publicar la información pública mencionada en el capítulo 2.2 este documento, en particular las Condiciones Generales de Suscripción [CGA][73] y las Condiciones Generales de Servicio [CGS], de forma sostenible y segura;
- poner sus servicios a disposición de cualquier Suscriptor que haya aceptado las Condiciones Generales de Suscripción [CGA];
- colaborar con los auditores durante los controles de cumplimiento y aplicar las medidas que se decidan con ellos tras los controles de cumplimiento.

9.6.2 Servicio de registro

La obligación de la AR es:

- cumplir con los procedimientos de registro descritos en esta PC-DPC.

9.6.3 Titulares de Certificados

Los beneficiarios de los Certificados están obligados a hacerlo:

- proteger los medios de acceso a las claves privadas y a los certificados;
- utilizar sus Certificados sólo para los usos previstos y definidos en la PC-DPC asociado;

[73] CGA : Por su acrónimo en francés « Conditions Générales de Abonnement » = Condiciones Generales de Suscripción

- revocar o solicitar la revocación de su certificado en caso de compromiso o sospecha de compromiso;
- revocar o solicitar la revocación de su certificado en caso de compromiso o sospecha de compromiso de los medios de acceso antes mencionados;
- verificar y cumplir con las obligaciones que les incumben descritas en este documento y en los Términos y Condiciones Generales de Servicios [CGS].

9.6.3.1 Suscriptor

Además de las obligaciones definidas en el capítulo 9.6.3, el Suscriptor tiene diferentes obligaciones dependiendo del tipo de Certificado, que se muestra a continuación.

[AC OTU][AC OTU LCP] Certificados de un solo uso

Para un Certificado de un solo uso, el Suscriptor de AC en línea está obligado a

- recoger y verificar o haber recogido y verificado bajo su responsabilidad la información de identidad proporcionada por el futuro Titular;
- comunicar al Titular sus obligaciones (véase el capítulo 9.6.3.2);
- informar al Titular del proceso de solicitud del Certificado y de las consecuencias de su uso en esta PC-DPC;
- transmitir, en su solicitud, los datos relativos a la identificación del futuro Titular, así como todos los consentimientos necesarios de este futuro Titular, tal como se definen en el capítulo 3.2.3.1 presente documento;
- constituir y firmar la solicitud de Certificado del futuro Titular;
- mantener el control exclusivo de sus recursos de autenticación ante la Autoridad de Registro;
- comunicar lo antes posible a la Autoridad de Registro cualquier acontecimiento que pueda afectar a la calidad de la identificación de sus futuros Titulares de registro;
- comunicar lo antes posible a la Autoridad de Registro cualquier acontecimiento que pueda afectar a la fiabilidad de sus medios de autenticación con esta última;
- a participar en prácticas no discriminatorias.

[AC ORG] Certificados de Organización

Para un Certificado de Organización, el Suscriptor de la AC está obligado a:

- completar el expediente de solicitud de creación de certificados proporcionando todos los elementos necesarios, los documentos justificativos y los poderes necesarios (véase el capítulo 4.1.2.2). La información y los documentos justificativos que se comuniquen a la Autoridad de Registro deberán ser exactos, sinceros y actualizados cuando se solicite la creación de un Certificado;

- informar a la Autoridad de Registro en caso de que los datos del Certificado dejen de ser válidos debido a un cambio en la Organización. A este respecto, el Suscriptor debe notificar a la AR sin demora, por carta certificada con acuse de recibo:
    - cualquier cambio en la identidad de la persona que actúe como representante o representante adjunto del Suscriptor, así como la fecha de entrada en vigor de dicho cambio, junto con los documentos justificativos;
    - cualquier cambio en la información proporcionada a la Autoridad de Registro, así como la fecha de entrada en vigor de dichos cambios.
- solicitar la revocación del Certificado en los casos enumerados en este documento. En este sentido, la modificación de la información contenida en el Certificado de Organización conlleva la revocación del Certificado y su sustitución a cargo de la Organización;
- comunicar lo antes posible a la Autoridad de Registro cualquier acontecimiento que pueda afectar a la fiabilidad de los medios de autenticación con esta última. A este respecto, los cambios (nombre, apellidos, dirección de correo electrónico) deben notificarse a la Autoridad de Registro;
- informar a la Autoridad de Registro si la Organización ya no existe. A este respecto, el Suscriptor deberá notificar sin demora al AR, por carta certificada con acuse de recibo, cualquier cambio (nombre, apellidos, dirección de correo electrónico, identificador de la Organización) que afecte a todos los Certificados de la Organización, acompañados de los documentos justificativos;
- informar a la autoridad de registro en caso de que se modifique la información relativa a la organización, no incluida en el Certificado de Organización y que no afecte a su validez. A este respecto, el Suscriptor debe notificar a la AR lo antes posible, por simple carta, los cambios en la información;
- tener prácticas no discriminatorias.

