Declaração de Práticas de Certificação

esFIRMA

Visão geral

Controlo de documentos

Classificação de segurança:	Público
Autor:	ESFIRMA
Versão:	1.19

Estatuto formal

Preparado por:	Avaliado por:	Aprovado por:
Serviço de Segurança Data: 10/03/2025	Gestor de Segurança Data: 10/03/2025	Comité de Segurança Data: 17/03/2025

Controle de versão

Ver	Descrição da alteração	Data
1.0	Criação de documentos	29/04/2016
1.1	Correções	02/06/2016
1.2	Revisão do ETSI	19/05/2017
1.3	Revisão dos tipos de certificados	
1.4	Revisar tipos de certificados, siglas e definições	02/06/2017
1.5	Ajustes de referência regulamentar, mudança de nome, mudança de certificados 1.3.2, 1.3.3.1, 1.3.3.2, 1.4.1.8, 3.1.1.8, 4.3.1, 6.1.5, 9.2.1, 9.4, 9.6.2, 9.6.4	06/11/2017
1.6	6.1.1 Duração da TSA	20/06/2018
1.7	Correção relativa à assinatura na emissão de certificados de software	08/08/2018
1.8	Adaptação devido a alterações regulamentares (Regulamento (UE) n.º 910/2014 e Regulamento (UE) 2016/679) e revisão das secções de renovação.	13/11/2018
1.9	3.1.1.1 Clarificação do segundo apelido facultativo. 3.1.1.2 OrganizationIdentifier condicional às Diretrizes do Fórum da CA/Navegador 3.1.1.4 Ajustando para erros tipográficos em descrições OID 3.1.1.7 NC do certificado EV da sede opcional	14/06/2019
1.10	Esclarecimentos diversos nos pontos 1.2.1, 1.5.4, 2.3, 3.2, 3.2.4-6, 4.1.1, 4.2.1-2, 4.3.1, 4.9.3, 4.9.10-11, 4.11.1-2, 5.2.2, 5.4.3, 5.4.8, 6.1.1, 6.1.5, 6.1.9, 6.2.5, 6.3.2, 6.5.1, 7.1, 7.1.4, 8.1 Alinhamento RFC 3647 1.5.3. movido para 1.5.2 Dados de contacto da organização 1.5.2 movido para 1.5.3 Organização que aprova o documento "SIGLAS DE DEFINIÇÕES" movido para 1.6 Acrónimos e definições 4.4.2 Transferido para 4.4.1 Conduta que constitui aceitação de certificado 4.4.3 Transferido para 4.4.2 Publicação do certificado 4.4.4 Transferido para 4.4.3 Notificação de Emissão a Terceiros Adicionado 4.6.1 Circunstâncias para a renovação do certificado Adicionado 4.6.2 Quem pode solicitar uma renovação Adicionado 4.6.3 Processamento de solicitação de renovação de certificado Adicionada 4.6.4 Notificação de reemissão de certificado ao assinante Adenda 4.6.5 Conduta que constitui a aceitação de um certificado de renovação Aditado 4.6.6 Publicação do certificado de renovação pela autoridade de certificação Acrescentado 4.6.7 Notificação da emissão do certificado pela AC a outras entidades Aditado 4.7.2 Procedimento com nova identificação 4.7. Movido para 4.7.3 Processando novas solicitações de chave de certificado 4.7.3 Transferido para 4.7.4 Notificação de emissão de certificado renovado 4.7.4 Transferido para 4.7.5 Conduta que constitui aceitação do certificado 4.7.5 Transferido para 4.7.6 Publicação do certificado 4.7.6 transferido para 4.7.7 Notificação da emissão a terceiros 4.11 movido para 4.10 Serviços de verificação de integridade de certificados 4.11.1 Transferido para 4.10.1 Características operacionais dos serviços 4.11.2 transferido para 4.10.2 Disponibilidade dos serviços Adicionado 4.10.3 Recursos opcionais 4.10 movido para 4.11 Rescisão da Subscrição 6.1.9 movido para 6.1.7 Finalidades do uso de chaves 6.2.9 Movido para 6.2.9 Método de Desativação de Chave Privada 6.2.10 movido para 6.2.10 Método de Destruição de Chave Privada Adicionada 6.2.11 Classificação do módulo criptográfico Adicionado 6.4.3 Outros aspetos dos dados de ativação	08/06/2020

	6.6.2.5 transferido para 6.6.3 Avaliação da Segurança do Ciclo de Vida 6.9 movido para 6.8 Fontes de tempo Adicionado 7.1.7 Usando a extensão de restrições de política Adicionado 7.1.8 Qualificadores de política, sintaxe e semântica Adicionada 7.1.9 Processando semântica para extensão crítica de políticas de certificado Adicionadas extensões de CRL e CRL 7.2.2 Adicionado número de versão 7.3.1 Adicionadas extensões OCSP 7.3.2 Adicionado 9.4.1 Plano de Privacidade Adicionada 9.4.2 Informação tratada como privada Adicionada 9.4.3 Informação Não Considerada Privada Adicionado 9.4.4 Responsabilidade de proteger informações privadas Adicionado 9.4.5 Aviso e Consentimento para Uso de Informações Privadas Acrescentado 9.4.6 Divulgação nos termos de processo judicial ou administrativo Acrescentado 9.4.7 Outras circunstâncias de divulgação de informações Adicionadas 9.6.2 Representações e garantias RA 9.6.2 Transferido para 9.6.3 Garantias oferecidas a assinantes e terceiros que dependem de certificados Acrescentado 9.6.4 Obrigação e Responsabilidade de Terceiros 9.6.2 Transferido para 9.6.5 Obrigação e Responsabilidade dos Outros Participantes 9.6.3 movido para 9.7 Declaração de exoneração de responsabilidade 9.6.4 transferido para 9.8 Limitação de responsabilidade em caso de perdas na transação 9.6.5 transferido para 9.9 Indemnizações Adicionado 9.10. Prazo e Conclusão Acrescentado 9.10.1 Termo Adicionado 9.10.2 Conclusão Adicionado 9.10.3 Terminação e efeito de sobrevivência Adicionado 9.11 Notificações individuais e comunicação com os participantes Adicionadas 9.12 Modificações Aditamento 9.12.1 Processo de alteração Aditado 9.12.2 Mecanismo de notificação e prazos Adicionado 9.12.3 Circunstâncias em que o OID deve ser alterado 9.6.10 transferido para 9.13 Procedimento de resolução de litígios 9.6.7 transferido para 9.14 Lei aplicável Adicionado 9.15 Conformidade com a Lei Aplicável Aditado 9.16 Outras disposições Adicionado 9.16.1 Acordo Integral Adicionada 9.16.2 Atribuição 9.6. Transferido para 9.16.3 Separabilidade Adicionado 9.16.4 Conformidade (honorários advocatícios e isenção de dever) 9.6.6 Transferido para 9.16.5 Força Maior Aditado 9.17 Outras disposições Novos certificados estão incluídos: certificado de funcionário público (Autenticação), certificado de funcionário público com pseudônimo (Autenticação), certificado de pessoa física vinculada a entidade (Autenticação), certificado de pessoa física vinculada a entidade (FIRMA), certificado de pessoa física com pseudônimo vinculado a entidade (Autenticação), certificado de pessoa física com pseudônimo vinculado a entidade (FIRMA)	
1.11	Novos certificados de selo eletrônico qualificados estão incluídos O perfil de certificado do e-Office é excluído. Adaptação por alteração regulamentar (Lei n.º 6/2020, de 11 de novembro, que regula determinados aspetos dos serviços de confiança eletrónicos).	03/05/2021

	A Seção 5.8 Rescisão do Serviço DPC adiciona o detalhe de como as informações de status dos certificados são fornecidas além de sua vida útil. As referências ao Ministério da Indústria, Energia e Turismo são atualizadas pelo Ministério da Economia e Transformação Digital.	
1.12	O ponto 5.2.1 é alterado alterando o nome de "Administrador do Registo" para "Operador do Registo". As referências ao Fórum CA/B são removidas.	10/05/2021
1.13	Ponto de Modificação 5.8 Cessação do Serviço, de acordo com o Plano de Rescisão A secção 4.9.1 é alterada para incluir o fim da certificação QSCD Ponto 6.5.1 da modificação, incluindo o fim da certificação DCCF. Supressão da referência ao documento de segurança esFIRMA da secção 6.6.2 (Operações de gestão) Substituição de "política de segurança" por "sistema de gestão da segurança da informação" na secção 6.6.2 (Classificação e gestão da informação e da propriedade) O ponto 6.9 é aditado em conformidade com ETSI TS 119 431-1: OVR-5.1-02 O ponto 9.6.4 é alterado, incluindo a cadeia de certificação como ponto de verificação. O sistema de integração com DIR3 é adicionado como um meio de verificar a identidade da entidade (3.2.2) A verificação do estatuto dos certificados na cadeia de certificação é aditada no ponto 4.9.6.	18/07/2022
1.14	Novas informações sobre o certificado TSA	16/03/2023
1.15	Configurações, informações sobre TSA e incorporação de carimbo de data/hora não qualificado	31/03/2023
1.16	Novas restrições de comprimento do elemento de perfil de certificado Novos subperfis europeus para pessoas singulares e selo eletrónico Simplificação dos pontos 3.2.2 e 3.2.3 O ponto 4.5.3 é aditado para separar as informações e obrigações de terceiros que se baseiam em certificados. Diferenças e considerações entre consultas de status de revogação de certificado usando OCSP e CRL 4.10.1	21/04/2023
1.17	A possibilidade de transferir a gestão dos certificados emitidos para outro prestador em caso de cessação do serviço é eliminada da secção 5.8.	10/02/2024
1.18	Está incluído o tempo máximo entre a validação da identidade e a emissão do certificado (ponto 3.2.3.2) Está incluído um processo excecional no caso de não ser possível confirmar o pedido de revogação em menos de 24 horas (secção 4.9.5) Novo ponto 1.4.3. Emissão de certificados de ensaio	26/07/2024
1.19	Revisão do ponto 9.11	17/03/2025

Índice

1. Introdução

1.1 Apresentação

Este documento declara as práticas de certificação de assinatura eletrônica da esFIRMA.

Os certificados emitidos são os seguintes:

- **Funcionário Público (FIRMA)**
  - de funcionário público de nível médio
  - Funcionário Público de Alto Nível
- **Funcionário Público (AUTENTICAÇÃO)**
  - Funcionário Público de Alto Nível
- **De Funcionário Público com pseudônimo (FIRMA)**
  - de funcionário público de nível médio
  - Funcionário Público de Alto Nível
- **De Funcionário Público com pseudônimo (AUTENTICAÇÃO)**
  - Funcionário Público de Alto Nível
- **De uma pessoa singular ligada a uma entidade (FIRMA)**
  - De uma pessoa singular ligada a uma entidade de nível intermédio
  - De uma pessoa singular ligada a uma entidade de alto nível
- **De uma pessoa singular ligada a uma entidade (AUTENTICAÇÃO)**
  - De uma pessoa singular ligada a uma entidade de alto nível
- **De um indivíduo ligado a uma entidade com um pseudónimo (FIRMA)**
  - De uma pessoa singular ligada a uma entidade de nível intermédio

    - De uma pessoa singular ligada a uma entidade de alto nível
- **De uma pessoa singular ligada a uma entidade com um pseudónimo (AUTENTICAÇÃO)**
    - De uma pessoa singular ligada a uma entidade de alto nível
- **Selo de Órgão**
    - Selo de Órgão Nível Médio
- **Selo Eletrônico para TSA/TSU**
    - Selo eletrônico para TSU em HSM
- **Selo Eletrónico**
    - Selo eletrónico em software
    - Selo eletrónico com gestão centralizada

1.2 Nome e identificação do documento

Este documento é a "Declaração de Práticas de Certificação" da esFIRMA.

1.2.1 Identificadores de certificado

Número OID	Políticas de certificado
	Funcionário Público (FIRMA)
1.3.6.1.4.1.47281.1.1.1	*Funcionário Público – Alto nível no cartão*
1.3.6.1.4.1.47281.1.1.4	*Funcionário Público – Nível Intermediário em HSM*
	Funcionário Público (AUTENTICAÇÃO)
1.3.6.1.4.1.47281.1.1.5	*Funcionário Público – Alto nível no cartão*
	De Funcionário Público com Pseudônimo (ASSINATURA)
1.3.6.1.4.1.47281.1.3.1	*Do EP com Pseudónimo – High Level on Card*
1.3.6.1.4.1.47281.1.3.4	*PE com Pseudónimo – Nível Intermédio em HSM*
	Funcionário Público Pseudónimo (AUTENTICAÇÃO)
1.3.6.1.4.1.47281.1.3.5	*Do EP com Pseudónimo – High Level on Card*
	De Pessoa Física vinculada a entidade (FIRMA)

1.3.6.1.4.1.47281.1.6.1	*Da PF vinculada à entidade – Assinatura Eletrônica Qualificada, em Cartão*
1.3.6.1.4.1.47281.1.6.4	*PF vinculado a entidades – Assinatura eletrônica centralizada*
	De uma pessoa singular ligada a uma entidade (AUTENTICAÇÃO)
1.3.6.1.4.1.47281.1.6.5	*PF vinculada a entidades – on Card*
	De uma pessoa singular com um pseudónimo ligado a uma entidade (FIRMA)
1.3.6.1.4.1.47281.1.7.1	*Da PF com pseudônimo vinculado a uma entidade – Assinatura Eletrônica Qualificada, em Cartão*
1.3.6.1.4.1.47281.1.7.4	*De PF com pseudónimo ligado a uma entidade – Firma-e Centralizado*
	De uma Pessoa com um pseudônimo, vinculado a uma entidade (AUTENTICAÇÃO)
1.3.6.1.4.1.47281.1.7.5	*Da PF com pseudônimo, vinculado a entidade – em Cartão*
	Selo de Órgão
1.3.6.1.4.1.47281.1.2.2	*Selo de Órgão – Nível Intermédio em Software*
1.3.6.1.4.1.47281.1.2.4	*Selo de Órgão – Nível Intermediário em HSM*
	Selo Eletrônico para TSA/TSU
1.3.6.1.4.1.47281.1.5.1	*E-Seal para TSA/TSU em HSM*
1.3.6.1.4.1.47281.1.5.2	*Selo eletrônico qualificado TSA/TSU em HSM*
	Selo Eletrónico
1.3.6.1.4.1.47281.1.8.2	*Selo Eletrônico em Software*
1.3.6.1.4.1.47281.1.8.4	*Selo Eletrônico Centralizado*

Em caso de contradição entre esta Declaração de Práticas de Certificação e outros documentos de práticas e procedimentos da esFIRMA, prevalecerão as disposições desta Declaração de Práticas.

Este documento está estruturado de acordo com IETF RFC 3647.

1.3 Participantes em serviços de certificação

1.3.1. Prestador de serviços de certificação

O prestador de serviços de certificação é a pessoa, singular ou coletiva, que emite e gere certificados para entidades finais, recorrendo a um Organismo de Certificação, ou prestando outros serviços relacionados com assinaturas eletrónicas.

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (ANTERIORMENTE AULOCE SA), adiante ESPUBLICO, com sede na Calle Bari 39 (Edif. Binary Building), C.P. 50.197, Zaragoza, CIF A-50.878.842, inscrita no Registo Mercantil de Saragoça no volume 2.649, fólio 215, página Z-28722, e que opera sob a designação comercial esFIRMA, designação comercial que será utilizada em todo o presente documento para a designar, é um prestador de serviços de certificação que atua em conformidade com o disposto no regime de obrigações e responsabilidades do Regulamento (UE) n.º 910/2014, da Lei n.º 6/2020, de 11 de novembro, que regula determinados aspetos dos serviços de confiança eletrónicos, da Lei Orgânica 3/2018, de 5 de dezembro, relativa à Proteção de Dados Pessoais e garantia dos direitos digitais e das normas técnicas do ETSI aplicáveis à emissão e gestão do Número de certificados qualificados, principalmente ETSI EN 319 411-1 e ETSI EN 319 411-2, a fim de facilitar o cumprimento dos requisitos legais e o reconhecimento internacional dos seus serviços.

Para a prestação de serviços de certificação, a esFIRMA estabeleceu uma hierarquia de organismos de certificação:

enFIRMA AC raiz 2

Esta é a autoridade de certificação raiz na hierarquia que emite certificados para outras autoridades de certificação e cujo certificado de chave pública foi autoassinado.

Dados de identificação:

NC:	ESFIRMA AC RAIZ 2 |
Impressão digital SHA-256:	C6:09:F9:4F:9C:CE:20:CB:2B:A0:2E:8B:5B:33:55:20:06:C1:5D :17:78:32:26:11:07:0F:A1:4F:FF:9D:C9:16
Válido a partir de:	2017-11-02T12:52:43Z

Válido até:	2042-11-02T12:52:43Z
Comprimento da chave RSA:	4.096 bits

ASSINATURA AC AAPP 2

Esta é a autoridade de certificação dentro da hierarquia que emite certificados para as entidades finais, e cujo certificado de chave pública foi assinado digitalmente por "esFIRMA AC RAÍZ 2".

Dados de identificação:

NC:	ESFIRMA AC AAPP 2
Impressão digital SHA-256:	2C:18:23:61:9D:80:73:11:6C:8F:14:8B:D3:85:79:DE:9C:05:39:16:02:DB:CE:B9:65:73:E4:A1:88:E1:32:6E
Válido a partir de:	2017-11-02T13:12:47Z
Válido até:	2030-11-02T13:12:47Z
Comprimento da chave RSA:	4.096 bits

Plataforma de Administração Electrónica

É a plataforma exclusiva de gestão do ciclo de vida do certificado para aplicação, aprovação, emissão e revogação.

Para completar a informação sobre as funcionalidades da Plataforma de Administração Eletrónica nos serviços de certificação, consulte a respetiva documentação.

1.3.2 Autoridades de registo

Uma autoridade de registo procede à verificação e identificação dos requerentes de certificados.

Em geral, o próprio prestador de serviços de certificação atua como autoridade de registo da identidade dos assinantes de certificados.

As autoridades de registro dos certificados sujeitos a esta Declaração de Práticas de Certificação, devido à sua condição de certificados corporativos, são também as unidades designadas para esta função pelos subscritores dos certificados, tais como o Secretário da corporação, o departamento pessoal ou o Representante Legal da Administração, desde que possuam os registros autênticos sobre a relação dos signatários com o assinante.

As funções de registo de assinantes são desempenhadas por delegação e de acordo com as instruções do prestador de serviços de certificação, nos termos definidos pelo Regulamento (UE) n.º 910/2014 e pela Lei n.º 6/2020, de 11 de novembro, que regula determinados aspetos dos serviços de confiança eletrónicos, e sob total responsabilidade do prestador de serviços de certificação perante terceiros.

1.3.3 Entidades Finais

As entidades finais são as pessoas e organizações destinatárias dos serviços de emissão, gestão e utilização de certificados digitais, para a utilização de identificação e assinatura eletrónica.

Serão as entidades finais dos serviços de certificação esFIRMA:

1. Subscritores do serviço de certificação.
2. Signatários.
3. Peças de utilizador.

1.3.4 Partes Utilizadoras

Os usuários são os indivíduos e organizações que recebem assinaturas digitais e certificados digitais.

Como prelúdio para confiar em certificados, os usuários devem verificá-los, conforme estabelecido nesta declaração de práticas de certificação e nas instruções correspondentes disponíveis no site da Autoridade de Certificação.

1.3.5 Outros participantes

Subscritores do Serviço de Certificação

Os subscritores do serviço de certificação são as administrações públicas ou entidades que os adquirem à esFIRMA para utilização no seu ambiente empresarial ou organizacional, e estão identificados nos certificados.

O assinante do serviço de certificação adquire uma licença de utilização do certificado, para uso próprio – certificados de selo eletrónico – ou para facilitar a certificação da identidade de uma pessoa específica devidamente autorizada para diversas ações no domínio organizacional do assinante – certificados de assinatura eletrónica. Neste último caso, essa pessoa é identificada no certificado, conforme previsto na secção seguinte.

O assinante do serviço de certificação é, por conseguinte, o cliente do prestador de serviços de certificação, em conformidade com o direito comercial, e tem os direitos e obrigações definidos pelo prestador de serviços de certificação, que são adicionais e não prejudicam os direitos e obrigações dos signatários, tal como autorizados e regulamentados nas normas técnicas europeias aplicáveis à emissão de certificados eletrónicos qualificados, em especial ETSI EN 319 411-2, pontos 5.4.2 e 6.3.4.e)

Signatários

Os signatários são as pessoas singulares que possuam ou tenham sob o seu controlo exclusivo, de acordo com o regime de obrigações e responsabilidades do Regulamento (UE) n.º 910/2014 e da Lei n.º 6/2020, de 11 de novembro, que regula determinados aspetos dos serviços de confiança eletrónicos, as chaves de assinatura digital para identificação e a assinatura eletrónica avançada ou qualificada; sendo tipicamente os titulares ou membros dos órgãos de administração, nos certificados de assinatura eletrónica do organismo, as pessoas ao serviço das Administrações Públicas, nos certificados dos funcionários públicos ou das pessoas que pertencem a uma entidade, nos certificados das pessoas singulares ligadas.

Os signatários estão devidamente autorizados pelo subscritor e devidamente identificados na certidão pelo seu nome e apelidos, e número de identificação fiscal válido

na jurisdição de emissão da certidão, ou com o pseudónimo correspondente nas certidões deste tipo.

Dada a existência de certificados para outras utilizações que não as assinaturas eletrónicas, como a identificação, é também utilizado o termo mais genérico "pessoa singular identificada no certificado", sempre com pleno respeito pelo cumprimento da legislação relativa às assinaturas eletrónicas no que respeita aos direitos e obrigações do signatário.

1.4 Utilização dos certificados

Esta seção lista os aplicativos para os quais cada tipo de certificado pode ser usado, define limitações para determinados aplicativos e proíbe certos aplicativos de certificados.

1.4.1 Utilizações permitidas para certificados

Devem ser tidas em conta as utilizações permitidas indicadas nos vários campos dos perfis de certificados, visíveis no sítio Web da https://www.esfirma.com

Certificado de Funcionário Público de Alto Nível no Cartão

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.1.1	Na hierarquia do CA esFIRMA
0.4.0.194112.1.2	De acordo com a política QCP-n-qscd
2.16.724.1.3.5.7.1	Funcionário público espanhol de alto nível

Os certificados das pessoas singulares de funcionários públicos de alto nível são certificados qualificados em conformidade com o artigo 28.º e o anexo I do Regulamento (UE) n.º 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.

Estas certidões são emitidas aos funcionários públicos para os identificar como pessoas ao serviço da Administração, órgão, entidade de direito público ou outra entidade, vinculando-os a esta, cumprindo os requisitos estabelecidos no artigo 43.º da Lei n.º 40/2015, de 1 de outubro, relativa ao Regime Jurídico do Setor Público, para a assinatura eletrónica do pessoal ao serviço das Administrações Públicas.

Os certificados de pessoas singulares de alto nível de funcionário público trabalham com um dispositivo seguro de criação de assinaturas, em conformidade com o anexo II do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014.

Do mesmo modo, os certificados de pessoas singulares de alto nível de funcionário público são emitidos de acordo com os elevados níveis de garantia dos perfis de certificados estabelecidos no ponto 10 do documento "Perfis de Certificados Eletrónicos" da Secretaria de Estado da Digitalização e Inteligência Artificial do Ministério dos Assuntos Económicos e da Transformação Digital.

Estes certificados garantem a identidade do assinante e do signatário e permitem a geração da "assinatura eletrónica qualificada", ou seja, a assinatura eletrónica avançada que se baseia num certificado qualificado e que foi gerada através de um dispositivo qualificado, em conformidade com o disposto no artigo 25.º, n.º 2, do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, , de 23 de julho de 2014, produz efeitos jurídicos equivalentes aos de uma assinatura manuscrita.

Eles também podem ser usados em aplicativos que não exigem a assinatura eletrônica equivalente à assinatura escrita, como os aplicativos listados abaixo:

a) Assinatura de e-mail segura.
b) Outras aplicações de assinatura digital.

O esFIRMA não oferece serviços de backup ou recuperação de chaves. Portanto, a esFIRMA não será responsável em nenhuma circunstância por qualquer perda de informações criptografadas que não possam ser recuperadas.

As informações de uso no perfil do certificado indicam o seguinte:

a) O campo "uso da chave" ativou e, portanto, permite que você execute as seguintes funções:
    a. Compromisso de conteúdo (para executar a função de assinatura eletrônica)

b) No campo "Declarações de certificado qualificado", aparece a seguinte declaração:
    a. QcCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que o certificado é usado exclusivamente em conjunto com um dispositivo seguro de criação de assinatura.
c) O campo "Aviso do Utilizador" descreve a utilização deste certificado.

Certificado de Funcionário Público de nível médio em HSM

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.1.4	Na hierarquia do CA esFIRMA
0.4.0.194112.1.0	De acordo com a política QCP-n
2.16.724.1.3.5.7.2	Funcionário público espanhol de nível médio

Os certificados de pessoas singulares de nível médio de funcionário público são certificados qualificados em conformidade com o artigo 28.º e o anexo I do Regulamento (UE) n.º 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.

Estas certidões são emitidas aos funcionários públicos para os identificar como pessoas ao serviço da Administração, órgão, entidade de direito público ou outra entidade, vinculando-os a esta, cumprindo os requisitos estabelecidos no artigo 43.º da Lei n.º

40/2015, de 1 de outubro, relativa ao Regime Jurídico do Setor Público, para a assinatura eletrónica do pessoal ao serviço das Administrações Públicas.

Os certificados das pessoas singulares de nível intermédio, funcionário público, são geridos centralmente.

Os certificados de pessoas singulares de funcionários públicos de nível médio são emitidos de acordo com os níveis médios de garantia dos perfis de certificados estabelecidos no ponto 10 do documento "Perfis de Certificados Eletrónicos" da Secretaria de Estado da Digitalização e Inteligência Artificial do Ministério da Economia e Transformação Digital.

Estes certificados garantem a identidade do assinante e da pessoa indicada no certificado, e permitem a geração da "assinatura electrónica avançada com base num certificado eletrónico qualificado".

Eles também podem ser usados em aplicativos que não exigem a assinatura eletrônica equivalente à assinatura escrita, como os aplicativos listados abaixo:

a) Assinatura de e-mail segura.
b) Outras aplicações de assinatura digital.

O esFIRMA não oferece serviços de backup ou recuperação de chaves. Portanto, a esFIRMA não será responsável em nenhuma circunstância por qualquer perda de informações criptografadas que não possam ser recuperadas.

As informações de uso no perfil do certificado indicam o seguinte:

a) O campo "uso da chave" ativou e, portanto, nos permite executar as seguintes funções:
    a. Compromisso de conteúdo (para executar a função de assinatura eletrônica)

b) No campo "Declarações de certificado qualificado", aparece a seguinte declaração:

a. qCCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.

c) O campo "Aviso do Utilizador" descreve a utilização deste certificado.

