Texto de Divulgação (PDS) dos certificados emitidos para as Administrações Públicas

Índice

TEXTO DIVULGATIVO - PDS

Este documento contém as informações essenciais a conhecer em relação ao serviço de certificação da Entidade de Certificação ESFIRMA.

Este documento segue a estrutura definida no Anexo A da norma ETSI EN 319 411-1, de acordo com as indicações da seção 4.3.4 da norma ETSI EN 319 412-5.

1.1. Controle documental

Classificação de segurança	PÚBLICO
Versão	2.2

1.2. Controle de versões

Versão	Mudanças	Descrição	Autor	Fechar
1.0	Original	Criação de documento	esFIRMA	28/04/2016
1.4		Subsanaciones	esFIRMA	07/06/2017
1.5		Mudança de denominação e referência a normativas	esFIRMA	06/11/2017
2.0		Inclusão de todos os certificados referentes às AAPP espanholas	esFIRMA	03/06/2020
2.1		Revisão Lei 6/2020	esFIRMA	08/04/2021

2.2	(1.3)	Adiciona-se referência ao site da esFIRMA.	esFIRMA	21/04/2023

2. Informação

2.1. Organização responsável

A Entidade de Certificação ESFIRMA, doravante "ESFIRMA", é uma iniciativa de:

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

2.2. Contato

Para qualquer consulta, dirijam-se a:

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

2.3. Contato para processos de revogação

O processo para solicitar a revogação de um certificado pode ser consultado em www.esfirma.com. Para qualquer outra consulta a respeito, dirijam-se a:

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

3. Tipo e finalidade do certificado

3.1. Certificados qualificados de funcionário público

Estes certificados são qualificados de acordo com o artigo 28 e com o Anexo I do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014 e cumprem o disposto pela normativa técnica identificada com a referência ETSI EN 319 411-2.

Esses certificados permitem identificar seus titulares como pessoal a serviço da Administração Pública, vinculando-os a ela, seguindo os requisitos estabelecidos no artigo 43 da Lei 40/2015, de 1 de outubro, do Regime Jurídico do Setor Público, para a assinatura eletrônica do pessoal a serviço das Administrações Públicas.

3.2. Certificados de funcionário público com pseudônimo

Esses certificados permitem identificar seus titulares como pessoal a serviço da Administração Pública, vinculando-os a ela, conforme permitido pelo artigo 43.2 da Lei 40/2015, de 1 de outubro, do Regime Jurídico do Setor Público, para a assinatura eletrônica do pessoal a serviço das Administrações Públicas, pessoal que, por razões de segurança pública, só será identificado com o número de identificação profissional ou outro pseudônimo de funcionário público, conforme indicado no Anexo I, alínea c) do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, e o artigo 6.1.a) da Lei 6/2020, de 11 de novembro, reguladora de determinados aspectos dos serviços eletrônicos de confiança.

3.3. Certificados em cartão

Os certificados que usam cartão funcionam com um dispositivo qualificado de criação de assinatura eletrônica, de acordo com o Anexo II do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014.

3.4. Certificados em a nuvem

Estes certificados são gerenciados de forma centralizada.

3.5. Certificados para autenticação

Os certificados com a função de identificação garantem a identidade do assinante e do signatário.

3.6. Certificados para firma avançada

Os certificados com a função de assinatura permitem a geração da "assinatura eletrônica avançada" que se baseia em um certificado qualificado sem a participação conjunta de um dispositivo qualificado de criação de assinatura.

3.7. Certificados para assinatura qualificada

Os certificados com a função de assinatura permitem a geração da "assinatura eletrônica qualificada"; ou seja, a assinatura eletrônica avançada baseada em um certificado qualificado quando gerada usando um dispositivo qualificado, portanto, de acordo com o estabelecido no artigo 25.2 do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, terá um efeito jurídico equivalente ao de uma assinatura manuscrita.

3.8. Certificados qualificados de selo eletrônico

Estes certificados são qualificados de acordo com o artigo 38 e com o Anexo III do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014 e cumprem o disposto pela norma técnica identificada com a referência ETSI EN 319 411-2.

