

Texto de Divulgación (PDS) de los certificados emitidos para las Administraciones Públicas



Índice

1.1.	CONTROL DOCUMENTAL	4
1.2.	CONTROL DE VERSIONES	4
2.	INFORMACIÓN	7
1.1.	ORGANIZACIÓN RESPONSABLE	7
1.2.	CONTACTO	7
1.3.	CONTACTO PARA PROCESOS DE REVOCACIÓN	7
3.	TIPO Y FINALIDAD DEL CERTIFICADO	8
3.1.	CERTIFICADOS CUALIFICADOS DE EMPLEADO PÚBLICO	8
3.2.	CERTIFICADOS DE EMPLEADO PÚBLICO CON PSEUDÓNIMO	8
3.3.	CERTIFICADOS EN TARJETA	8
3.4.	CERTIFICADOS EN LA NUBE	9
3.5.	CERTIFICADOS PARA AUTENTICACIÓN	9
3.6.	CERTIFICADOS PARA FIRMA AVANZADA	9
3.7.	CERTIFICADOS PARA FIRMA CUALIFICADA	9
3.8.	CERTIFICADOS CUALIFICADOS DE SELLO ELECTRÓNICO	9
3.9.	CERTIFICADOS DE SELLO AVANZADO	10
3.10.	TIPOS DE CERTIFICADOS	10
3.11.	ENTIDAD DE CERTIFICACIÓN EMISORA	11
3.12.	VALIDACIÓN DE LOS CERTIFICADOS	11
4.	LÍMITES DE USO DEL CERTIFICADO	13
4.1.	LÍMITES DE USO DIRIGIDOS A LOS FIRMANTES	13
4.2.	LÍMITES DE USO DIRIGIDOS A LOS VERIFICADORES	13
5.	OBLIGACIONES DE LOS SUSCRIPTORES	15
5.1.	GENERACIÓN DE CLAVES	15
5.2.	SOLICITUD DE CERTIFICADOS	15
5.3.	VERACIDAD DE LA INFORMACIÓN	15
5.4.	OBLIGACIONES DE CUSTODIA	16
6.	OBLIGACIONES DE LOS FIRMANTES Y CREADORES DE SELLOS	17
6.1.	OBLIGACIONES DE CUSTODIA	17
6.2.	OBLIGACIONES DE USO CORRECTO	17
6.3.	TRANSACCIONES PROHIBIDAS	18
7.	OBLIGACIONES DE LOS VERIFICADORES	19
7.1.	DECISIÓN INFORMADA	19
7.2.	REQUISITOS DE VERIFICACIÓN DE LA FIRMA	19
7.3.	CONFIANZA EN UN CERTIFICADO NO VERIFICADO	20

7.4.	EFFECTO DE LA VERIFICACIÓN	20
7.5.	USO CORRECTO Y ACTIVIDADES PROHIBIDAS	20
7.6.	CLÁUSULA DE INDEMNIDAD	21
8.	OBLIGACIONES DE ESFIRMA	22
8.1.	EN RELACIÓN CON LA PRESTACIÓN DE CERTIFICACIÓN DIGITAL	22
8.2.	EN RELACIÓN CON LAS COMPROBACIONES DEL REGISTRO	22
8.3.	PERÍODOS DE CONSERVACIÓN	23
9.	GARANTÍAS LIMITADAS Y RECHAZO DE GARANTÍAS	24
9.1.	GARANTÍA DE ESFIRMA POR LOS SERVICIOS DE CERTIFICACIÓN DIGITAL	24
9.2.	EXCLUSIÓN DE LA GARANTÍA	25
10.	ACUERDOS APLICABLES Y DPC	27
10.1.	ACUERDOS APLICABLES	27
10.2.	DPC	27
11.	POLÍTICA DE INTIMIDAD	28
12.	POLÍTICA DE PRIVACIDAD	29
13.	POLÍTICA DE REINTEGRO	30
14.	LEY APLICABLE, JURISDICCIÓN COMPETENTE Y RÉGIMEN DE RECLAMACIONES Y DISPUTAS	31
14.1.	ACREDITACIONES Y SELLOS DE CALIDAD	31
14.2.	VINCULACIÓN CON LA LISTA DE PRESTADORES	31
14.3.	DIVISIBILIDAD DE LAS CLÁUSULAS, SUPERVIVENCIA, ACUERDO ÍNTEGRO Y NOTIFICACIÓN	32