Certificado de funcionário público de alto nível no cartão para autenticação

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.1.5	Na hierarquia do CA esFIRMA
0.4.0.2042.1.2	Em conformidade com a política do PCN+
2.16.724.1.3.5.7.1	Funcionário público espanhol de alto nível

Estes certificados são certificados emitidos em conformidade com a política de certificação normalizada (NCP+) e cumprem as disposições da norma técnica identificada com a referência EN 319 411-1 do ETSI.

Estas certidões são emitidas aos funcionários públicos para os identificar como pessoas ao serviço da Administração, órgão, entidade de direito público ou outra entidade, vinculando-os a esta, cumprindo os requisitos estabelecidos na Lei 40/2015, de 1 de outubro, sobre o Regime Jurídico do Setor Público.

Estes certificados de funcionários públicos de alto nível pessoas singulares trabalham com um dispositivo seguro de criação de assinaturas, em conformidade com o anexo II do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014.

Os certificados de pessoas singulares de funcionários públicos de alto nível são emitidos de acordo com os elevados níveis de garantia dos perfis de certificados estabelecidos no ponto 10 do documento "Perfis de Certificados Eletrónicos" da Secretaria de Estado da Digitalização e Inteligência Artificial do Ministério da Economia e Transformação Digital.

Estes certificados garantem a identidade do assinante e da pessoa indicada no certificado, e permitem a autenticação deste último em aplicações e websites.

O esFIRMA não oferece serviços de backup ou recuperação de chaves. Portanto, a esFIRMA não será responsável em nenhuma circunstância por qualquer perda de informações criptografadas que não possam ser recuperadas.

As informações de uso no perfil do certificado indicam o seguinte:

d) O campo "uso da chave" ativou e, portanto, nos permite executar as seguintes funções:
    a. Assinatura digital (para executar a função de autenticação)

e) O campo "Aviso do Utilizador" descreve a utilização deste certificado.

Certificado de Selo de Órgão de nível médio em software

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.2.2	Na hierarquia do CA esFIRMA
0.4.0.194112.1.1	De acordo com a política QCP-l
2.16.724.1.3.5.6.2	Funcionário público espanhol de nível médio

Os certificados de selo eletrónico de nível médio são certificados qualificados em conformidade com o artigo 38.º e o anexo III do Regulamento (UE) n.º 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.

Estes certificados são emitidos para a identificação e autenticação do exercício de competência em atos administrativos automatizados nos termos do artigo 42.º da Lei n.º 40/2015, de 1 de outubro, relativa ao Regime Jurídico do Setor Público.

Os certificados de selo eletrónico de nível médio são emitidos de acordo com os níveis médios de garantia dos perfis de certificação estabelecidos no ponto 9 do documento "Perfis de Certificados Eletrónicos" da Secretaria de Estado da Digitalização e Inteligência Artificial do Ministério da Economia e Transformação Digital.

Estes certificados garantem a identidade do assinante e do organismo público incluído no certificado.

O esFIRMA não oferece serviços de backup ou recuperação de chaves. Portanto, a esFIRMA não será responsável em nenhuma circunstância por qualquer perda de informações criptografadas que não possam ser recuperadas.

As informações de uso no perfil do certificado indicam o seguinte:

a) O campo "uso da chave" ativou e, portanto, nos permite executar as seguintes funções:
    a. Compromisso de conteúdo (para executar a função de assinatura eletrônica)

b) No campo "Declarações de certificado qualificado", aparece a seguinte declaração:
    a. QcCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.
c) O campo "Aviso do Utilizador" descreve a utilização deste certificado.

Certificado de Selo de Órgão de nível intermediário em HSM

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.2.4	Na hierarquia do CA esFIRMA
0.4.0.194112.1.1	De acordo com a política QCP-l
2.16.724.1.3.5.6.2	Funcionário público espanhol de nível médio

Os certificados de selo eletrónico de nível médio são certificados qualificados em conformidade com o artigo 38.º e o anexo III do Regulamento (UE) n.º 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.

Estes certificados são emitidos para a identificação e autenticação do exercício de competência em atos administrativos automatizados nos termos do artigo 42.º da Lei n.º 40/2015, de 1 de outubro, relativa ao Regime Jurídico do Setor Público.

Os certificados de selo eletrônico do órgão de nível médio são gerenciados centralmente.

Os certificados de selo eletrónico de nível médio são emitidos de acordo com os níveis médios de garantia dos perfis de certificação estabelecidos no ponto 9 do documento "Perfis de Certificados Eletrónicos" da Secretaria de Estado da Digitalização e Inteligência Artificial do Ministério da Economia e Transformação Digital.

Estes certificados garantem a identidade do assinante e do organismo público incluído no certificado.

O esFIRMA não oferece serviços de backup ou recuperação de chaves. Portanto, a esFIRMA não será responsável em nenhuma circunstância por qualquer perda de informações criptografadas que não possam ser recuperadas.

As informações de uso no perfil do certificado indicam o seguinte:

a) O campo "uso da chave" ativou e, portanto, nos permite executar as seguintes funções:
    a. Compromisso de conteúdo (para executar a função de assinatura eletrônica)

b) No campo "Declarações de certificado qualificado", aparece a seguinte declaração:
    a. QcCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.
c) O campo "Aviso do Utilizador" descreve a utilização deste certificado.

Certificado de Funcionário Público com Pseudónimo de Alto Nível no Cartão

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.3.1	Na hierarquia do CA esFIRMA
0.4.0.194112.1.2	De acordo com a política QCP-n-qscd
2.16.724.1.3.5.4.1	Funcionário público espanhol com um pseudónimo de alto nível

Os certificados de pessoas singulares de funcionários públicos com um pseudónimo de alto nível são certificados qualificados em conformidade com o artigo 28.º e o anexo I do Regulamento (UE) n.º 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.

Estes certificados são emitidos aos funcionários públicos para os identificar (através de pseudónimo) como pessoas ao serviço da Administração, órgão, entidade de direito público ou outra entidade, vinculando-os a esta, cumprindo os requisitos estabelecidos no artigo 43.º da Lei n.º 40/2015, de 1 de outubro, sobre o Regime Jurídico do Setor Público, para a assinatura eletrónica do pessoal ao serviço das Administrações Públicas.

Os certificados de pessoas singulares de funcionários públicos com um pseudónimo de alto nível funcionam com um dispositivo seguro de criação de assinaturas, em conformidade com o anexo II do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014.

Do mesmo modo, os certificados de pessoas singulares dos funcionários públicos com um pseudónimo de elevado nível são emitidos de acordo com os elevados níveis de garantia dos perfis de certificados estabelecidos no ponto 11 do documento "Perfis de Certificados Eletrónicos" da Secretaria de Estado da Digitalização e Inteligência Artificial do Ministério dos Assuntos Económicos e da Transformação Digital.

Estes certificados permitem a geração da "assinatura eletrónica qualificada", ou seja, a assinatura eletrónica avançada que se baseia num certificado qualificado e que foi gerada através de um dispositivo qualificado, em conformidade com o disposto no artigo 25.º,

n.º 2, do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, tem um efeito jurídico equivalente ao de uma assinatura manuscrita.

Eles também podem ser usados em aplicativos que não exigem a assinatura eletrônica equivalente à assinatura escrita, como os aplicativos listados abaixo:

a) Assinatura de e-mail segura.
b) Outras aplicações de assinatura digital.

O esFIRMA não oferece serviços de backup ou recuperação de chaves. Portanto, a esFIRMA não será responsável em nenhuma circunstância por qualquer perda de informações criptografadas que não possam ser recuperadas.

As informações de uso no perfil do certificado indicam o seguinte:

a) O campo "uso da chave" ativou e, portanto, permite que você execute as seguintes funções:
    a. Compromisso de conteúdo (para executar a função de assinatura eletrônica)

b) No campo "Declarações de certificado qualificado", aparece a seguinte declaração:
    a. QcCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que o certificado é usado exclusivamente em conjunto com um dispositivo seguro de criação de assinatura.
c) O campo "Aviso do Utilizador" descreve a utilização deste certificado.

Certificado de Funcionário Público com pseudônimo de nível médio, em HSM

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.3.4	Na hierarquia do CA esFIRMA

0.4.0.194112.1.0	De acordo com a política QCP-n
2.16.724.1.3.5.4.2	Funcionário público espanhol com pseudónimo de nível médio

Os certificados de pessoas singulares de funcionários públicos com um pseudónimo de nível médio são certificados qualificados em conformidade com o artigo 28.º e o anexo I do Regulamento (UE) n.º 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.

Estes certificados são emitidos aos funcionários públicos para os identificar (através de pseudónimo) como pessoas ao serviço da Administração, órgão, entidade de direito público ou outra entidade, vinculando-os a esta, cumprindo os requisitos estabelecidos no artigo 43.º da Lei n.º 40/2015, de 1 de outubro, sobre o Regime Jurídico do Setor Público, para a assinatura eletrónica do pessoal ao serviço das Administrações Públicas.

Os certificados de pessoas singulares de funcionários públicos com um pseudónimo de nível médio são geridos centralmente.

Os certificados de pessoas singulares de funcionários públicos com um pseudónimo de nível médio são emitidos de acordo com os níveis médios de garantia dos perfis de certificados estabelecidos no ponto 11 do documento "Perfis de Certificados Eletrónicos" da Secretaria de Estado da Digitalização e Inteligência Artificial do Ministério da Economia e Transformação Digital.

Estes certificados permitem a geração da "assinatura eletrónica avançada com base num certificado eletrónico qualificado".

Eles também podem ser usados em aplicativos que não exigem a assinatura eletrônica equivalente à assinatura escrita, como os aplicativos listados abaixo:

c) Assinatura de e-mail segura.
d) Outras aplicações de assinatura digital.

O esFIRMA não oferece serviços de backup ou recuperação de chaves. Portanto, a esFIRMA não será responsável em nenhuma circunstância por qualquer perda de informações criptografadas que não possam ser recuperadas.

As informações de uso no perfil do certificado indicam o seguinte:

a) O campo "uso da chave" ativou e, portanto, nos permite executar as seguintes funções:
    a. Compromisso de conteúdo (para executar a função de assinatura eletrônica)

b) No campo "Declarações de certificado qualificado", aparece a seguinte declaração:
    a. qCCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.
c) O campo "Aviso do Utilizador" descreve a utilização deste certificado.

Certificado de Funcionário Público com pseudônimo, alto nível no cartão para autenticação

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.3.5	Na hierarquia do CA esFIRMA
0.4.0.2042.1.2	Em conformidade com a política do PCN+
2.16.724.1.3.5.4.1	Funcionário público espanhol com um pseudónimo de alto nível

Estes certificados são certificados emitidos em conformidade com a política de certificação normalizada (NCP+) e cumprem as disposições da norma técnica identificada com a referência EN 319 411-1 do ETSI.

Estas certidões são emitidas aos funcionários públicos para os identificar (através de pseudónimo) como pessoas ao serviço da Administração, órgão, entidade de direito

público ou outra entidade, vinculando-os a esta, cumprindo os requisitos estabelecidos na Lei n.º 40/2015, de 1 de outubro, relativa ao Regime Jurídico do Setor Público.

Estes certificados de pessoas singulares que são funcionários públicos com um pseudónimo de alto nível funcionam com um dispositivo seguro de criação de assinaturas, em conformidade com o anexo II do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014.

Os certificados de pessoas singulares de funcionários públicos com um pseudónimo de alto nível são emitidos de acordo com os elevados níveis de garantia dos perfis de certificados estabelecidos no ponto 11 do documento "Perfis de Certificados Eletrónicos" da Secretaria de Estado da Digitalização e Inteligência Artificial do Ministério dos Assuntos Económicos e da Transformação Digital.

Estes certificados garantem a identidade do assinante e da pessoa indicada no certificado, e permitem a autenticação deste último em aplicações e websites.

O esFIRMA não oferece serviços de backup ou recuperação de chaves. Portanto, a esFIRMA não será responsável em nenhuma circunstância por qualquer perda de informações criptografadas que não possam ser recuperadas.

As informações de uso no perfil do certificado indicam o seguinte:

f) O campo "uso da chave" ativou e, portanto, nos permite executar as seguintes funções:
    a. Assinatura digital (para executar a função de autenticação)

g) O campo "Aviso do Utilizador" descreve a utilização deste certificado.

Certificado de Selo Eletrônico Qualificado TSA/TSU

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.5.2	Na hierarquia do CA esFIRMA

0.4.0.194112.1.1	De acordo com a política QCP-l

Os certificados de selo eletrónico TSA/TSU são certificados qualificados em conformidade com o artigo 38.º e o anexo III do Regulamento (UE) n.º 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 319 421 e ETSI EN 319 422.

Este certificado permite que as unidades de carimbo de data/hora ou TSUs emitam carimbos de data/hora quando recebem um pedido de acordo com as especificações do RFC3161.

As chaves são geradas em suporte a um dispositivo HSM.

As informações de uso no perfil do certificado indicam o seguinte:

a) O campo "uso da chave" ativou e, portanto, nos permite executar as seguintes funções:
    a. Compromisso de conteúdo
b) O campo "estender o uso da chave" tem o seguinte recurso habilitado:
    a. Carimbo de data/hora
c) No campo "Declarações de certificado qualificado", aparece a seguinte declaração:
    a. QcCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.
d) O campo "Aviso do Utilizador" descreve a utilização deste certificado. Opcional
e) Inclui a extensão "privateKeyUsage", que limita o uso da chave privada, seguindo as recomendações das normas ETSI EN 319 421 e ETSI EN 319 422.

Outras considerações:

- Os controlos são estabelecidos para garantir a cessação da utilização da chave privada antes da expiração da sua validade.
- No caso de uma alteração de certificado, as chaves associadas serão destruídas conforme descrito no ciclo de vida.

- As chaves privadas são destruídas após o tempo definido de uso, substituição, revogação ou outras causas terem expirado.
- A destruição é realizada de tal forma que a chave privada não pode ser recuperada, seguindo o procedimento estabelecido pelo fabricante do módulo criptográfico que as armazena.
- Para a validação a longo prazo dos carimbos de data/hora, pode ser utilizado o último LCR emitido pela esFIRMA de acordo com as orientações fornecidas. No momento da verificação, pode ser considerado válido se, no momento da data do carimbo de data/hora, a chave privada não foi comprometida, o algoritmo de impressão digital não foi colidido e os algoritmos usados estavam fora do alcance dos ataques criptográficos da época.

Certificado de Selo Eletrônico TSA/TSU

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.5.1	Na hierarquia do CA esFIRMA
0.4.0.194112.1.1	De acordo com a política QCP-l

Este certificado permite que as unidades de carimbo de data/hora ou TSUs emitam carimbos de data/hora quando recebem um pedido de acordo com as especificações do RFC3161.

As chaves são geradas em suporte a um dispositivo HSM.

As informações de uso no perfil do certificado indicam o seguinte:

f) O campo "uso da chave" ativou e, portanto, nos permite executar as seguintes funções:
   a. Compromisso de conteúdo

g) O campo "estender o uso da chave" tem o seguinte recurso habilitado:
   a. Carimbo de data/hora

h) O campo "Aviso do Utilizador" descreve a utilização deste certificado. Opcional

i) Inclui a extensão "privateKeyUsage", que limita o uso da chave privada, seguindo as recomendações das normas ETSI EN 319 421 e ETSI EN 319 422.

Outras considerações:

- Os controlos são estabelecidos para garantir a cessação da utilização da chave privada antes da expiração da sua validade.
- No caso de uma alteração de certificado, as chaves associadas serão destruídas conforme descrito no ciclo de vida.
- As chaves privadas são destruídas após o tempo definido de uso, substituição, revogação ou outras causas terem expirado.
- A destruição é realizada de tal forma que a chave privada não pode ser recuperada, seguindo o procedimento estabelecido pelo fabricante do módulo criptográfico que as armazena.
- Para a validação a longo prazo dos carimbos de data/hora, pode ser utilizado o último LCR emitido pela esFIRMA de acordo com as orientações fornecidas. No momento da verificação, pode ser considerado válido se, no momento da data do carimbo de data/hora, a chave privada não foi comprometida, o algoritmo de impressão digital não foi colidido e os algoritmos usados estavam fora do alcance dos ataques criptográficos da época.

Certidão de pessoa singular vinculada, em Cartão para assinatura

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.6.1	Na hierarquia do CA esFIRMA
0.4.0.194112.1.2	De acordo com a política QCP-n-qscd

Estes certificados são qualificados em conformidade com o artigo 28.º e o anexo I do Regulamento (UE) n.º 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.

Estes certificados funcionam com um dispositivo seguro de criação de assinaturas, em conformidade com o anexo II do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014.

Estes certificados garantem a identidade do assinante e do signatário e permitem a geração da "assinatura eletrónica qualificada", ou seja, a assinatura eletrónica avançada que se baseia num certificado qualificado e que foi gerada através de um dispositivo qualificado, em conformidade com o disposto no artigo 25.º, n.º 2, do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, , de 23 de julho de 2014, produz efeitos jurídicos equivalentes aos de uma assinatura manuscrita.

Eles também podem ser usados em aplicativos que não exigem a assinatura eletrônica equivalente à assinatura escrita, como os aplicativos listados abaixo:

c) Assinatura de e-mail segura.
d) Outras aplicações de assinatura digital.

O esFIRMA não oferece serviços de backup ou recuperação de chaves. Portanto, a esFIRMA não será responsável em nenhuma circunstância por qualquer perda de informações criptografadas que não possam ser recuperadas.

As informações de uso no perfil do certificado indicam o seguinte:

d) O campo "uso da chave" ativou e, portanto, permite que você execute as seguintes funções:
    a. Compromisso de conteúdo (para executar a função de assinatura eletrônica)

e) No campo "Declarações de certificado qualificado", aparece a seguinte declaração:
    a. QcCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que o certificado é usado exclusivamente em conjunto com um dispositivo seguro de criação de assinatura.

f) O campo "Aviso do Utilizador" descreve a utilização deste certificado. Opcional

Certidão de pessoa singular vinculada, centralizada, para assinatura

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.6.4	Na hierarquia do CA esFIRMA
0.4.0.194112.1.0	De acordo com a política QCP-n

Estes certificados são qualificados em conformidade com o artigo 28.º e o anexo I do Regulamento (UE) n.º 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.

Esses certificados são gerenciados centralmente.

Estes certificados garantem a identidade do assinante e da pessoa indicada no certificado, e permitem a geração da "assinatura electrónica avançada com base num certificado eletrónico qualificado".

Eles também podem ser usados em aplicativos que não exigem a assinatura eletrônica equivalente à assinatura escrita, como os aplicativos listados abaixo:

e) Assinatura de e-mail segura.
f) Outras aplicações de assinatura digital.

O esFIRMA não oferece serviços de backup ou recuperação de chaves. Portanto, a esFIRMA não será responsável em nenhuma circunstância por qualquer perda de informações criptografadas que não possam ser recuperadas.

As informações de uso no perfil do certificado indicam o seguinte:

h) O campo "uso da chave" ativou e, portanto, nos permite executar as seguintes funções:
    a. Compromisso de conteúdo (para executar a função de assinatura eletrônica)

i) No campo "Declarações de certificado qualificado", aparece a seguinte declaração:
   a. qCCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.
j) O campo "Aviso do Utilizador" descreve a utilização deste certificado. Opcional

Certidão de pessoa singular ligada, em cartão para autenticação

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.6.5	Na hierarquia do CA esFIRMA
0.4.0.2042.1.2	Em conformidade com a política do PCN+

Estes certificados são certificados emitidos em conformidade com a política de certificação normalizada (NCP+) e cumprem as disposições da norma técnica identificada com a referência EN 319 411-1 do ETSI.

Estes certificados funcionam com um dispositivo seguro de criação de assinaturas, em conformidade com o anexo II do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014.

Estes certificados garantem a identidade do assinante e da pessoa indicada no certificado, e permitem a autenticação deste último em aplicações e websites.

O esFIRMA não oferece serviços de backup ou recuperação de chaves. Portanto, a esFIRMA não será responsável em nenhuma circunstância por qualquer perda de informações criptografadas que não possam ser recuperadas.

As informações de uso no perfil do certificado indicam o seguinte:

k) O campo "uso da chave" ativou e, portanto, nos permite executar as seguintes funções:

a. Assinatura digital (para executar a função de autenticação)

l) O campo "Aviso do Utilizador" descreve a utilização deste certificado. Opcional

Certidão de uma pessoa singular ligada, com pseudónimo, num cartão para assinatura

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.7.1	Na hierarquia do CA esFIRMA
0.4.0.194112.1.2	De acordo com a política QCP-n-qscd

Estes certificados são qualificados em conformidade com o artigo 28.º e o anexo I do Regulamento (UE) n.º 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.

Estes certificados funcionam com um dispositivo seguro de criação de assinaturas, em conformidade com o anexo II do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014.

Estes certificados garantem a identidade do assinante.
Estes certificados garantem a identidade do signatário através de um pseudónimo.
Estes certificados permitem a geração da "assinatura eletrónica qualificada", ou seja, a assinatura eletrónica avançada que se baseia num certificado qualificado e que foi gerada através de um dispositivo qualificado, em conformidade com o disposto no artigo 25.º, n.º 2, do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, tem um efeito jurídico equivalente ao de uma assinatura manuscrita.

Eles também podem ser usados em aplicativos que não exigem a assinatura eletrônica equivalente à assinatura escrita, como os aplicativos listados abaixo:

e) Assinatura de e-mail segura.
f) Outras aplicações de assinatura digital.

O esFIRMA não oferece serviços de backup ou recuperação de chaves. Portanto, a esFIRMA não será responsável em nenhuma circunstância por qualquer perda de informações criptografadas que não possam ser recuperadas.

As informações de uso no perfil do certificado indicam o seguinte:

g) O campo "uso da chave" ativou e, portanto, permite que você execute as seguintes funções:
   a. Compromisso de conteúdo (para executar a função de assinatura eletrônica)

h) No campo "Declarações de certificado qualificado", aparece a seguinte declaração:
   a. QcCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.
   b. QcSSCD (0.4.0.1862.1.4), que informa que o certificado é usado exclusivamente em conjunto com um dispositivo seguro de criação de assinatura.

i) O campo "Aviso do Utilizador" descreve a utilização deste certificado. Opcional

Certidão de pessoa singular vinculada, com pseudónimo, centralizado, para assinatura

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.6.4	Na hierarquia do CA esFIRMA
0.4.0.194112.1.0	De acordo com a política QCP-n

Estes certificados são qualificados em conformidade com o artigo 28.º e o anexo I do Regulamento (UE) n.º 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.

Esses certificados são gerenciados centralmente.
Estes certificados garantem a identidade do assinante.
Estes certificados garantem a identidade do signatário através de um pseudónimo.

Estes certificados permitem a geração da "assinatura eletrónica avançada com base num certificado eletrónico qualificado".

Eles também podem ser usados em aplicativos que não exigem a assinatura eletrônica equivalente à assinatura escrita, como os aplicativos listados abaixo:

g) Assinatura de e-mail segura.
h) Outras aplicações de assinatura digital.

O esFIRMA não oferece serviços de backup ou recuperação de chaves. Portanto, a esFIRMA não será responsável em nenhuma circunstância por qualquer perda de informações criptografadas que não possam ser recuperadas.

As informações de uso no perfil do certificado indicam o seguinte:

m) O campo "uso da chave" ativou e, portanto, nos permite executar as seguintes funções:
    a. Compromisso de conteúdo (para executar a função de assinatura eletrônica)

n) No campo "Declarações de certificado qualificado", aparece a seguinte declaração:
    a. qCCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.
o) O campo "Aviso do Utilizador" descreve a utilização deste certificado. Opcional

Certidão de uma pessoa singular ligada, com um pseudónimo, num cartão para autenticação

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.7.5	Na hierarquia do CA esFIRMA
0.4.0.2042.1.2	Em conformidade com a política do PCN+

Estes certificados são certificados emitidos em conformidade com a política de certificação normalizada (NCP+) e cumprem as disposições da norma técnica identificada com a referência EN 319 411-1 do ETSI.

Estes certificados funcionam com um dispositivo seguro de criação de assinaturas, em conformidade com o anexo II do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014.

Estes certificados garantem a identidade do assinante.
Estes certificados garantem a identidade do signatário através de um pseudónimo.
Estes certificados permitem a autenticação destes últimos em aplicações e websites.

O esFIRMA não oferece serviços de backup ou recuperação de chaves. Portanto, a esFIRMA não será responsável em nenhuma circunstância por qualquer perda de informações criptografadas que não possam ser recuperadas.

As informações de uso no perfil do certificado indicam o seguinte:

p) O campo "uso da chave" ativou e, portanto, nos permite executar as seguintes funções:
    a. Assinatura digital (para executar a função de autenticação)

q) O campo "Aviso do Utilizador" descreve a utilização deste certificado. Opcional

Certificado de Selo Eletrônico em software

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.8.2	Na hierarquia do CA esFIRMA
0.4.0.194112.1.1	De acordo com a política QCP-l

Estes certificados são qualificados em conformidade com o artigo 38.º e o anexo III do Regulamento (UE) n.º 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.

O esFIRMA não oferece serviços de backup ou recuperação de chaves. Portanto, a esFIRMA não será responsável em nenhuma circunstância por qualquer perda de informações criptografadas que não possam ser recuperadas.

As informações de uso no perfil do certificado indicam o seguinte:

a) O campo "uso da chave" ativou e, portanto, nos permite executar as seguintes funções:
    a. Assinatura digital (para função de autenticação)
    b. Compromisso de conteúdo (para executar a função de assinatura eletrônica)
    c. Encriptação de chaves

b) No campo "Declarações de certificado qualificado", aparece a seguinte declaração:
    a. QcCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.
c) O campo "Aviso do Utilizador" descreve a utilização deste certificado. Opcional

Certificado de Selo Eletrônico com gerenciamento centralizado

Este certificado tem os seguintes OIDs:

1.3.6.1.4.1.47281.1.8.4	Na hierarquia do CA esFIRMA
0.4.0.194112.1.1	De acordo com a política QCP-l

Estes certificados são qualificados em conformidade com o artigo 38.º e o anexo III do Regulamento (UE) n.º 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.

Esses certificados são gerenciados centralmente.

O esFIRMA não oferece serviços de backup ou recuperação de chaves. Portanto, a esFIRMA não será responsável em nenhuma circunstância por qualquer perda de informações criptografadas que não possam ser recuperadas.

As informações de uso no perfil do certificado indicam o seguinte:

d) O campo "uso da chave" ativou e, portanto, nos permite executar as seguintes funções:
    a. Compromisso de conteúdo (para executar a função de assinatura eletrônica)

e) No campo "Declarações de certificado qualificado", aparece a seguinte declaração:
    a. QcCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.

f) O campo "Aviso do Utilizador" descreve a utilização deste certificado. Opcional

1.4.2 Limites e proibições de utilização de certificados

Os certificados são utilizados para a sua própria função e finalidade estabelecida, não podendo ser utilizados para outras funções e para outros fins.

Do mesmo modo, os certificados só devem ser utilizados em conformidade com a legislação aplicável, especialmente tendo em conta as restrições à importação e exportação em vigor num determinado momento.