Esses certificados permitem identificar seus titulares como Administrações Públicas, seguindo os requisitos estabelecidos no artigo 40 da Lei 40/2015, de 1 de outubro, do Regime Jurídico do Setor Público, que incluirão o número de identificação fiscal e a denominação correspondente, bem como, se for o caso, a identidade do titular no caso dos selos eletrônicos de órgãos administrativos.

3.9. Certificados de selo avançado

Os certificados com a função de assinatura permitem a geração do "selo eletrônico avançado" baseado em um certificado qualificado sem a participação conjunta de um dispositivo qualificado de criação de assinatura.

3.10. Tipos de certificados

Certificado	**Suporte**	**Perfil**	**OIDs**
Funcionário público de alto nível, para assinatura	Cartão	Assinatura	● 1.3.6.1.4.1.47281.1.1.1 ● 0.4.0.194112.1.2 ● 2.16.724.1.3.5.7.1
Funcionário público de nível médio, para assinatura	HSM centralizado	Assinatura	● 1.3.6.1.4.1.47281.1.1.4 ● 0.4.0.194112.1.0 ● 2.16.724.1.3.5.7.2
Funcionário público de alto nível, para autenticação	*Cartão*	*Autent*	● *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	**Suporte**	**Perfil**	**OIDs**
Funcionário público com pseudônimo de nível alto, para assinatura	Cartão	Assinatura	● 1.3.6.1.4.1.47281.1.3.1 ● 0.4.0.194112.1.2 ● 2.16.724.1.3.5.4.1

Funcionário público com pseudônimo de nível médio, para assinatura	HSM centralizado	Assinatura	• 1.3.6.1.4.1.47281.1.3.4 • 0.4.0.194112.1.0 • 2.16.724.1.3.5.4.2
Funcionário público com pseudônimo de nível alto, para autenticação	*Cartão*	*Autent*	• *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	**Suporte**	**Perfil**	**OIDs**
Selo eletrônico, nível Médio	Software	Assinatura	• 1.3.6.1.4.1.47281.1.2.2 • 0.4.0.194112.1.2 • 2.16.724.1.3.5.6.2
Selo eletrônico, nível Médio, centralizado	HSM centralizado	Assinatura	• 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. Entidade de Certificação emissora

Esses certificados são emitidos pela ESFIRMA, identificada pelos dados indicados anteriormente.

3.12. Validação dos certificados

As listas de certificados revogados e serviços OCSP estão no site da esFIRMA e nas URLs indicadas em cada um dos certificados.

4. Limites de uso do certificado

4.1. Limites de uso direcionados aos signatários

O signatário e o criador de selos devem utilizar o serviço de certificação fornecido pela esFIRMA exclusivamente para os usos autorizados no contrato assinado entre a esFIRMA e o ASSINANTE, e que são reproduzidos posteriormente.

Do mesmo modo, o signatário e o criador de selos se comprometem a utilizar o serviço de certificação digital de acordo com as instruções, manuais ou procedimentos fornecidos pela esFIRMA.

O signatário e o criador de selos devem cumprir qualquer lei e regulamentação que possa afetar seu direito de uso das ferramentas criptográficas que empregue.

O signatário e o criador de selos não podem adotar medidas de inspeção, alteração ou engenharia reversa dos serviços de certificação digital da esFIRMA, sem prévia permissão expressa.

4.2. Limites de uso direcionados aos verificadores

Os certificados são usados para sua própria função e finalidade estabelecida, sem poder ser usados em outras funções e com outras finalidades.

Da mesma forma, os certificados devem ser usados apenas de acordo com a lei aplicável, especialmente levando em consideração as restrições de importação e exportação existentes em cada momento.

Os certificados não podem ser utilizados para assinar solicitações de emissão, renovação, suspensão ou revogação de certificados, nem para assinar certificados de chave pública de qualquer tipo, nem assinar listas de revogação de certificados (LRC).

