

Texto de Divulgação (PDS) dos certificados para a ENTIDADE



Índice

Informação	5
Organização responsável	5
Contacto	5
Contacto para processos de revogação	5
Tipo e finalidade do certificado	6
Certificados qualificados de pessoas físicas relacionadas	6
Certificados de uma pessoa física com pseudónimo	6
Certificados de cartão	6
Certificados Cloud	6
Certificados para autenticação	7
Certificados de Assinatura Avançada	7
Certificados para assinatura qualificada	7
Tipos de certificados	8
Autoridade Certificadora Emitidora	9
Validação de certificados	9
Limites de utilização dos certificados	10
Limites de utilização direccionados a sinalizadores	10
Limites de utilização direccionados para verificadores	10
Obrigações dos subscritores	12
Geração de chaves	12
Pedido de certificados	12
Veracidade da informação	12
Obrigações de custódia	13
Obrigações dos signatários e criadores de selos	13
Obrigações de custódia	13
Obrigações de uso correto	13
Transações proibidas	14
Obrigações dos verificadores	15
Decisão informada	15
Requisitos de Verificação de Assinatura	15
Confiar num certificado não verificado	16
Efeito da verificação	16
Uso Adequado e Atividades Proibidas	16

Cláusula de indemnização	17
Obrigações de ESFIRMA	18
No que diz respeito à prestação de certificação digital	18
Em relação às verificações de registo	18
Períodos de retenção	19
Garantias Limitadas e Isenções de Garantias	19
Garantia ESFIRMA para serviços de certificação digital	19
Exclusão da Garantia	21
Acordos e DPCs Aplicáveis	22
Acordos Aplicáveis	22
CPD	22
Política de Privacidade	23
Política de Privacidade	24
Política de Reembolso	24
Legislação aplicável, jurisdição competente e regime de reclamações e litígios	24
Acreditações e selos de qualidade	25
Ligação para a lista de prestadores	25
Separabilidade dos termos, sobrevivência, acordo total e notificação	25

TEXTO INFORMATIVO - PDS

Este documento contém a informação essencial a conhecer relativamente ao serviço de certificação do Organismo de Certificação ESFIRMA.

Este documento segue a estrutura definida no Anexo A da ETSI EN 319 411-1, em conformidade com as indicações da secção 4.3.4 da ETSI EN 319 412-5.

Controlo de documentos

Classificação de Segurança	PÚBLICO
Versão	2.3

Controlo de Versões

Versão	Alterações	Descrição	Autor	Data
2.0	Original	Criação de documentos	esFIRMA	03/06/2020
2.1		O certificado de selo eletrónico é adicionado e generalizado para a entidade.	esFIRMA	21/10/2020
2.2		Revisão da Lei 6/2020	esFIRMA	08/04/2021
2.3	(1.3)	Foi adicionada uma referência ao site da esFIRMA.	esFIRMA	21/04/2023
2.4		Acrescentou referência ao procedimento de resolução de litígios	esFIRMA	15/07/2026

1. Informação

1.1. Organização responsável

O Organismo de Certificação ESFIRMA, doravante designado "ESFIRMA", é uma iniciativa de:

SERVIÇOS PÚBLICOS PARA A ADMINISTRAÇÃO SA (ESFIRMA) CALLE BARI
39 (EDIF. EDIFÍCIO BINÁRIO)
50197 - ZARAGOZA
(+34) 976300110

1.2. Contacto

Para quaisquer questões, por favor contacte:

SERVIÇOS PÚBLICOS PARA A ADMINISTRAÇÃO SA (ESFIRMA) CALLE BARI
39 (EDIF. EDIFÍCIO BINÁRIO)
50197 - ZARAGOZA
(+34) 976300110

1.3. Contacto para processos de revogação

O processo para solicitar a revogação de um certificado pode ser encontrado em www.esfirma.com. Para quaisquer questões adicionais, por favor contacte:

SERVIÇOS PÚBLICOS PARA A ADMINISTRAÇÃO SA (ESFIRMA) CALLE BARI
39 (EDIF. EDIFÍCIO BINÁRIO)
50197 - ZARAGOZA
(+34) 976300110

2. Tipo e finalidade do certificado

2.1. Certificados qualificados de pessoas físicas relacionadas

Estes certificados são qualificados de acordo com o artigo 28 e o anexo I do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, e cumprem as disposições dos regulamentos técnicos identificados com a referência ETSI EN 319 411-2.