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

Os certificados não foram concebidos, não podem ser utilizados e não estão autorizados para utilização ou revenda como equipamento de controlo de situações perigosas ou para utilizações que exijam ações à prova de falhas, tais como a exploração de instalações nucleares, sistemas de navegação aérea ou de comunicações, ou sistemas de controlo de

armas, em que 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 https://www.esfirma.com

O uso de certificados digitais de forma a violar este DPC e o restante da documentação aplicável, especialmente o contrato assinado com o assinante e os textos de divulgação ou PDS, é considerado uso indevido para os fins legais apropriados, e isenta a esFIRMA de qualquer responsabilidade por esse uso indevido, seja do signatário ou de qualquer terceiro.

A esFIRMA não tem autorização de acesso ou obrigação legal de supervisionar os dados sobre os quais a utilização de uma chave certificada pode ser aplicada. Assim, e em consequência desta impossibilidade técnica de acesso ao conteúdo da mensagem, não é possível à esFIRMA emitir qualquer avaliação sobre o referido conteúdo, pelo que o assinante, o signatário ou o responsável pela custódia assume qualquer responsabilidade decorrente do conteúdo associado à utilização de um certificado.

Da mesma forma, o assinante, o signatário ou o responsável pela custódia será responsável por qualquer responsabilidade que possa surgir da utilização da mesma fora dos limites e condições de uso estabelecidos neste DPC, dos documentos legais que vinculam cada certificado, ou dos contratos ou acordos com as entidades de registro ou seus assinantes. bem como qualquer outro uso indevido do mesmo derivado desta seção ou que possa ser interpretado como tal de acordo com a legislação vigente.

Os certificados são utilizados exclusivamente e apenas a partir da Plataforma Eletrónica de Administração ou extensões e complementos da mesma que a empresa ESPUBLICO coloca à disposição do assinante.

1.4.3 Emissão de certificados de ensaio

A esFIRMA emite certificados de ensaio no âmbito da hierarquia de produção, a fim de realizar ensaios técnicos de interoperabilidade e permitir a sua avaliação pela entidade supervisora.

Os dados contidos nos certificados de ensaio são fictícios e estão em conformidade com as orientações emitidas pela entidade supervisora.

Estes certificados de teste não são legalmente válidos, pelo que a esFIRMA está isenta de qualquer responsabilidade em resultado da sua utilização por terceiros.

1.5 Gestão de Políticas

1.5.1 Organização que administra o documento

Serviço de Segurança da ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)
CALLE BARI 39 (Edifício binário)
50197 - ZARAGOZA
(+34) 976300110

Identificação do Registo	Registo Mercantil de Saragoça
Tomé	2649
Fólio	215
Folha	Z-28722
CIF	A-50.878.842

1.5.2 Dados de contacto da organização

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)
CALLE BARI 39 (Edifício binário)
50197 - ZARAGOZA
(+34) 976300110

1.5.3 Organização que aprova o documento

Comité de Segurança da ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)

O Comité de Segurança esFIRMA, composto pelo seu Presidente, pelo Gestor de Informação e Serviços e pelo Gestor de Segurança da esFirma, é responsável pela aprovação da presente Declaração de Práticas.

Tanto as funções como os membros deste Comité estão definidos na Política de Segurança da esFirma.

1.5.4 Procedimentos de gestão documental

O sistema documental e organizativo da esFIRMA garante, através da existência e aplicação dos procedimentos correspondentes, a correta manutenção deste documento e das respetivas especificações de serviço.

A esFIRMA procede a revisões deste documento pelo menos anualmente ou quando exigido por alterações nas orientações e documentos que deve cumprir.

Conforme definido na Política de Segurança esFIRMA, o Serviço de Segurança será a entidade responsável pela manutenção deste documento.

O Serviço de Segurança é responsável pela elaboração, manutenção e administração do DPC, pelos textos de divulgação (PDS), pelas folhas de entrega e aceitação e pelo resto da documentação legal (acordos, contratos, etc.) da esFirma.

Sempre que haja alterações de importância suficiente na gestão dos certificados definidos neste DPC, é criada uma nova revisão deste documento, que aparece na caixa inicial "controle de versão" dentro da seção "informações gerais".

A ação do Serviço de Segurança é executada a pedido do seu chefe, de acordo com as necessidades que surjam.

A esFirma pode fazer alterações que não exijam notificação quando não afetem

diretamente os direitos dos signatários e assinantes dos certificados ou dos assinantes dos selos.
Quando a esFirma vai introduzir alterações que modifiquem os direitos dos signatários e subscritores dos certificados e dos assinantes dos selos, deve notificá-la publicamente para que apresentem os seus comentários ao Serviço de Segurança no prazo de 15 dias após a publicação de futuras alterações.

Para notificar publicamente as alterações produzidas, será publicado na seção "documentação" no site https://www.esfirma.com

As revisões deste DPC serão publicadas no site esFirma após serem aprovadas pelo Comitê de Segurança EsFirma.

1.6 Acrónimos e definições

1.6.1. Acrónimos

AC (*ou também CA)*	*Autoridade* de certificação
RA (ou também RA)	*Autoridade de registo* Autoridade de registo
DPC	Centro de Processamento de Dados
CPS (ou também DPC)	*Declaração de Práticas de Certificação*. Declaração de Práticas de Certificação
CRL (ou também LRC)	*Lista de Revogação de Certificados.* Lista de certificados revogados
DN	*Nome distinto.* Nome distintivo dentro do certificado digital
Identificação	Documento de Identidade Nacional
ETSI PT	*Instituto Europeu de Normalização das Telecomunicações – Norma Europeia.*
EV (para SSL)	*Validação Estendida* Validação estendida, em certificados SSL.
FIPS	*Publicação Padrão de Processamento de Informações*

	Federais
HSM	*Módulo de Segurança de Hardware*
IETF	*Força-Tarefa de Engenharia da Internet*
NIF	Número de Identificação Fiscal
PNT	*Protocolo de* Tempo de Rede
OCSP	*Protocolo de Status do Certificado Online.* Protocolo de Acesso ao Status do Certificado
OIDE	*Identificador de objeto*. Identificador de objeto
PDS	*Declarações de divulgação da PKI* .
PIN	*Número de Identificação Pessoal*. Número de Identificação Pessoal
PKI	*Infraestrutura de chave pública*. Infraestrutura de chave pública
QSCD (ou também DCCF)	*Dispositivo Qualificado de Criação de Assinatura/Selo Eletrônico.* Dispositivo qualificado de criação de assinatura/carimbo
QCP	*Política de Certificado Qualificada* Política de Certificado Qualificada
QCP-n	*Política de Certificado Qualificado - pessoa singular Política de Certificado Qualificado* para pessoas singulares.
QCP-l	*Política de Certificado Qualificada - pessoa jurídica Política de Certificado Qualificada* para Pessoas Jurídicas.
QCP-n-qscd	*Política de Certificado Qualificado-pessoa Natural-qscd Política de Certificado Qualificado* para Pessoas Físicas em Dispositivo de Assinatura/Selo Qualificado
QCP-l-qscd	*Política de Certificado Qualificada-pessoa jurídica-qscd Política de Certificado Qualificado*

	para Pessoas Jurídicas com um Dispositivo de Assinatura/Selo Qualificado
RFC	*Pedido de comentários* Documento RFC
ASR	Rivest-Shamir-Adleman. Tipo de algoritmo de encriptação
SHA	*Algoritmo de hash seguro.* Algoritmo de hash seguro
SSL	*Camada de soquetes segura.* Um protocolo projetado pela Netscape e transformado em um padrão de rede, permite a transmissão de informações criptografadas entre um navegador de Internet e um servidor.
TCP/IP	*Controlo de transmissão. Protocolo/Protocolo Internet*. Sistema de protocolos, definido no âmbito do IEFT.
TSA	*Autoridade de carimbo de data/hora* eletrónica Autoridade de carimbo de data/hora
TSU	*Unidade de carimbo de data/hora* Unidade de carimbo de data/hora.
UTC	*Tempo* Universal Coordenado
VPN	*Rede Privada Virtual.* Rede Privada Virtual

1.6.2 Definições

Autoridade de certificação	*É a entidade responsável pela emissão e gestão de certificados digitais.*
Autoridade de registo	*Entidade responsável pela gestão dos pedidos, identificação e registo dos requerentes de um certificado. Você pode fazer parte da Autoridade de Certificação ou ser um estranho.*
Certidão	*Arquivo que associa a chave pública a alguns dados de identificação do Sujeito/Signatário e é assinado pela AC.*
Chave Pública	*Um valor matemático publicamente conhecido e utilizado para a verificação de uma assinatura digital ou a encriptação de dados.*
Chave Privada	*Valor matemático conhecido apenas pelo Sujeito/Signatário e utilizado para a criação de uma assinatura digital ou a desencriptação de dados.* *A chave privada da autoridade de certificação será usada para assinatura de certificado e assinatura de CRL.* *A chave privada do serviço TSA será usada para assinar os carimbos de data/hora.*
CPS	*Um conjunto de práticas adotadas por uma Autoridade de Certificação para a emissão de certificados de acordo com uma política de certificação específica.*
LCR	*Um arquivo que contém uma lista de certificados que foram revogados em um determinado período de tempo e que é assinado pela autoridade de certificação.*
Dados de ativação	*Dados privados, como PIN ou palavras-passe utilizadas para ativar a chave privada*
DCCF	*Dispositivo de criação de assinatura qualificado. Software ou elemento de hardware, devidamente certificado, utilizado pelo Sujeito/Signatário para a geração de assinaturas eletrônicas, de modo que as operações criptográficas sejam realizadas dentro do dispositivo e seu controle seja garantido apenas pelo Sujeito/Signatário.*
Assinatura digital	*O resultado da transformação de uma mensagem, ou qualquer tipo de dados, pela aplicação da chave privada em conjunto com*

	algoritmos conhecidos, garantindo assim: *a) que os dados não foram alterados (exaustividade)* *b) que a pessoa que assina os dados é quem diz ser (identificação)* *c) que a pessoa que assina os dados não pode negar tê-lo feito (não repúdio na origem)*
OIDE	*Identificador numérico único registado sob a normalização ISO e referente a um objeto ou classe de objeto específico.*
Par de chaves	*Um conjunto formado pela chave pública e privada, ambas matematicamente relacionadas entre si.*
PKI	*Um conjunto de hardware, software, recursos humanos, procedimentos, etc., que compõem um sistema baseado na criação e gestão de certificados de chave pública.*
Requerente	*No contexto deste documento, o requerente será uma pessoa singular autorizada, com procuração especial, a realizar determinados procedimentos em nome e representação da entidade.*
Subscritor	*No contexto deste documento, a entidade jurídica proprietária do certificado (a nível empresarial)*
Assunto/Signatário	*No contexto deste documento, a pessoa singular cuja chave pública é certificada pela AC e tem, ou tem acesso exclusivo a, uma chave privada válida para gerar assinaturas digitais.*
Parte do Usuário	*No contexto deste documento, uma pessoa que voluntariamente confia no certificado digital e o utiliza como meio de atestar a autenticidade e integridade do documento assinado*

2. Publicação de informações e depósito de certificados

2.1 Depósito de certificado

A esFIRMA dispõe de um Depositário de Certificados, no qual são publicadas informações relativas aos serviços de certificação:

https://www.esfirma.com

Este serviço está disponível 24 horas por dia, 7 dias por semana e, no caso de uma falha do sistema fora do controlo da esFIRMA, a esFIRMA envidará todos os esforços para disponibilizar novamente o serviço dentro do período estabelecido na secção 5.7.4 da presente Declaração de Práticas de Certificação.

2.2 Publicação de informações de certificação

A esFIRMA publica a seguinte informação no seu Depósito:

- Listas de certificados revogados e outras informações sobre o status de revogação de certificados.
- As políticas de certificado aplicáveis.
- A Declaração de Práticas de Certificação.
- PKI Disclosure Statements (PDS), pelo menos em espanhol e inglês.

2.3 Frequência de publicação

As informações do prestador de serviços de certificação, incluindo as políticas e a Declaração de Práticas de Certificação, são publicadas assim que estiverem disponíveis.

As alterações à Declaração de Práticas de Certificação são regidas pelas disposições da secção 1.5 deste documento.

As informações sobre o status de revogação do certificado são publicadas de acordo com as seções 4.9.7 e 4.9.8 desta Declaração de Práticas de Certificação.

2.4 Controlo de Acessos

O esFIRMA não limita o acesso de leitura às informações estabelecidas na seção 2.2, mas estabelece controles para impedir que pessoas não autorizadas adicionem, modifiquem ou excluam registros do Depósito, para proteger a integridade e autenticidade das informações, especialmente as informações de status de revogação.

A esFIRMA utiliza sistemas fiáveis para o Depósito, pelo que:

- Apenas pessoas autorizadas podem fazer anotações e modificações.
- A autenticidade das informações pode ser verificada.
- Quaisquer alterações técnicas que afetem os requisitos de segurança podem ser detetadas.

3. Identificação e autenticação

3.1 Registo inicial

3.1.1 Tipos de nomes

Todos os certificados contêm um nome X.501 distinto no campo *Assunto*, incluindo um componente de *Nome Comum* (CN), relativo à identidade do assinante e da pessoa singular identificada no certificado, bem como várias informações de identidade adicionais no campo *SubjectAlternativeName*.

Os nomes contidos nos certificados são os seguintes.

3.1.1.1 Certificado de assinatura de funcionário público, de alto nível, em cartão

País (C)	"É"
Organização (O)	Nome (nome (nome oficial) da administração, organismo, entidade de direito público ou outra entidade que subscreva o certificado, à qual o trabalhador está vinculado
organizationalUnitName (UO)	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Apelido	Primeiro e segundo apelidos (facultativos), de acordo com o documento de identidade (DNI/Passaporte)
Nome próprio	Nome próprio, de acordo com o documento de identidade (DNI/Passaporte)
Número de série	DNI/NIE do funcionário
Denominação comum (NC)	Nome Apelido1 Apelido2 – NIF do trabalhador
Tipo de certificadoOID: 2.16.724.1.3.5.7.1.1	CERTIFICADO QUALIFICADO DE ASSINATURA DE FUNCIONÁRIO PÚBLICO DE ALTO NÍVEL
Nome da entidade subscritoraOID: 2.16.724.1.3.5.7.1.2	Nome da entidade subscritora
NIF OID do assinante: 2.16.724.1.3.5.7.1.3	Subscrição da entidade NIF
DNI/NIE do responsável OID: 2.16.724.1.3.5.7.1.4	DNI ou NIE da pessoa responsável

Nome da bateria OID: 2.16.724.1.3.5.7.1.6	Nome próprio do mantenedor do certificado
Primeiro sobrenome OID: 2.16.724.1.3.5.7.1.7	Apelido do responsável pelo certificado
Segundo apelido OID: 2.16.724.1.3.5.7.1.8	Segundo apelido do responsável pelo certificado. Opcional.
E-mail OID: 2.16.724.1.3.5.7.1.9	E-mail do responsável pelo certificado. Opcional.

3.1.1.2 Certidão de assinatura de funcionário público, nível intermediário, em HSM

País (C)	"É"
Organização (O)	Nome (nome (nome oficial) da administração, organismo ou entidade de direito público que subscreve o certificado, ao qual o trabalhador está vinculado
organizationalUnitName (UO)	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Apelido	Primeiro e segundo apelidos (facultativos), de acordo com o documento de identidade (DNI/Passaporte)
Nome próprio	Nome próprio, de acordo com o documento de identidade (DNI/Passaporte)
Número de série	DNI/NIE do funcionário
Denominação comum (NC)	Nome Apelido1 Apelido2 – NIF do trabalhador
Tipo de certificadoOID: 2.16.724.1.3.5.7.2.1	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO DE NÍVEL MÉDIO
Nome da entidade subscritoraOID: 2.16.724.1.3.5.7.2.2	Nome da entidade subscritora
NIF entidade assinanteOID: 2.16.724.1.3.5.7.2.3	Entidade subscritora do NIF
DNI/NIE do responsável OID: 2.16.724.1.3.5.7.2.4	DNI ou NIE da pessoa responsável
Número de autenticação pessoal OID: 2.16.724.1.3.5.7.2.5	NRP ou PIN do Mantenedor do Assinante do Certificado
Nome da bateria OID: 2.16.724.1.3.5.7.2.6	Nome próprio do mantenedor do certificado

Primeiro sobrenome OID: 2.16.724.1.3.5.7.2.7	Apelido do responsável pelo certificado
Segundo apelido OID: 2.16.724.1.3.5.7.2.8	Segundo apelido do responsável pelo certificado. Opcional.
E-mail OID: 2.16.724.1.3.5.7.2.9	E-mail do responsável pelo certificado. Opcional.

3.1.1.3 Certificado de autenticação de funcionário público, de alto nível, no cartão

País (C)	"É"
Organização (O)	Nome (nome (nome oficial) da administração, organismo, entidade de direito público ou outra entidade que subscreva o certificado, à qual o trabalhador está vinculado
organizationalUnitName (UO)	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Apelido	Primeiro e segundo apelidos (facultativos), de acordo com o documento de identidade (DNI/Passaporte)
Nome próprio	Nome próprio, de acordo com o documento de identidade (DNI/Passaporte)
Número de série	DNI/NIE do funcionário
Denominação comum (NC)	Nome Apelido1 Apelido2 – NIF do trabalhador
Tipo de certificadoOID: 2.16.724.1.3.5.7.1.1	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO COM ALTO NÍVEL DE AUTENTICAÇÃO
Nome da entidade subscritoraOID: 2.16.724.1.3.5.7.1.2	Nome da entidade subscritora
NIF OID do assinante: 2.16.724.1.3.5.7.1.3	Subscrição da entidade NIF
DNI/NIE do responsável OID: 2.16.724.1.3.5.7.1.4	DNI ou NIE da pessoa responsável
Nome da bateria OID: 2.16.724.1.3.5.7.1.6	Nome próprio do mantenedor do certificado
Primeiro sobrenome OID: 2.16.724.1.3.5.7.1.7	Apelido do responsável pelo certificado
Segundo apelido OID: 2.16.724.1.3.5.7.1.8	Segundo apelido do responsável pelo certificado. Opcional.
E-mail OID: 2.16.724.1.3.5.7.1.9	E-mail do responsável pelo certificado. Opcional.

3.1.1.4 Certificado de selo de órgão, nível intermediário, em software

País (C)	"É"
Organização (O)	Nome do assinante (nome "oficial")
organizationalUnitName (UO)	SELO ELETRÓNICO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Número de série	DNI/NIE da organização subscritora
Denominação comum (NC)	Nomeação do sistema ou aplicação de um processo automático.
Tipo de certificadoOID: 2.16.724.1.3.5.6.2.1	SELO ELETRÔNICO DE NÍVEL MÉDIO
Nome da entidade subscritora OID: 2.16.724.1.3.5.6.2.2	Nome da entidade subscritora
Entidade assinante NIFOID: 2.16.724.1.3.5.6.2.3	Entidade subscritora do NIF
Nome do sistemaOID: 2.16.724.1.3.5.6.2.5	Nome do sistema
E-mail OID: 2.16.724.1.3.5.6.2.9	E-mail da pessoa responsável pelo selo

3.1.1.5 Certificado de selo de órgão, nível intermediário, em HSM

País (C)	"É"
Organização (O)	Nome do assinante (nome "oficial")
organizationalUnitName (UO)	SELO ELETRÓNICO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Número de série	DNI/NIE da organização subscritora
Denominação comum (NC)	Nomeação do sistema ou aplicação de um processo automático.
Tipo de certificadoOID: 2.16.724.1.3.5.6.2.1	SELO ELETRÔNICO DE NÍVEL MÉDIO
Nome da entidade subscritora OID: 2.16.724.1.3.5.6.2.2	Nome da entidade subscritora
Entidade assinante NIFOID: 2.16.724.1.3.5.6.2.3	Entidade subscritora do NIF
Nome do sistemaOID: 2.16.724.1.3.5.6.2.5	Nome do sistema

3.1.1.6 Certidão de assinatura de funcionário público com pseudônimo, alto nível, em cartão

País (C)	"É"
Organização (O)	Nome (nome (nome oficial) da administração, organismo ou entidade de direito público que subscreve o certificado, ao qual o trabalhador está vinculado
organizationalUnitName (UO)	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO COM PSEUDÔNIMO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Pseudónimo	Pseudónimo obrigatório de acordo com a norma ETSI EN 319 412-2 para este tipo de certificado
Denominação comum (NC)	Pseudónimo e a Agência
Tipo de certificadoOID: 2.16.724.1.3.5.4.1.1	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO COM PSEUDÔNIMO DE ALTO NÍVEL
Nome da entidade subscritoraOID: 2.16.724.1.3.5.4.1.2	Nome da entidade subscritora
Entidade assinante NIFOID: 2.16.724.1.3.5.4.1.3	Entidade subscritora do NIF
Pseudónimo OID: 2.16.724.1.3.5.4.1.12	Pseudónimo utilizado pelo signatário e autorizado pelo subscritor

3.1.1.7 Certidão de assinatura de funcionário público com pseudônimo, nível intermediário, em HSM

País (C)	"É"
Organização (O)	Nome (nome (nome oficial) da administração, organismo ou entidade de direito público que subscreve o certificado, ao qual o trabalhador está vinculado
organizationalUnitName (UO)	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO COM PSEUDÔNIMO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Pseudónimo	Pseudónimo obrigatório de acordo com a norma ETSI EN 319 412-2 para este tipo de certificado
Denominação comum (NC)	Pseudónimo e a Agência

Tipo de certificadoOID: 2.16.724.1.3.5.4.2.1	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO COM PSEUDÔNIMO DE NÍVEL MÉDIO
Nome da entidade subscritoraOID: 2.16.724.1.3.5.4.2.2	Nome da entidade subscritora
Entidade assinante NIFOID: 2.16.724.1.3.5.4.2.3	Entidade subscritora do NIF
Pseudónimo OID: 2.16.724.1.3.5.4.2.12	Pseudónimo utilizado pelo signatário e autorizado pelo subscritor

3.1.1.8 Certidão de autenticação de funcionário público, com pseudônimo, alto nível, em cartão

País (C)	"É"
Organização (O)	Nome (nome (nome oficial) da administração, organismo, entidade de direito público ou outra entidade que subscreva o certificado, à qual o trabalhador está vinculado
organizationalUnitName (UO)	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
pseudónimo	Pseudónimo obrigatório de acordo com a norma ETSI EN 319 412-2
Denominação comum (NC)	Cargo ou cargo ou "PSEUDÓNIMO" – NÚMERO DE IDENTIFICAÇÃO – NOME OFICIAL DA ORGANIZAÇÃO
Tipo de certificadoOID: 2.16.724.1.3.5.4.1.1	CERTIFICADO DE AUTENTICAÇÃO DE FUNCIONÁRIO PÚBLICO COM PSEUDÔNIMO
Nome da entidade subscritoraOID: 2.16.724.1.3.5.4.1.2	Nome da entidade subscritora
Entidade assinante NIFOID: 2.16.724.1.3.5.4.1.3	Entidade subscritora do NIF

3.1.1.9 Certificado de selo eletrônico TSA/TSU

País (C)	"É"
Organização (O)	Nome do assinante (nome "oficial")
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1

Denominação comum (NC)	Designação da TSU

3.1.1.10 Certificado de assinatura de uma pessoa singular relacionada, num cartão

Espanha Subperfil:

País (C)	"É"
Organização (O)	Nome (nome (nome oficial) da entidade que subscreve o certificado, à qual o trabalhador está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Apelido	Primeiro e segundo apelidos (facultativos), de acordo com o documento de identidade (DNI/Passaporte)
Nome próprio	Nome próprio, de acordo com o documento de identidade (DNI/Passaporte)
Número de série	DNI/NIE do indivíduo
Denominação comum (NC)	Apelido1 Apelido2 Nome – NIF pessoa singular (ASSINATURA)
Tipo de certificado OID : 1.3.6.1.4.1.47281.0.7.1	CERTIFICADO DE PESSOA SINGULAR LIGADA A ENTIDADE
Nome da entidade subscritora OID: 1.3.6.1.4.1.47281.0.7.2	Nome da entidade subscritora
NIF OID do assinante: 1.3.6.1.4.1.47281.0.7.3	Subscrição da entidade NIF
DNI/NIE do responsável OID: 1.3.6.1.4.1.47281.0.7.4	DNI ou NIE da pessoa responsável
Nome da bateria OID: 1.3.6.1.4.1.47281.0.7.6	Nome próprio do mantenedor do certificado
Primeiro sobrenome OID: 1.3.6.1.4.1.47281.0.7.7	Apelido do responsável pelo certificado
Segundo apelido OID: 1.3.6.1.4.1.47281.0.7.8	Segundo apelido do responsável pelo certificado. Opcional.
E-mail OID: 1.3.6.1.4.1.47281.0.7.9	E-mail do responsável pelo certificado. Opcional.

Subperfil Europa:

País (C)	País

Organização (O)	Nome (nome (nome oficial) da entidade que subscreve o certificado, à qual o trabalhador está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Apelido	Primeiro e segundo apelidos (facultativos), de acordo com o documento de identidade
Nome próprio	Nome próprio, de acordo com o documento de identidade
Número de série	Número do documento de identidade da pessoa singular
Denominação comum (NC)	Apelido1 Apelido2 Nome próprio – número do documento (ASSINATURA)
Tipo de certificado OID : 1.3.6.1.4.1.47281.0.19.1	PV
Nome da entidade subscritora OID: 1.3.6.1.4.1.47281.0.19.2	Corresponde à organização do sujeito
Identificador de entidade de subscrição OID : 1.3.6.1.4.1.47281.0.19.3	Corresponde ao organizationIdentifier do sujeito
ID do controlador OID : 1.3.6.1.4.1.47281.0.19.4	DNI ou NIE da pessoa responsável
Nome da bateria OID: 1.3.6.1.4.1.47281.0.19.6	Nome próprio do mantenedor do certificado
Primeiro sobrenome OID: 1.3.6.1.4.1.47281.0.19.7	Apelido do responsável pelo certificado
Sobrenome do meio OID: 1.3.6.1.4.1.47281.0.19.8	Segundo apelido do responsável pelo certificado. Opcional.
Unidade da entidade subscritora OID: 1.3.6.1.4.1.47281.0.19.10	Corresponde à Unidade Organizacional do sujeito. Opcional

3.1.1.11 Certificado de assinatura de pessoa singular relacionada, em HSM

Espanha Subperfil:

País (C)	"É"
Organização (O)	Nome (nome (nome oficial) da entidade subscritora, à qual o trabalhador está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1

Apelido	Primeiro e segundo apelidos (facultativos), de acordo com o documento de identidade (DNI/Passaporte)
Nome próprio	Nome próprio, de acordo com o documento de identidade (DNI/Passaporte)
Número de série	DNI/NIE do funcionário
Denominação comum (NC)	Apelido1 Apelido2 Nome próprio – NIF pessoa singular
Tipo de certificado OID : 1.3.6.1.4.1.47281.0.7.1	CERTIFICADO DE PESSOA SINGULAR LIGADA A ENTIDADE
Nome da entidade subscritora OID: 1.3.6.1.4.1.47281.0.7.2	Nome da entidade subscritora
NIF OID do assinante: 1.3.6.1.4.1.47281.0.7.3	Subscrição da entidade NIF
DNI/NIE do responsável OID: 1.3.6.1.4.1.47281.0.7.4	DNI ou NIE da pessoa responsável
Nome da bateria OID: 1.3.6.1.4.1.47281.0.7.6	Nome próprio do mantenedor do certificado
Primeiro sobrenome OID: 1.3.6.1.4.1.47281.0.7.7	Apelido do responsável pelo certificado
Segundo apelido OID: 1.3.6.1.4.1.47281.0.7.8	Segundo apelido do responsável pelo certificado. Opcional.
E-mail OID: 1.3.6.1.4.1.47281.0.7.9	E-mail do responsável pelo certificado. Opcional.

