

Texto divulgativo – PDS para
certificados corporativos de **emisor**

logal**ty**

Información general

Control documental

Versión:	1.0
Fecha edición:	23/10/2018
Fichero:	LGT_PDS_corporativo v1r0.docx
Formato:	Office 2018
Autores:	AC/FAD

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Astrea Fecha: 18/02/2018	Nombre: DG Fecha: 23/10/2018	Nombre: LOGALTY Fecha: 23/10/2018

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
0.1	Todo	Versión inicial	Astrea	18/02/2018
1.0	1.1.1	Cambio SME	DG	23/10/2018

Índice

INFORMACIÓN GENERAL	2
CONTROL DOCUMENTAL	2
ESTADO FORMAL	2
CONTROL DE VERSIONES	2
ÍNDICE	3
1 TEXTOS DE DIVULGACIÓN	4
CERTIFICADOS CORPORATIVOS	4
1.1.1 Información de contacto.....	4
1.1.2 Tipos y finalidades de los certificados.....	5
1.1.3 Límites de uso del certificado.....	14
1.1.4 Obligaciones de los suscriptores.....	16
1.1.5 Obligaciones de los firmantes.....	17
1.1.6 Obligaciones de los verificadores.....	18
1.1.7 Obligaciones de LOGALTY.....	21
1.1.8 Garantías limitadas y rechazo de garantías	22
1.1.9 Acuerdos aplicables y DPC.....	24
1.1.10 Reglas de confianza para firmas longevas	24
1.1.11 Política de intimidad.....	25
1.1.12 Política de privacidad	25
1.1.13 Política de reintegro	26
1.1.14 Ley aplicable, jurisdicción competente y régimen de reclamaciones y disputas	26
1.1.15 Acreditaciones y sellos de calidad	26
1.1.16 Vinculación con la lista de prestadores	27
1.1.17 Divisibilidad de las cláusulas, supervivencia, acuerdo íntegro y notificación.....	27

1 Textos de divulgación

Certificados Corporativos

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

1.1.1 Información de contacto

1.1.1.1 Organización responsable

La Entidad de Certificación LOGALTY, en lo sucesivo “LOGALTY”, es una iniciativa de:

LOGALTY SERVICIOS DE TERCERO DE CONFIANZA SL

AVENIDA DE LA INDUSTRIA, 49
28108 ALCOBENDAS, MADRID (ESPAÑA)

PHONE: +34 915 145 800

FAX: +34 917 913 085

1.1.1.1.1. Contacto

Para cualquier consulta, diríjense a:

LOGALTY SERVICIOS DE TERCERO DE CONFIANZA SL

AVENIDA DE LA INDUSTRIA, 49
28108 ALCOBENDAS, MADRID (ESPAÑA)

PHONE: +34 915 145 800

FAX: +34 917 913 085

1.1.1.1.2. Contacto para procesos de revocación

Para cualquier consulta, diríjense a:

LOGALTY SERVICIOS DE TERCERO DE CONFIANZA SL**(LOGALTY TRUST SERVICES)**

AVENIDA DE LA INDUSTRIA, 49

28108 ALCOBENDAS, MADRID (ESPAÑA)

EMAIL: revoke.ca@logalty.com

1.1.2 Tipos y finalidades de los certificados

1.1.2.1 Certificado Persona Física vinculada a empresa/organización emitido en DCCF-HSM

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.2.1
De acuerdo con la política QCP-n-qscd	0.4.0.194112.1.2

Los certificados de persona física vinculada a empresa/organización emitidos en DCCF-HSM, son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Los certificados de persona física vinculada a empresa/organización emitidos en DCCF-HSM, funcionan con dispositivo cualificado de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados son gestionados de forma centralizada.

Estos certificados garantizan la identidad del firmante y su vinculación con el suscriptor del servicio de certificación, y permiten la generación de la “**firma electrónica cualificada**”; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido

generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

- a) Firma de correo electrónico seguro.
- b) Otras aplicaciones de firma digital.