TEXTO DIVULGATIVO - PDS

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

Este documento sigue la estructura definida en el Anexo A de la norma ETSI EN 319 411-1, de acuerdo con las indicaciones del apartado 4.3.4 de la norma ETSI EN 319 412-5.

1.1. Control documental

Clasificación de seguridad	PÚBLICO
Versión	2.2

1.2. Control de versiones

Versión	Cambios	Descripción	Autor	Fecha
1.0	Original	Creación documento	esFIRMA	28/04/2016
1.4		Subsanaciones	esFIRMA	07/06/2017
1.5		Cambio denominación y referencia a normativas	esFIRMA	06/11/2017
2.0		Inclusión de todos los certificados referentes a las AAPP españolas	esFIRMA	03/06/2020
2.1		Revisión Ley 6/2020	esFIRMA	08/04/2021

2.2	(1.3)	Se añade referencia a web de esFIRMA.	esFIRMA	21/04/2023
-----	-------	---------------------------------------	---------	------------

2. Información

2.1. Organización responsable

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

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)
CALLE BARI 39 (EDIF. BINARY BUILDING)
50197 - ZARAGOZA
(+34) 976300110

2.2. Contacto

Para cualquier consulta, diríjense a:

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)
CALLE BARI 39 (EDIF. BINARY BUILDING)
50197 - ZARAGOZA
(+34) 976300110

2.3. Contacto para procesos de revocación

El proceso para solicitar la revocación de un certificado se puede consultar en www.esfirma.com. Para cualquier otra consulta al respecto, diríjense a:

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)
CALLE BARI 39 (EDIF. BINARY BUILDING)
50197 - ZARAGOZA
(+34) 976300110

3. Tipo y finalidad del certificado

3.1. Certificados cualificados de empleado público

Estos certificados son 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 permiten identificar a sus titulares como personal al servicio de la Administración Pública, vinculándolos con ésta, siguiendo los requisitos establecidos en el artículo 43 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para la firma electrónica del personal al servicio de las Administraciones Públicas.

3.2. Certificados de empleado público con pseudónimo

Estos certificados permiten identificar a sus titulares como personal al servicio de la Administración Pública, vinculándolos con ésta, según permite el artículo 43.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para la firma electrónica del personal al servicio de las Administraciones Públicas, personal el cual, por razones de seguridad pública, sólo se identificará con el número de identificación profesional u otro pseudónimo de empleado público, según lo indicado en el Anexo I, apartado c) del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, y el artículo 6.1.a) de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

3.3. Certificados en tarjeta

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

3.4. Certificados en la nube

Estos certificados son gestionados de forma centralizada.

3.5. Certificados para autenticación

Los certificados con la función de identificación garantizan la identidad del suscriptor y del firmante.

3.6. Certificados para firma avanzada

Los certificados con la función de firma permiten la generación de la “firma electrónica avanzada” que se basa en un certificado cualificado sin la participación conjuntamente de un dispositivo cualificado de creación de firma.

3.7. Certificados para firma cualificada

Los certificados con la función de firma permiten la generación de la “firma electrónica cualificada”; es decir, la firma electrónica avanzada que se basa en un certificado cualificado cuando haya 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.

3.8. Certificados cualificados de sello electrónico

Estos certificados son 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 permiten identificar a sus titulares como Administraciones Públicas, siguiendo los requisitos establecidos en el artículo 40 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que incluirán el número de identificación fiscal y la denominación correspondiente, así como, en su caso, la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos.