Subperfil Europa:

País (C)	País
Organização (O)	Nome (nome (nome oficial) da entidade que subscreve o certificado, à qual o trabalhador está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Apelido	Primeiro e segundo apelidos (facultativos), de acordo com o documento de identidade
Nome próprio	Nome próprio, de acordo com o documento de identidade
Número de série	Número do documento de identidade da pessoa singular
Denominação comum (NC)	Apelido1 Apelido2 Nome próprio – número do documento

Nome da bateria OID: 1.3.6.1.4.1.47281.0.19.6	Nome do Mantenedor do Certificado, corresponde ao Nome Próprio
Primeiro sobrenome OID: 1.3.6.1.4.1.47281.0.19.7	Apelido do responsável pelo certificado
Sobrenome do meio OID: 1.3.6.1.4.1.47281.0.19.8	Segundo apelido do responsável pelo certificado. Opcional.

3.1.1.12 Certificado de autenticação de pessoa singular ligada, em cartão

Espanha Subperfil:

País (C)	"É"
Organização (O)	Nome (nome (nome oficial) da entidade que subscreve o certificado, à qual o trabalhador está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Apelido	Primeiro e segundo apelidos (facultativos), de acordo com o documento de identidade (DNI/Passaporte)
Nome próprio	Nome próprio, de acordo com o documento de identidade (DNI/Passaporte)
Número de série	DNI/NIE do funcionário
Denominação comum (NC)	Apelido1 Apelido2 Nome – NIF pessoa singular (AUTENTICAÇÃO)
Tipo de certificado OID : 1.3.6.1.4.1.47281.0.7.1	CERTIFICADO DE PESSOA SINGULAR LIGADA A ENTIDADE
Nome da entidade subscritora OID: 1.3.6.1.4.1.47281.0.7.2	Nome da entidade subscritora
NIF OID do assinante: 1.3.6.1.4.1.47281.0.7.3	Subscrição da entidade NIF
DNI/NIE do responsável OID: 1.3.6.1.4.1.47281.0.7.4	Corresponde ao número de série do sujeito
Nome da bateria OID: 1.3.6.1.4.1.47281.0.7.6	Nome próprio do mantenedor do certificado
Primeiro sobrenome OID: 1.3.6.1.4.1.47281.0.7.7	Apelido do responsável pelo certificado

Segundo apelido OID: 1.3.6.1.4.1.47281.0.7.8	Segundo apelido do responsável pelo certificado. Opcional.
E-mail OID: 1.3.6.1.4.1.47281.0.7.9	E-mail do responsável pelo certificado. Opcional.

Subperfil Europa:

País (C)	País
Organização (O)	Nome (nome (nome oficial) da entidade que subscreve o certificado, à qual o trabalhador está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Apelido	Primeiro e segundo apelidos (facultativos), de acordo com o documento de identidade
Nome próprio	Nome próprio, de acordo com o documento de identidade
Número de série	Número do documento de identidade da pessoa singular
Denominação comum (NC)	Apelido1 Apelido2 Nome próprio – número do documento (AUTENTICAÇÃO)
Nome da bateria OID: 1.3.6.1.4.1.47281.0.19.6	Nome do Mantenedor do Certificado, corresponde ao Nome Próprio
Primeiro sobrenome OID: 1.3.6.1.4.1.47281.0.19.7	Apelido do responsável pelo certificado
Sobrenome do meio OID: 1.3.6.1.4.1.47281.0.19.8	Segundo apelido do responsável pelo certificado. Opcional.

3.1.1.13 Certificado de assinatura de uma pessoa singular ligada, num cartão, com um pseudónimo

Espanha Subperfil:

País (C)	"É"
Organização (O)	Nome (nome (nome oficial) da entidade que subscreve o certificado, à qual o trabalhador está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
pseudónimo	Pseudónimo obrigatório de acordo com a norma ETSI EN 319 412-2

Denominação comum (NC)	Cargo ou "PSEUDÓNIMO" – NÚMERO DE IDENTIFICAÇÃO – NOME DA ENTIDADE

Subperfil Europa:

País (C)	País
Organização (O)	Nome (nome (nome oficial) da entidade que subscreve o certificado, à qual o trabalhador está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
pseudónimo	Pseudónimo obrigatório de acordo com a norma ETSI EN 319 412-2
Denominação comum (NC)	PSEUDÓNIMO - NOME DA ENTIDADE

3.1.1.14 Certificado de assinatura de pessoa singular relacionada, em HSM

Espanha Subperfil:

País (C)	"É"
Organização (O)	Nome (nome (nome oficial) da entidade subscritora, à qual o trabalhador está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
pseudónimo	Pseudónimo obrigatório de acordo com a norma ETSI EN 319 412-2
Denominação comum (NC)	Cargo ou "PSEUDÓNIMO" – NÚMERO DE IDENTIFICAÇÃO – NOME DA ENTIDADE

Subperfil Europa:

País (C)	País
Organização (O)	Nome (nome (nome oficial) da entidade que subscreve o certificado, à qual o trabalhador está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
pseudónimo	Pseudónimo obrigatório de acordo com a norma ETSI EN 319 412-2
Denominação comum (NC)	PSEUDÓNIMO - NOME DA ENTIDADE

3.1.1.15 Certificado de autenticação de uma pessoa singular ligada, em cartão, com um

pseudónimo

Espanha Subperfil:

País (C)	"É"
Organização (O)	Nome (nome (nome oficial) da entidade que subscreve o certificado, à qual o trabalhador está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Denominação comum (NC)	Cargo ou "PSEUDÓNIMO" – NÚMERO DE IDENTIFICAÇÃO – NOME DA ENTIDADE

Subperfil Europa:

País (C)	País
Organização (O)	Nome (nome (nome oficial) da entidade que subscreve o certificado, à qual o trabalhador está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
pseudónimo	Pseudónimo obrigatório de acordo com a norma ETSI EN 319 412-2
Denominação comum (NC)	PSEUDÓNIMO - NOME DA ENTIDADE

3.1.1.16 Certificado de selo eletrónico, em software

Espanha Subperfil:

País (C)	"É"
Organização (O)	Nome do assinante (nome "oficial")
organizationalUnitName (UO)	SELO ELETRÓNICO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Número de série	DNI/NIE da organização subscritora
Denominação comum (NC)	Nomeação do sistema ou aplicação de um processo automático.

Subperfil Europa:

País (C)	País
Organização (O)	Nome do assinante (nome "oficial")
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1

Número de série	Subscrevendo a identificação da organização (legalPersonSemanticsIdentifier)

3.1.1.17 Certificado de selo eletrónico com gestão centralizada

Espanha Subperfil:

País (C)	"É"
Organização (O)	Nome do assinante (nome "oficial")
organizationalUnitName (UO)	SELO ELETRÓNICO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Número de série	DNI/NIE da organização subscritora
Denominação comum (NC)	Nomeação do sistema ou aplicação de um processo automático.

Subperfil Europa:

País (C)	País
Organização (O)	Nome do assinante (nome "oficial")
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Número de série	Subscrevendo a identificação da organização (legalPersonSemanticsIdentifier)

3.1.2. Significado das denominações

Os nomes contidos nos campos *SubjectName* e *SubjectAlternativeName* dos certificados são compreensíveis em linguagem natural, conforme estabelecido na seção anterior.

3.1.3 Utilização de anónimos e pseudónimos

Em nenhuma circunstância podem ser utilizados pseudónimos para identificar uma entidade/empresa/organização, e em caso algum são emitidos certificados anónimos, exceto que, por razões de segurança pública, os sistemas de assinatura eletrónica podem referir-se apenas ao número de identificação profissional do funcionário público.

3.1.4 Interpretação dos formatos dos nomes

Os formatos de nomes devem ser interpretados de acordo com a lei do país de estabelecimento do assinante, nos seus próprios termos.

O campo "país" será sempre Espanha, porque os certificados são emitidos exclusivamente para as administrações públicas espanholas.

A certidão comprova a relação entre uma pessoa singular e a Administração, organismo, entidade de direito público ou outra entidade a que esteja ligada, independentemente da nacionalidade da pessoa singular. Isso decorre da natureza societária do certificado, do qual a corporação é assinante, e da pessoa física vinculada à pessoa autorizada a usá-lo.

No caso de certificados emitidos a assinantes espanhóis, o campo "número de série" deve incluir o NIF do signatário para efeitos de admissão do certificado para efeitos de realização de procedimentos junto das administrações espanholas.

3.1.5 Unicidade dos nomes

Os nomes dos assinantes do certificado serão únicos, para cada política de certificado da esFIRMA.

Um nome de subscritor que já tenha sido utilizado não pode ser atribuído a um subscritor diferente, situação que, em princípio, não tem de ocorrer, graças à presença do Número de Identificação Fiscal, ou equivalente, no esquema de nomenclatura.

Um assinante pode solicitar mais de um certificado, desde que a combinação dos seguintes valores na solicitação seja diferente de um certificado válido:

- Número de Identificação Fiscal (NIF) ou outro identificador legalmente válido da pessoa singular.
- Número de Identificação Fiscal (NIF) ou outro identificador legalmente válido do assinante.
- Tipo de certificado (campo Descrição do certificado).

3.1.6 Resolução de litígios relativos à atribuição de nomes

Os requerentes de certificados não devem incluir nos pedidos nomes que possam violar os direitos de terceiros por parte do futuro assinante.

A esFIRMA não será obrigada a determinar de antemão que um requerente de certificado tem direitos de propriedade industrial sobre o nome que aparece num pedido de certificado, mas procederá, em princípio, à sua certificação.

E você não atuará como árbitro ou mediador, ou de outra forma resolverá qualquer disputa relativa à propriedade de nomes de pessoas ou organizações, nomes de domínio, marcas comerciais ou nomes comerciais.

No entanto, no caso de receber uma notificação relativa a um conflito de nomes, de acordo com a lei do país do assinante, pode tomar as medidas adequadas para bloquear ou retirar o certificado emitido.

Em qualquer caso, o prestador de serviços de certificação reserva-se o direito de rejeitar um pedido de certificado devido a um conflito de nomes.

Qualquer controvérsia ou conflito decorrente deste documento será definitivamente resolvido por arbitragem por lei de um árbitro, no âmbito da Corte Arbitral Espanhola, de acordo com suas Regras e Estatutos, que é encarregado da administração da arbitragem e da nomeação do árbitro ou tribunal arbitral. As partes declaram o seu compromisso de cumprir a adjudicação emitida no documento contratual que formaliza o serviço.

3.2 Validação inicial da identidade

A identidade dos assinantes do certificado é estabelecida no momento da assinatura do contrato entre a esFIRMA e o assinante ou antes da ativação do serviço esFIRMA, momento em que se verifica a existência do assinante, e a documentação fornecida justificando a sua identidade, o cargo e/ou condição em que assinam e o seu endereço, em conformidade com as disposições dos regulamentos de direito administrativo aplicáveis.

A identidade das pessoas singulares identificadas nos certificados é validada pelos registos empresariais da Administração, organismo, entidade de direito público ou outra entidade subscritora dos certificados. O assinante produzirá uma certificação dos dados necessários e enviá-la-á à esFIRMA, pelos meios por ela habilitados, para o registo da identidade dos signatários. Quando o assinante não tiver um Secretariado, esta certificação será emitida pelo Responsável pelo serviço de certificação designado.

O responsável pelo tratamento dos dados pessoais de cada Administração, órgão, entidade de direito público ou outra entidade, é cada um deles, sendo a SOCIEDADE responsável pelo tratamento desses dados.

Para evitar qualquer conflito de interesses, as Administrações Públicas ou outras entidades subscritoras são entidades independentes do Prestador de Serviços Fiduciários "esFIRMA" e da empresa ESPUBLICO.[1]

3.2.1 Comprovativo da Posse da Chave Privada

A posse da chave privada é demonstrada em virtude do procedimento fiável de entrega e aceitação do certificado pelo signatário a partir da Plataforma Eletrónica de Administração, aquando da assinatura da ficha de aceitação, e da sua utilização na referida plataforma.

3.2.2 Identificação da entidade

Nas administrações públicas, não é exigida documentação que ateste a existência da administração pública, organismo ou entidade de direito público, uma vez que tal identidade faz parte do âmbito societário da Administração Geral do Estado ou de outras Administrações Públicas do Estado.

A EsFIRMA verifica a existência de cada Administração Pública, órgão ou entidade de direito público, quando necessário, perante o inventário das entidades do setor público do Ministério das Finanças e Função Pública em https://www.hacienda.gob.es/es-

[1] ETSI EN 319 411-1 Ap 6.2.2.2.q)

ES/CDI/Paginas/Inventario/Inventario.aspx, perante um Diário da República do seu âmbito ou através da integração com o Sistema Comum de Diretórios (DIR3).

No caso de a entidade não fazer parte do âmbito societário da Administração Geral do Estado ou de outras Administrações Públicas do Estado, a ESFIRMA verificará a existência da entidade através dos documentos relevantes ou da consulta de registos públicos, conforme indicado nos regulamentos de direito administrativo aplicáveis.

As pessoas singulares com capacidade para atuar em nome de uma Administração, organismo, entidade de direito público ou outra entidade subscritora dos certificados, podem atuar como representantes dos mesmos em relação às disposições do presente CPD, desde que exista uma situação prévia de representação legal ou voluntária entre a pessoa singular e a Administração. entidade, entidade de direito público ou outra entidade subscritora dos certificados, que exija o seu reconhecimento pela esFIRMA, o que será efetuado através de um dos seguintes procedimentos:

1. Caso o titular do cargo de Secretário tenha o poder de fé pública, serão recolhidos e verificados os seguintes documentos:
    a. Certidão do Secretário que nomeia o representante legal, com as seguintes informações:
        i. Nome e apelido do representante legal
        ii. Documento: NIF do representante
        iii. CIF da entidade que representa
        iv. Nome da entidade que representa
        v. Endereço postal da entidade que representa

2. Caso o titular do cargo de Secretário não tenha o poder de fé pública, serão recolhidos e verificados os seguintes documentos:
    a. Uma certidão do Secretário da nomeação do representante legal contendo as seguintes informações:
        i. Detalhes do representante:
            1. Nome e apelido do representante legal
            2. Documento: NIF do representante
        ii. Dados da entidade que representa:
            1. CIF

2. Designação
3. Endereço para correspondência

iii. Informação sobre a validade da representação

b. Documentação oficial que permita comprovar os dados relativos à representação ou capacidade de atuação detida pelo representante legal.
c. Todos os documentos necessários para comprovar os pontos acima mencionados de forma fidedigna, de acordo com o disposto no regulamento de direito administrativo aplicável, e a sua inscrição no registo público correspondente, se necessário.

Após verificação da documentação recolhida, o Representante Legal procederá à assinatura do contrato de prestação de serviços de certificação entre a esFIRMA (ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA) e a entidade através da qual são reguladas as condições em que a ESFIRMA prestará os serviços de certificação à entidade que se constitui como Autoridade de Registo. nomear os operadores autorizados a exercer as funções correspondentes à AR.

Uma vez assinados eletronicamente os documentos, as funções de RA serão ativadas para os utilizadores da entidade que constem do contrato como operadores autorizados a desempenhar esta função.

3.2.3 Autenticação da identidade de uma pessoa singular

Esta secção descreve os métodos de verificação da identidade de uma pessoa singular identificada num certificado.

O procedimento de solicitação e geração de certificados é realizado por meio de procedimento eletrônico na Plataforma de Administração Eletrônica disponível para o assinante e signatários.

O procedimento eletrónico para a emissão de uma certidão a uma pessoa singular seguirá os seguintes passos e serão gerados os seguintes documentos:

1. Requerimento pelo indivíduo através da Plataforma de Administração Eletrónica (com respetivo registo de entrada e abertura do ficheiro).
2. Um certificado em que o operador de verificação certifica a ligação entre o requerente e a entidade.

3. Ordem de emissão assinada pelo Operador de Verificação e Autorização da entidade, que é registada à saída e notificada à ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (anexando cópia do certificado e pedido do utilizador).

O procedimento eletrônico para emissão de certificado de selo eletrônico seguirá as seguintes etapas e serão gerados os seguintes documentos:

1. Ordem de emissão do Representante Legal através da Plataforma de Administração Eletrónica (com respetivo registo de entrada e abertura de ficheiro). Para apresentar esse pedido, o representante legal deve identificar-se na plataforma através de meios de identificação eletrónica, para os quais a presença da pessoa singular tenha sido garantida em conformidade com o artigo 8.º do Regulamento eIDAS em relação aos níveis de segurança «substanciais» ou «elevados».

3.2.3.1 Nos certificados

As informações de identificação das pessoas singulares identificadas nos certificados são validadas comparando as informações constantes do pedido da Administração, do organismo, da entidade de direito público ou de outra entidade que subscreva os certificados com os registos da Administração, organismo, entidade de direito público ou outra entidade a que estejam ligados, gerados nos termos do ponto 3.2 do presente DPC, Garantir a exatidão das informações a certificar.

3.2.3.2 Necessidade de presença pessoal

A presença física direta não é necessária para requerer certificados devido à relação já acreditada entre a pessoa singular e a Administração, organismo, entidade de direito público ou outra entidade a que esteja vinculada. Esta acreditação reflete-se na validação do pedido pelo Operador de Verificação autorizado pelo assinante, que declara a identificação presencial e inequívoca do signatário.

Para aceitar a certidão, não é necessária a presença física direta do signatário, uma vez que tal pode ser feito através de uma assinatura eletrónica avançada. Durante este procedimento, é confirmada a identidade da pessoa singular identificada no certificado.

O certificado deve ser emitido no prazo máximo de 15 dias de calendário a contar da validação da identidade da pessoa singular pelo operador de verificação e autorização. Por conseguinte, se tiverem decorrido 15 dias de calendário desde que o operador de verificação e autorização valida a identidade do requerente e ordena a emissão, o requerente não aceita o seu certificado, o processo expira e a pessoa deve apresentar um novo pedido.

3.2.3.3 Relações da pessoa singular

A justificação documental da ligação de uma pessoa singular identificada num certificado à Administração, organismo, entidade de direito público ou outra entidade é dada pela sua inscrição nos Registos do Pessoal da Administração, organismo, entidade de direito público ou outra entidade a que a pessoa singular esteja ligada.

3.2.4 Informações de assinante não verificadas

O esFIRMA não inclui qualquer informação de assinante não verificada nos certificados.

3.2.5 Critérios de interoperabilidade

A esFIRMA não tem relações de interoperabilidade com outras autoridades de certificação externas.

A esFIRMA não emite certificados de AC subordinados a terceiros e a sua autoridade de certificação emissora não está tecnicamente limitada.

3.3 Identificação e autenticação dos pedidos de renovação

3.3.1 Validação para renovação de rotina do certificado

esFirma não renova certificados. A esFirma emitirá um novo certificado, seguindo o procedimento de candidatura registado na Plataforma Eletrónica de Administração.

3.3.2 Identificação e autenticação da renovação após a revogação

A esFIRMA não renova certificados.

3.4 Identificação e autenticação do pedido de revogação

Os pedidos e relatórios relativos à revogação de um certificado são autênticos, verificando se provêm de uma pessoa autorizada.
Os métodos aceitáveis para este tipo de ensaio são os seguintes:

- O envio de um pedido de revogação pelo assinante ou pela pessoa singular identificada no certificado, assinado eletronicamente.
- A utilização da "frase de verificação de identidade", ou outros métodos de autenticação pessoal, que consiste em informações conhecidas apenas pela pessoa singular identificada no certificado e que lhe permite revogar automaticamente o seu certificado.
- Comparência física num escritório da entidade subscritora.
- Outros meios de comunicação, como o telefone, quando existam garantias razoáveis da identidade do requerente da revogação, na opinião da esFIRMA.

A esFIRMA não coloca retenções de certificados. Os pedidos de suspensão são tratados como pedidos de revogação.

4. Requisitos de operação do ciclo de vida do certificado

4.1 Pedido de Certificado

4.1.1 Legitimidade para solicitar a emissão

A Administração, organismo, entidade de direito público ou outra entidade deve celebrar um contrato de prestação de serviços de certificação com a esFIRMA.

Da mesma forma, antes da emissão e entrega de um certificado, há um pedido de certificados em um formulário de solicitação de certificado através da Plataforma de Administração Eletrônica.

Existe uma autorização do subscritor para que o requerente faça o pedido, que é legalmente instrumentada através de um formulário de pedido de certificado assinado pelo requerente em nome da Administração, órgão, entidade de direito público ou outra entidade.

4.1.2 Procedimento de registo e responsabilidades

A esFIRMA recebe pedidos de certidões feitos por Administrações, organismos, entidades de direito público ou outras entidades.

As candidaturas são feitas através de um documento em formato eletrónico, preenchido pela Administração, entidade, entidade de direito público ou outra entidade, cujo destinatário seja a esFIRMA, do qual constarão os dados das pessoas a quem serão emitidos certificados. O pedido será feito pelo operador autorizado pelo assinante (responsável pela certificação) e que tenha sido identificado no contrato entre este assinante e a esFIRMA.

O pedido deve ser acompanhado de documentação que justifique a identidade e outras circunstâncias da pessoa singular identificada no certificado, em conformidade com o disposto no ponto 3.2.3. Deve também ser anexado um endereço físico, ou outras informações, que permitam o contacto da pessoa singular identificada na certidão.

4.2 Tratamento do pedido de certificação

4.2.1 Execução de funções de identificação e autenticação

Uma vez recebido um pedido de certificado, a esFIRMA garante que os pedidos de certificado são completos, precisos e devidamente autorizados, antes de serem processados.

Em caso afirmativo, a esFIRMA verifica as informações fornecidas, verificando se os requisitos descritos na secção 3.2 foram corretamente cumpridos.

A documentação que justifique a aprovação do pedido deve ser conservada e devidamente registada e com garantias de segurança e integridade pelo período de 15 anos a contar da caducidade do certificado ou do fim do serviço prestado, mesmo em caso de perda antecipada de validade por revogação, conforme os certificados sejam qualificados.

O esFIRMA mantém procedimentos documentados que identificam e exigem atividade de verificação adicional para solicitações de certificados de alto risco, phishing ou outros usos fraudulentos, consultando diferentes listas de reputação de domínio e os próprios critérios de mitigação de risco do esFIRMA.

4.2.2 Aprovação ou rejeição do pedido

A esFIRMA aprova o pedido de certidão e procede à sua emissão e entrega, na sequência do pedido que ocorre na Plataforma Eletrónica de Administração.

Em caso de suspeita de que a informação não está correta ou que pode afetar a reputação do Organismo de Certificação ou dos assinantes, a esFIRMA negará o pedido, ou interromperá a sua aprovação até que tenha realizado as verificações complementares que considere adequadas.

Caso as verificações adicionais não indiquem a exatidão das informações a verificar, a esFIRMA negará definitivamente o pedido.

A esFIRMA notifica o requerente da aprovação ou recusa do pedido.

A esFIRMA pode automatizar os procedimentos de verificação da exatidão das informações que constarão dos certificados e de aprovação dos pedidos.

4.2.3 Prazo para a resolução do pedido

A esFIRMA atende aos pedidos de certificados por ordem de chegada, dentro de um prazo razoável, podendo ser especificada uma garantia a prazo máximo no contrato de emissão de certificados.

As candidaturas permanecem ativas até serem aprovadas ou rejeitadas.

4.3 Emissão do certificado

4.3.1 Ações da autoridade competente durante o processo de emissão

Após a aprovação do pedido de certificação, o certificado é emitido de forma segura e disponibilizado ao signatário para aceitação através do envio de um link para o dispositivo móvel e/ou endereço de e-mail designado pelo subscritor no pedido de certificado, de acordo com o procedimento indicado no ponto 4.4.2 ou através do sistema de mensagens da Plataforma de Administração Eletrónica.

Durante o processo, é ASSINATURA:

- Protege a confidencialidade e integridade dos dados de registo disponíveis para si.
- Utiliza sistemas e produtos fiáveis, protegidos contra qualquer alteração e que garantem a segurança técnica e, se for caso disso, criptográfica dos processos de certificação que suportam.
- Gera o par de chaves, usando um procedimento de geração de certificado vinculado com segurança ao procedimento de geração de chaves.
- Ele emprega um procedimento de geração de certificado que vincula com segurança o certificado às informações de registro, incluindo a chave pública certificada.
- Assegura que o certificado é emitido por sistemas que utilizam proteção contra falsificação e que garantem a confidencialidade das chaves durante o processo de geração dessas chaves.
- Inclui no certificado as informações estabelecidas no anexo 1 do Regulamento (UE) n.º 910/2014, em conformidade com o disposto nos pontos 3.1.1 e 7.1.
- Indica a data e a hora em que um certificado foi emitido.

4.3.2 Notificação da emissão ao assinante

A esFIRMA notifica a Administração, órgão, entidade de direito público ou outra entidade subscritora do certificado, e a pessoa singular identificada no certificado, através dos seus

endereços de correio eletrónico, já incluídos na informação na Plataforma Eletrónica de Administração, da emissão do certificado.

4.4 Entrega e aceitação do certificado

Durante este processo, a esFIRMA deve realizar as seguintes ações:

- Comprovar definitivamente a identidade da pessoa singular identificada no certificado, com a colaboração da Administração, do organismo, da entidade de direito público ou de outra entidade, em conformidade com o disposto nos pontos 3.2.2, 3.2.3 e 4.3.1.
- Entregar a folha de entrega e aceitação do certificado à pessoa singular nele identificada, que tenha o seguinte conteúdo mínimo:
    - Informações básicas sobre a utilização do certificado, incluindo, em particular, informações sobre o prestador de serviços de certificação e a Declaração de Práticas de Certificação aplicável, tais como as suas obrigações, poderes e responsabilidades
    - Informações sobre o certificado.
    - Aviso de receção, pelo signatário, da receção da certidão e da aceitação dos elementos acima referidos.
    - Regime de obrigações do signatário.
    - Responsabilidade do signatário.
    - Método de atribuição exclusiva ao signatário dos seus dados de ativação da chave privada e do certificado, em conformidade com o disposto nos pontos 6.2 e 6.4.
    - A data do ato de entrega e aceitação.
- Obter a assinatura, escrita ou eletrónica, da pessoa identificada na certidão.

Quando necessário, a Administração, órgão, entidade de direito público ou outra entidade colabora nestes processos, devendo registar os atos anteriores e conservar os documentos originais acima referidos (folhas de entrega e aceitação), enviando cópia eletrónica à esFIRMA, bem como os originais quando a esFIRMA requeira o acesso aos mesmos.