Estos certificados no permiten el cifrado de documentos, contenidos ni mensajes de datos. En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

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

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

1.1.2.2 Certificado Persona Física vinculada a empresa/organización en software gestión centralizada

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.2.2
De acuerdo con la política QCP-n	0.4.0.194112.1.0

Los certificados de persona física vinculada a empresa/organización en software gestión centralizada, son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados no funcionan con dispositivo seguro de creación de firma.

Estos certificados son gestionados de forma centralizada.

Estos certificados garantizan la identidad del firmante y su vinculación con el suscriptor del servicio de certificación, y permiten la generación de la “**firma electrónica avanzada**” basada en certificado electrónico cualificado.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

- a) Firma de correo electrónico seguro.
- b) Otras aplicaciones de firma digital.

Estos certificados no permiten el cifrado de documentos, contenidos ni mensajes de datos. En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

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

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

- Firma digital (para realizar la función de autenticación)
- Compromiso con el contenido (para realizar la función de firma electrónica)

b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:

- QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

c) En el campo “Qualified Certificate Statements” **no aparece** la declaración QcSSCD (0.4.0.1862.1.4), ya que este certificado no se usa con un dispositivo cualificado.

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

1.1.2.3 Certificado de Persona Física vinculada a empresa/organización en software distribuido

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.2.3
De acuerdo con la política QCP-n	0.4.0.194112.1.0

Los certificado de persona física vinculada a empresa/organización en software distribuido, son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados no funcionan con dispositivo seguro de creación de firma.

Estos certificados son gestionados de forma distribuida sin la participación de una herramienta de gestión centralizada.

Estos certificados garantizan la identidad del firmante y su vinculación con el suscriptor del servicio de certificación, y permiten la generación de la “**firma electrónica avanzada**” basada en certificado electrónico cualificado.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

- a) Firma de correo electrónico seguro.
- b) Otras aplicaciones de firma digital.

Estos certificados no permiten el cifrado de documentos, contenidos ni mensajes de datos. En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

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

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

1.1.1.2.4 Certificado Sello electrónico de persona jurídica emitido en DCCF-HSM

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.3.1
De acuerdo con la política QCP-I-qscd	0.4.0.194112.1.3

Los certificados de sello electrónico de persona jurídica emitido en DCCF-HSM, son certificados cualificados de acuerdo con el artículo 38 y con el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

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

Estos certificados son gestionados de forma centralizada.

Estos certificados garantizan la identidad del suscriptor del servicio de certificación, y permiten la generación del “sello electrónico cualificado”; es decir, el sello electrónico avanzado que se basa en un certificado cualificado y que ha sido generado empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 35.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, disfrutará de la presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado.

En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

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

- a) El campo “key usage” tiene activadas, y por tanto permite realizar, las siguientes funciones:
- Firma digital (para realizar la función de autenticación)
 - Compromiso con el contenido (para realizar la función de firma electrónica)

b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:

- QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
- QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo cualificado de creación de firma.

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

1.1.2.5 Certificado Sello electrónico de persona jurídica en software gestión centralizada

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.3.2
De acuerdo con la política QCP-I-qscd	0.4.0.194112.1.1

Los certificados de sello electrónico de persona jurídica en software gestión centralizada , son certificados cualificados de acuerdo con el artículo 38 y con el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados **no funcionan** con dispositivo cualificado de creación de firma.

Estos certificados son gestionados de forma centralizada.

En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

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

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

1.1.2.6 Certificado de Sello electrónico de Persona Jurídica en software gestión distribuido

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.3.3
De acuerdo con la política QCP-I-qscd	0.4.0.194112.1.1

Los certificados de sello electrónico de persona jurídica en software gestión distribuido distribuidos de sello electrónico de persona jurídica, son certificados cualificados de acuerdo con el artículo 38 y con el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados **no funcionan** con dispositivo cualificado de creación de firma.

Estos certificados son gestionados de forma distribuida sin la participación de una herramienta de gestión centralizada.