3.9. Certificados de sello avanzado

Los certificados con la función de firma permiten la generación del “sello electrónico avanzado” que se basa en un certificado cualificado sin la participación conjuntamente de un dispositivo cualificado de creación de firma.

3.10. Tipos de certificados

Certificado	Soporte	Perfil	OIDs
Empleado público nivel alto, para firma	Tarjeta	Firma	<ul style="list-style-type: none">● 1.3.6.1.4.1.47281.1.1.1● 0.4.0.194112.1.2● 2.16.724.1.3.5.7.1
Empleado público nivel medio, para firma	HSM centralizado	Firma	<ul style="list-style-type: none">● 1.3.6.1.4.1.47281.1.1.4● 0.4.0.194112.1.0● 2.16.724.1.3.5.7.2
<i>Empleado público nivel alto, para autenticación</i>	<i>Tarjeta</i>	<i>Autent</i>	<ul style="list-style-type: none">● 1.3.6.1.4.1.47281.1.1.5● 0.4.0.2042.1.2● 2.16.724.1.3.5.7.1

Certificado	Soporte	Perfil	OIDs
Empleado público con pseudónimo nivel alto, para firma	Tarjeta	Firma	<ul style="list-style-type: none"> ● 1.3.6.1.4.1.47281.1.3.1 ● 0.4.0.194112.1.2 ● 2.16.724.1.3.5.4.1
Empleado público con pseudónimo nivel medio, para firma	HSM centralizado	Firma	<ul style="list-style-type: none"> ● 1.3.6.1.4.1.47281.1.3.4 ● 0.4.0.194112.1.0 ● 2.16.724.1.3.5.4.2
<i>Empleado público con pseudónimo nivel alto, para autenticación</i>	<i>Tarjeta</i>	<i>Autent</i>	<ul style="list-style-type: none"> ● 1.3.6.1.4.1.47281.1.3.5 ● 0.4.0.2042.1.2 ● 2.16.724.1.3.5.4.1

Certificado	Soporte	Perfil	OIDs
Sello electrónico, nivel Medio	Software	Firma	<ul style="list-style-type: none"> ● 1.3.6.1.4.1.47281.1.2.2 ● 0.4.0.194112.1.2 ● 2.16.724.1.3.5.6.2
Sello electrónico, nivel Medio, centralizado	HSM centralizado	Firma	<ul style="list-style-type: none"> ● 1.3.6.1.4.1.47281.1.2.4 ● 0.4.0.194112.1.2 ● 2.16.724.1.3.5.6.2

3.11. Entidad de Certificación emisora

Estos certificados son emitidos por ESFIRMA, identificada mediante los datos indicados anteriormente.

3.12. Validación de los certificados

Las listas de certificados revocados y servicios OCSP se encuentran en la web de esFIRMA y en las URL indicadas en cada uno de los certificados.

4. Límites de uso del certificado

4.1. Límites de uso dirigidos a los firmantes

El firmante y el creador de sellos han de utilizar el servicio de certificación prestado por esFIRMA exclusivamente para los usos autorizados en el contrato firmado entre el esFIRMA y el SUSCRIPTOR, y que se reproducen posteriormente.

Asimismo, el firmante y el creador de sellos se obligan a utilizar el servicio de certificación digital de acuerdo con las instrucciones, manuales o procedimientos suministrados por esFIRMA.

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

El firmante y el creador de sellos no pueden adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de certificación digital de esFIRMA, sin previo permiso expreso.

4.2. 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 ESFIRMA.

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

El prestador esFIRMA 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 esFIRMA emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o el creador de sellos, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor 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.

5. Obligaciones de los suscriptores

5.1. Generación de claves

En los certificados en tarjeta, el suscriptor autoriza al firmante a generar sus claves privada y pública dentro de un dispositivo cualificado de creación de firma electrónica, y solicita, en nombre del firmante, la emisión del certificado a esFIRMA.

En los certificados en nube, el suscriptor autoriza al firmante a generar sus claves privada y pública, y solicita, en nombre del firmante, la emisión del certificado a esFIRMA.