4.4.1 Conduta que constitui aceitação do certificado

Após a aprovação do pedido de certificação, o certificado é emitido de forma segura e o signatário é notificado para aceitação através do envio de um link para o dispositivo móvel e/ou endereço de e-mail designado pelo subscritor no pedido de certificado ou através do sistema de mensagens da Plataforma de Administração Eletrónica.

Nos certificados emitidos em software, o certificado e as chaves são gerenciados em um HSM, com o signatário tendo controle exclusivo sobre seu uso.

No caso de certificados emitidos num cartão, estes são enviados para o gestor de certificação do assinante e o PIN correspondente é enviado diretamente para o endereço postal do signatário.

Além disso, a aceitação da certidão pela pessoa singular identificada na certidão ocorre através da assinatura da folha de entrega e aceitação, através da Plataforma Eletrónica de Administração.

4.4.2 Publicação do certificado

No caso do certificado TSA/TSU, a esFIRMA publica-o no seu sítio Web.

4.4.3 Notificação da emissão a terceiros

A esFIRMA não notifica terceiros sobre o problema.

4.5 Usando o par de chaves e o certificado

4.5.1 Utilização pelo Subscritor ou Signatário

A esFIRMA obriga ao seguinte:

- Fornecer à esFIRMA informação completa e adequada, de acordo com os requisitos da presente Declaração de Práticas de Certificação, especialmente no que diz respeito ao procedimento de aceitação.
- Expressar o seu consentimento antes da emissão e entrega de um certificado.

- Utilizar o certificado em conformidade com o disposto no ponto 1.4.
- Quando o certificado trabalhar em conjunto com uma DCCF, reconhecer a sua capacidade para produzir assinaturas eletrónicas qualificadas; ou seja, equivalente a assinaturas manuscritas, bem como outros tipos de assinaturas eletrônicas e mecanismos de criptografia de informações.
- Seja especialmente diligente na custódia da sua chave privada, a fim de evitar o uso não autorizado, de acordo com o disposto nas secções 6.1, 6.2 e 6.4.
- Comunicar à esFIRMA e a qualquer pessoa que se acredite poder confiar no certificado, sem atrasos injustificáveis:
    - A perda, roubo ou potencial comprometimento da sua chave privada.
    - Perda de controlo sobre a sua chave privada, devido ao comprometimento dos dados de ativação (por exemplo, código PIN) ou por qualquer outro motivo.
    - Imprecisões ou alterações no conteúdo do certificado que o assinante conhece ou possa conhecer.
- Pare de utilizar a chave privada após o período indicado no ponto 6.3.2.
- Que todas as informações fornecidas pelo signatário que constam da certidão estão corretas.
- Que o certificado é usado exclusivamente para usos legais e autorizados, de acordo com a Declaração de Práticas de Certificação.
- Que nenhuma pessoa não autorizada jamais teve acesso à chave privada do certificado e que ele é o único responsável pelos danos causados por sua violação do dever de proteger a chave privada.
- Que o signatário é uma entidade final e não um prestador de serviços de certificação, e que não utilizará a chave privada correspondente à chave pública listada no certificado para assinar qualquer certificado (ou qualquer outro formato de chave pública certificada), ou Lista de Revogação de Certificados, título de prestador de serviços de certificação, ou de outra forma.

4.5.2 Utilização pelo Subscritor

A esFIRMA obriga contratualmente o subscritor a:

- Fornecer ao Organismo de Certificação informação completa e adequada, de acordo com os requisitos da presente Declaração de Práticas de Certificação, especialmente no que diz respeito ao procedimento de aceitação.
- Expressar o seu consentimento antes da emissão e entrega de um certificado.
- Utilizar o certificado em conformidade com o disposto no ponto 1.4.
- Comunique à esFIRMA e a qualquer pessoa que o subscritor acredite poder confiar no certificado, sem atrasos injustificáveis:
    - A perda, roubo ou potencial comprometimento da sua chave privada.
    - Perda de controlo sobre a sua chave privada, devido ao comprometimento dos dados de ativação (por exemplo, código PIN) ou por qualquer outro motivo.
    - Imprecisões ou alterações no conteúdo do certificado que o assinante conhece ou possa conhecer.
    - Perda, alteração, utilização não autorizada, furto ou comprometimento, se for caso disso, do cartão.
- Transferir para as pessoas singulares identificadas no certificado o cumprimento das suas obrigações específicas e estabelecer mecanismos que garantam o seu efetivo cumprimento.
- Não monitorizar, manipular ou realizar atos de engenharia reversa na implementação técnica dos serviços de certificação da esFIRMA, sem autorização prévia por escrito.
- Não comprometer a segurança dos serviços de certificação do prestador de serviços de certificação da esFIRMA, sem autorização prévia por escrito.
- Que todas as afirmações feitas na petição inicial estão corretas.
- Que todas as informações fornecidas pelo assinante contidas no certificado estão corretas.
- Que o certificado é usado exclusivamente para usos legais e autorizados, de acordo com a Declaração de Práticas de Certificação.
- Que nenhuma pessoa não autorizada jamais teve acesso à chave privada do certificado e que ele é o único responsável pelos danos causados por sua violação do dever de proteger a chave privada.
- Que o assinante é uma entidade final e não um provedor de serviços de certificação, e que não usará a chave privada correspondente à chave pública listada no certificado para assinar qualquer certificado (ou qualquer outro

formato de chave pública certificada), ou Lista de Revogação de Certificados, título de provedor de serviços de certificação, ou em qualquer outro caso.

4.5.3 Utilização pelo Terceiro Confiador do Certificado

A esFIRMA informa o terceiro que se baseia em certificados que deve assumir as seguintes obrigações:

- Ser informado de forma independente sobre o facto de o certificado ser adequado para a utilização prevista.
- Verificar a validade, suspensão ou revogação dos certificados emitidos, para os quais utilizará informações sobre o estado dos certificados.
- Verifique todos os certificados na hierarquia de certificados, antes de confiar na assinatura digital ou em qualquer um dos certificados na hierarquia.
- Reconheça que, para ser considerado um certificado qualificado, deve ser incluído na Lista de Confiança nacional.
- Reconhecer que as assinaturas eletrónicas verificadas, produzidas num Dispositivo de Criação de Assinatura Qualificada (DCCF) são legalmente consideradas assinaturas eletrónicas qualificadas; ou seja, equivalente a assinaturas manuscritas, bem como que o certificado permite a criação de outros tipos de assinaturas eletrónicas e mecanismos de encriptação.
- Esteja ciente de quaisquer limitações no uso do certificado, independentemente de serem encontradas no próprio certificado ou no contrato do terceiro que confia no certificado.
- Tenha em conta quaisquer precauções estabelecidas num contrato ou outro instrumento, independentemente da sua natureza jurídica.
- Não monitorizar, manipular ou realizar atos de engenharia reversa na implementação técnica dos serviços de certificação da esFIRMA, sem autorização prévia por escrito.
- Não comprometer a segurança dos serviços de certificação da esFIRMA, sem autorização prévia por escrito.

A esFIRMA informa o terceiro que se baseia em certificados que deve assumir as seguintes responsabilidades:

- Que você tem informações suficientes para tomar uma decisão informada, a fim de confiar no certificado ou não.

- Que você é o único responsável por confiar ou não nas informações contidas no certificado.
- Que será o único responsável se não cumprir as suas obrigações enquanto terceiro que invoca o certificado.

4.6. Renovação dos certificados

A esFIRMA não renova certificados. A esFirma emitirá um novo certificado, seguindo o procedimento de candidatura registado na Plataforma Eletrónica de Administração.

4.6.1 Circunstâncias para a renovação do certificado

Não aplicável.

4.6.2 Quem pode solicitar a renovação

Não aplicável.

4.6.3 Processamento do pedido de renovação do certificado

Não aplicável.

4.6.4 Notificação de emissão de novo certificado ao assinante

Não aplicável.

4.6.5 Conduta que constitui a aceitação de um certificado de renovação

Não aplicável.

4.6.6 Publicação do certificado de renovação pela autoridade competente

Não aplicável.

4.6.7 Notificação da emissão do certificado pela AC a outras

entidades

Não aplicável.

4.7 Renovação de chaves e certificados

4.7.1 Quem pode solicitar o certificado de uma nova chave pública

Não aplicável.

4.7.2 Procedimento com nova identificação

Não aplicável.

4.7.3 Processando novas solicitações de chave de certificado

A esFIRMA avisará o subscritor da necessidade de proceder a uma nova aparência do signatário e assinatura do formulário de aceitação, nos casos em que tal seja necessário devido ao termo do prazo legal de identificação de 5 anos.

Essa comparência e identificação devem ser efetuadas em conformidade com o disposto no ponto 3.2.

A assinatura da folha de aceitação será efetuada em conformidade com o disposto no ponto 4.4.2.

4.7.4 Notificação da emissão do certificado renovado

Não se aplica porque não há renovações.

4.7.5 Conduta que constitui aceitação do certificado

Não aplicável.

4.7.6 Publicação do certificado

Não aplicável.

4.7.7 Notificação da emissão a terceiros

A esFIRMA não notifica terceiros sobre o problema.

4.8 Modificando certificados

A modificação de certificados deve ser tratada como uma nova emissão de certificado, conforme descrito nos pontos 4.1, 4.2, 4.3 e 4.4.

4.9 Revogação e suspensão de certificados

4.9.1 Causas de revogação de certificados

A esFIRMA extinguirá a validade dos certificados eletrónicos por revogação quando ocorrer qualquer uma das seguintes causas:

1) Circunstâncias que afetam as informações contidas no certificado:
   a) Alteração de qualquer um dos dados contidos no certificado, após a correspondente emissão do certificado que inclui as modificações.
   b) Descoberta de que alguns dos dados contidos na solicitação de certificado estão incorretos.
   c) Descoberta de que alguns dos dados contidos no certificado estão incorretos.

2) Circunstâncias que afetam a segurança da chave ou do certificado:
   a) Comprometimento da chave privada, da infraestrutura ou dos sistemas do provedor de serviços de certificação que emitiu o certificado, desde que afete a confiabilidade dos certificados emitidos a partir desse incidente.
   b) Violação, pela esFIRMA, dos requisitos estabelecidos nos procedimentos de gestão de certificados, estabelecidos na presente Declaração de Práticas de Certificação.
   c) Comprometimento ou suspeita de comprometimento da segurança da chave ou certificado emitido.

d) Acesso ou uso não autorizado, por terceiros, da chave privada correspondente à chave pública contida no certificado.

e) A utilização irregular do certificado pela pessoa singular identificada no certificado, ou a falta de diligência na guarda da chave privada.

3) Circunstâncias que afetam o assinante ou a pessoa singular identificada no certificado:

a) Cessação da relação jurídica de prestação de serviços entre a esFIRMA e o assinante.

b) Alteração ou cessação da relação jurídica subjacente ou causa que levou à emissão do certificado à pessoa singular identificada no certificado.

c) Violação pelo requerente do certificado dos requisitos pré-estabelecidos para a aplicação do mesmo.

d) Violação, pelo assinante ou pela pessoa identificada na certidão, das suas obrigações, responsabilidades e garantias, estabelecidas no documento legal correspondente.

e) A incapacidade superveniente ou morte do porta-chaves.

f) A cessação da entidade jurídica que subscreve o certificado, bem como o fim da autorização do subscritor ao titular da chave ou a cessação da relação entre o subscritor e a pessoa identificada no certificado.

g) Pedido de revogação do certificado por parte do assinante, em conformidade com o disposto no ponto 3.4.

4) Outras circunstâncias:

a) A cessação do serviço de certificação esFIRMA, de acordo com o disposto na secção 5.8.

b) O uso do certificado que é prejudicial e contínuo para esFIRMA. Neste caso, um uso é considerado prejudicial com base nos seguintes critérios:

- Natureza e número de queixas recebidas.
- A identidade das entidades que apresentam as queixas.
- A legislação pertinente em vigor num determinado momento.
- A resposta do assinante ou da pessoa identificada na certidão às reclamações recebidas.

c) Perda da certificação de qualquer um dos dispositivos de criação de assinatura qualificados que a esFIRMA estava a utilizar como Prestador de Serviços de Confiança Qualificado,

4.9.2 Legitimidade para requerer a revogação

Podem solicitar a revogação de um certificado:

- A pessoa identificada no certificado, através de um pedido dirigido à esFIRMA ou ao assinante.
- O subscritor do certificado, mediante pedido dirigido à esFIRMA.

4.9.3 Procedimentos de pedido de revogação

O pedido de extinção deve incluir as seguintes informações:

- Data do pedido de revogação.
- Identidade do assinante ou signatário.
- Fundamentação pormenorizada do pedido de revogação.

O pedido deve ser autenticado, pela esFIRMA, de acordo com os requisitos estabelecidos na secção 3.4 desta política, antes de proceder à revogação.

O esFIRMA pode incluir qualquer outro requisito para a confirmação dos pedidos de revogação[2].

O serviço de revogação está localizado na Plataforma de Administração Eletrônica, onde o signatário e o assinante gerenciam seus certificados.

No caso de o destinatário de um pedido de extinção por uma pessoa singular identificada na certidão ser a entidade assinante, uma vez autenticado o pedido, esta última deve enviar um pedido a este respeito à esFIRMA.

O pedido de revogação será processado após a sua receção, e o subscritor e a pessoa singular identificada no certificado serão informados sobre a alteração do estado do certificado revogado.

O esFIRMA não reativa o certificado depois de este ter sido revogado.

---

[2] Ponto 6.2.4.a) iii) da norma EN 319 411-1 do ETSI

Um serviço 24/7 está disponível no número de telefone +34 976 579 516, para solicitar a revogação de certificados. A comunicação é gravada e gravada, a fim de ser utilizados como suporte e garantia de aceitação da revogação solicitada.

4.9.4 Prazo para solicitar a revogação

Os pedidos de revogação serão enviados imediatamente assim que a causa da revogação for conhecida, e não excederão 24 horas[3].

4.9.5 Prazo para o processamento do pedido

Os pedidos de revogação serão efetivados no prazo máximo de 24 horas[4].

Se, devido a circunstâncias excecionais, não for possível confirmar o pedido de revogação dentro deste prazo de 24 horas, a revogação será efetuada o mais rapidamente possível; e deve elaborar um relatório sobre as circunstâncias que impediram a revogação dentro do prazo estabelecido e as medidas a tomar para que esta situação não se repita.

4.9.6 Obrigação de consultar informações sobre a revogação de certificados por terceiros

Os terceiros devem verificar o estado dos certificados em que desejam confiar.

Um método pelo qual o status dos certificados pode ser verificado é consultando a Lista de Revogação de Certificados mais recente emitida pela Autoridade de Certificação esFIRMA.

As Listas de Revogação de Certificados são publicadas no Depositário da Autoridade de Certificação, bem como nos seguintes endereços Web, indicados nos certificados:

[3] Ponto 6.2.4, alínea a), subalínea vi), da norma ETSI EN 319 411-1

[4] Ponto 6.2.4-03a da norma ETSI EN 319 411-1

- *RAIZ CA:*
    - https://crls2.esfirma.com/acraiz/acraiz2.crl
    - https://crls1.esfirma.com/acraiz/acraiz2.crl

- *AC INTERMÉDIA:*
    - https://crls1.esfirma.com/acaapp/acaapp2.crl
    - https://crls2.esfirma.com/acaapp/acaapp2.crl

Além disso, os terceiros terão de verificar o estado dos certificados incluídos na cadeia de certificação.

4.9.7 Frequência de emissão de listas de revogação de certificados (LCR)

A esFIRMA emite uma CRL pelo menos a cada 24 horas e sempre que ocorre uma revogação.

O LCR indica o momento programado para a emissão de um novo LCR, embora um LCR possa ser emitido antes do prazo indicado no LCR anterior, para refletir as revogações.

A CRL deve manter o certificado revogado ou suspenso até que ele expire.

4.9.8 Prazo máximo de publicação das LCR

As CRLs são publicadas no Depósito num período razoável imediatamente após a sua geração, que em caso algum excede alguns minutos.

4.9.9 Disponibilidade dos Serviços de Verificação de Integridade de Certificados Online

esFIRMA informa sobre o status de revogação de certificados, usando o protocolo OCSP, que permite saber o status de validade dos certificados on-line a partir dos endereços:

- http://ocsp.esfirma.com/acaapp2/
- http://ocsp1.esfirma.com/acaapp2/
- http://ocsp2.esfirma.com/acaapp2/

Em caso de falha dos sistemas de verificação do estado do certificado por razões alheias à vontade da esFIRMA, esta deve envidar todos os esforços para assegurar que este serviço permaneça inativo durante o período mínimo possível, que não pode exceder um dia.

O esFIRMA fornece informações a terceiros que dependem de certificados sobre o funcionamento do serviço de informação sobre o estado dos certificados.

Os serviços de verificação de integridade de certificados são gratuitos[5].

A esFIRMA mantém a informação sobre o estado de revogação disponível após o período de validade do certificado[6].

4.9.10 Obrigação de consultar os serviços de verificação do estado de saúde dos certificados

É obrigatório verificar o estado dos certificados antes de confiar neles, prioritariamente, através do acesso ao serviço OCSP.

esFIRMA suporta o método GET para OCSP.

O esFIRMA atualiza o OCSP pelo menos a cada quatro dias e imediatamente em condições normais.

As respostas OCSP têm um tempo máximo de expiração de 48 horas.

Para saber o status dos Certificados de CA subordinados, as informações fornecidas por meio do OCSP são atualizadas pelo menos a cada seis meses e dentro de 24 horas após a revogação de um Certificado de CA subordinado.

5 ETSI EN 319 411-2 AP 6.3.10

6 Ap 6.3.10.b) do ETSI EN 319 411-2

Se o respondente OCSP receber uma solicitação de status para um certificado que não foi emitido, ele retornará *"revogado, certificateHold 1 de janeiro de 1970",* registrando tais solicitações como parte dos procedimentos de resposta de segurança esFIRMA.

4.9.11 Outras formas de informações sobre a revogação do certificado

Em alternativa, os terceiros que dependem de certificados poderão verificar o estado de revogação dos certificados consultando as CRLs mais recentes emitidas pela esFIRMA. Estes são publicados no site da esFIRMA, bem como nos endereços web indicados nos certificados.

O esFIRMA não delega suas respostas OCSP usando o grampeamento OCSP.

4.9.12 Requisitos especiais em caso de compromisso de chave privada

O comprometimento da chave privada esFIRMA é notificado a todos os participantes nos serviços de certificação, na medida do possível, através da publicação deste facto no site da esFIRMA, bem como, se considerar necessário, noutros meios, incluindo em papel.

4.9.13 Causas de suspensão de certificados

esFIRMA não suspende certificados.

4.9.14 Pedido de suspensão

esFIRMA não suspende certificados

4.9.15 Procedimentos para o pedido de suspensão

esFIRMA não suspende certificados.

4.9.16 Período máximo de suspensão

esFIRMA não suspende certificados.

4.10 Serviços de verificação de integridade de certificados

4.10.1 Características operacionais dos serviços

Os serviços de verificação de integridade do certificado são fornecidos por meio de uma interface de consulta na Web, na Web https://www.esfirma.com

Também podem ser verificados acedendo ao serviço OCSP nos endereços Web indicados na secção 4.9.9

As entradas de revogação em uma resposta CRL ou OCSP nunca são excluídas.

Diferenças e considerações entre consultas de status de revogação de certificado usando OCSP e CRL:

- Tanto o OCSP quanto a CRL exibem as informações mais recentes sobre o status de revogação de um certificado não expirado. No entanto, a CRL requer um processo de publicação de alguns minutos que pode resultar em discrepâncias temporárias entre os dois métodos. Eventualmente, o status de revogação de um certificado não expirado é o mesmo na consulta via OCSP e CRL.
- As CRLs não incluem certificados revogados que já expiraram, enquanto a OCSP inclui essas informações. Adicionar certificados expirados a uma CRL aumenta o tempo necessário para verificar a validade dos certificados porque a lista é maior e leva mais tempo para baixar e processar. Além disso, há um crescimento indefinido das LCR até ao final da validade do emitente.
- A EsFIRMA emite uma Última CRL, que se refere à última CRL emitida antes de o certificado de emissão de CRL deixar de ser válido devido a expiração, revogação ou outros casos. Essa CRL, juntamente com um arquivo de assinatura LTA, é usada para verificar se um certificado era válido ou não em um determinado momento. Se a Última CRL não puder ser validada, o certificado deve ser considerado inválido. Uma vez verificada a última CRL, o status do certificado deve ser verificado na CRL.
- O OCSP requer conexão em tempo real com a autoridade de certificação para obter o status de revogação, enquanto as CRLs podem ser baixadas e armazenadas localmente para uso offline.
- O OCSP pode ser menos privado do que as CRLs, pois as solicitações OCSP podem revelar à autoridade de certificação os sites que um cliente está visitando.

4.10.2 Disponibilidade dos Serviços

Os serviços de verificação de integridade do certificado e o serviço de carimbo de data/hora estão disponíveis 24 horas por dia, 7 dias por semana, durante todo o ano, com exceção dos desligamentos programados.

Os serviços de verificação de integridade de certificados são gratuitos.

4.10.3 Recursos opcionais

Não aplicável.

4.11 Rescisão da Subscrição

Após o período de validade do certificado, a assinatura do serviço terminará.

4.12 Depósito e Recuperação de Chaves

4.12.1 Política e Práticas de Depósito e Recuperação de Chaves

A esFIRMA não presta serviços essenciais de depósito e recuperação.

4.12.2 Política e práticas de encapsulamento e recuperação de chave de sessão

Sem estipulação.

5. Controlos de segurança física, de gestão e operacionais

5.1 Controlos de Segurança Física

A esFIRMA estabeleceu controlos de segurança física e ambiental para proteger os recursos das instalações onde os sistemas estão localizados, os próprios sistemas e os equipamentos utilizados para o registo e aprovação de candidaturas, geração técnica de certificados e gestão de hardware criptográfico.

Especificamente, a política de segurança física e ambiental aplicável à geração de certificados, dispositivos criptográficos e serviços de gerenciamento de revogação estabeleceu requisitos para as seguintes contingências:

- Controles de acesso físico.
- Proteção contra catástrofes naturais.
- Medidas de proteção contra incêndios.
- Falha dos sistemas de suporte (e-power, telecomunicações, etc.)
- Colapso da estrutura.
- Inundações.
- Proteção contra roubo.
- Saída não autorizada de equipamentos, informações, suportes e aplicações relacionados com componentes utilizados para os serviços do prestador de serviços de certificação.

Estas medidas são aplicáveis às instalações onde os certificados são produzidos sob a total responsabilidade da esFIRMA, que os fornece a partir das suas instalações de alta segurança, tanto a operação principal como, se for caso disso, de contingência, que são devidamente auditadas periodicamente.

As instalações dispõem de sistemas de manutenção preventiva e corretiva com assistência 24 horas por dia, 365 dias por ano, com assistência no prazo de 24 horas após a notificação.

5.1.1 Localização e construção das instalações

A proteção física é conseguida através da criação de perímetros de segurança claramente definidos em torno dos serviços. A qualidade e robustez dos materiais de construção da instalação garante níveis adequados de proteção contra intrusões de força bruta e está localizada em uma área de baixo risco de desastre e permite acesso rápido.

A sala onde as operações criptográficas são realizadas no Centro de Processamento de Dados:

- Tem redundância nas suas infraestruturas.
- Dispõe de várias fontes alternativas de eletricidade e arrefecimento em caso de emergência.
- As operações de manutenção não exigem que o Centro esteja offline em nenhum momento.
- 99,995% de fiabilidade mensal

A esFIRMA dispõe de instalações que protegem fisicamente a prestação de serviços de aprovação de pedidos de certificação e gestão de revogação de compromissos causados pelo acesso não autorizado a sistemas ou dados, bem como da sua divulgação

5.1.2 Acesso físico

O DPC onde a esFIRMA CA está localizada tem uma classificação TIER IV.

O acesso físico às instalações da esFIRMA onde são realizados os processos de certificação é limitado e protegido por uma combinação de medidas físicas e processuais. Assim:

- Limita-se a pessoal expressamente autorizado, com identificação no momento do acesso e registo, incluindo filmagem e arquivo de CCTV.

- O acesso aos quartos é feito através de leitores de cartões de identificação.

- Para aceder ao rac onde estão localizados os processos criptográficos, é necessário obter autorização prévia da esFIRMA aos administradores do serviço de alojamento que possuem a chave para abrir a gaiola.

5.1.3 Eletricidade e ar condicionado

As instalações da esFIRMA possuem equipamentos estabilizadores de corrente e um sistema de alimentação elétrica duplicado com um grupo gerador.

As salas que abrigam equipamentos de informática possuem sistemas de controle de temperatura com equipamentos de ar condicionado.

5.1.4 Exposição à água

As instalações estão localizadas em uma zona de inundação de baixo risco.

As salas onde estão alojados equipamentos informáticos dispõem de um sistema de deteção de humidade.

5.1.5 Prevenção e proteção contra incêndios

As instalações e ativos da esFIRMA dispõem de sistemas automáticos de deteção e extinção de incêndios.

5.1.6 Armazenamento de mídia

Apenas o pessoal autorizado tem acesso à mídia de armazenamento.

O mais alto nível de informações de classificação é mantido em um cofre fora das instalações do Centro de Processamento de Dados.

5.1.7 Tratamento de resíduos

A eliminação de suportes, tanto de papel como magnéticos, é realizada por meio de mecanismos que garantem a impossibilidade de recuperar a informação.

No caso de mídia magnética, a formatação, exclusão permanente ou destruição física da mídia é realizada usando um software especializado que executa um mínimo de 3 passagens de apagamento e com padrões de apagamento variáveis.

No caso de documentação em papel, por retalhadoras ou em contentores previstos para o efeito, a destruir posteriormente, sob controlo.

5.1.8 Backup externo

A esFIRMA utiliza um armazém externo seguro para a guarda de documentos, dispositivos magnéticos e eletrónicos independentes do centro de operações.

São necessárias pelo menos duas pessoas expressamente autorizadas para o acesso, depósito ou remoção de dispositivos.

5.2 Controlos processuais

A esFIRMA garante que os seus sistemas são operados de forma segura, para o que estabeleceu e implementou procedimentos para as funções que afetam a prestação dos seus serviços.

O pessoal ao serviço da esFIRMA executa os procedimentos administrativos e de gestão de acordo com a política de segurança.

5.2.1 Recursos confiáveis

A esFIRMA identificou, de acordo com a sua política de segurança, as seguintes funções ou papéis com o estatuto de fiáveis:

- **Auditor Interno:** Responsável pelo cumprimento dos procedimentos operacionais. Trata-se de uma pessoa externa ao departamento de Sistemas de Informação. As tarefas do Auditor Interno são incompatíveis no tempo com as tarefas de Certificação e incompatíveis com os Sistemas. Estas funções estarão subordinadas ao chefe de operações, reportando-se tanto a este como à direção técnica.
- **Administrador de Sistemas**: Responsável pelo correto funcionamento do suporte de hardware e software da plataforma de certificação
- **Administrador de CA**: Responsável pelas ações a serem realizadas com o material criptográfico, ou com o desempenho de qualquer função que envolva a ativação

das chaves privadas das autoridades de certificação descritas neste documento, ou qualquer um dos seus elementos.

