

**Texto de Divulgação do Certificado de
Autoridade Qualificada com Carimbo
Eletrónico Temporal (PDS)**



Índice

1.	Informações de Contacto	6
1.1.	Organização responsável	6
1.2.	Contacto	6
1.3.	Contacto para processos de revogação	6
2.	Tipo e finalidade do certificado	7
2.1.	Autoridade Certificadora Emitidora	8
3.	Limites de utilização dos certificados	8
3.1.	Limites de utilização direccionados a sinalizadores	8
3.2.	Limites de utilização direccionados para verificadores	8
4.	Obrigações dos subscritores	9
4.1.	Geração de chaves	9
4.2.	Pedido de certificados	9
4.3.	Obrigações de reporte	10
4.4.	Obrigações de custódia	10
4.5.	Obrigações de uso correto	10
4.6.	Transações proibidas	11
5.	Obrigações dos verificadores	11
5.1.	Decisão informada	11
5.2.	Requisitos de Verificação de Carimbo Temporal	12
5.3.	Confiar num certificado não verificado	12
5.4.	Uso Adequado e Atividades Proibidas	13
5.5.	Cláusula de indemnização	13
6.	Obrigações de ESFIRMA	14
6.1.	No que diz respeito à prestação de certificação digital	14

ESFIRMA: *Certificado tsa/tsu PDS*

6.2.	Em relação às verificações de registo	14
6.3.	Períodos de retenção	15
7.	Garantias Limitadas e Isenções de Garantias	15
7.1.	Garantia ESFIRMA para serviços de certificação digital	15
7.2.	Exclusão da Garantia	17
8.	Acordos e políticas	17
8.1.	Acordos Aplicáveis	17
8.2.	CPD	17
8.3.	Política de Privacidade	17
8.4.	Política de Privacidade	18
8.5.	Política de Reembolso	18
8.6.	Lei aplicável e jurisdição competente	18
8.7.	Acreditações e selos de qualidade	19
8.8.	Ligação para a lista de prestadores	19
8.9.	Separabilidade dos termos, sobrevivência, acordo total e notificação	19

Certificado de Selo Eletrónico da Autoridade de Carimbagem Eletrónica

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.

Informação Geral

Controlo de documentos

Classificação de Segurança:	Público
Entidade-alvo:	ESFIRMA
Versão:	1.7

Controlo de Versões

Versão	Partes que mudam	Descrição da mudança	Autor da alteração	Data da alteração
1.0	Original	Criação de documentos	esFIRMA	7/05/2017
1.4		Correções	esFIRMA	7/06/2017
1.5	1.1 -1.3 8.6	Mudança de nome	esFIRMA	6/11/2017
1.6	1.3	Foi adicionada uma referência ao site da esFIRMA.	esFIRMA	21/04/2023
1.7	2 8.6	Referência ao BTSP adicionada Acrescentou referência ao procedimento de resolução de litígios	esFIRMA	05/06/2026

1. Informações de Contacto

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 (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 (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 (EDIFÍCIO BINÁRIO)
50197 - ZARAGOZA
(+34) 976300110

2. Tipo e finalidade do certificado

Este certificado tem os seguintes OIDs e declarações de conformidade associadas:

- 1.3.6.1.4.1.47281.1.5.2: Identificador próprio segundo a hierarquia ESFIRMA.
- 0.4.0.194112.1.1: Identificador de Política da UE (QCP-I)
- 0.4.0.2023.1.1 (itu-t(0) organização-identificada(4) etsi(0) política de carimbo temporal(2023) identificadores de política(1) melhores práticas-ts-política (1): Identificador de Política de Boas Práticas para carimbos temporais (BTSP).

De acordo com os requisitos regulamentares aplicáveis, a TSA da ESFIRMA apoia, apoia e inclui explicitamente o identificador BTSP, indicando assim a sua declaração formal de conformidade com a referida norma de melhores práticas do setor.

Os certificados da Autoridade Eletrónica de Carimbo Temporal são certificados 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 as referências ETSI EN 319 412-3. ETSI EN 319 421 e ETSI EN 319 422.

Estes certificados permitem a assinatura de provas digitais da hora eletrónica.