En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

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

- a) El campo “key usage” tiene activadas, y por tanto permite realizar, las siguientes funciones:
 - Firma digital (para realizar la función de autenticación)
 - Compromiso con el contenido (para realizar la función de firma electrónica)

- b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
 - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

- c) En el campo “Qualified Certificate Statements” **no aparece** la declaración QcSSCD (0.4.0.1862.1.4), ya que este certificado no se usa con un dispositivo cualificado.

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

1.1.2.7 Certificado de Autenticación Web EV

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.4.1
De acuerdo con la política QCP-w	0.4.0.194112.1.4
De acuerdo con CAB FORUM – SSL EV	2.23.140.1.1

Los certificados de autenticación web EV, son certificados cualificados de acuerdo con el artículo 45 y con el Anexo IV del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten a direcciones web para la identificación y el establecimiento de canales seguros entre el navegador de un usuario (verificador) y el servidor web del titular de este certificado. Cumple los requisitos del Guidelines for Issuance and Management of extended validation certificates del CA/BROWSER FORUM (<http://www.cabforum.org>).

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

- a) El campo “key usage” tiene activadas, y por tanto permite realizar, las siguientes funciones:
 - a. Digital Signature (para la función de autenticación)
 - b. Key Encipherment (para la gestión y transporte de claves)

- b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
 - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

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

1.1.2.7.1 Entidad de Certificación emisora

Los certificados indicados son emitidos por LOGALTY, identificada mediante los datos indicados anteriormente.

1.1.3 Límites de uso del certificado

1.1.3.1 Límites de uso dirigidos a los firmantes

El firmante ha de utilizar el servicio de certificación de los certificados prestado por LOGALTY exclusivamente para los usos autorizados en el contrato firmado entre LOGALTY y el SUSCRIPTOR, y que se reproducen posteriormente (sección “obligaciones de los firmantes”).

Asimismo, el firmante se obliga a utilizar el servicio de certificación digital de acuerdo con las instrucciones, manuales o procedimientos suministrados por LOGALTY.

El firmante ha de cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas que emplee.

El firmante no puede adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de certificación digital de LOGALTY, sin previo permiso expreso.

1.1.3.2 Límites de uso dirigidos a los verificadores

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

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

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

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, visibles en el web de LOGALTY (<https://www.logalty.es/certificateauthority/>).

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

LOGALTY no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de LOGALTY emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en este texto de divulgación, o en los contratos con los suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

1.1.4 Obligaciones de los suscriptores

1.1.4.1 Generación de claves

El suscriptor autoriza a LOGALTY a generar las claves, privada y pública, para la identificación y la firma electrónica de los firmantes, y solicita en su nombre la emisión del certificado.

1.1.4.2 Solicitud de certificados

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

1.1.4.3 Obligaciones de información

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

El suscriptor tiene que informar inmediatamente a LOGALTY:

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

1.1.4.4 Obligaciones de custodia

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

1.1.5 Obligaciones de los firmantes

1.1.5.1 Obligaciones de custodia

El firmante se obliga a custodiar el código de identificación personal o cualquier soporte técnico entregado por LOGALTY, las claves privadas y, si fuese necesario, las especificaciones propiedad de LOGALTY que le sean suministradas. El firmante se obliga a custodiar el código de identificación personal (PIN).

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

1.1.5.2 Obligaciones de uso correcto

El firmante tiene que utilizar el servicio de certificación de certificados prestado por LOGALTY, exclusivamente para los usos autorizados en la DPC y en cualquier otra instrucción, manual o procedimiento suministrado al suscriptor.

El firmante tiene que cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas empleadas.

El firmante no podrá adoptar medidas de inspección, alteración o descompilación de los servicios de certificación digital prestados.

El firmante reconocerá:

- a) Que cuando utilice cualquier certificado, y mientras el certificado no haya expirado ni haya sido suspendido o haya sido revocado, habrá aceptado dicho certificado y estará operativo.

- b) Que no actúa como entidad de certificación y, por lo tanto, se obliga a no utilizar las claves privadas correspondientes a las claves públicas contenidas en los certificados con el propósito de firmar certificado alguno.
- c) Que en caso de quedar comprometida la clave privada, su uso queda inmediata y permanentemente suspendido.