En los certificados de sello electrónico, el suscriptor autoriza a esFIRMA a generar las claves, privada y pública, para su uso por los creadores de sellos, y solicita en su nombre la emisión del certificado de sello electrónico.

5.2. Solicitud de certificados

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

5.3. Veracidad de la 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 ESFIRMA:

- 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.

5.4. Obligaciones de custodia

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

6. Obligaciones de los firmantes y creadores de sellos

6.1. Obligaciones de custodia

El firmante o creador de sellos se obliga a custodiar el código de identificación personal, las claves privadas, cuando existan la tarjeta o cualquier otro soporte técnico entregado por esFIRMA y, si fuese necesario, las especificaciones propiedad de esFIRMA que le sean suministradas.

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

6.2. Obligaciones de uso correcto

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

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

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

El firmante o creador de sellos debe dejar de emplear la clave privada en caso de compromiso de dicha clave, de revocación, o de compromiso de las claves de la CA.

El firmante o creador de sellos reconocerá:

- a) Que cuando utilice cualquier certificado, y mientras el certificado no haya expirado 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.

6.3. Transacciones prohibidas

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

Los servicios de certificación digital (y los de sellado de tiempo electrónico) prestados por ESFIRMA 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.

7. Obligaciones de los verificadores

7.1. Decisión informada

ESFIRMA 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 ESFIRMA, se rigen por la DPC de ESFIRMA y se compromete a cumplir los requisitos técnicos, operativos y de seguridad descritos en la mencionada DPC.

7.2. Requisitos de verificación de la firma

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 a ESFIRMA (con LRCs, por ejemplo) para determinar la validez de todos los certificados de la cadena de certificados, ya que únicamente puede

considerarse correctamente verificado 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, 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 o creador de sellos.

7.3. Confianza en un certificado no verificado

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

7.4. Efecto de la verificación

En virtud de la correcta verificación de estos certificados, de conformidad con este texto divulgativo (PDS), el verificador puede confiar en la identificación y, en su caso, clave pública del firmante.

7.5. 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 ESFIRMA, 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 ESFIRMA, sin previo consentimiento escrito.

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

Los servicios de certificación digital prestados por ESFIRMA 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.

7.6. Cláusula de indemnidad

El tercero que confía en el certificado se compromete a mantener indemne a ESFIRMA 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.

ESFIRMA no será responsable de los daños y perjuicios ocasionados en los términos indicados en el artículo 11 de Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

8. Obligaciones de ESFIRMA

8.1. En relación con la prestación de certificación digital

ESFIRMA se obliga a:

- a) Emitir, entregar, administrar y revocar certificados, de acuerdo con las instrucciones suministradas por el suscriptor, en los casos y por los motivos descritos en la DPC de ESFIRMA.
- 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, la fecha de expiración de los certificados.
- 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.

8.2. En relación con las comprobaciones del registro

ESFIRMA 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.

En el caso que ESFIRMA detecte errores en los datos que se deben incluir en los certificados o que justifiquen 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 ESFIRMA corrija los datos sin gestión previa de la incidencia

correspondiente con el suscriptor, deberá notificar los datos finalmente certificados al suscriptor.

ESFIRMA 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.

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.

8.3. Períodos de conservación

ESFIRMA conserva la información relativa a los servicios prestados de acuerdo con el artículo 24.2.h) del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, durante al menos 15 años desde la extinción del certificado o la finalización del servicio prestado.

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

9. Garantías limitadas y rechazo de garantías

9.1. Garantía de ESFIRMA por los servicios de certificación digital

ESFIRMA 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.