2.2. Certificados de uma pessoa física com pseudónimo

Estes certificados permitem que o titular do certificado seja identificado com a informação do pseudónimo, de acordo com o Anexo I, secção c) do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, que está inequívocamente registado como tal, de acordo com o artigo 6.1.a) da Lei 6/2020, de 11 de novembro, regulação de certos aspetos dos serviços fiduciários eletrónicos.

2.3. Certificados de cartão

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

2.4. Certificados Cloud

Estes certificados são geridos centralmente.

2.5. Certificados para autenticação

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

2.6. Certificados de Assinatura Avançada

Certificados com função de assinatura permitem a geração da "assinatura eletrónica avançada" baseada num certificado qualificado sem a participação conjunta de um dispositivo qualificado de criação de assinatura.

2.7. Certificados para assinatura qualificada

Os certificados com função de assinatura permitem a geração da "assinatura eletrónica qualificada"; isto é, a assinatura eletrónica avançada baseada num certificado **qualificado quando gerada** utilizando um dispositivo qualificado, portanto, em conformidade com as disposições do Artigo 25.2 do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, terá efeito legal equivalente ao de uma assinatura manuscrita.

2.8. Certificados eletrónicos qualificados

Estes certificados são qualificados de acordo com o Artigo 38 e o Anexo III do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, e cumprem as disposições dos regulamentos técnicos identificados com a referência ETSI EN 319 411-2.

2.9. Certificados Avançados de Selo

Os certificados com função de assinatura permitem a geração do "selo eletrónico avançado" baseado num certificado qualificado sem a intervenção conjunta de um dispositivo qualificado de criação de assinatura.

2.10. Tipos de certificados

Certificado	Apoio	Perfil	OIDs
<i>Pessoa física ligada, para assinatura qualificada</i>	<i>Cartão</i>	<i>Assinatura</i>	• 1.3.6.1.4.1.47281.1.6.1 • 0.4.0.194112.1.2
<i>Pessoa física ligada, para assinatura avançada</i>	<i>HSM Centralizado</i>	<i>Assinatura</i>	• 1.3.6.1.4.1.47281.1.6.4 • 0.4.0.194112.1.0
<i>Pessoa física ligada, para autenticação</i>	<i>Cartão</i>	<i>Autent</i>	• 1.3.6.1.4.1.47281.1.6.5 • 0.4.0.2042.1.2

Certificado	Apoio	Perfil	OIDs
<i>Uma pessoa física ligada por pseudónimo, para uma assinatura qualificada</i>	<i>Cartão</i>	<i>Assinatura</i>	• 1.3.6.1.4.1.47281.1.7.1 • 0.4.0.194112.1.2
<i>Uma pessoa natural ligada por um pseudónimo, para assinatura avançada</i>	<i>HSM Centralizado</i>	<i>Assinatura</i>	• 1.3.6.1.4.1.47281.1.7.4 • 0.4.0.194112.1.0

<i>Uma pessoa natural ligada por um pseudónimo, para autenticação</i>	<i>Cartão</i>	<i>Autent</i>	• 1.3.6.1.4.1.47281.1.7.5 • 0.4.0.2042.1.2
---	---------------	---------------	--

Certificado	Apoio	Perfil	OIDs
<i>Selo eletrónico</i>	<i>SW</i>	<i>Autenticação, Assinatura e Encriptação</i>	• 1.3.6.1.4.1.47281.1.8.2 • 0.4.0.194112.1.1
<i>Selo eletrónico</i>	<i>HSM Centralizado</i>	<i>Assinatura</i>	• 1.3.6.1.4.1.47281.1.8.4 • 0.4.0.194112.1.1

2.11. Autoridade Certificadora Emitidora

Estes certificados são emitidos pela ESFIRMA, identificados pelos dados indicados acima.