Os certificados não foram projetados, não podem ser destinados e não é autorizado o seu uso ou revenda como equipamentos de controle de situações perigosas ou para usos que requerem ações à prova de falhas, como o funcionamento de instalações nucleares, sistemas de navegação ou comunicações aéreas, ou sistemas de controle de armamento, onde uma falha possa diretamente resultar em morte, lesões pessoais ou danos ambientais graves.

Deve-se levar em consideração os limites indicados nos diversos campos dos perfis de certificados, visíveis no site da ESFIRMA.

O uso de certificados digitais em operações que contrariam este texto de divulgação (PDS) ou os contratos com os assinantes é considerado uso indevido para fins legais apropriados, isentando assim a ESFIRMA, de acordo com a legislação em vigor, de qualquer responsabilidade por este uso indevido dos certificados realizados pelo signatário ou por qualquer terceiro.

O prestador esFIRMA não tem acesso aos dados aos quais se pode aplicar o uso de um certificado. Portanto, e como consequência dessa impossibilidade técnica de acessar o conteúdo da mensagem, não é possível por parte da esFIRMA emitir qualquer avaliação sobre esse conteúdo, assumindo assim o assinante, o signatário ou o criador de selos, qualquer responsabilidade decorrente do conteúdo associado ao uso de um certificado.

Da mesma forma, o assinante será responsável por qualquer responsabilidade que possa resultar do uso fora dos limites e condições de uso estabelecidos neste texto de divulgação, ou nos contratos com os assinantes, bem como de qualquer outro uso indevido do mesmo decorrente desta seção ou que possa ser interpretado como tal de acordo com a legislação em vigor.

5. Obrigações dos assinantes

5.1. Geração de chaves

Nos certificados em cartão, o subscritor autoriza o signatário a gerar suas chaves privada e pública dentro de um dispositivo qualificado de criação de assinatura eletrônica, e solicita, em nome do signatário, a emissão do certificado à esFIRMA.

Nos certificados em nuvem, o assinante autoriza o signatário a gerar suas chaves privada e pública e solicita, em nome do signatário, a emissão do certificado para esFIRMA.

Nos certificados de selo eletrônico, o assinante autoriza a esFIRMA a gerar as chaves, privada e pública, para uso pelos criadores de selos, e solicita em seu nome a emissão do certificado de selo eletrônico.

5.2. Solicitação de certificados

O assinante compromete-se a fazer os pedidos, quando necessário, desses certificados de acordo com o procedimento e, se necessário, os componentes técnicos fornecidos pela ESFIRMA, em conformidade com o estabelecido na declaração de práticas de certificação (DPC) e na documentação de operações da ESFIRMA.

5.3. Veracidade da informação

O assinante é responsável por garantir que todas as informações incluídas em seu pedido de certificado sejam precisas, completas para a finalidade do certificado e atualizadas a todo momento.

O assinante deve informar imediatamente a ESFIRMA:

- De qualquer inexatidão detectada no certificado após sua emissão.

- Das mudanças que ocorram nas informações fornecidas e/ou registradas para a emissão do certificado.

5.4. Obrigações de custódia

O assinante compromete-se a guardar todas as informações geradas em sua atividade como entidade de registro.

6. Obrigações dos signatários e criadores de selos

6.1. Obrigações de custódia

O signatário ou criador de selos é obrigado a guardar o código de identificação pessoal, as chaves privadas, quando houver o cartão ou qualquer outro suporte técnico fornecido pela esFIRMA e, se necessário, as especificações de propriedade da esFIRMA que lhe forem fornecidas.

Em caso de perda ou roubo da chave privada do certificado, ou caso suspeite que a chave privada perdeu confiabilidade por qualquer motivo, tais circunstâncias devem ser notificadas imediatamente à esFIRMA diretamente ou por meio do assinante.

6.2. Obrigações de uso correto

O signatário ou criador de selos deve utilizar o serviço de certificação fornecido pela esFIRMA, exclusivamente para os usos autorizados na DPC e em qualquer outra instrução, manual ou procedimento fornecido ao assinante.