A informação de utilização no perfil do certificado indica o seguinte:

- a) O campo "uso de chaves" ativou, e por isso permite-nos executar, as seguintes funções:
 - a. Compromisso de conteúdo (para desempenhar a função de assinatura eletrónica)
- b) No campo "extKeyUsage", é ativada a seguinte indicação:
 - a. "timeStamping" para realizar a função eletrónica de timestamping.
- c) No campo "Declarações de Certificado Qualificadas", aparece a seguinte declaração:
 - a. qCCcumprimento (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.

2.1. Autoridade Certificadora Emitidora

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

3. Limites de utilização dos certificados

3.1. Limites de utilização direcionados a sinalizadores

Deve ser utilizado o serviço qualificado de carimbo eletrónico de data, fornecido pela ESFIRMA exclusivamente para os usos autorizados no contrato assinado entre a ESFIRMA e o ASSINANTE, e que são reproduzidos posteriormente (secção "obrigações dos signatários").

O serviço eletrónico de carimbo temporal deve ser utilizado de acordo com as instruções, manuais ou procedimentos fornecidos pela ESFIRMA.

Quaisquer leis e regulamentos que possam afetar a utilização das ferramentas criptográficas que utiliza devem ser cumpridos.

Não podem ser tomadas inspeções, alterações ou medidas de engenharia reversa para os serviços eletrónicos de carimbo temporal 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 (LRCs).

ESFIRMA: *Certificado tsa/tsu PDS*

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.

Os limites indicados nos vários campos dos perfis de certificados, visíveis no site da ESFIRMA, devem ser tidos em conta <https://www.esfirma.com>

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.

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

O subscritor autoriza a ESFIRMA a gerar as chaves, privadas e públicas, para a emissão deste certificado.

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. Obrigações de reporte

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.
- Da perda, roubo, roubo ou qualquer outro tipo de perda de controlo da chave privada pelo custodiante.

4.4. Obrigações de custódia

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

Para salvaguardar o código de identificação pessoal ou qualquer suporte técnico fornecido pela ESFIRMA, as chaves privadas e, se necessário, as especificações detidas pela ESFIRMA que lhe são fornecidas.

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 à ESFIRMA através do assinante.

4.5. Obrigações de uso correto

O certificado deve ser utilizado apenas para os usos autorizados no DPC e em quaisquer outras instruções, manuais ou procedimentos fornecidos ao assinante.

Quaisquer leis e regulamentos que possam afetar o seu direito de utilizar as ferramentas criptográficas utilizadas devem ser cumpridos.

Não podem ser adotadas medidas para inspecionar, alterar ou descompilar os serviços digitais de certificação prestados.

Além disso:

- a) Que quando qualquer certificado for utilizado, e desde que o certificado não tenha expirado, sido suspenso ou revogado, esse certificado terá sido aceite 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.
- c) Que, caso a chave privada seja comprometida, o seu uso é imediatamente e permanentemente suspenso.

4.6. Transações proibidas

Está indicada a obrigação de não utilizar as chaves privadas, certificados ou qualquer outro suporte técnico prestado pela ESFIRMA na execução de qualquer transação proibida pela lei aplicável.

Os serviços digitais de certificação (e os serviços de carimbo eletrónico temporal) fornecidos pela ESFIRMA não foram concebidos e não permitem a sua utilização ou revenda como equipamentos de controlo de situações perigosas, nem 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 armamento, onde um erro pode causar diretamente a vida, danos físicos ou danos ambientais graves.

5. Obrigações dos verificadores

5.1. 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 deverá reconhecer que a utilização do Registo ESFIRMA e das Listas de Revogação de Certificados (doravante designados como "os LRCs" ou "CRLs") é regido pelo DPC ESFIRMA e compromete-se a cumprir os requisitos técnicos, operacionais e de segurança descritos no referido DPC.