2.12. Validação de certificados

As listas de certificados revogados e serviços OCSP podem ser encontradas no site da esFIRMA e nos URLs indicados em cada um dos certificados.

3. Limites de utilização dos certificados

3.1. Limites de utilização direcionados a sinalizadores

O signatário deve utilizar o serviço de certificação fornecido pela esFIRMA exclusivamente para os usos autorizados no contrato assinado entre a esFIRMA e o SUBSCRITOR, e que são reproduzidos abaixo.

Da mesma forma, o signatário compromete-se a utilizar o serviço de certificação digital de acordo com as instruções, manuais ou procedimentos fornecidos pela esFIRMA.

O signatário tem de cumprir quaisquer leis e regulamentos que possam afetar o seu direito de utilizar as ferramentas criptográficas que utiliza.

O signatário não pode adotar medidas de inspeção, alteração ou engenharia reversa dos serviços de certificação digital da esFIRMA sem autorização prévia e expressa.

3.2. Limites de utilização direcionados para verificadores

Os certificados são usados para a sua própria função e propósito estabelecido, e não podem ser usados para outras funções ou para outros fins.

De igual modo, os certificados devem ser usados apenas de acordo com a legislação aplicável, especialmente tendo em conta as restrições à importação e exportação em vigor em cada momento.

Os certificados não podem ser usados para assinar pedidos de emissão, renovação, suspensão ou revogação de certificados, nem para assinar certificados de chave pública de qualquer tipo, nem para assinar listas de revogação de certificados.

Os certificados não foram concebidos, não podem ser usados nem estão autorizados para uso ou revenda como equipamentos de controlo de situações perigosas ou para usos que exijam ações de segurança em falhas, como a operação de instalações nucleares, sistemas de navegação aérea ou comunicações, ou sistemas de controlo de armas, onde uma falha possa levar diretamente à morte, Danos pessoais ou danos ambientais graves.

Devem ser tidos em conta os limites indicados nos vários campos dos perfis de certificados, visíveis no site da ESFIRMA.

O uso de certificados digitais em transações que contrariem este texto de divulgação (PDS), ou contratos com subscritores, é considerado uso impróprio para fins legais adequados, pelo que a ESFIRMA está isenta, de acordo com a legislação vigente, de qualquer responsabilidade por este uso impróprio dos certificados feito pelo signatário ou por qualquer terceiro.

O fornecedor esFIRMA não tem acesso aos dados sobre os quais pode ser aplicado o uso de um certificado. Assim, e como consequência desta impossibilidade técnica de aceder ao conteúdo da mensagem, não é possível para a esFIRMA emitir qualquer avaliação sobre esse conteúdo, pelo que o assinante ou o signatário assume qualquer responsabilidade decorrente do conteúdo associado à utilização de um certificado.

Da mesma forma, o assinante será responsável por qualquer responsabilidade que possa surgir do uso do mesmo fora dos limites e condições de uso estabelecidos neste texto de divulgação, ou nos contratos com os subscritores, bem como de qualquer outro uso indevido do mesmo derivado desta secção ou que possa ser interpretado como tal de acordo com a legislação vigente.

4. Obrigações dos subscritores

4.1. Geração de chaves

Nos certificados de cartão, o assinante autoriza o signatário a gerar as suas chaves privadas e públicas dentro de um dispositivo qualificado de criação de assinatura eletrónica, e solicita, em nome do signatário, a emissão do certificado ao esFIRMA.

Nos certificados gerados em HSM/cloud ou software, o assinante autoriza o signatário ou criador do selo a gerar as suas chaves privadas e públicas, e solicita, em nome do signatário ou criador do selo, a emissão do certificado ao esFIRMA.

4.2. Pedido de certificados

O subscritor compromete-se a fazer pedidos, quando necessário, para estes certificados de acordo com o procedimento e, se necessário, os componentes técnicos fornecidos pela ESFIRMA, de acordo com as disposições da declaração de práticas de certificação (CPD) e da documentação operacional da ESFIRMA.

4.3. Veracidade da informação

O assinante é responsável por garantir que toda a informação incluída na sua candidatura ao certificado é precisa, completa para efeitos do certificado e está sempre atualizada.