En caso de que el Suscriptor recurra a un proveedor de servicios técnicos, es su responsabilidad asegurarse de que éste cumple con estas obligaciones, especialmente porque este proveedor de servicios puede tener secretos específicos del Suscriptor: claves privadas correspondientes a Certificados de autenticación y firma de mensajes. Por lo tanto, es responsabilidad del Suscriptor asegurarse de que las medidas para proteger el acceso a estos secretos se apliquen correctamente.

9.6.3.2 Titulares

Además de las obligaciones definidas en el capítulo 9.6.3, el futuro Titular tiene la obligación de proporcionar información y documentos justificativos, solicitados por el Suscriptor, que certifica como exactos y actualizados al solicitar el Certificado.

Las obligaciones del futuro Titular también se definen en el contrato celebrado con su representante, en lo sucesivo denominado "el Suscriptor".

9.6.4 Usuarios de certificados

Los usuarios de Certificados deben:

- verificar y cumplir con las obligaciones que les incumben en este documento y en los Términos y Condiciones Generales de Servicios [CGS]. Estas obligaciones serán para los

Certificados de un solo uso descritos por el Suscriptor en el contrato que lo vincula al futuro Titular (véase el capítulo 9.6.3.1). El presente contrato establece el funcionamiento de una firma en forma electrónica, las implicaciones de esta elección, los procedimientos para llevarla a cabo con los consentimientos necesarios de acuerdo con lo establecido en su Contrato de Suscripción;

- verificar y respetar el uso para el que se ha expedido un Certificado;
- para cada Certificado de la Cadena de Certificación, desde el Certificado del suscriptor hasta la AC raíz, verificar la firma digital de la AC emisora del Certificado correspondiente y comprobar la validez de este Certificado (fechas de validez, estado de revocación).

9.6.5 Otros participantes

No se aplica.

9.7 Límite de garantía

Las Autoridades de Certificación en línea se comprometen a expedir Certificados de conformidad con el presente documento, así como con el estado actual de la técnica y la tecnología.

TSP MediaCert garantiza a través de sus servicios:

- la autenticación del Suscriptor con su Certificado por la Autoridad de Registro;
- la generación de Certificados de acuerdo con la solicitud del Suscriptor, previamente autenticado y verificado;
- el suministro de información sobre la situación de los Certificados expedidos, a petición del Suscriptor, por las Autoridades de Certificación de conformidad con el presente documento;
- el control exclusivo de la clave privada del Certificado por parte del Dispositivo Portador del Certificado y la destrucción de la misma clave tras una única sesión de uso en el caso de un Certificado de un solo uso.

No se ofrecen otras garantías.

9.8 Limitación de responsabilidad

TSP MediaCert sólo puede ser considerada responsable en el caso de que se demuestre el incumplimiento de sus obligaciones.

La TSP MediaCert no podrá ser considerada responsable en el caso de un fallo en el alcance de una entidad Suscriptora, en particular en el caso de:

- uso de un Certificado caducado;
- uso de un Certificado revocado;
- uso de un Certificado en una aplicación distinta de las descritas en el capítulo 4.5 esta PC-DPC.

En general, TSP MediaCert no es responsable de los documentos e información proporcionados por el Suscriptor y no garantiza su exactitud ni las consecuencias de hechos dañinos, acciones, negligencia u omisiones del Suscriptor, su representante o el Titular.

El Suscriptor se compromete a no comprometerse en nombre y representación de TSP MediaCert, al que no podrá sustituir en ningún caso.

9.9 Indemnizaciones

La emisión de Certificados por parte de las AC afectadas por este documento se lleva a cabo como parte de servicios de nivel superior como la suscripción electrónica.

El contrato marco firmado entre el cliente y Worldline, o su agente debidamente autorizado, especifica las condiciones para la compensación en caso de daño. En ausencia de un contrato marco, se aplicarán los Términos y Condiciones Generales de Venta de Worldline.

9.10 Duración y terminación anticipada de la validez de la PC

9.10.1 Período de validez

La PC-DPC se hace efectivo una vez validado por la entidad responsable de este documento (ver capítulo 1.6.1). Deberá permanecer en vigor al menos hasta el final de la vigencia del último Certificado expedido en virtud de la presente PC-DPC.