- **Operador de AC:** Responsável conjuntamente com o Administrador da AC pela custódia do material de ativação da chave criptográfica, também responsável pelas operações de backup e manutenção da AC.
- **Operador de Registo:** Pessoa responsável pela aprovação dos pedidos de certificação feitos pelo assinante.
- **Gerente de Segurança**: Responsável por coordenar, controlar e fazer cumprir as medidas de segurança definidas pelas políticas de segurança da esFIRMA. Você deve ser responsável por aspetos relacionados à segurança da informação: lógico, físico, de rede, organizacional, etc.
- **Gestor de Informação e Serviços**: Define os requisitos de informação e serviços em termos de segurança. Este papel é, em última instância, responsável pela utilização que faz das informações e dos serviços e, por conseguinte, pelo seu nível de proteção.
- **Especialista em Validação**: Responsável pela validação de pedidos de certificados.
- **Oficial de Revogação:** Responsável pela operação de alteração do status dos certificados.

As pessoas que ocupam os lugares acima referidos estão sujeitas a procedimentos específicos de investigação e controlo.

5.2.2 Número de pessoas por tarefa

A esFIRMA garante pelo menos duas pessoas para executar as tarefas detalhadas nas Políticas de Certificação correspondentes. Especialmente na manipulação do dispositivo de custódia das chaves raiz da Autoridade de Certificação.

5.2.3 Identificação e autenticação para cada função

As pessoas designadas para cada função são identificadas pelo auditor interno, que garantirá que cada pessoa execute as operações para as quais foi designada.

Cada pessoa controla apenas os ativos necessários para a sua função, garantindo assim que nenhuma pessoa tenha acesso a recursos não alocados.

O acesso aos recursos é feito dependendo do ativo usando cartões criptográficos e códigos de ativação.

5.2.4 Funções que exigem separação de funções

As seguintes tarefas são executadas por, pelo menos, duas pessoas:

- Emissão e revogação de certificados, e acesso ao depósito.
- Geração, emissão e destruição de certificados da Autoridade de Certificação.
- Implementação do Organismo de Certificação.

5.2.5 Sistema de Gestão PKI

O sistema PKI é composto pelos seguintes módulos:

- Componente/módulo de gestão da Autoridade de Certificação Subordinada.
- Componente/módulo de gestão da Autoridade de Registo.
- Componente/módulo de gestão de pedidos.
- Componente/Módulo de Gestão de Chaves (HSM).
- Componente/módulo de banco de dados.
- Componente/módulo de gerenciamento de CRL.
- Componente/Módulo de Gerenciamento de Serviços OCSP.
- Componente/módulo de gerenciamento da Autoridade de Carimbo de Hora (TSA)

5.3 Controlos do pessoal

5.3.1 Histórico, qualificações, experiência e requisitos de habilitação

Todo o pessoal que executa tarefas qualificadas como confiáveis trabalha no local de produção há pelo menos um ano e tem contratos de trabalho permanentes.

Todo o pessoal é qualificado e foi devidamente instruído para executar as operações que lhe foram atribuídas.

Os funcionários em cargos de confiança não têm interesses pessoais que entrem em conflito com o desempenho da função que lhes é confiada.

O esFIRMA garante que o pessoal de registo é fiável para realizar tarefas de registo.

O Operador do Registo concluiu um curso de preparação para a execução das tarefas de validação dos pedidos.

Em geral, a esFIRMA afasta um colaborador das suas funções de confiança quando toma conhecimento da existência da prática de um ato criminoso suscetível de afetar o desempenho das suas funções.
A esFIRMA não atribuirá a um site de confiança ou de gestão uma pessoa que não seja adequada para o cargo, especialmente porque foi condenada por um crime ou contravenção que afete a sua adequação ao cargo.

5.3.2 Procedimentos de investigação histórica

A esFIRMA realiza verificações de antecedentes de potenciais funcionários antes de serem contratados ou entrarem no trabalho.

A esFIRMA obtém o consentimento inequívoco do titular dos dados para essa investigação prévia, e trata e protege todos os seus dados pessoais em conformidade com o REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e com a Lei Orgânica 3/2018, de 5 de dezembro, sobre a Proteção de Dados Pessoais e garantia dos direitos digitais.

A investigação será repetida com periodicidade suficiente.

Todas as verificações são realizadas na medida permitida pela legislação aplicável. Os motivos que podem levar à rejeição do candidato a um cargo de confiança são os seguintes:

- Falsidades na candidatura a emprego, feita pelo candidato.

- Referências profissionais muito negativas ou pouco confiáveis em relação ao candidato.

A candidatura a emprego informa sobre a necessidade de se submeter a uma investigação prévia, alertando que a recusa em submeter-se à investigação implicará a rejeição da candidatura.

5.3.3 Requisitos de formação

A esFIRMA forma pessoal em cargos de confiança e de gestão nos termos estabelecidos nas Políticas de Certificação. Para o efeito, as ações correspondentes são definidas no Plano de Formação ESFIRMA.

A formação inclui, pelo menos, os seguintes conteúdos:

- Princípios e mecanismos de segurança da hierarquia de certificação, bem como o ambiente de utilizador da pessoa a treinar.
- Tarefas que a pessoa deve executar.
- Políticas e procedimentos de segurança da esFIRMA. Utilização e operação de máquinas e aplicações instaladas.
- Gestão e processamento de incidentes e comprometimentos de segurança.
- Continuidade de negócios e procedimentos de emergência.
- Procedimento de gestão e segurança em relação ao tratamento de dados pessoais.

5.3.4 Requisitos e frequência das atualizações da formação

O esFIRMA atualiza a formação do pessoal conforme necessário e com frequência suficiente para desempenhar as suas funções de forma competente e satisfatória, especialmente quando são efetuadas alterações substanciais às tarefas de certificação

5.3.5 Sequência e frequência da rotação de postos de trabalho

Não aplicável.

5.3.6 Penalidades por Ações Não Autorizadas

A esFIRMA dispõe de um sistema sancionatório para clarificar as responsabilidades decorrentes de ações não autorizadas, adaptado à legislação laboral aplicável e, em particular, coordenado com o sistema sancionatório da convenção coletiva aplicável ao pessoal.

As medidas disciplinares incluem a suspensão e o despedimento da pessoa responsável pela ação danosa, de forma proporcional à gravidade da ação não autorizada.

5.3.7 Requisitos para contratação de profissionais

Os funcionários contratados para executar tarefas confiáveis assinam antecipadamente as cláusulas de confidencialidade e os requisitos operacionais utilizados pela esFIRMA. Qualquer ação que comprometa a segurança dos processos aceitos poderá, uma vez avaliada, levar à rescisão do contrato de trabalho.

No caso de a totalidade ou parte dos serviços de certificação serem operados por terceiros, os controlos e previsões realizados nesta secção, ou noutras partes do CPD, serão aplicados e cumpridos pelo terceiro que desempenha as funções de exploração dos serviços de certificação, no entanto, o organismo de certificação será responsável, em todos os casos, pela execução efetiva. Estes aspetos são especificados no instrumento jurídico utilizado para acordar a prestação de serviços de certificação por um terceiro que não a esFIRMA.

5.3.8 Fornecimento de documentação ao pessoal

O prestador de serviços de certificação fornecerá a documentação de que o seu pessoal necessita rigorosamente em todos os momentos, a fim de realizar o seu trabalho de forma competente e satisfatória.

5.4 Procedimentos de auditoria de segurança

5.4.1 Tipos de eventos registados

A esFIRMA produz e mantém um registo de, pelo menos, os seguintes eventos relacionados com a segurança da entidade:

- Ligar e desligar o sistema.
- Tenta criar, excluir, definir senhas ou alterar privilégios.
- Tentativas de login e logout.
- Tentativas de obter acesso não autorizado ao sistema CA através da rede.
- Tentativas de acesso não autorizado ao sistema de arquivos.
- Acesso físico aos logs.
- Alterações na configuração e manutenção do sistema.
- Registos de aplicações de AC.
- Ligar e desligar a aplicação CA.
- Alterações nos detalhes e/ou chaves da AC.
- Alterações na criação de políticas de certificado.
- Geração de chaves próprias.
- Criação e revogação de certificados.
- Registros da destruição da mídia contendo as chaves, dados de ativação.
- Eventos relacionados ao ciclo de vida do módulo criptográfico, como receber, usar e desinstalar o módulo.
- As atividades de firewalls e roteadores[7]
- A cerimónia de geração de chaves e bases de dados de gestão de chaves.
- Logs de acesso físico.
- Manutenção e alterações na configuração do sistema.
- Mudanças de pessoal.
- Relatórios de compromissos e discrepâncias.
- Registos da destruição de material que contenha informações essenciais, dados de ativação ou informações pessoais do assinante, no caso de certificados individuais, ou da pessoa singular identificada no certificado, no caso de certificados de organização.
- Posse de dados de ativação, para operações com a chave privada da Autoridade de Certificação.
- Relatórios abrangentes de tentativas de intrusão física em infraestruturas que suportam a emissão e gestão de certificados.

[7] Ap 6.4.5.a) do ETSI EN 319 411-1

As entradas do Registro incluem os seguintes itens:

- Data e hora de entrada.
- Número de série ou sequência da entrada, em registos automáticos.
- Identidade da entidade que introduz o registo.
- Tipo de bilhete.

Todos os eventos relacionados com a preparação de dispositivos de criação de assinaturas qualificados que são utilizados por signatários ou depositários são registados[8].

5.4.2 Frequência do processamento dos registos de auditoria

O esFIRMA revê os seus registos quando existe um alerta do sistema causado pela existência de um incidente.

O processamento de logs de auditoria consiste em uma revisão dos logs que inclui a verificação de que os logs não foram adulterados, uma breve inspeção de todas as entradas de log e uma investigação mais aprofundada de quaisquer alertas ou irregularidades nos logs. As ações tomadas a partir da revisão de auditoria são documentadas.

A esFIRMA mantém um sistema que lhe permite garantir:

- Espaço suficiente para armazenamento de logs
- Os arquivos de log não são reescritos.
- Que as informações salvas incluam, pelo menos: tipo de evento, data e hora, usuário que executa o evento e resultado da operação.
- Os arquivos de log serão armazenados em arquivos estruturados que podem ser incorporados a um banco de dados para exploração posterior.

5.4.3 Período de retenção do log de auditoria

O esFIRMA armazena informações de log por um período de 1 a 15 anos, dependendo do tipo de informação registrada.

[8] Ap 6.4.5.a) do ETSI EN 319 411-2

A esFIRMA disponibiliza estes registos de auditoria ao seu Auditor Qualificado, mediante pedido.

5.4.4 Protegendo logs de auditoria

Os logs dos sistemas:

- Estão protegidos contra manipulação, eliminação ou eliminação[9] assinando os ficheiros que os contêm.
- Eles são armazenados em dispositivos à prova de fogo.
- A sua disponibilidade é protegida armazenando-os em instalações fora do centro onde a AC está localizada.

O acesso aos ficheiros de registo está reservado apenas a pessoas autorizadas. Da mesma forma, os dispositivos são operados em todos os momentos por pessoal autorizado.
Há um procedimento interno onde os processos de gerenciamento de dispositivos que contêm dados de log de auditoria são detalhados.

5.4.5 Procedimentos de backup

O esFIRMA dispõe de um procedimento de cópia de segurança adequado para que, em caso de perda ou destruição de ficheiros relevantes, as cópias de segurança correspondentes dos registos estejam disponíveis num curto período de tempo.

O esFIRMA implementou um procedimento de backup seguro para logs de auditoria, fazendo uma cópia semanal de todos os logs em um meio externo. Além disso, uma cópia é mantida em um centro de custódia externo.

5.4.6 Localizando o sistema de acumulação de logs de auditoria

As informações de auditoria de eventos são coletadas internamente e de forma automatizada pelo sistema operacional, comunicações de rede e software de gerenciamento de certificados, bem como dados gerados manualmente, que serão

[9] Ap 7.10.f) do ETSI EN 319 401

armazenados por pessoal devidamente autorizado. Tudo isso compõe o sistema de acumulação de trilhas de auditoria.

5.4.7 Notificação do evento de auditoria à pessoa causadora do evento

Quando o sistema de acumulação de log de auditoria registra um evento, não é necessário enviar uma notificação para o indivíduo, organização, dispositivo ou aplicativo que causou o evento.

5.4.8 Análise de vulnerabilidade

A análise de vulnerabilidade é coberta pelos processos de auditoria da esFIRMA.

As verificações de vulnerabilidade devem ser executadas, revisadas e revisadas por meio de um exame desses eventos monitorados. Essas análises devem ser executadas diariamente, mensalmente e anualmente.

Os dados de auditoria dos sistemas são armazenados para serem utilizados na investigação de qualquer incidente e localizar vulnerabilidades.

O programa de segurança da esFIRMA inclui uma avaliação de risco anual.

5.5. Ficheiros de informação

A esFIRMA garante que toda a informação relativa aos certificados é conservada durante um período de tempo adequado, conforme estabelecido na secção 5.5.2 desta política.

5.5.1 Tipos de registos arquivados

Os seguintes documentos envolvidos no ciclo de vida do certificado são armazenados pela esFIRMA (ou pelas entidades de registo):

- Todos os dados de auditoria do sistema (PKI, TSA e OCSP).

- Todos os dados relativos aos certificados, incluindo os contratos com os signatários e os dados relativos à sua identificação e localização
- Pedidos de emissão e revogação de certificados, incluindo todos os relatórios relativos ao processo de revogação[10].
- Quaisquer opções específicas que o signatário ou assinante tenha durante o contrato de assinatura[11].
- Tipo de documento apresentado no pedido de certificado.
- Identidade da autoridade de registo que aceita o pedido de certificado.
- Número de identificação único fornecido pelo documento acima.
- Todos os certificados emitidos ou publicados.
- CRLs emitidas ou registros do status dos certificados gerados.
- O histórico de chaves geradas.
- Comunicações entre elementos PKI.
- Políticas e Práticas de Certificação
- Todos os dados de auditoria identificados na secção 5.4
- Informações de solicitação de certificação.
- Documentação fornecida para justificar os pedidos de certificação.
- Informações sobre o ciclo de vida do certificado.

A esFIRMA é responsável pelo correto arquivamento de todo este material.

5.5.2 Período de conservação dos registos

esFIRMA arquiva os registos acima especificados durante, pelo menos, 15 anos.

5.5.3 Proteção de ficheiros

O esFIRMA protege o ficheiro para que apenas pessoas devidamente autorizadas possam ter acesso ao mesmo. O arquivo é protegido contra visualização, modificação, exclusão ou qualquer outra manipulação, armazenando-o em um sistema confiável.

O esFIRMA assegura a correta proteção dos ficheiros, atribuindo pessoal qualificado para o seu processamento e armazenando-os em cofres à prova de fogo e instalações externas.

10 ETSI EN 319 411-1 Ap 6.4.5.h)

11 Ponto 6.4.5, alínea c), subalínea iv), da norma EN 319 411-1 do ETSI

5.5.4 Procedimentos de backup

O esFIRMA dispõe de um centro de armazenamento externo para garantir a disponibilidade de cópias do arquivo eletrónico. Os documentos físicos são armazenados em locais seguros, com acesso restrito apenas a pessoal autorizado.

O esFIRMA realiza, no mínimo, backups incrementais diários de todos os seus documentos eletrônicos e faz backups completos semanalmente para casos de recuperação de dados.

Além disso, a esFIRMA (ou as organizações que desempenham a função de registo) mantém uma cópia dos documentos em papel num local seguro e diferente das instalações do próprio Organismo de Certificação.

5.5.5 Requisitos de carimbo de data e hora

Os registros são datados com uma fonte confiável via NTP.

O esFIRMA tem um procedimento onde descreve a configuração dos tempos dos equipamentos utilizados na emissão de certificados.
O tempo usado para registrar os eventos no log de auditoria deve ser sincronizado com o UTC pelo menos uma vez por dia[12].

Essas informações não precisam ser assinadas digitalmente.

5.5.6 Localizando o sistema de arquivos

O esFIRMA dispõe de um sistema centralizado de recolha de informação sobre a atividade das equipas envolvidas no serviço de gestão de certificados.

[12] Ponto 7.10.d) da norma ETSI EN 319 401

5.5.7 Procedimentos para obtenção e verificação de informações arquivísticas

esFIRMA tem um procedimento que descreve o processo para verificar se as informações no arquivo estão corretas e acessíveis.

5.6 Renovação das chaves

Antes que o uso da chave privada AC/SUBCA/TSA expire, uma alteração de chave será feita. A CA/SUBCA antiga e sua chave privada só serão usadas para assinatura de CRL enquanto houver certificados ativos emitidos por essa CA/SUBCA. Um novo AC /SUBCA/TSA será gerado com uma nova chave privada e um novo DN. A chave privada da TSA será destruída.

A alteração das senhas dos assinantes é realizada através da realização de um novo processo de emissão.

5.7 Compromisso chave e recuperação de desastres

5.7.1 Procedimentos de gestão de incidentes e compromissos

Os backups das seguintes informações são armazenados em instalações de armazenamento externas ao esFIRMA, que são disponibilizadas em caso de comprometimento ou desastre: dados técnicos de solicitações de certificados, dados de auditoria e logs de banco de dados de todos os certificados emitidos.

As cópias de segurança das chaves privadas esFIRMA são geradas e mantidas de acordo com a secção 6.2.4

5.7.2 Corrupção de recursos, aplicativos ou dados

Quando ocorrer um evento de corrupção de recursos, aplicações ou dados, o incidente será reportado à segurança e serão iniciados os procedimentos de gestão adequados, que incluem escalada, investigação e resposta ao incidente. Se necessário, serão iniciados os principais procedimentos de comprometimento ou recuperação de desastres do esFIRMA.

5.7.3 Comprometimento da chave privada da entidade

Em caso de suspeita ou conhecimento do compromisso da esFIRMA, serão ativados os principais procedimentos de compromisso, liderados por uma equipa de resposta que avaliará a situação, desenvolverá um plano de ação, que será executado sob a aprovação da gestão do Organismo de Certificação.

Em caso de comprometimento da chave privada esFIRMA, pode ser o caso de os status dos certificados e processos de revogação usando essa chave podem não ser válidos[13]. Em qualquer caso, todos os certificados ativos serão revogados, gerando posteriormente uma CRL final que incluirá todos os certificados revogados, expirados ou não. As instruções para a validação de um certificado ou carimbo de data/hora serão publicadas no site esFIRMA.

A esFIRMA desenvolveu um Plano de Contingência para recuperar sistemas críticos, se necessário num centro de dados alternativo.

O caso de comprometimento da chave raiz deve ser tomado como um caso separado no processo de contingência e continuidade de negócios. Este incidente afeta, em caso de substituição das senhas, os reconhecimentos por diferentes aplicativos e serviços públicos e privados. Uma recuperação na eficácia das chaves em termos de negócios dependerá principalmente da duração desses processos. O documento de contingência e continuidade de negócios tratará dos termos puramente operacionais para que as novas chaves estejam disponíveis, e não o seu reconhecimento por terceiros.

Qualquer falha no cumprimento das metas estabelecidas por este Plano de Contingência será tratada como razoavelmente inevitável, a menos que tal falha seja devida ao não cumprimento das obrigações da CA de implementar tais processos.

5.7.4 Continuidade de negócios após um desastre

A esFIRMA irá restaurar os serviços críticos (suspensão e revogação e publicação de informações sobre o estado do certificado) de acordo com o Plano de Continuidade de Negócios existente.

---

13 Ponto 6.4.8, alínea g), subalínea ii), da norma ETSI EN 319 411-1

A esFIRMA dispõe de um centro alternativo, se necessário, para a implementação dos sistemas de certificação descritos no plano de continuidade das atividades.

Tanto o serviço de gestão de revogações como o serviço de consulta são considerados serviços críticos e são declarados como tal no Plano de Continuidade de Negócios esFIRMA.

5.8 Cessação do Serviço

A esFIRMA assegura que as eventuais interrupções para os assinantes e terceiros são mínimas em resultado da cessação dos serviços do prestador de serviços de certificação e, em particular, assegura a manutenção contínua dos registos necessários para fornecer provas da certificação em caso de investigação civil ou criminal.

Antes de cessar os seus serviços, a esFIRMA desenvolve um Plano de Rescisão, com as seguintes disposições:

- Disponibilizar os fundos necessários para continuar a conclusão das atividades de revogação.
- Comunicará ao Ministério da Economia e Transformação Digital, com pelo menos 2 meses de antecedência, a cessação da sua atividade e o destino dos certificados, especificando se a gestão é transferida e para quem, ou se a sua validade será extinta.
- Notificará ainda o Ministério dos Assuntos Económicos e da Transformação Digital da abertura de qualquer processo de falência contra a esFIRMA, bem como de quaisquer outras circunstâncias relevantes que possam impedir a continuação da atividade.
- Informará todos os Signatários/Subscritores, Terceiros de confiança e outras autoridades competentes com as quais tenha acordos ou outros tipos de relação da rescisão com um pré-aviso mínimo de 6 meses.
- Revoga qualquer autorização concedida às entidades subcontratadas para atuarem em nome da autoridade competente no procedimento de emissão de certificados.
- Destrua ou desative as chaves privadas da autoridade de certificação para uso.
- Os certificados de Unidade de carimbo de data/hora (TSU) serão revogados.

- Todos os certificados ativos e o sistema de verificação e revogação serão mantidos até a extinção de todos os certificados emitidos por 15 anos. Para o efeito, será emitido um LCR final que incluirá todos os certificados revogados, caducados ou não, estabelecendo os meios necessários para garantir a sua conservação a longo prazo.

6. Controlos técnicos de segurança

6.1 Geração e instalação de pares de chaves

6.1.1 Geração de pares de chaves

O par de chaves da autoridade de certificação intermédia "ESFIRMA AC AAPP 2" é criado pelo organismo de certificação raiz "ESFIRMA AC ROOT 2" de acordo com os procedimentos da cerimónia esFIRMA, dentro do perímetro de alta segurança destinado a esta tarefa.

As atividades realizadas durante a cerimónia de geração de chaves foram registadas, datadas e assinadas por todos os indivíduos que nela participaram, com a presença de um Auditor da CISA. Estes registos são conservados para efeitos de auditoria e acompanhamento durante um período adequado determinado pela esFIRMA.

Para gerar a chave das autoridades de certificação raiz e intermediárias, são usados dispositivos com as certificações Common Criteria EAL 4+ ou FIPS 140-2 Nível 3.

RAIZ	4.096 bits	25 anos
INTERMEDIÁRIO	4.096 bits	13 anos
- Certificados de entidade final	2.048 bits	2 anos
- Certificado TSA	4.096 bits	5 anos (2 anos chave privada)

Mais informações nos seguintes locais do PDS:

CERTIDÃO	PDS
Funcionário Público (FIRMA)	

CERTIDÃO	PDS
	Espanhol: https://esfirma.com/doc-pki/PDS-V2.0/PDS-AAPP-ES.pdf Inglês: https://esfirma.com/doc-pki/PDS-V2.0/PDS-AAPP-EN.pdf
Funcionário Público – Alto Nível 1.3.6.1.4.1.47281.1.1.1	
Funcionário Público – Nível Médio 1.3.6.1.4.1.47281.1.1.4	
Funcionário Público (AUTENTICAÇÃO)	
Funcionário Público – Alto Nível 1.3.6.1.4.1.47281.1.1.5	
De Funcionário Público com Pseudônimo (ASSINATURA)	
Do EP com Pseudónimo – Alto Nível 1.3.6.1.4.1.47281.1.3.1	
Do EP com Pseudónimo – Nível Intermédio 1.3.6.1.4.1.47281.1.3.4	
Funcionário Público Pseudónimo (AUTENTICAÇÃO)	
De Funcionário Público com Pseudónimo – 1.3.6.1.4.1.47281.1.3.5	
Selo de Órgão	
Selo de Órgão – Nível Intermédio 1.3.6.1.4.1.47281.1.2.2	
Selo de Órgão – Nível Médio Centralizado *1.3.6.1.4.1.47281.1.2.4*	
De Pessoa Física vinculada a entidade (FIRMA)	Espanhol: https://esfirma.com/doc-pki/PDS-V2.0/PDS-PFV-ES.pdf Inglês:

CERTIDÃO	PDS
	https://esfirma.com/doc-pki/PDS-V2.0/PDS-PFV-EN.pdf
PF vinculado a entidades – Qualificado F. 1.3.6.1.4.1.47281.1.6.1	
PF vinculado a entidades – F. Centralizado 1.3.6.1.4.1.47281.1.6.4	
De uma pessoa singular ligada a uma entidade (AUTENTICAÇÃO)	
Da PF ligada a uma entidade 1.3.6.1.4.1.47281.1.6.5	
De uma pessoa singular com um pseudónimo ligado a uma entidade (FIRMA)	
De PF com pseudônimo vinculado a entidade – Assinatura Qualificada 1.3.6.1.4.1.47281.1.7.1	
De PF com pseudônimo vinculado a entidade – Firma Centralizado 1.3.6.1.4.1.47281.1.7.4	
De uma Pessoa com um pseudônimo, vinculado a uma entidade (AUTENTICAÇÃO)	
Da PF com pseudônimo, ligado a uma entidade 1.3.6.1.4.1.47281.1.7.5	
Selo Eletrónico	
Selo Eletrônico em Software 1.3.6.1.4.1.47281.1.8.2	
Selo Eletrônico Centralizado 1.3.6.1.4.1.47281.1.8.4	
Selo Eletrônico para TSA/TSU	Espanhol: https://esfirma.com/doc-pki/PDS-V1.5/TSADS-ES.pdf Inglês: https://esfirma.com/doc-pki/PDS-V1.5/TSADS-EN.pdf
E-Seal para TSA/TSU em HSM 1.3.6.1.4.1.47281.1.5.2	

Nos certificados de cartão, o subscritor 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 à esFIRMA.

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

esFIRMA nunca gera chaves em software para serem enviadas através de canais inseguros para o signatário.

As chaves são geradas usando o algoritmo de chave pública RSA, com um comprimento mínimo de 2048 bits, o algoritmo de chave pública da curva elíptica de 256 bits 1.2.840.10045.3.1.7 (NIST-P256/secp256r1).

6.1.2 Enviando a chave privada para o signatário

Em certificados em um dispositivo de assinatura seguro, a chave privada é devidamente protegida dentro do dispositivo seguro.

Nos certificados de software, a chave privada do signatário é criada no sistema informático utilizado por este signatário quando faz o pedido de certificado, para que a chave privada seja devidamente protegida dentro do sistema informático do signatário.

6.1.3 Envio da chave pública ao emissor do certificado

O método de encaminhamento da chave pública para o provedor de serviços de certificação é PKCS#10, outra prova criptográfica equivalente, ou qualquer outro método aprovado pela esFIRMA.