O assinante deve informar imediatamente a ESFIRMA:

- Quaisquer imprecisões detetadas no certificado após a sua emissão.

- Quaisquer alterações que ocorram na informação fornecida e/ou registada para a emissão do certificado.

4.4. Obrigações de custódia

O assinante compromete-se a salvaguardar toda a informação gerada na sua atividade enquanto entidade de registo.

5. Obrigações dos signatários e criadores de selos

5.1. Obrigações de custódia

O signatário ou criador dos selos é obrigado a salvaguardar 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 fornecidas pela esFIRMA.

No caso de perda ou roubo da chave privada do certificado, ou no caso de suspeitar que a chave privada perdeu fiabilidade por qualquer motivo, tais circunstâncias devem ser imediatamente notificadas diretamente à esFIRMA ou através do assinante.

5.2. Obrigações de uso correto

O signatário ou criador dos selos deve utilizar o serviço de certificação fornecido pela esFIRMA, exclusivamente para os usos autorizados no DPC e em quaisquer outras instruções, manuais ou procedimentos fornecidos ao assinante.

O signatário ou criador dos selos tem de cumprir quaisquer leis e regulamentos que possam afetar o seu direito de utilizar as ferramentas criptográficas utilizadas.

O signatário ou criador dos selos não pode adotar medidas para inspecionar, alterar ou descompilar os serviços digitais de certificação prestados.

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

O signatário ou criador dos selos reconhecerá:

- a) Que quando usar qualquer certificado, e desde que o certificado não tenha expirado, sido suspenso ou revogado, terá aceite esse certificado e estará operacional.
- b) Que não atua como autoridade certificadora e, por isso, compromete-se a não utilizar as chaves privadas correspondentes às chaves públicas contidas nos certificados para efeitos de assinatura de qualquer certificado.

5.3. Transações proibidas

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

Os serviços de certificação digital fornecidos pela ESFIRMA não foram concebidos e não permitem a sua utilização ou revenda como equipamento de controlo para situações perigosas, ou para usos que exijam ações à prova de erros, como a operação de instalações nucleares, sistemas de navegação aérea ou comunicação, sistemas de controlo de tráfego aéreo ou sistemas de controlo de armamentos. onde um erro pode causar diretamente a vida, danos físicos ou danos ambientais graves.

6. Obrigações dos verificadores

6.1. Decisão informada

A ESFIRMA informa o verificador que tem acesso a informação suficiente para tomar uma decisão informada no momento da verificação de um certificado e para confiar na informação contida nesse certificado.

Além disso, o verificador deve reconhecer que a utilização das Listas de Registo e Revogação de Certificados da ESFIRMA (doravante designadas como "as LRCs" ou "as CRLs") é regida pela DPC da ESFIRMA e compromete-se a cumprir os requisitos técnicos, operacionais e de segurança descritos na referida DPC.

6.2. Requisitos de Verificação de Assinatura

A verificação será normalmente realizada automaticamente pelo software do verificador e, em qualquer caso, de acordo com o DPC, com os seguintes requisitos:

- É necessário utilizar o software adequado para a verificação de uma assinatura digital com os algoritmos e comprimentos de chave autorizados no certificado e/ou para executar qualquer outra operação criptográfica, e estabelecer a cadeia de certificados na qual se baseia a assinatura eletrónica a verificar, uma vez que a assinatura eletrónica é verificada usando esta cadeia de certificados.
- É necessário garantir que a cadeia de certificados identificada seja a mais adequada para a assinatura eletrónica a verificar, uma vez que uma assinatura eletrónica pode basear-se em mais do que uma cadeia de certificados, e cabe ao verificador garantir que a cadeia mais adequada seja usada para a verificar.
- É necessário verificar o estado de revogação dos certificados na cadeia com as informações fornecidas à ESFIRMA (com LRCs, por exemplo) para determinar a validade de todos os certificados na cadeia de certificados, uma vez que apenas

Uma assinatura eletrónica pode ser considerada corretamente verificada se cada um dos certificados da cadeia estiver correto e atualizado.