1.1.5.3 Transacciones prohibidas

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

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

1.1.6 Obligaciones de los verificadores

1.1.6.1 Decisión informada

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

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

1.1.6.2 Requisitos de verificación de la firma electrónica

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

- Es necesario utilizar el software apropiado para la verificación de una firma digital con los algoritmos y longitudes de claves autorizados en el certificado y/o ejecutar cualquier otra operación criptográfica, y establecer la cadena de certificados en que se basa la firma electrónica a verificar, ya que la firma electrónica se verifica utilizando esta cadena de certificados.

- Es necesario asegurar que la cadena de certificados identificada es la más adecuada para la firma electrónica que se verifica, ya que una firma electrónica puede basarse en más de una cadena de certificados, y es decisión del verificador asegurarse el uso de la cadena más adecuada para verificarla.

- Es necesario comprobar el estado de revocación de los certificados de la cadena con la información suministrada al Registro de LOGALTY (con LRCs, por ejemplo) para determinar la validez de todos los certificados de la cadena de certificados, ya que únicamente puede considerarse correctamente verificada una firma electrónica si todos y cada uno de los certificados de la cadena son correctos y se encuentran vigentes.

- Es necesario asegurar que todos los certificados de la cadena autorizan el uso de la clave privada por el suscriptor del certificado y el firmante, ya que existe la posibilidad de que alguno de los certificados incluya límites de uso que impidan confiar en la firma electrónica que se verifica. Cada certificado de la cadena dispone de un indicador que hace referencia a las condiciones de uso aplicables, para su revisión por los verificadores.

- Es necesario verificar técnicamente la firma de todos los certificados de la cadena antes de confiar en el certificado utilizado por el firmante.

1.1.6.3 Confianza en un certificado no verificado

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

1.1.6.4 Efecto de la verificación

En virtud de la correcta verificación de los certificados, de conformidad con este texto divulgativo, el verificador puede confiar en la identificación y, en su caso, clave pública del firmante, dentro de las limitaciones de uso correspondientes, para generar mensajes cifrados.

1.1.6.5 Uso correcto y actividades prohibidas

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

El verificador se obliga a no inspeccionar, interferir o realizar ingeniería inversa de la implantación técnica de los servicios públicos de certificación de LOGALTY, sin previo consentimiento escrito.

Adicionalmente, el verificador se obliga a no comprometer intencionadamente la seguridad de los servicios públicos de certificación de LOGALTY.

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

1.1.6.6 Cláusula de indemnidad

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

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.
- Falta de comprobación de la totalidad de medidas de aseguramiento prescritas en la DCP o resto de normas de aplicación.

LOGALTY no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

1.1.7 Obligaciones de LOGALTY

1.1.7.1 En relación a la prestación del servicio de certificación digital

LOGALTY se obliga a:

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

1.1.7.2 En relación a las comprobaciones del registro

LOGALTY se obliga a la emisión de certificados en base a los datos suministrados por el suscriptor, por lo cual podrá realizar las comprobaciones que considere oportunas respecto de la identidad y otras informaciones personales y complementarias de los suscriptores y, cuando resulte procedente, de los firmantes.

Estas comprobaciones podrán incluir la justificación documental aportada por el firmante por medio del suscriptor, si LOGALTY lo considera necesario, y cualquier otro documento e información relevantes facilitados por el suscriptor y/o el firmante.

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

LOGALTY se reserva el derecho a no emitir el certificado, cuando considere que la justificación documental resulte insuficiente para la correcta identificación y autenticación del suscriptor y/o del firmante.

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

1.1.7.3 Periodos de conservación

LOGALTY archiva los registros correspondientes a las solicitudes de emisión y revocación de certificados durante al menos 15 años.

LOGALTY almacena la información de los logs durante un periodo de entre 1 y 15 años, en función del tipo de información registrada.

1.1.8 Garantías limitadas y rechazo de garantías

1.1.8.1 Garantía de LOGALTY por los servicios de certificación digital

LOGALTY garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Entidad de Certificación.