Quando as chaves são geradas em um DCCF, o esFIRMA garante que a chave pública enviada ao provedor de serviços de certificação venha de um par de chaves geradas por esse DCCF.[14]

[14] ETSI EN 319 411-2 Ponto 6.5.1.b)

6.1.4 Distribuição da chave pública do prestador de serviços de certificação

As chaves da esFIRMA são comunicadas a terceiros que confiam em certificados, garantindo a integridade da chave e autenticando a sua origem, publicando-as no Depositário.

Os usuários podem acessar o Vault para obter as chaves públicas e, adicionalmente, em aplicativos S/MIME, a mensagem de dados pode conter uma cadeia de certificados, que são distribuídos aos usuários.

O certificado das autoridades de certificação raiz e subordinadas estará disponível para os usuários no site da esFIRMA.

6.1.5 Tamanhos das chaves

O comprimento das chaves de autoridade de certificação raiz é RSA 4096 bits.
O comprimento da chave da autoridade de certificação subordinada é RSA 4096 bits.
O comprimento das chaves TSA é RSA 4096 bits.
As chaves para certificados de entidade final são RSA 2048 ou chave pública de curva elíptica de 4096 bits ou 256 bits 1.2.840.10045.3.1.7 (NIST-P256/secp256r1).

6.1.6 Geração de parâmetros de chave pública e verificação de qualidade

A chave pública da autoridade de certificação raiz, das autoridades de certificação subordinadas e dos certificados de assinante é codificada de acordo com a RFC 5280.

Qualidade do parâmetro de chave pública

- Comprimento do módulo = 4096
- Algoritmo de geração de chaves: rsagen1
- Sumário: SHA256.

Todas as chaves são geradas em bens de equipamento, conforme indicado na secção 6.1.1.

6.1.7 Finalidades do Uso de Chaves

Os principais usos para certificados de CA são exclusivamente para assinar certificados e CRLs.

Os usos de chaves para certificados de entidade final são exclusivamente para assinatura digital e não repúdio.

6.2 Proteção de Chave Privada e Controles de Módulo Criptográfico

6.2.1 Padrões do módulo criptográfico

Em relação aos módulos que gerem as chaves esFIRMA e os subscritores de certificados de assinatura eletrónica, é assegurado o nível exigido pelas normas indicadas nas secções anteriores.

6.2.2 Controlo por mais de uma pessoa (n de m) sobre a chave privada

Um controle de várias pessoas é necessário para a ativação da chave privada da autoridade de certificação. No caso deste DPC, existe uma política de **3 em cada 5** pessoas para a ativação das senhas.

Os dispositivos criptográficos são fisicamente protegidos, conforme determinado neste documento.

6.2.3 Depósito de Chave Privada

O esFIRMA não armazena cópias das chaves privadas dos signatários.

6.2.4 Backup de chave privada

O esFIRMA faz uma cópia de segurança das chaves privadas das AC que permitem recuperá-las em caso de desastre, perda ou deterioração das mesmas. Tanto a geração da cópia como a sua recuperação requerem a participação de pelo menos duas pessoas.

Estes ficheiros de recuperação são armazenados em armários à prova de fogo e no centro de custódia externo.

As chaves de signatário no hardware não podem ser copiadas, pois não podem sair do dispositivo criptográfico.

6.2.5 Arquivamento de chave privada

As chaves privadas da autoridade de certificação são arquivadas por um período de **10 anos** após a emissão do último certificado. Eles serão armazenados em arquivos seguros à prova de fogo e no centro de custódia externo. Pelo menos duas pessoas serão necessárias para recuperar a chave privada das autoridades de certificação no dispositivo criptográfico inicial.

6.2.6 Inserindo a chave privada no módulo criptográfico

As chaves privadas são geradas diretamente nos módulos criptográficos de produção da esFIRMA.

6.2.7 Armazenando chaves privadas em módulos criptográficos

As chaves privadas da Autoridade de Certificação são armazenadas criptografadas nos módulos criptográficos de produção esFIRMA.

6.2.8 Método de Ativação de Chave Privada

A chave privada esFIRMA é ativada através da execução do procedimento de arranque seguro correspondente do módulo criptográfico, pelas pessoas indicadas na secção 6.2.2.

As chaves da AC são ativadas por um processo de m de n.

A ativação das chaves privadas da autoridade de certificação intermediária é tratada com o mesmo processo m de n que as chaves da autoridade de certificação.

6.2.9 Método de Desativação de Chave Privada

Para desativar a chave privada esFIRMA, siga os passos descritos no manual do administrador do equipamento criptográfico correspondente.

Por sua vez, o signatário deve inserir o PIN para a nova ativação.

6.2.10 Método de destruição de chave privada

Antes da destruição das chaves, o certificado das chaves públicas associadas a elas será revogado.

Os dispositivos que têm qualquer parte das chaves privadas esFIRMA armazenadas serão fisicamente destruídos ou reiniciados em um nível baixo. Para remoção, as etapas descritas no manual do administrador do computador criptográfico serão seguidas.

Finalmente, os backups serão destruídos com segurança.

As chaves do signatário no software podem ser destruídas excluindo-as, seguindo as instruções do aplicativo que as hospeda.

As chaves de hardware do signatário podem ser destruídas através de uma aplicação informática especial nas instalações da RA ou da esFIRMA.

6.2.11 Classificação do Módulo Criptográfico

Os módulos criptográficos estão sujeitos aos controlos de engenharia previstos nas normas descritas ao longo desta secção.

Os algoritmos de geração de chaves utilizados são comummente aceites para a utilização da chave a que se destinam.

Todas as operações criptográficas esFIRMA são realizadas em módulos com certificações FIPS 140-2 nível 3.

6.3 Outros aspetos da gestão de pares de chaves

6.3.1 Ficheiro de chave pública

O esFIRMA arquiva regularmente as suas chaves públicas de acordo com a secção 5.5 deste documento.

6.3.2 Períodos de utilização de chaves públicas e privadas

Os períodos de utilização das chaves são os determinados pela duração do certificado, após os quais não podem continuar a ser utilizadas.

6.4 Dados de ativação

6.4.1 Geração e instalação de dados de ativação

Os dados de ativação dos dispositivos que protegem as chaves privadas do esFIRMA são gerados de acordo com as disposições da seção 6.2.2 e os procedimentos de cerimônia de chave.

A criação e distribuição de tais dispositivos é registrada.

Da mesma forma, o esFIRMA gera os dados de ativação de forma segura.

6.4.2 Proteção dos dados de ativação

Os dados de ativação dos dispositivos que protegem as chaves privadas das Autoridades de Certificação raiz e subordinadas são protegidos pelos titulares dos cartões de administradores dos módulos criptográficos, conforme consta no documento da cerimônia de chaves.

O signatário do certificado é responsável pela proteção da sua chave privada, com uma palavra-passe tão completa quanto possível. O signatário deve lembrar-se desta palavra-passe.

6.4.3 Outros aspetos dos dados de ativação

Não aplicável.

6.5. Controlos de segurança informática

A esFIRMA utiliza sistemas fiáveis para oferecer os seus serviços de certificação. A esFIRMA realizou controlos e auditorias informáticas de forma a estabelecer uma gestão adequada dos seus ativos informáticos com o nível de segurança exigido na gestão dos sistemas de certificação eletrónica.

O equipamento utilizado é inicialmente configurado com os perfis de segurança adequados pelo pessoal dos sistemas esFIRMA, nos seguintes aspetos:

- Configurações de segurança do sistema operacional.
- Configurações de segurança do aplicativo.
- Dimensionamento correto do sistema.
- Configurações de usuário e permissões.
- Registrar configurações de eventos.
- Plano de backup e recuperação.
- Configurações de antivírus.
- Requisitos de tráfego de rede.

6.5.1 Requisitos técnicos específicos para a segurança informática

Cada servidor esFIRMA inclui as seguintes funcionalidades:

- Controle de acesso aos serviços SubCA e gerenciamento de privilégios.
- Impor a separação de funções para a gestão de privilégios.
- Identificação e autenticação de funções associadas a identidades.
- Arquivamento do histórico e dos dados de auditoria do assinante e da SubCA.
- Auditoria de eventos relacionados à segurança.
- Autodiagnóstico de segurança relacionado aos serviços SubCA.
- Chave SubCA e mecanismos de recuperação do sistema.

As funcionalidades expostas são realizadas através de uma combinação de sistema operacional, software PKI, proteção física e procedimentos.

No caso de a esFIRMA distribuir dispositivos de criação de assinatura qualificados, verificará sempre se esses dispositivos continuam a ser certificados como DCCF.[15]

A verificação da certificação DCCF é realizada durante todo o período de validade do certificado[16]. Caso a DCCF perca a sua certificação como tal, a esFIRMA procederá à revogação dos certificados emitidos na referida DCCF, informando os titulares dos mesmos.

O esFIRMA requer autenticação multifator para todas as contas capazes de causar diretamente a emissão de certificados.

6.5.2 Avaliação do nível de segurança informática

A autoridade de certificação e os pedidos de registo utilizados pela esFIRMA são fiáveis.

6.6 Controlos técnicos do ciclo de vida

6.6.1 Controlos de Desenvolvimento de Sistemas

As aplicações são desenvolvidas e implementadas pela esFIRMA de acordo com as normas de desenvolvimento e controlo de mudanças.

As aplicações possuem métodos para verificar a integridade e autenticidade, bem como a exatidão da versão a ser utilizada.

6.6.2 Controlos de Gestão de Segurança

A esFIRMA desenvolve as atividades necessárias à formação e sensibilização dos colaboradores em termos de segurança. Os materiais utilizados na formação e os documentos que descrevem os processos são atualizados após aprovação por um grupo

15 ETSI 319 411-2 Ap 6.5.1.a)

16 ETSI EN 319 411-2 Ponto 6.5.1.c)

de gestão da segurança. No exercício desta função, dispõe de um plano anual de formação.

A esFIRMA exige, por contrato, medidas de segurança equivalentes às de qualquer prestador externo envolvido nos trabalhos de certificação.

Classificação e gestão da informação e dos ativos

A esFIRMA mantém um inventário de bens e documentação e um procedimento de gestão deste material para garantir a sua utilização.

O sistema de gestão de segurança da informação da esFIRMA detalha os procedimentos de gestão da informação onde é classificada de acordo com o seu nível de confidencialidade.

Os documentos estão catalogados em quatro níveis: PÚBLICO, RESTRITO, USO INTERNO e CONFIDENCIAL.

Operações de gestão

O esFIRMA dispõe de um procedimento adequado de gestão e resposta a incidentes, através da implementação de um sistema de alerta e da geração de relatórios periódicos.

A esFIRMA documentou todo o procedimento relativo às funções e responsabilidades do pessoal envolvido no controlo e manuseamento dos elementos contidos no processo de certificação.

Tratamento e segurança dos meios de comunicação

Todos os meios são tratados de forma segura de acordo com os requisitos de classificação da informação. A mídia que contém dados confidenciais é destruída com segurança se não for necessária novamente.

Planeamento do sistema

O departamento de Sistemas da esFIRMA mantém um registo das capacidades do equipamento. Juntamente com a aplicação do controle de recursos de cada sistema, um possível redimensionamento pode ser previsto.

Relatórios de incidentes e respostas
A esFIRMA dispõe de um procedimento de monitorização de incidentes e da sua resolução.

Procedimentos operacionais e responsabilidades
esFIRMA define atividades, atribuídas a pessoas com um papel de confiança, além das pessoas encarregadas de realizar operações diárias que não são confidenciais.

Gestão do sistema de acesso

esFIRMA faz todos os esforços razoáveis para confirmar que o sistema de acesso é limitado a pessoas autorizadas.

Em especial:

AC Geral

- Firewall, antivírus e controles baseados em IDS estão disponíveis em alta disponibilidade.
- Os dados sensíveis são protegidos através de técnicas criptográficas ou controlos de acesso com forte identificação.
- O esFIRMA tem um procedimento documentado para gerir registos e cancelamentos de utilizadores e uma política de acesso detalhada na sua política de segurança.
- A esFIRMA tem procedimentos em vigor para garantir que as operações são realizadas em conformidade com a política de funções.
- Cada pessoa tem um papel associado para realizar as operações de certificação.
- Os colaboradores da esFIRMA são responsáveis pelos seus atos através do compromisso de confidencialidade assinado com a empresa.

Geração de certificados

A autenticação para o processo de emissão é realizada por meio de um sistema de n operadores para a ativação da chave privada esFIRMA.

Gestão de Revogação
A revogação será realizada por autenticação forte para os aplicativos de um administrador autorizado. Os sistemas de log gerarão as provas que garantem o não repúdio da ação realizada pelo administrador da esFIRMA.

Estado de revogação
O aplicativo de status de revogação tem controle de acesso baseado em certificado ou autenticação de dois fatores para evitar tentativas de modificar as informações de status de revogação.

6.6.3 Avaliação da segurança do ciclo de vida

A esFIRMA garante que o hardware criptográfico utilizado para a assinatura do certificado não é adulterado durante o transporte, inspecionando o material entregue.

O hardware criptográfico é movido em mídia preparada para evitar qualquer manipulação.

esFIRMA registra todas as informações pertinentes do dispositivo para adicionar ao catálogo de ativos.

O uso de hardware de assinatura de certificado criptográfico requer o uso de pelo menos dois funcionários confiáveis.

A esFIRMA realiza testes periódicos para garantir o correto funcionamento do dispositivo.

O dispositivo de hardware criptográfico só é adulterado por pessoal confiável.
A chave de assinatura privada esFIRMA armazenada no hardware criptográfico será excluída assim que o dispositivo for removido.

A configuração do sistema esFIRMA, bem como as suas modificações e atualizações, são documentadas e controladas.

A esFIRMA tem um contrato de manutenção de dispositivos. As alterações ou atualizações são autorizadas pelo gestor de segurança e refletidas nos relatórios de trabalho correspondentes. Essas configurações serão feitas por pelo menos duas pessoas confiáveis.

6.7 Controlos de Segurança de Rede

O esFIRMA protege o acesso físico aos dispositivos de gestão de rede, e tem uma arquitetura que ordena o tráfego gerado com base nas suas características de segurança, criando secções de rede claramente definidas. Esta divisão é feita através do uso de firewalls.

As informações confidenciais transferidas através de redes não seguras são encriptadas utilizando protocolos SSL ou o sistema VPN com autenticação de dois fatores.

6.8 Fontes de tempo

O esFIRMA tem um procedimento coordenado de sincronização de tempo via NTP. O valor de tempo na TSU é rastreável até um valor de tempo distribuído por um UTC(k) laboratório, o ROA (Observatório Real da Marinha) e mantém a precisão de assista com pelo menos quatro fontes de tempo STRATUM-1.

6.9 Algoritmos de assinatura e parâmetros do sistema de assinatura centralizado

O serviço de assinatura centralizada gera chaves para os signatários com o algoritmo RSA com um comprimento de chave de 2048 bits com primos prováveis usando o algoritmo FIPS 186-4 B.3.6 e DRBG (Deterministic Random Bit Generator) no Modo Aleatório Real (ruído de hardware) de acordo com o NIST SP 800-90A e testes contínuos de acordo com o FIPS 140-2. Fora do módulo HSM, as chaves são armazenadas criptografadas com o algoritmo AES-GCM e um comprimento de chave de 256 bits. A chave de criptografia é derivada do PIN do usuário e da chave mestra do HSM. A chave mestra HSM usa o

algoritmo ECDSA NIST-P256/secp256r1 (OID 1.2.840.10045.3.1.7) e requer 3 de 5 cartões para ativação e foi gerada em uma cerimônia de inicialização de alta segurança. O PIN do usuário é derivado de um sal de servidor com o algoritmo PBKDF2-SHA1. O transporte do SAD (Signature Activation Data) do SIC (Signature Interaction Component) para o SAM (Signature Activation Module) é protegido por AES-GCM com uma chave de 256 bits derivada de uma troca de chaves usando o algoritmo ECDH de acordo com o NIST SP 800-56A. A chave do servidor é publicada no repositório web esFirma, seção "Informações de segurança de assinatura remota". O sistema permite a geração de assinaturas eletrônicas com o algoritmo RSA PKCS#1 v1.5, DSA com chave de curva elíptica e algoritmo de resumo SHA-256 e SHA-512.

7. Perfis de certificado, CRL e OCSP

7.1 Perfil do certificado

Todos os certificados qualificados emitidos sob esta política estão em conformidade com os seguintes padrões X.509 versão 3, RFC 5280, RFC 3739 e ETSI:

- ETSI EN 319 412-2 para certificados emitidos a pessoas singulares
- ETSI EN 319 412-3 para os certificados emitidos a pessoas coletivas
- ETSI EN 319 412-5 para a definição de QCStatements de certificados qualificados em conformidade com o RD (UE) 910/2014.

O esFIRMA gera números de série de certificados não sequenciais superiores a zero (0) que contêm pelo menos 128 bits de saída de um CSPRNG.

7.1.1 Número da versão

esFIRMA emite certificados X.509 Versão 3

7.1.2 Extensões de certificado

As extensões dos certificados estão detalhadas nos documentos de perfil acessíveis a partir do site da esFIRMA https://www.esfirma.com

7.1.3 Identificadores de objeto (OIDs) de algoritmos

O ID do objeto do algoritmo de assinatura é:

- 1.2.840.113549.1.1.11 sha256ComRSAEncryption
- 1.2.840.10045.4.3.2 sha256ComECDSA

O identificador de objeto do algoritmo de chave pública é:

- 1.2.840.113549.1.1.1 rsaEncriptação
- 1.2.840.10045.3.1.7 NIST-P256/secp256r1
-

7.1.4 Formatação de nomes

Os certificados devem conter as informações necessárias para a sua utilização, conforme determinado pela política correspondente.

A codificação do certificado segue a recomendação RFC 5280 "X.509 Internet Public Key Infrastructure Certificate and Certificate Revocation List (CRL)
Visualizar perfis em https://www.esfirma.com

7.1.5 Restrição de nomes

Os nomes contidos nos certificados são restritos a X.500 "Distinguished Names", que são únicos e inequívocos.

7.1.6 Identificador de objeto (OID) de tipos de certificado

Todos os certificados incluem um identificador de política de certificados ao abrigo do qual foram emitidos, em conformidade com a estrutura indicada no ponto 1.2.1

7.1.7 Usando a extensão de restrições de política

Não aplicável

7.1.8 Qualificadores de política, sintaxe e semântica

Não aplicável

7.1.9 Processando semântica para extensão crítica de políticas de certificado

A extensão "Política de Certificado" identifica a política que define as práticas que o esFIRMA associa explicitamente ao certificado. A extensão pode conter um qualificador de política. Ver 7.1.6

7.1.10 Restrições de comprimento do elemento

Para todos os perfis, as seguintes restrições de comprimento máximo de caracteres são definidas para os seguintes elementos:

Elemento	**Comprimento máximo esFIRMA**	**Longitude Base**	**Norma**
2.5.4.42 *(nome_dado,GN)*	**127**	32000***	RFC5280
2.5.4.10 (nomedaorganização)	**256**	64	RFC5280
2.5.4.11 (organizationalUnitName)	**256**	32	RFC5280
2.5.4.4 (apelidos)	**256**	40	RFC5280
2.5.4.3 (nome comum, CN)	**400**	64	RFC5280
2.5.4.5 (número de série, SN)	32*	32	RFC5280
2.5.4.97 (organizationIdentifier)	**32**	MÁX**	X520
2.5.4.65 (pseudónimo)	**64***	128	RFC5280
2.5.4.12 (título)	64*	64	RFC5280

*As normas ETSI EN 319 412-2 4.2.4 e ETSI EN 319 412-3 4.2.1 permitem exceder os limites estabelecidos no RFC 5280 (desde que indicado no DPC) para os campos de assunto indicados de acordo com o tipo de certificado (givenName, sobrenome, pseudônimo, commonName, organizationName e organizationalUnitName), mas não o resto dos campos. O comprimento destes campos está de acordo com RFC 5280.
** MAX indica que o limite superior não é especificado (RFC5280 Apêndice B. Notas ASN1)
32000 ub-name usado em vez de ub-givenname (16)

Os comprimentos máximos para todos os outros elementos são especificados no RFC-5280

7.2 Perfil da Lista de Revogação de Certificados

De acordo com o padrão IETF RFC 3280

7.2.1 Número da versão

Os CRLs emitidos pela esFIRMA são a versão 2.

7.2.2 Extensões de CRL e CRL

crlExtensões:

2.5.29.35 (Identificador da chave da autoridade)

2.5.29.20 (número CRL)

crlEntryExtensions

2.5.29.21 (Código da razão)

7.3 Perfil OCSP

De acordo com o padrão IETF RFC 6960

7.3.1 Número da versão

Os OCSPs emitidos pela esFIRMA são a versão 3.

7.3.2 Extensões OCSP

responseExtensions

Id: 1.3.6.1.5.5.7.48.1.2 (Extensão Nonce OCSP)

Crítica: verdadeira

8. Auditoria de conformidade

A esFIRMA anunciou que o início da sua atividade como prestador de serviços de certificação pelo Ministério da Economia e Transformação Digital está sujeito às revisões de controlo que este organismo considere necessárias.

8.1 Frequência da auditoria de conformidade

A esFIRMA realiza anualmente uma auditoria de conformidade, para além das auditorias internas que realiza a seu critério ou a qualquer momento, devido a uma suspeita de incumprimento de uma medida de segurança.

A esFIRMA monitoriza o cumprimento deste documento e controla rigorosamente a qualidade do seu serviço, realizando autoauditorias pelo menos trimestrais com base numa amostra selecionada aleatoriamente do maior de um certificado ou de pelo menos três por cento dos Certificados por si emitidos durante o período que se inicia imediatamente após a autoauditoria anterior.

8.2 Identificação e qualificação do auditor

As auditorias são conduzidas por uma empresa de auditoria terceirizada independente que demonstra competência técnica e experiência em segurança de computadores, segurança de sistemas de informação e auditorias de conformidade de serviços de certificação de chave pública e elementos relacionados.

8.3 Relação do auditor com a entidade auditada

As empresas de auditoria são de reconhecido prestígio com departamentos especializados na realização de auditorias informáticas, pelo que não existe qualquer conflito de interesses que possa distorcer as suas ações em relação à esFIRMA.

8.4 Lista dos elementos sujeitos a auditoria

A auditoria verifica em relação a esta ASSINATURA:

a) Que a entidade dispõe de um sistema de gestão que garanta a qualidade do serviço prestado.
b) Que a entidade cumpra os requisitos do DPC e demais documentação relacionada com a emissão dos diferentes certificados digitais.
c) Que o DPC e outra documentação legal relacionada estão de acordo com o que foi acordado pela esFIRMA e com as disposições dos regulamentos vigentes.
d) Que a entidade gere adequadamente os seus sistemas de informação

Em especial, os elementos sujeitos a auditoria serão os seguintes:

a) Processos de AC, RAs e elementos relacionados.
b) Sistemas de informação.
c) Proteção do centro de dados.
d) Documentos.

8.5 Medidas a tomar em resultado de uma falta de conformidade

Uma vez recebido pela administração o relatório da auditoria de conformidade realizada, as deficiências encontradas são analisadas com a empresa que executou a auditoria e é desenvolvido e executado um plano corretivo para resolver essas deficiências.

Se a esFIRMA não for capaz de desenvolver e/ou executar tal plano ou se as deficiências encontradas representarem uma ameaça imediata à segurança ou integridade do sistema, deve notificar imediatamente a direção da esFIRMA, que pode realizar as seguintes ações:

- Cessar temporariamente as operações.
- Revogue a chave da autoridade de certificação e regenere a infraestrutura.
- Encerre o serviço CA.
- Outras ações complementares que possam ser necessárias.

8.6 Tratamento dos relatórios de auditoria

Os relatórios dos resultados da auditoria são entregues aos quadros superiores da esFIRMA no prazo máximo de 15 dias após a realização da auditoria.

9. Requisitos comerciais e legais

9.1 Taxas

9.1.1 Taxa de Emissão ou Renovação de Certificados

A esFIRMA pode estabelecer uma taxa para a emissão de certificados, dos quais, se for caso disso, os assinantes serão informados oportunamente.

9.1.2 Taxa de Acesso ao Certificado

A esFIRMA não estabeleceu qualquer taxa de acesso aos certificados.

9.1.3 Taxa de Acesso à Informação sobre o Estado do Certificado

A esFIRMA não estabeleceu qualquer taxa de acesso à informação sobre o estado do certificado.

9.1.4 Taxas por Outros Serviços

Sem estipulação.

9.1.5 Política de Levantamentos

Sem estipulação.

9.2 Responsabilidade financeira

A esFIRMA dispõe de recursos financeiros suficientes para manter as suas operações e cumprir as suas obrigações, bem como para enfrentar o risco de responsabilidade por danos, conforme estabelecido na norma ETSI EN 319 401-1 7.12 c), em relação à gestão da cessação de serviços e plano de cessação.

9.2.1 Cobertura de Seguro

A esFIRMA tem a garantia de cobertura suficiente da sua responsabilidade civil, através de um seguro de responsabilidade civil profissional que cumpra o disposto no regime de obrigações e responsabilidades do Regulamento (UE) n.º 910/2014, e com o artigo 9.º, n.º 3, alínea b), da Lei n.º 6/2020, de 11 de novembro, que regula determinados aspetos dos serviços de confiança eletrónicos, com um seguro mínimo de 3.000.000 euros.

9.2.2 Outros ativos

Sem estipulação.

9.2.3 Cobertura de seguro para assinantes e terceiros que dependem de certificados

A esFIRMA tem a garantia de cobertura suficiente da sua responsabilidade civil, através de um seguro de responsabilidade civil profissional que cumpra o disposto no regime de obrigações e responsabilidades do Regulamento (UE) n.º 910/2014, e com o artigo 9.º, n.º 3, alínea b), da Lei n.º 6/2020, de 11 de novembro, que regula determinados aspetos dos serviços de confiança eletrónicos com um seguro mínimo de 3.000.000 euros.

9.3 Confidencialidade das informações

9.3.1 Informações confidenciais

As seguintes informações são mantidas confidenciais pela esFIRMA:

- Pedidos de certificados, aprovados ou indeferidos, bem como quaisquer outras informações pessoais obtidas para a emissão e manutenção de certificados, exceto as informações indicadas na seção seguinte.
- Chaves privadas geradas e/ou armazenadas pelo prestador de serviços de certificação.
- Logs de transações, incluindo logs completos e logs de auditoria de transações.
- Registos de auditoria interna e externa, criados e/ou mantidos pelo Organismo de Certificação e pelos seus auditores.
- Continuidade de negócios e planos de emergência.
- Política e planos de segurança.

- Documentação das operações e outros planos de operação, tais como arquivamento, acompanhamento e outros documentos similares.
- Todas as outras informações identificadas como "Confidenciais".

9.3.2 Informações não confidenciais

As seguintes informações são consideradas não confidenciais:

- Certificados emitidos ou em vias de emissão.
- A ligação do assinante a um certificado emitido pela Autoridade de Certificação.
- O nome e apelidos da pessoa singular identificada no certificado, bem como quaisquer outras circunstâncias ou dados pessoais do titular, caso sejam significativos para a finalidade do certificado.
- O endereço eletrónico da pessoa singular identificada no certificado, ou o endereço eletrónico atribuído pelo assinante, se for significativo em termos da finalidade do certificado.
- Os usos e limites econômicos descritos no certificado.
- O prazo de validade do certificado, bem como a data de emissão do certificado e a data de validade.
- O número de série do certificado.
- Os diferentes estados ou situações do certificado e a data de início de cada um deles, especificamente: geração e/ou entrega pendente, válido, revogado, suspenso ou expirado e o motivo que causou a mudança de status.
- Listas de revogação de certificados (CRLs), bem como outras informações de status de revogação.
- Quaisquer outras informações não listadas na seção anterior.