- É necessário garantir que todos os certificados na cadeia autorizam o uso da chave privada pelo assinante do certificado, uma vez que existe a possibilidade de alguns dos certificados incluírem limites de utilização que impeçam a confiança na verificação da assinatura eletrónica. Cada certificado na cadeia tem um indicador que se refere às condições de utilização aplicáveis, para revisão pelos verificadores.
- É necessário verificar tecnicamente a assinatura de todos os certificados na cadeia antes de confiar no certificado utilizado pelo signatário.

6.3. Confiar num certificado não verificado

Se o verificador depender de um certificado não verificado, assumirá todos os riscos decorrentes desta ação.

6.4. Efeito da verificação

Em virtude da verificação correta destes certificados, de acordo com este texto informativo (PDS), o verificador pode confiar na identificação e, quando apropriado, na chave pública do signatário.

6.5. Uso Adequado e Atividades Proibidas

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

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

Além disso, o verificador compromete-se a não comprometer intencionalmente a segurança dos serviços públicos eletrónicos de carimbos de hora ou certificação da ESFIRMA.

Os serviços digitais de certificação fornecidos pela ESFIRMA não foram concebidos e não permitem a utilização ou revenda, como equipamentos de controlo de situações perigosas ou para usos que exijam ações à prova de erros, como a operação de instalações nucleares, sistemas de navegação aérea ou comunicação, sistemas de controlo de tráfego aéreo ou sistemas de controlo de armas. onde um erro pode causar a morte, danos físicos ou danos ambientais graves.

6.6. Cláusula de indemnização

O terceiro que confia no certificado compromete-se a isentar a ESFIRMA de quaisquer danos resultantes de qualquer ação ou omissão que resulte em responsabilidade, dano ou perda, despesas de qualquer tipo, incluindo despesas legais e de representação legal que possam ser incorridas, pela publicação e utilização do certificado, quando ocorrer qualquer uma das seguintes causas:

- Incumprimento das obrigações do terceiro que se baseia no certificado.
- Confiança imprudente num certificado, tendo em conta as circunstâncias.
- Falha em verificar o estado de um certificado, para determinar que não está suspenso ou revogado.
- Falha em verificar todas as medidas de segurança prescritas no DCP ou noutras regulamentações de implementação.

A ESFIRMA não será responsável pelos danos causados nos termos indicados no Artigo 11 da Lei 6/2020, de 11 de novembro, que regula certos aspetos dos serviços eletrónicos de trust.

7. Obrigações de ESFIRMA

7.1. No que diz respeito à prestação de certificação digital

A ESFIRMA compromete-se a:

- a) Emitir, entregar, administrar e revogar certificados, de acordo com as instruções fornecidas pelo subscritor, nos casos e pelas razões descritas no DPC ESFIRMA.
- b) Realizar os serviços com os meios técnicos e materiais adequados, e com pessoal que cumpra as qualificações e condições de experiência estabelecidas no DPC.
- c) Cumprir os níveis de qualidade do serviço, de acordo com o que está estabelecido no DPC, nos aspetos técnicos, operacionais e de segurança.
- d) Notifique o assinante, com antecedência, da data de validade dos certificados.
- e) Comunique aos terceiros que o solicitem o estado dos certificados, de acordo com o que está estabelecido no DPC para os diferentes serviços de verificação de certificados.

7.2. Em relação às verificações de registo

A ESFIRMA compromete-se a emitir certificados com base nos dados fornecidos pelo subscritor, para os quais poderá realizar as verificações que considerar adequadas.

No caso de o ESFIRMA detetar erros nos dados que devem ser incluídos nos certificados ou que justifiquem esses dados, poderá efetuar as alterações que considerar necessárias

necessário antes de emitir o certificado ou suspender o processo de emissão e gerir o incidente correspondente com o assinante. No caso de o ESFIRMA corrigir os dados sem gerir previamente o incidente correspondente com o assinante, deve notificar o assinante de que os dados foram finalmente certificados.

A ESFIRMA reserva-se o direito de não emitir o certificado quando considerar que a justificação documental é insuficiente para a identificação e autenticação corretas do assinante e/ou do domínio.

As obrigações acima referidas serão suspensas nos casos em que o assinante atue como autoridade de registo e tenha os elementos técnicos correspondentes à geração de chaves, emissão de certificados e registo de dispositivos de assinatura corporativa.