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

LOGALTY garantiza al tercero que confía en el certificado:

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

Adicionalmente, LOGALTY garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado reconocido/cualificado, de acuerdo con el anexo I del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, persona física identificada en el certificado, se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la Entidad de Certificación, con los límites que se establezcan. En ningún caso LOGALTY responderá por caso fortuito y en caso de fuerza mayor.

1.1.8.2 Exclusión de la garantía

LOGALTY rechaza toda otra garantía diferente a la anterior que no sea legalmente exigible.

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

1.1.9 Acuerdos aplicables y DPC

1.1.9.1 Acuerdos aplicables

Los acuerdos aplicables a los certificados son los siguientes:

- Contrato de servicios de certificación, que regula la relación entre LOGALTY y la empresa suscriptora de los certificados.
- Condiciones generales del servicio incorporadas en el texto de divulgación del certificado o PDS.
- DPC, que regulan la emisión y utilización de los certificados.

1.1.9.2 DPC

Los servicios de certificación de LOGALTY se regulan técnicamente y operativamente por la DPC de LOGALTY, por sus actualizaciones posteriores, así como por documentación complementaria.

La DPC y la documentación de operaciones se modifica periódicamente en el Registro y se puede consultar en la página de Internet: <https://www.logalty.es/certificateauthority/>

1.1.10 Reglas de confianza para firmas longevas

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

LOGALTY recomienda, para la fiabilidad de la firma electrónica de un documento a lo largo del tiempo, el uso de los estándares indicados en el apartado 7.3 (reglas de confianza para firmas longevas) de la Guía de Aplicación de la Norma Técnica de Interoperabilidad "Política de Firma y Sello Electrónicos y de Certificados de la Administración"¹.

Las consideraciones generales para las reglas de confianza de firmas longevas se recogen en el subapartado IV.3 de la NTI de Política de Firma y Sello Electrónicos y de Certificados de la Administración².

1.1.11 Política de intimidad

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

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

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

LOGALTY no cede a ninguna persona los datos entregados específicamente para la prestación del servicio de certificación.

1.1.12 Política de privacidad

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

¹ 2ª edición electrónica, de mayo de 2017.

² Entrada en vigor el 4 de noviembre de 2016.

Asimismo, se contempla que la documentación justificativa de la aprobación de la solicitud debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante el plazo de 15 años desde la expiración del certificado, incluso todo en caso de pérdida anticipada de vigencia por revocación.

1.1.13 Política de reintegro

LOGALTY no reintegrará el coste del servicio de certificación en ningún caso.

1.1.14 Ley aplicable, jurisdicción competente y régimen de reclamaciones y disputas

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

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

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

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

1.1.15 Acreditaciones y sellos de calidad

LOGALTY se encuentra incluida³ en la lista de prestadores de confianza (TSL) española <https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf>

Asimismo, está registrada como prestador de servicios electrónicos de confianza **no cualificados y otros servicios**, en el Ministerio de Energía, Turismo y Agenda Digital, respecto de los siguientes servicios:

³ Inclusión pendiente de la evaluación de conformidad y la conformidad del supervisor a fecha de creación de este documento.

- Servicio no cualificado de entrega electrónica certificada
 - Comunicación electrónica certificada
 - Notificación electrónica certificada
- Servicio no cualificado de conservación de firmas electrónicas
 - Custodia adicional de prueba electrónica
- Otros servicios
 - Contratación Electrónica certificada
 - Publicación electrónica certificada

Servicios visibles desde el web:

<https://sedeaplicaciones.minetur.gob.es/Prestadores/Prestador.aspx>

De acuerdo con lo indicado en el Reglamento UE 910/2014, LOGALTY realizará auditorías de conformidad cada 2 años.

1.1.16 Vinculación con la lista de prestadores

<http://www.minetur.gob.es/telecomunicaciones/es-es/servicios/firmaelectronica/paginas/prestadores.aspx>

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

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

Los requisitos contenidos en las secciones 9.6 (Obligaciones), 9.8 (responsabilidad), 8 (Auditoría de conformidad) y 9.3 (Confidencialidad) de la Declaración de Prácticas de Certificación de LOGALTY continuarán vigentes tras la terminación del servicio.

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