5.2. Requisitos de Verificação de Carimbo Temporal

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 um carimbo temporal com os algoritmos e comprimentos de chave autorizados no certificado e/ou para executar qualquer outra operação criptográfica, e para estabelecer a cadeia de certificados em que o carimbo temporal a verificar se baseia, uma vez que é verificado usando esta cadeia de certificados.
- É necessário garantir que a cadeia de certificados identificada é a mais adequada para o carimbo temporal a ser verificado, uma vez que um carimbo temporal pode basear-se em mais do que uma cadeia de certificados, e cabe ao verificador garantir que a cadeia mais adequada seja usada para o verificar.
- É necessário verificar o estado de revogação dos certificados na cadeia com as informações fornecidas ao Registo ESFIRMA (com LRCs, por exemplo) para determinar a validade de todos os certificados na cadeia de certificados, uma vez que um carimbo temporal só pode ser verificado corretamente se cada um dos certificados da cadeia estiver correto e atualizado.
- É necessário garantir que todos os certificados da cadeia autorizam o uso da chave privada pelo assinante do certificado, pois existe a possibilidade de alguns dos certificados incluírem limites de utilização que impeçam a confiança na verificação do carimbo temporal. 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 para carimbo eletrónico de data.

5.3. Confiar num certificado não verificado

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

5.4. 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 de carimbo eletrónico e certificação digital fornecidos pela ESFIRMA não foram concebidos e não permitem a utilização ou revenda de equipamentos de controlo de situações perigosas nem 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.

5.5. 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.

ESFIRMA: *Certificado tsa/tsu PDS*

- Falha em verificar todas as medidas de segurança prescritas no DCP ou noutras regulamentações de implementação.

A ESFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

6. Obrigações de ESFIRMA

6.1. No que diz respeito à prestação de certificação digital

A ESFIRMA compromete-se a:

- a) Emitir, entregar, administrar, suspender, revogar e renovar certificados, de acordo com as instruções fornecidas pelo subscritor, nos casos e 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.

6.2. 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 a ESFIRMA detetar erros nos dados que devem ser incluídos nos certificados ou que justifiquem esses dados, pode fazer as alterações que considerar necessárias antes

ESFIRMA: Certificado tsa/tsu PDS

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.

6.3. Períodos de retenção

A ESFIRMA arquiva os registos correspondentes a pedidos de emissão e revogação de certificados por pelo menos 15 anos.

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

7. Garantias Limitadas e Isenções de Garantias

7.1. 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.

ESFIRMA: *Certificado tsa/tsu PDS*

- 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 armazém, certifica-se que o certificado foi emitido ao assinante e ao domínio 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 eletrónico qualificado deve conter, de acordo com o Anexo III do Regulamento (UE) 910/2014 do Parlamento Europeu, do Conselho de 23 de julho de 2014, e com as indicações adicionais para a criação de carimbos temporais qualificados de acordo com o Artigo 42 deste Regulamento.
- Que, caso gere as chaves privadas do assinante, 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.

7.2. 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, descriptar ou utilizar qualquer certificado digital emitido pelo ESFIRMA, exceto nos casos em que exista uma declaração escrita em contrário.

8. Acordos e políticas

8.1. 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 empresa que subscreve os certificados.
- Termos Gerais de Serviço incorporados no texto de divulgação do certificado ou PDS.
- DPC, que regula a emissão e utilização de certificados.

8.2. CPD

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

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

8.3. 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:

ESFIRMA: *Certificado tsa/tsu PDS*

- a) A pessoa em relação a quem a 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.

8.4. 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.

Da mesma forma, prevê-se que a documentação que justifica a aprovação do pedido deve ser mantida e devidamente registada, com garantias de segurança e integridade por um período de 15 anos a contar da expiração do certificado, incluindo tudo em caso de perda antecipada de validade devido à revogação.

8.5. Política de Reembolso

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

8.6. Lei aplicável e jurisdição competente

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.

ESFIRMA: Certificado tsa/tsu PDS

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 ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN SA.

8.7. Acreditações e selos de qualidade

Sem estipulação.

8.8. Ligação para a lista de prestadores

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

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

As cláusulas deste texto de divulgação são independentes umas das outras, pelo que, se alguma cláusula for considerada inválida ou inexecutável, as restantes cláusulas do PDS continuarão a ser aplicáveis, salvo acordo expresse em contrário entre as partes.

Os requisitos contidos nas secções 9.6.1 (Obrigações e Responsabilidade), 8 (Auditoria de Conformidade) e 9.3 (Confidencialidade) do DPC da ESFIRMA continuarão a aplicar-se 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 enviando um email para o endereço info@esfirma.com