O signatário ou criador de selos deve cumprir qualquer lei e regulamentação que possa afetar seu direito de uso das ferramentas criptográficas empregadas.

O signatário ou criador de selos não poderá adotar medidas de inspeção, alteração ou descompilação dos serviços de certificação digital prestados.

O signatário ou criador de selos deve parar de usar a chave privada em caso de comprometimento dessa chave, revogação ou comprometimento das chaves da CA.

O signatário ou criador de selos reconhecerá:

a) Que ao utilizar qualquer certificado, e enquanto o certificado não tiver expirado ou sido revogado, terá aceitado esse certificado e estará operacional.

b) Que não atua como entidade de certificação e, portanto, se compromete a não utilizar as chaves privadas correspondentes às chaves públicas contidas nos certificados com o propósito de assinar qualquer certificado.

6.3. Transações proibidas

O signatário ou criador de selos se compromete a não utilizar suas chaves privadas, os certificados, os cartões ou qualquer outro suporte técnico fornecido pela esFIRMA na realização de qualquer transação proibida pela lei aplicável.

Os serviços de certificação digital (e os de selagem de tempo eletrônico) fornecidos pela ESFIRMA não foram projetados nem permitem sua utilização ou revenda como equipamentos de controle de situações perigosas, ou para usos que exijam ações à prova de falhas, como a operação de instalações nucleares, sistemas de navegação ou comunicação aérea, sistemas de controle de tráfego aéreo ou sistemas de controle de armamento, nos quais um erro poderia diretamente causar a morte, danos físicos ou danos ambientais graves.

7. Obrigações dos verificadores

7.1. Decisão informada

ESFIRMA informa ao verificador que tem acesso a informações suficientes para tomar uma decisão informada no momento de verificar um certificado e confiar nas informações contidas nesse certificado.

Adicionalmente, o verificador reconhecerá que o uso do Registro e das Listas de Revogação de Certificados (doravante, "as LRCs" ou "as CRLs) da ESFIRMA, são regidas pela DPC da ESFIRMA e se compromete a cumprir os requisitos técnicos, operacionais e de segurança descritos na mencionada DPC.

7.2. Requisitos de verificação da assinatura

A verificação será executada normalmente de forma automática pelo software do verificador e, em qualquer caso, de acordo com a DPC, com os seguintes requisitos:

- É necessário utilizar o software apropriado para a verificação de uma assinatura digital com os algoritmos e comprimentos de chaves autorizados no certificado e/ou executar qualquer outra operação criptográfica, e estabelecer a cadeia de certificados na qual se baseia a assinatura eletrônica a ser verificada, pois a assinatura eletrônica é verificada utilizando essa cadeia de certificados.
- É necessário garantir que a cadeia de certificados identificada é a mais adequada para a assinatura eletrônica que se verifica, já que uma assinatura eletrônica pode basear-se em mais de uma cadeia de certificados, e é decisão do verificador garantir o uso da cadeia mais adequada para verificá-la.
- É necessário verificar o estado de revogação dos certificados da cadeia com as informações fornecidas a ESFIRMA (com LRCs, por exemplo) para determinar a validade de todos os certificados da cadeia de certificados, já que apenas pode ser considerado corretamente

verificado uma assinatura eletrônica se todos e cada um dos certificados da cadeia estão corretos e em vigor.

- É necessário garantir que todos os certificados da cadeia autorizam o uso da chave privada pelo assinante do certificado, pois existe a possibilidade de que alguns dos certificados incluam limites de uso que impeçam a confiança em a assinatura eletrônica que é verificado. Cada certificado da cadeia possui um indicador que faz referência às condições de uso aplicáveis, para revisão pelos verificadores.
- É necessário verificar tecnicamente a assinatura de todos os certificados da cadeia antes de confiar no certificado utilizado pelo signatário ou criador de selos.

7.3. Confiança em um certificado não verificado

Se o verificador confiar em um certificado não verificado, assumirá todos os riscos decorrentes dessa ação.