7.3. Períodos de retenção

A ESFIRMA mantém informações relativas aos serviços prestados de acordo com o artigo 24.2.h) do Regulamento (UE) 910/2014 do Parlamento Europeu, de 23 de julho de 2014, por pelo menos 15 anos a contar da expiração do certificado ou do término do serviço prestado.

A ESFIRMA armazena informação de registo por um período entre 1 e 15 anos, dependendo do tipo de informação registada.

8. Garantias Limitadas e Isenções de Garantias

8.1. Garantia ESFIRMA para serviços de certificação digital

A ESFIRMA garante ao assinante:

- Que não existem erros factuais na informação contida nos certificados, conhecidos ou emitidos pelo Organismo Certificador.
- Que não existem erros factuais na informação contida nos certificados, devido à falta de diligência devida na gestão da candidatura do certificado ou na criação do mesmo.
- Que os certificados cumpram todos os requisitos materiais estabelecidos no DPC.
- Que os serviços de revogação e a utilização do depósito cumpram todos os requisitos materiais estabelecidos no DPC.

A ESFIRMA garante ao terceiro que depende do certificado:

- Que a informação contida ou incorporada por referência no certificado está correta, exceto quando indicado em contrário.
- No caso de certificados publicados no depósito, que o certificado foi emitido ao subscritor identificado e que o certificado foi aceite.
- Que, na aprovação do pedido de certificado e na emissão do certificado, todos os requisitos materiais estabelecidos no DPC foram cumpridos.
- A rapidez e segurança na prestação de serviços, especialmente serviços de revogação e depósito.

Além disso, a ESFIRMA garante ao assinante e ao terceiro que depende do certificado:

- Que o certificado contém a informação que um certificado qualificado deve conter, de acordo com o Anexo I do Regulamento da UE 910/2014.

- Que, no caso de gerar as chaves privadas do assinante ou, quando apropriado, da pessoa física identificada no certificado, a sua confidencialidade é mantida durante o processo.
- Responsabilidade do Organismo de Certificação, dentro dos limites estabelecidos. Em nenhum caso a ESFIRMA será responsável por acontecimentos fortuitos e em caso de força maior.
- A chave privada da autoridade certificadora utilizada para emitir certificados não foi comprometida, a menos que a esFIRMA não tenha comunicado o contrário, segundo o DPC.
- Não originou nem introduziu declarações falsas ou erradas na informação de qualquer certificado, nem deixou de incluir as informações necessárias fornecidas pelo assinante e validadas pelo esFIRMA no momento da emissão do certificado.
- Todos os certificados cumprem os requisitos formais e de conteúdo do DPC, incluindo todos os requisitos legais atuais e aplicáveis.
- Está sujeita aos procedimentos operacionais e de segurança definidos no CPD.

8.2. Exclusão da Garantia

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

Especificamente, o ESFIRMA não garante qualquer software utilizado por qualquer pessoa para assinar, verificar assinaturas, encriptar, desencriptar ou utilizar qualquer certificado digital emitido pelo ESFIRMA, exceto nos casos em que exista uma declaração escrita em contrário.

9. Acordos e DPCs Aplicáveis

9.1. Acordos Aplicáveis

Os acordos aplicáveis a este certificado são os seguintes:

- Contrato de serviços de certificação, que regula a relação entre a ESFIRMA e a Entidade Jurídica que subscreve os certificados.
- Termos Gerais de Serviço incorporados neste texto de Divulgação de Certificado ou PDS.
- DPC, que regula a emissão e utilização de certificados.

9.2. CPD

Os serviços de certificação da ESFIRMA são regulados técnica e operacionalmente pelo CPD da ESFIRMA, pelas suas atualizações subsequentes, bem como por documentação complementar.

O CPD e a documentação das operações são periodicamente modificados e podem ser consultados no site: <https://www.esfirma.com>.

10. Política de Privacidade

A ESFIRMA não pode divulgar nem pode ser obrigada a divulgar qualquer informação confidencial relativa a certificados sem um pedido específico prévio de:

- a) A pessoa relativamente a quem o ESFIRMA tem o dever de manter a informação confidencial, ou
- b) Uma ordem judicial, administrativa ou qualquer outra prevista na legislação vigente.