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

- Que el certificado contiene las informaciones que debe contener un certificado cualificado, de acuerdo con el Anexo I del Reglamento UE 910/2014.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, de la 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 ESFIRMA responderá por caso fortuito y en caso de fuerza mayor.
- La clave privada de la entidad de certificación utilizada para emitir certificados no ha sido comprometida, a menos que esFIRMA no haya comunicado lo contrario, de acuerdo con la DPC.
- No ha originado ni ha introducido declaraciones falsas o erróneas en la información de ningún certificado, ni ha dejado de incluir información necesaria aportada por el suscriptor y validada por esFIRMA, en el momento de la emisión del certificado.
- Todos los certificados cumplen los requisitos formales y de contenido de la DPC, incluyendo todos los requisitos legales en vigor y aplicables.
- Queda vinculada por los procedimientos operativos y de seguridad descritos en la DPC.

9.2. Exclusión de la garantía

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

Específicamente, ESFIRMA no garantiza software alguno utilizado por cualquier persona para firmar, verificar firmas, cifrar, descifrar, o utilizar de otra forma certificado digital alguno

emitido por ESFIRMA, excepto en los casos en que exista una declaración escrita en sentido contrario.

10. Acuerdos aplicables y DPC

10.1. Acuerdos aplicables

Los acuerdos aplicables a este certificado son los siguientes:

- Contrato de servicios de certificación, que regula la relación entre ESFIRMA y la Administración Pública/Persona Jurídica suscriptora de los certificados.
- Condiciones generales del servicio incorporadas en este texto de divulgación del certificado o PDS.
- DPC, que regula la emisión y utilización de los certificados.

10.2. DPC

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

La DPC y la documentación de operaciones se modifica periódicamente y se puede consultar en la página de Internet: <https://www.esfirma.com>

11. Política de intimidad

ESFIRMA 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 ESFIRMA 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.

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

El tratamiento de dichos datos por terceros por motivo de la prestación de un servicio a esFIRMA, entre otros, a título meramente enunciativo pero no limitativo, se produce en el marco de un encargo del tratamiento a que se refiere el artículo 28 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), y 33 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) y en su virtud es conforme con los requisitos del RGPD y de la LOPDGDD, y garantiza la protección de los derechos del interesado.

12. Política de privacidad

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

La información a que se refiere el apartado 7.3 se conservada por los periodos indicados debidamente registrada y con garantías de seguridad e integridad.

13. Política de reintegro

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

14. Ley aplicable, jurisdicción competente y régimen de reclamaciones y disputas

Las relaciones con ESFIRMA 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 esFIRMA por cualquier medio que deje constancia a la dirección de contacto indicada en el punto de información de contacto de esta PDS.

Si las partes no alcanzaran un acuerdo al respecto, cualquiera de ellas podrá someter el conflicto a la jurisdicción civil, con sujeción a los Tribunales del domicilio social de ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA.

14.1. Acreditaciones y sellos de calidad

EsFIRMA dispone de la cualificación “eIDAS-compliant” para los siguientes servicios:

- a) Servicio de expedición de certificados electrónicos cualificados de firma electrónica
- b) Servicio de expedición de certificados electrónicos cualificados de sello electrónico
- c) Servicio de expedición de certificados electrónicos cualificados de autenticación de sitios web
- d) Servicio de expedición de sellos electrónicos cualificados de tiempo

14.2. Vinculación con la lista de prestadores

EsFIRMA es prestador cualificado de servicios de certificación por lo que forma parte de la Lista de Prestadores cualificados (TSL) que mantiene el supervisor nacional y que se puede obtener en la siguiente dirección:

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

EsFIRMA está incluida en la “Trust List” de la Unión Europea como Prestador cualificado de servicios electrónicos de confianza:

<https://webgate.ec.europa.eu/tl-browser/#/tl/ES/27>

14.3. Divisibilidad de las cláusulas, supervivencia, acuerdo íntegro y notificación

Las cláusulas del presente texto de divulgación (PDS) 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 de “Obligaciones y responsabilidad”, “Auditoría de conformidad” y “Confidencialidad” de la DPC de ESFIRMA continuarán vigentes tras la terminación del servicio.

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

Las partes se notifican hechos mutuamente mediante un procedimiento envío email a la dirección info@esfirma.com