7.4. Efeito da verificação

Em virtude da correta verificação desses certificados, de acordo com este texto divulgativo (PDS), o verificador pode confiar na identificação e, se for o caso, na chave pública do signatário.

7.5. Uso correto e atividades proibidas

O verificador compromete-se a não utilizar nenhum tipo de informação sobre o estado dos certificados ou qualquer outro tipo fornecido pela ESFIRMA, na realização de qualquer transação proibida pela lei aplicável à referida transação.

O verificador compromete-se a não inspecionar, interferir ou realizar engenharia reversa na implementação técnica dos serviços públicos de certificação da ESFIRMA, sem prévio consentimento por escrito.

Adicionalmente, o verificador se compromete a não comprometer intencionalmente a segurança dos serviços públicos de certificação da ESFIRMA.

Os serviços de certificação digital fornecidos pela ESFIRMA não foram projetados nem permitem a utilização ou revenda, como equipamentos de controle de situações perigosas ou para usos que exijam ações à prova de falhas, como a operação de instalações nucleares, sistemas de navegação ou comunicação aérea, sistemas de controle de tráfego aéreo, ou sistemas de controle de armamento, onde um erro poderia causar a morte, danos físicos ou danos ambientais graves.

7.6. Cláusula de indenização

O terceiro que confia no certificado compromete-se a manter a ESFIRMA isenta de qualquer dano decorrente de qualquer ação ou omissão que resulte em responsabilidade, dano ou perda, despesa de qualquer tipo, incluindo as judiciais e de representação legal em que possa incorrer, pela publicação e uso do certificado, quando ocorrer uma das seguintes causas:

- Incumprimento das obrigações do terceiro que confia no certificado.
- Confiança temerária em um certificado, de acordo com as circunstâncias.
- Falta de verificação do estado de um certificado, para determinar se ele não está suspenso ou revogado.
- Falta de verificação da totalidade das medidas de garantia prescritas na DCP ou restante das normas de aplicação.

A ESFIRMA não será responsável pelos danos e prejuízos causados nos termos indicados no artigo 11 da Lei 6/2020, de 11 de novembro, que regula determinados aspectos dos serviços eletrônicos de confiança.

8. Obrigações da ESFIRMA

8.1. Em relação à prestação de certificação digital

ESFIRMA se compromete a:

a) Emitir, entregar, administrar y revogar certificados, de acordo com as instruções fornecidas pelo assinante, nos casos e pelos motivos descritos na DPC da ESFIRMA.

b) Executar os serviços com os meios técnicos e materiais adequados e com pessoal que cumpra as condições de qualificação e experiência estabelecidas na DPC.

c) Cumprir os níveis de qualidade do serviço, em conformidade com o estabelecido na DPC, nos aspectos técnicos, operacionais e de segurança.

d) Notificar o assinante, com antecedência, a data de expiração dos certificados.

e) Comunicar às terceiras pessoas que o solicitarem, o estado dos certificados, de acordo com o estabelecido na DPC para os diferentes serviços de verificação de certificados.

8.2. Em relação às verificações do registro

ESFIRMA se compromete a emitir certificados com base nos dados fornecidos pelo assinante, podendo realizar as verificações que considerar apropriadas.

No caso em que a ESFIRMA detectar erros nos dados que devem ser incluídos nos certificados ou que justifiquem esses dados, poderá realizar as alterações que considerar necessárias antes de emitir o certificado ou suspender o processo de emissão e gerir com o assinante o incidente correspondente. Caso a ESFIRMA corrija os dados sem gestão prévia do incidente correspondente com o assinante, deverá notificar os dados finalmente certificados ao assinante.

ESFIRMA reserva-se o direito de não emitir o certificado, quando considerar que a justificação documental seja insuficiente para a correta identificação e autenticação do assinante.

As obrigações anteriores ficarão suspensas nos casos em que o assinante atuar como autoridade de registro e possuir os elementos técnicos correspondentes à geração de chaves, emissão de certificados e gravação de dispositivos de assinatura corporativos.