9.10.2 Terminación anticipada

Esta PC-DPC permanece en uso hasta que se libera una nueva versión.

9.10.3 Efectos del fin de validez y de las demás cláusulas aplicables

A pesar de la sustitución de esta PC-DPC por una nueva versión, los últimos Certificados expedidos en el momento de su validez aplicarán este documento a dichos Certificados y a los distintos agentes hasta la expiración de los Certificados en cuestión.

9.11 Notificaciones individuales y comunicaciones entre participantes

TSP MediaCert informará a sus suscriptores por correo electrónico a más tardar un (1) mes antes de la publicación de la nueva versión de este documento, en caso de cualquier cambio que afecte a esta PC-DPC.

El Suscriptor también será informado de la implementación efectiva de la nueva versión de la PC-DPC a más tardar un (1) mes después de su publicación a través de un comunicado firmado por correo electrónico.
Además, el Suscriptor será informado de cualquier cambio en las CGS, CGA[74] o CGV a través de un mensaje de correo electrónico.

Todos los componentes y actores de las AC son informados, a través de un comunicado interno, de las modificaciones introducidas en este documento y de los posibles impactos que puedan derivarse de las mismas.

[74] CGA : Por su acrónimo en francés « Conditions Générales de Abonnement » = Condiciones Generales de Suscripción

En este documento no se exige a los Suscriptores que validen los cambios. En efecto, la utilización de los servicios después de la notificación de los cambios realizados implica la aceptación automática de estos cambios.

9.12 Enmiendas a la PC

9.12.1 Procedimientos de modificación

Se aplican todos los requisitos y prácticas descritos en la [PG].

9.12.2 Mecanismo y período de información para las modificaciones

En el caso de un cambio que requiera la modificación de esta PC-DPC, en el capítulo 9.11 se proporciona información sobre el mecanismo y el período de información para las enmiendas.

9.12.3 Circunstancias en las que debe modificarse el OID

Se aplican todos los requisitos y prácticas descritos en la [PG].

9.13 Disposiciones relativas a la resolución de conflictos

Se aplican todos los requisitos y prácticas descritos en la [PG].

El contrato marco firmado entre el Suscriptor y Worldline, o su representante debidamente autorizado, especifica las disposiciones relativas a la resolución de disputas. En ausencia de un contrato marco, se aplicarán los Términos y Condiciones Generales de Venta de Worldline.

El contacto autorizado para cualquier comentario, solicitud de información adicional, quejas o archivos de disputa relacionados con esta PC-DCP se define en el capítulo 1.6.2. Todas las solicitudes deberán presentarse por correo electrónico con acuse de recibo o por correo certificado con acuse de recibo.

9.14 Jurisdicciones competentes

Se aplican todos los requisitos y prácticas descritos en la [PG].

El contrato marco firmado entre el cliente y Worldline, o su representante debidamente autorizado, especifica esta disposición. En ausencia de un contrato marco, se aplicarán los Términos y Condiciones Generales de Venta de Worldline.

9.15 Cumplimiento de las leyes y reglamentos

Se aplican todos los requisitos y prácticas descritos en la [PG].

9.16 Disposiciones diversas

9.16.1 Acuerdo global

No se aplica.

9.16.2 Transferencia de actividades

No se aplica.

9.16.3 Consecuencias de una cláusula inválida

No se aplica.

9.16.4 Solicitud y renuncia

No se aplica.

9.16.5 Fuerza mayor

Se aplican todos los requisitos y prácticas descritos en la [PG].

El contrato marco firmado entre el cliente y Worldline, o su representante debidamente autorizado, especifica esta disposición. En ausencia de un contrato marco, se aplicarán los Términos y Condiciones Generales de Venta de Worldline.

9.17 Otras provisiones

9.17.1 Independencia de las partes y no discriminación

Se aplican todos los requisitos y prácticas descritos en la [PG].

9.17.2 Análisis de riesgos

Se aplican todos los requisitos y prácticas descritos en la [PG].

9.17.3 Documentos contractuales

En caso de contradicción entre los artículos de las Condiciones Generales de Suscripción [CGA][75] y las disposiciones del Acuerdo de Servicios de Nivel Superior (Acuerdo Marco), prevalecerán las cláusulas de las Condiciones Generales de Suscripción [CGA] basadas en la Política de Certificación aplicable - Declaración de Prácticas de Certificación.

[75] CGA : Por su acrónimo en francés « Conditions Générales de Abonnement » = Condiciones Generales de Suscripción