No entanto, o subscritor concorda que certas informações, pessoais ou não, fornecidas na candidatura do certificado, serão incluídas nos seus certificados e no mecanismo de verificação do estado do certificado, e que essas informações não serão confidenciais, conforme exigido por lei.

A ESFIRMA não transfere a qualquer pessoa os dados fornecidos especificamente para a prestação do serviço de certificação.

O tratamento desses dados por terceiros para o fim de prestar um serviço à esFIRMA, incluindo, mas não se limitando a, ocorre no âmbito de uma ordem de processamento referida no artigo 28 REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 sobre a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação destes dados e à revogação da Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados) e do artigo 33 da Lei Orgânica 3/2018, de 5 de dezembro, sobre a Proteção de Dados Pessoais e Garantia dos Direitos Digitais (LOPDGDD), em virtude da qual está em conformidade com os requisitos do RGPD e da LOPDGDD, e garante a proteção dos direitos do sujeito aos dados.

11. Política de Privacidade

A ESFIRMA tem uma política de privacidade na secção 9.4 do DPC, e um regulamento específico de privacidade relativo ao processo de registo, confidencialidade do registo, proteção do acesso a informações pessoais e consentimento dos utilizadores.

A informação referida na secção 7.3 deverá ser mantida nos períodos indicados, devidamente registada e com garantias de segurança e integridade.

12. Política de Reembolso

A ESFIRMA não reembolsará o custo do serviço de certificação em circunstância alguma.

13. Legislação aplicável, jurisdição competente e regime de reclamações e litígios

As relações com a ESFIRMA serão regidas pela legislação espanhola sobre serviços fiduciários em vigor em todos os momentos, bem como pela legislação civil e comercial, conforme aplicável.

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

Em caso de divergência entre as partes, estas devem tentar um acordo amigável prévio. Para tal, as partes devem enviar uma comunicação à esFIRMA, preenchendo o formulário de reclamação e sugestão disponível no site da esFIRMA por qualquer dos meios aí indicados. A queixa será tratada de acordo com os procedimentos internos para a resolução de queixas, recursos e litígios.

Se as partes não chegarem a acordo a este respeito, qualquer uma delas pode submeter a disputa à jurisdição civil, sujeita aos Tribunais da sede registada da ESFIRMA.

13.1. Acreditações e selos de qualidade

A EsFIRMA possui a qualificação "compatível com eIDAS" para os seguintes serviços:

- a) Serviço para a emissão de certificados eletrónicos qualificados para assinatura eletrónica.
- b) Serviço para a emissão de certificados eletrónicos qualificados com selo eletrónico.
- c) Serviço para a emissão de certificados eletrónicos qualificados para autenticação de websites.
- d) Serviço de emissão de carimbos eletrónicos eletrónicos qualificados.

13.2. Ligação para a lista de prestadores

A EsFIRMA é um prestador qualificado de serviços de certificação e, por isso, faz parte da Lista de Prestadores Qualificados (TSL) mantida pelo supervisor nacional e que pode ser obtida no seguinte endereço: <https://sedeaplicaciones.minetur.gob.es/Prestadores/>

A EsFIRMA está incluída na "Lista de Trusts" da União Europeia como Prestadora Qualificada

dos serviços fiduciários eletrónicos:

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

13.3. Separabilidade dos termos, sobrevivência, acordo total e notificação

As disposições deste texto de divulgação (PDS) são independentes umas das outras, pelo que, se alguma cláusula for considerada inválida ou inexecutável, as restantes cláusulas do PDS continuarão a aplicar-se, salvo acordo expresso em contrário entre as partes.

Os requisitos contidos nas secções "Obrigações e Responsabilidade", "Auditoria de Conformidade" e "Confidencialidade" do DPC da ESFIRMA permanecerão em vigor após a cessação do serviço.

Este texto contém o testamento completo e todos os acordos entre as partes.

As partes notificam-se mutuamente dos factos através de um procedimento enviado por email para a morada info@esfirma.com