8.3. Períodos de conservação

ESFIRMA conserva as informações relativas aos serviços prestados de acordo com o artigo 24.2.h) do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, por pelo menos 15 anos após a extinção do certificado ou a finalização do serviço prestado.

ESFIRMA armazena as informações dos logs por um período entre 1 e 15 anos, dependendo do tipo de informação registrada.

9. Garantias limitadas e rejeição de garantias

9.1. Garantia da ESFIRMA pelos serviços de certificação digital

ESFIRMA garante ao assinante:

- Que não há erros de fato nas informações contidas nos certificados, conhecidos ou realizados pela Entidade de Certificação.

- Que não há erros de fato nas informações contidas nos certificados, devido à falta de diligência adequada na gestão do pedido de certificado ou na sua criação.

- Que os certificados cumprem com todos os requisitos materiais estabelecidos na DPC.

- Que os serviços de revogação e o uso do depósito cumprem todos os requisitos materiais estabelecidos na DPC.

ESFIRMA garante ao terceiro que confia no certificado:

- Que a informação contida ou incorporada por referência no certificado está correta, exceto quando indicado o contrário.

- Em caso de certificados publicados no depósito, que o certificado foi emitido ao assinante identificado no mesmo e que o certificado foi aceito.

- Que na aprovação do pedido de certificado e na emissão do certificado, todos os requisitos materiais estabelecidos na DPC foram cumpridos.

- A rapidez e segurança na prestação dos serviços, especialmente dos serviços de revogação e depósito.

Adicionalmente, ESFIRMA garante ao assinante e a terceiros que confiam no certificado:

- Que o certificado contém as informações que devem constar em um certificado qualificado, de acordo com o Anexo I do Regulamento UE 910/2014.
- Que, no caso de gerar as chaves privadas do assinante ou, se for o caso, da pessoa física identificada no certificado, mantém-se a confidencialidade durante o processo.
- A responsabilidade da Entidade de Certificação, dentro dos limites estabelecidos. Em nenhum caso, a ESFIRMA será responsável por caso fortuito ou força maior.
- A chave privada da entidade de certificação utilizada para emitir certificados não foi comprometida, a menos que esFIRMA não tenha comunicado o contrário, de acordo com a DPC.
- Não originou nem introduziu declarações falsas ou incorretas nas informações de nenhum certificado, nem deixou de incluir informações necessárias fornecidas pelo assinante e validadas pela esFIRMA, no momento da emissão do certificado.
- Todos os certificados cumprem os requisitos formais e de conteúdo da DPC, incluindo todos os requisitos legais em vigor e aplicáveis.
- Fica vinculada pelos procedimentos operacionais e de segurança descritos na DPC.

9.2. Exclusão da garantia

ESFIRMA rejeita qualquer outra garantia diferente da anterior que não seja legalmente exigível.

Especificamente, ESFIRMA não garante nenhum software utilizado por qualquer pessoa para assinar, verificar assinaturas, criptografar, descriptografar ou utilizar de outra forma qualquer certificado digital emitido pela ESFIRMA, exceto nos casos em que haja uma declaração escrita em sentido contrário.

10. Acordos aplicáveis e DPC

10.1. Acordos aplicáveis

Os acordos aplicáveis a este certificado são os seguintes:

- Contrato de serviços de certificação, que regula a relação entre ESFIRMA e a Administração Pública/Pessoa Jurídica assinante dos certificados.

- Condições gerais do serviço incorporadas em este texto de divulgação do certificado ou PDS.

- DPC, que regula a emissão e utilização dos certificados.

10.2. DPC

Os serviços de certificação da ESFIRMA são regulados tecnicamente e operacionalmente pela DPC da ESFIRMA, pelas suas atualizações posteriores, bem como por documentação complementar.

A DPC e a documentação de operações são modificadas periodicamente e podem ser consultadas na página da Internet: https://www.esfirma.com

11. Política de privacidade

ESFIRMA não pode divulgar nem pode ser obrigada a divulgar informações confidenciais em relação a certificados sem um pedido específico prévio que provenha de:

a) A pessoa em relação à qual a ESFIRMA tem o dever de manter as informações confidenciais, ou

b) Uma ordem judicial, administrativa ou qualquer outra prevista na legislação vigente.

No entanto, o assinante aceita que determinadas informações, pessoais e de outros tipos, fornecidas no pedido de certificados, sejam incluídas nos seus certificados e no mecanismo de verificação do estado dos certificados, e que as informações mencionadas não sejam confidenciais, por imperativo legal.

ESFIRMA não cede a nenhuma pessoa os dados entregues especificamente para a prestação do serviço de certificação.

O tratamento desses dados por terceiros devido à prestação de um serviço à esFIRMA, entre outros, a título meramente enunciativo, mas não limitativo, ocorre no âmbito de uma encomenda de tratamento a que se refere o artigo 28 do REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados), e 33 da Lei Orgânica 3/2018, de 5 de dezembro, de Proteção de Dados Pessoais e garantia dos direitos digitais (LOPDGDD) e, em virtude disso, está em conformidade com os requisitos do RGPD e da LOPDGDD, e garante a proteção dos direitos do interessado.

12. Política de privacidade

ESFIRMA possui uma política de privacidade na seção 9.4 da DPC e regulamentação específica de privacidade em relação ao processo de registro, confidencialidade do registro, proteção do acesso às informações pessoais e consentimento do usuário.

As informações referentes ao parágrafo 7.3 são mantidas pelos períodos indicados, devidamente registradas e com garantias de segurança e integridade.

13. Política de reembolso

ESFIRMA não reembolsará o custo do serviço de certificação em nenhum caso.

14. Lei aplicável, jurisdição competente e regime de reclamações e disputas

As relações com a ESFIRMA serão regidas pela lei espanhola em matéria de serviços de confiança vigente em cada momento, bem como pela legislação civil e comercial no que for aplicável.

A jurisdição competente é a indicada na Lei 1/2000, de 7 de janeiro, de Julgamento Civil.

Em caso de discrepância entre as partes, as partes tentarão a resolução amigável prévia. Para esse fim, as partes devem enviar uma comunicação à esFIRMA por qualquer meio que deixe registro no endereço de contato indicado no ponto de informação de contato desta PDS.

Se as partes não alcançarão um acordo a respeito, qualquer uma delas poderá submeter o conflito à jurisdição civil, sujeito aos Tribunais do domicílio social da ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA.

14.1. Acreditações e selos de qualidade

EsFIRMA possui a qualificação "eIDAS-compliant" para os seguintes serviços:

a) Serviço de emissão de certificados eletrônicos qualificados de assinatura eletrônica
b) Serviço de emissão de certificados eletrônicos qualificados de selo eletrônico
c) Serviço de emissão de certificados eletrônicos qualificados de autenticação de sites
d) Serviço de emissão de selos eletrônicos qualificados de tempo

14.2. Vinculação com a lista de prestadores

EsFIRMA é um prestador qualificado de serviços de certificação, fazendo parte da Lista de Prestadores qualificados (TSL) mantida pelo supervisor nacional, que pode ser obtida no seguinte endereço:
https://sedeaplicaciones.minetur.gob.es/Prestadores/

EsFIRMA está incluída na "Trust List" da União Europeia como Prestador qualificado de serviços eletrônicos de confiança:
https://webgate.ec.europa.eu/tl-browser/#/tl/ES/27

14.3. Divisibilidade das cláusulas, sobrevivência, acordo integral e notificação

As cláusulas do presente texto de divulgação (PDS) são independentes entre si, motivo pelo qual, se qualquer cláusula for considerada inválida ou inaplicável, o restante das cláusulas das PDS continuarão sendo aplicáveis, exceto acordo expresso em contrário das partes.

Os requisitos contidos nas seções deObrigações e responsabilidade", "Auditoria de conformidade" y "Confidencialidade" da DPC da ESFIRMA continuarão vigentes após o término do serviço.

Este texto contém a vontade completa e todos os acordos entre as partes.

As partes notificam-se mutuamente de fatos por meio de um procedimento envio email para o endereço info@esfirma.com