9.3.3 Divulgação de Informações sobre Suspensão e Revogação

Ver secção anterior.

9.3.4 Divulgação Legal de Informações

A esFIRMA divulga informações confidenciais apenas nos casos previstos na lei.

Especificamente, os registros que garantem a confiabilidade dos dados contidos no certificado, bem como os registros relacionados à confiabilidade dos dados e aqueles relacionados à operação[17], serão divulgados se necessário para fornecer provas da certificação em um processo judicial, mesmo sem o consentimento do assinante do certificado.

A esFIRMA indicará estas circunstâncias na política de privacidade prevista na secção 9.4.

9.3.5 Divulgação de informações a pedido do proprietário

O esFIRMA inclui, na política de privacidade prevista no ponto 9.4, requisitos para permitir a divulgação das informações do assinante e, quando aplicável, da pessoa singular identificada no certificado, diretamente a este ou a terceiros.

9.3.6 Outras circunstâncias de divulgação de informações

Sem estipulação.

9.4 Privacidade de Informações Pessoais

A esFIRMA compromete-se a cumprir a regulamentação relativa à proteção de dados pessoais, com as correspondentes medidas de segurança, conforme estabelecido no REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. e na Lei Orgânica 3/2018, de 5 de dezembro, sobre a Proteção de Dados Pessoais e garantia dos direitos digitais.

A esFIRMA obtém os dados pessoais contidos nos ficheiros através da captura dos dados pelo ASSINANTE, que deve tê-los obtido legalmente junto da parte competente, nas condições previstas nos regulamentos sobre assinaturas eletrónicas e sobre a proteção de dados pessoais.

[17] Ponto 7.10.c) da norma ETSI EN 319 401

A esFIRMA tem a qualidade de subcontratante de dados pessoais e, como tal, trata os dados única e exclusivamente para as finalidades contidas na presente Declaração de Práticas de Certificação, de acordo com as instruções do responsável pelo tratamento dos dados, que é o ASSINANTE e que estão incluídas no Anexo "*Anexo 1: Para o tratamento de dados pessoais pela ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. na sua qualidade de SUBCONTRATANTE*", que rege o contrato de prestação do serviço "Gestiona" entre o ASSINANTE e a ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.

9.4.1 Plano de Privacidade

A esFIRMA desenvolveu uma política de privacidade em conformidade com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE, e com a Lei Orgânica 3/2018, de 5 de dezembro, sobre a Proteção de Dados Pessoais e garantia dos direitos digitais, e documentou nesta Declaração de Práticas de Certificação, bem como no Anexo "Anexo 1: *Para o tratamento de dados pessoais pela ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. na sua qualidade de PROCESSADOR DE DADOS*" que rege o contrato de prestação do serviço "Gerir" entre o ASSINANTE e a ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A., os aspetos, procedimentos e medidas de segurança e organização em conformidade com o regime de obrigações e responsabilidades constantes dos regulamentos anteriores.

9.4.2 Informações tratadas como privadas

Informações pessoais sobre um indivíduo que não estão disponíveis publicamente no o conteúdo de um certificado ou CRL é considerado privado.

9.4.3 Informações não consideradas privadas

A informação pessoal sobre um indivíduo disponível no conteúdo de um certificado ou CRL é considerada não privada, uma vez que é necessária para a prestação do serviço contratado, sem prejuízo dos direitos correspondentes ao titular dos dados pessoais ao abrigo da legislação LOPD/GDPR.

9.4.4 Responsabilidade de proteger informações privadas

As informações confidenciais em conformidade com os regulamentos sobre a proteção de dados pessoais estão protegidas contra perda, destruição, danificação, falsificação e tratamento ilícito ou não autorizado, de acordo com os requisitos estabelecidos neste documento, que estão alinhados com as obrigações previstas no REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e da livre circulação desses dados e que revoga a Diretiva 95/46/CE, e a Lei Orgânica 3/2018, de 5 de dezembro, relativa à proteção de dados pessoais e garantia dos direitos digitais.

9.4.5 Aviso e Consentimento para o Uso de Informações Privadas

Antes de iniciarem uma relação contratual, deve ser oferecida às partes interessadas a informação prévia sobre o tratamento dos seus dados pessoais e exercício de direitos, e se for caso disso, obterão o consentimento obrigatório para o tratamento diferenciado do tratamento principal para a prestação dos serviços contratados.

9.4.6 Divulgação em processo judicial ou administrativo

A esFIRMA não divulga nem transfere dados pessoais, exceto nos casos previstos nas secções 9.3.2 a 9.3.6, e na secção 5.8, em caso de cessação do serviço de certificação.

9.4.7 Outras circunstâncias de divulgação de informações

Os dados pessoais não são transferidos para terceiros, a menos que legalmente obrigado.

9.5 Direitos de Propriedade Intelectual

9.5.1 Propriedade dos certificados e informações de revogação

Apenas a esFIRMA detém direitos de propriedade intelectual sobre os certificados que emite, sem prejuízo dos direitos dos assinantes, titulares de chaves e terceiros, aos quais concede gratuitamente uma licença não exclusiva de reprodução e distribuição de certificados, desde que a reprodução seja completa e não altere qualquer elemento do certificado, sendo necessária em relação às assinaturas digitais e/ou sistemas de

encriptação no âmbito de utilização do certificado. e de acordo com a documentação que os vincula.

Além disso, os certificados emitidos pela esFIRMA contêm um aviso legal relativo à propriedade dos mesmos.

Aplicam-se as mesmas regras à utilização de informações sobre a revogação de certificados.

9.5.2 Propriedade da Declaração de Práticas de Certificação

Apenas a esFIRMA tem direitos de propriedade intelectual sobre esta Declaração de Práticas de Certificação.

9.5.3 Propriedade das informações de nome

O assinante e, se for caso disso, a pessoa singular identificada no certificado, conserva todos os direitos, caso existam, sobre a marca, produto ou nome comercial contido no certificado.

O assinante é o proprietário do nome distinto do certificado, que consiste nas informações especificadas no ponto 3.1.1

9.5.4 Propriedade da chave

Os pares de chaves pertencem aos signatários do certificado.

Quando uma chave é dividida em partes, todas as partes da chave são de propriedade do proprietário da chave.

9.6 Obrigações e responsabilidade civil

9.6.1 Obrigações do Organismo de Certificação "esFIRMA"

A esFIRMA garante, sob sua inteira responsabilidade, que cumpre todos os requisitos estabelecidos no DPC, sendo a única responsável pelo cumprimento dos procedimentos descritos, mesmo que parte ou a totalidade das operações sejam externalizadas.

A esFIRMA presta serviços de certificação de acordo com esta Declaração de Práticas de Certificação.

Antes da emissão e entrega do certificado ao assinante, a esFIRMA informa o subscritor dos termos e condições relativos à utilização do certificado, do seu preço e das suas limitações de utilização, através de um contrato de subscritor que incorpora por referência os textos de divulgação (PDS) de cada um dos certificados adquiridos.

O documento de texto de divulgação, também denominado PDS, está em conformidade com o conteúdo do anexo A da norma ETSI EN 319 411-1 v1.1.1 (2016-02), um documento que pode ser transmitido por meios eletrónicos, utilizando um meio de comunicação duradouro ao longo do tempo e numa linguagem compreensível.
A esFIRMA comunica permanentemente quaisquer alterações[18] que ocorram nas suas obrigações, publicando novas versões da sua documentação legal no seu website https://www.esfirma.com

O esFIRMA vincula os assinantes, detentores de chaves e terceiros que confiam em certificados através do referido texto de divulgação ou PDS, em linguagem escrita e compreensível, com os seguintes conteúdos mínimos:

- Requisitos para cumprir o disposto nos pontos 4.5.3, 9.2, 9.6.7, 9.6.8, 9.6.9 e 9.6.10.
- Indicar a política aplicável, indicando que os certificados não são emitidos ao público.
- Declaração de que as informações contidas no certificado estão corretas, salvo notificação em contrário pelo assinante.
- Consentimento para o armazenamento das informações utilizadas para o registo do subscritor e para a transferência dessas informações para terceiros,

[18] Ap 6.2.3.b) do ETSI EN 319 411-1

em caso de cessação das operações do Organismo de Certificação sem revogação de certificados válidos.

- Limites de utilização do certificado, incluindo os estabelecidos no ponto 1.4.2
- Informações sobre a forma de validar um certificado, incluindo o requisito de verificar o seu estatuto e as condições em que o certificado pode ser razoavelmente fiável, o que é aplicável quando o assinante atua como terceiro confiador no certificado.
- A forma como a responsabilidade financeira do Organismo de Certificação é garantida.
- Limitações de responsabilidade aplicáveis, incluindo as utilizações para as quais o Organismo de Certificação aceita ou exclui a sua responsabilidade.
- Período de arquivamento das informações de solicitação de certificado.
- Período de arquivamento do log de auditoria.
- Procedimentos de Resolução de Litígios Aplicáveis.
- Lei aplicável e jurisdição competente.
- Se o Organismo de Certificação foi declarado em conformidade com a política de certificação e, se aplicável, de acordo com que sistema.

9.6.2. Obrigação e Responsabilidade da AR

As RAs são as entidades delegadas pela AC para realizar as tarefas de registo e aprovação de pedidos de certificados, pelo que a RA está também obrigada nos termos definidos nas Práticas de Certificação para a emissão de certificados, nomeadamente:

• Respeitar as disposições deste CPS e do PDS correspondente.

• Proteger as suas chaves privadas que os servirão no exercício das suas funções.

• Verificar a identidade dos Sujeitos/Signatários e Requerentes dos certificados quando necessário, credenciando definitivamente a identidade do Signatário, no caso de certificados individuais, ou do porta-chaves, no caso de certificados de organização, de acordo com o disposto nas seções correspondentes deste documento.

• Verificar a exatidão e autenticidade das informações fornecidas pelo Candidato.

• Fornecer ao signatário, no caso de certificados individuais, ou ao futuro titular de chaves, no caso de certificados da organização, acesso ao certificado.

• Entregar, quando apropriado, o dispositivo criptográfico correspondente.

• Arquivar, pelo período previsto na legislação em vigor, os documentos fornecidos pelo requerente ou signatário.

• Respeitar o disposto nos contratos celebrados com a esFIRMA e com o Sujeito/Signatário.
• Informar a esFIRMA das causas de revogação, desde que tenham conhecimento.
• Fornecer informações básicas sobre a política e o uso do certificado, incluindo especialmente informações sobre esFIRMA e a Declaração de Práticas de Certificação aplicável, bem como as suas obrigações, poderes e responsabilidades.
• Fornecer informações sobre o certificado e o dispositivo criptográfico.
• Recolher informações e provas do titular da receção do certificado e, se for caso disso, do dispositivo criptográfico, e aceitação de tais elementos.
• Informar o titular da chave privada e os seus dados de ativação do certificado e, se for caso disso, do dispositivo criptográfico do método de imputação exclusiva, de acordo com o disposto nas secções correspondentes do presente documento.
Estas obrigações aplicam-se mesmo nos casos de entidades por elas delegadas, como os pontos de verificação presencial (PVP).
As informações sobre a utilização e as responsabilidades do subscritor são fornecidas através do
Aceitação das cláusulas de utilização antes da confirmação do pedido de certificado e por correio eletrónico.

As ARs assinam um contrato de prestação de serviços com a esFIRMA através do qual a esFIRMA delega as funções de registro às RAs, consistindo principalmente em:
1.- Obrigações prévias à emissão de um certificado.
a) Informar adequadamente os requerentes da assinatura das suas obrigações e responsabilidades.
b) A identificação adequada dos candidatos, que devem ser pessoas qualificadas ou qualificadas.
autorizado a solicitar um certificado digital.
c) A correta verificação da validade e validade destes dados dos requerentes, e
da Entidade, no caso de existir uma relação de relação de relação ou representação.
d) Aceder à aplicação da Autoridade de Registo para gerir as candidaturas e certificados emitidos.
2.- Obrigações uma vez emitido o certificado.
a) Celebrar os contratos de Prestação de Serviços de Certificação Digital com os candidatos. Na maioria dos processos de emissão, este contrato é formalizado através da aceitação de condições nos sites que fazem parte do processo

de emissão do certificado, não podendo a emissão ser efetuada sem prévia aceitação das condições de utilização.

b) A manutenção dos certificados durante a sua validade (cessação, suspensão, revogação).

c) Arquivar as cópias da documentação apresentada e dos contratos devidamente assinados pelos candidatos de acordo com as Políticas de Certificação publicadas pela esFIRMA e legislação em vigor.

Assim, as ARs são responsáveis pelas consequências em caso de incumprimento das suas tarefas de registo, e através das quais também se comprometem a respeitar as normas regulamentares internas da entidade certificadora esFIRMA (Políticas e CPS) que devem ser perfeitamente controladas pelas ARs e que devem servir de manual de referência.

No caso de uma reivindicação por um Sujeito, uma Entidade ou um usuário, a autoridade de certificação deve fornecer o

prova de ação diligente e se se verificar que a origem da reclamação reside num erro na validação ou verificação dos dados, a AC pode, por força dos acordos assinados com as AR, obrigar a AR responsável a assumir as consequências.

Porque, embora a AC seja legalmente responsável perante o Sujeito, uma Entidade, ou Parte Utilizadora, e que para o efeito tenha seguro de responsabilidade civil, de acordo com o presente contrato, a AR tem a obrigação contratual de "identificar e autenticar corretamente o Requerente e, se for caso disso, a Entidade correspondente", devendo por força disso responder a esta ASSINATURA pelas suas violações.

Naturalmente, não é intenção da esFIRMA descarregar todo o ónus da assunção de responsabilidade para as AR, em termos de eventuais danos cuja origem resultaria de uma violação das tarefas delegadas nas AR. Por esta razão, tal como previsto para a AC, a AR está sujeita a um regime de controlo que será exercido pela esFIRMA, não só através dos controlos dos arquivos e procedimentos de conservação dos arquivos assumidos pela AR através da realização de auditorias para avaliar, entre outros, os recursos utilizados e o conhecimento e controlo dos procedimentos operacionais para a oferta dos serviços de AR.

As mesmas responsabilidades devem ser assumidas pela AR em virtude de violações do entidades delegadas, tais como pontos de verificação no local (PVP), sem

prejuízo do seu direito de ter repercussões contra eles.

9.6.3 Garantias oferecidas aos assinantes e a terceiros que dependem de certificados

A esFIRMA, na documentação que a vincula a assinantes e terceiros que se baseiam em certificados, estabelece e renuncia a garantias, e limitações de responsabilidade aplicáveis.

esFIRMA, no mínimo, garante ao assinante:

- Que não existem erros factuais nas informações contidas nos certificados, conhecidos ou feitos pelo Organismo de Certificação.
- Que não existem erros factuais nas informações contidas nos certificados, devido à falta de diligência na gestão do pedido de certificado ou na criação do certificado.
- Que os certificados cumprem todos os requisitos materiais estabelecidos na Declaração de Práticas de Certificação.
- Que os serviços de revogação e a utilização do Depósito cumprem todos os requisitos materiais estabelecidos na Declaração de Práticas de Certificação.

A esFIRMA, no mínimo, garantirá ao terceiro que confia no certificado:

- Que as informações contidas ou incorporadas mediante remissão no certificado estão corretas, salvo indicação em contrário.
- Que na aprovação do pedido de certificado e na emissão do certificado, todos os requisitos materiais estabelecidos na Declaração de Práticas de Certificação foram cumpridos.
- A rapidez e segurança na prestação de serviços, especialmente serviços de revogação.

Além disso, a esFIRMA garante ao assinante e ao terceiro que confia no certificado:

- Que o certificado contém as informações que um certificado qualificado deve conter, em conformidade com o anexo 1 do Regulamento (UE) n.º 910/2014.
- Que, no caso de gerar as chaves privadas do assinante ou, se for caso disso, da pessoa singular identificada no certificado, a sua confidencialidade é mantida durante o processo.
- A responsabilidade do Organismo de Certificação, dentro dos limites que são estabelecidos. Em caso algum a ESFIRMA será responsável por casos fortuitos e em caso de força maior.

- A chave privada da autoridade de certificação usada para emitir certificados não foi comprometida, a menos que o esFIRMA não tenha comunicado o contrário.
- Não originou ou introduziu declarações falsas ou erradas nas informações de qualquer certificado, nem deixou de incluir as 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 desta Declaração de Prática, incluindo todos os requisitos legais aplicáveis e aplicáveis.
- Você está vinculado aos procedimentos operacionais e de segurança descritos nesta Declaração de Prática.

9.6.4 Responsabilidade civil e responsabilidade de terceiros

É obrigação da Parte Utilizadora cumprir as disposições dos regulamentos em vigor e, além disso:

- Verificar a validade dos certificados e toda a cadeia de certificação, antes de realizar qualquer operação baseada neles. O esFIRMA dispõe de vários mecanismos para realizar esta verificação, como o acesso a listas de certificados revogados ou serviços de consulta online OCSP.
- Conhecer, estar vinculado e concordar em estar vinculado às garantias, limites e responsabilidades aplicáveis à aceitação e uso dos certificados nos quais você confia.
- Verificar a validade da qualificação de uma assinatura associada a um certificado emitido pela esFIRMA, verificando se a autoridade de certificação que emitiu o certificado está publicada na lista de confiança do supervisor nacional correspondente.

9.6.5 Responsabilidade dos outros participantes

Não estipulado

9.7. Renúncia de Garantia

De acordo com a legislação em vigor, a responsabilidade da esFIRMA e das suas RAs não se estende aos casos em que o uso indevido do certificado tem origem em
conduta imputável ao Sujeito e à Parte Utilizadora por:

- Não prestação de informações adequadas, inicialmente ou posteriormente, tais como:
- em resultado de alterações nas circunstâncias refletidas no certificado eletrónico, quando a sua inexatidão não pôde ser detetada pelo prestador de serviços de certificação
- Negligência no que diz respeito à retenção de dados de criação de assinatura e sua confidencialidade.
- Não ter solicitado a revogação dos dados do certificado eletrónico em caso de dúvida sobre a manutenção da confidencialidade
- Ter utilizado a assinatura após o termo do prazo de validade do certificado eletrónico
- Exceder os limites que aparecem no certificado eletrônico.
- Em conduta imputável à Parte Utilizadora se o Utilizador agir com negligência, ou seja, quando não verificar ou ter em conta as restrições contidas no certificado quanto às suas possíveis utilizações e limite do montante das transações; ou quando não tem em conta o estatuto de validade do certificado
- Danos causados ao Sujeito ou a terceiros que lhe sejam confiados devido à inexatidão dos dados contidos no certificado eletrónico, caso estes tenham sido acreditados através de documento público, inscrito num registo público, se necessário.
- Uma utilização inadequada ou fraudulenta do certificado no caso de o Sujeito/Titular o ter cedido ou autorizado a sua utilização a favor de uma terceira pessoa em virtude de um negócio jurídico como o mandato ou procuração, sendo da exclusiva responsabilidade do Sujeito/Titular controlar as chaves associadas ao seu certificado.

A esFIRMA e as suas ARs não serão responsáveis, em caso algum, quando confrontadas com qualquer uma destas circunstâncias:

- Estado de guerra, desastres naturais ou qualquer outro caso de força maior.
- Para a utilização dos certificados, desde que exceda as disposições dos regulamentos e Políticas de Certificação em vigor
- Devido ao uso indevido ou fraudulento de certificados ou CRLs emitidos pela autoridade de certificação

- Para o uso das informações contidas no Certificado ou na CRL.
- Pelos danos causados no período de verificação das causas de extinção.
- Pelo conteúdo das mensagens ou documentos assinados ou encriptados digitalmente.
- Para a não recuperação de documentos encriptados com a chave pública do Sujeito.

9.8. Limitação de Responsabilidade por Perdas na Transação

O limite máximo que o esFIRMA permite nas transações económicas realizadas é de 0 (zero) euros.

9.9. Compensação

Ver secção 9.2

9.10. Prazo e Conclusão

9.10.1 Vigência

Ver secção 5.8

9.10.2 Rescisão

Ver secção 5.8

9.10.3 Efeito da rescisão e sobrevivência

Ver secção 5.8

9.11. Comunicações às partes interessadas e à entidade supervisora

A esFIRMA estabelece no contrato com o assinante os meios de notificação entre ambas as partes.

Em geral, as comunicações comuns ou coletivas serão feitas através de www.esfirma.com ou da Plataforma Eletrónica de Administração. No caso de notificações individuais, será utilizado e-mail ou correio postal.

Em caso de incidente que possa afetar a segurança, os dados pessoais ou a integridade de uma pessoa singular ou coletiva, aplicar-se-ão as disposições do procedimento de gestão de incidentes esFIRMA.

A esFIRMA dispõe de procedimentos para comunicar à entidade supervisora alterações relevantes na prestação de serviços de confiança.

9.12. Alterações

9.12.1 Procedimento de modificação

A AC reserva-se o direito de alterar este documento por razões técnicas ou para refletir quaisquer alterações nos procedimentos que tenham ocorrido devido a requisitos legais, regulamentos (eIDAS, Órgãos Nacionais de Supervisão, etc.) ou como resultado da otimização do ciclo de trabalho. Cada nova versão deste CPS substitui todas as versões anteriores, que permanecem, no entanto, aplicáveis aos certificados emitidos enquanto essas versões estavam em vigor e até à primeira data de expiração desses certificados. Será publicada pelo menos uma atualização anual. Essas atualizações serão refletidas na caixa de versão no início do documento.
As alterações que possam ser feitas a este CPS não exigem notificação, a menos que afetem diretamente os direitos dos Sujeitos/Signatários dos certificados, caso em que podem enviar seus comentários à organização da administração das políticas no prazo de 15 dias após a publicação.

9.12.2 Mecanismo de notificação e prazos

Todas as alterações propostas a esta política serão imediatamente publicadas no site da esFIRMA. Neste mesmo documento há uma seção de alterações e versões onde você pode descobrir sobre as mudanças que ocorreram desde a sua criação e a data dessas modificações.

As alterações a este documento são comunicadas aos organismos e empresas terceiros que emitem certificados ao abrigo deste SPC, bem como aos auditores correspondentes. Em particular, as alterações a este SPC serão notificadas aos Órgãos Nacionais de Supervisão.

Os signatários/subscritores e os terceiros afetados podem enviar os seus comentários à organização de administração da política no prazo de 15 dias a contar da receção da notificação.

9.12.3 Circunstâncias em que o OID deve ser alterado

Não estipulado

9.13 Procedimento de resolução de litígios

A esFIRMA estabelece, no contrato de subscrição e no texto de divulgação ou PDS, os procedimentos de mediação e resolução de litígios aplicáveis.

9.14. Legislação aplicável

A esFIRMA estabelece, no contrato de subscrição e no texto de divulgação ou PDS, que a lei aplicável à prestação de serviços, incluindo a política e práticas de certificação, é a Lei Espanhola.

9.15. Cumprimento da Lei Aplicável

Ver ponto 9.14.

9.16. Outras disposições

9.16.1 Acordo Integral

Os Titulares e terceiros que confiam nos Certificados assumem integralmente o conteúdo desta Declaração de Práticas e Políticas de Certificação

9.16.2 Repartição

As partes neste DPC não podem ceder nenhum dos seus direitos ou obrigações ao abrigo do presente DPC ou dos acordos aplicáveis sem o consentimento por escrito da esFIRMA.

9.16.3 Separabilidade

A esFIRMA estabelece, no contrato de subscrição, e no texto de divulgação ou PDS, cláusulas de separação, sobrevivência, acordo integral e notificação:

- Nos termos da cláusula de divisibilidade, a nulidade de uma cláusula não afetará o resto do contrato.
- Nos termos da cláusula de sobrevivência, certas regras continuarão em vigor após o termo da relação jurídica que regula o serviço entre as partes. Para o efeito, o Organismo de Certificação garante que, pelo menos, os requisitos contidos nas secções 9.6.1 (Obrigações e responsabilidade), 8 (Auditoria de conformidade) e 9.3 (Confidencialidade), continuam após a cessação do serviço e das condições gerais de emissão/utilização.
- Por força da cláusula de todo o contrato, entender-se-á que o documento legal que regula o serviço contém a vontade completa e todos os acordos entre as partes.
- A cláusula de notificação estabelecerá o procedimento segundo o qual as partes se notificam mutuamente dos factos.

9.16.4 Compliance (Honorários Advocatícios e Renúncia)

A esFIRMA pode pedir uma indemnização e honorários advocatícios a uma parte por danos, perdas e despesas relacionadas com a conduta de tal parte. O facto de esFIRMA não aplica uma disposição deste CPS não elimina o direito de esFIRMA fazer cumprir as mesmas disposições mais tarde ou o direito de fazer cumprir qualquer outra disposição do presente CCP. Para ser eficaz, qualquer renúncia deve ser por escrito e assinada pela esFIRMA

9.16.5 Força Maior

esFIRMA inclui no texto de divulgação ou PDS, cláusulas que limitam a sua responsabilidade em caso fortuito e em caso de força maior.

9.17 Outras disposições

9.17.1 Cláusula de indemnização do subscritor

esFIRMA inclui no contrato com o assinante, uma cláusula pela qual o subscritor se compromete a isentar a Entidade Certificadora de qualquer dano decorrente 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, para a publicação e utilização do certificado, quando se verifique uma das seguintes causas:

- Falsidade ou declaração errada feita pelo utilizador do certificado.
- Erro do utilizador do certificado ao fornecer os dados da aplicação, se a ação ou omissão envolver intenção ou negligência em relação ao Organismo de Certificação ou a qualquer pessoa que confie no certificado.
- Negligência na proteção da chave privada, empregando um sistema confiável ou mantendo as precauções necessárias para evitar comprometimento não autorizado, perda, divulgação, modificação ou uso da chave privada.
- Utilização pelo subscritor de um nome (incluindo nomes comuns, endereço de correio eletrónico e nomes de domínio), ou de outras informações constantes do certificado, que infrinja os direitos de propriedade intelectual ou industrial de terceiros.

9.17.2 Cláusula de indemnização de terceiros que confiam no certificado

esFIRMA inclui no texto de divulgação ou PDS, uma cláusula pela qual o terceiro que confia no certificado concorda em isentar o Organismo de Certificação de qualquer dano decorrente 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, para a publicação e utilização do certificado, quando se verifique uma das seguintes causas:

- Incumprimento das obrigações do terceiro que invoca o certificado.
- Recurso imprudente a um certificado, tendo em conta as circunstâncias.
- Falha na verificação do status de um certificado, para determinar que ele não está suspenso ou revogado.

O terceiro que se baseia no certificado compromete-se a isentar a ESFIRMA de qualquer dano decorrente 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, para a publicação e uso do certificado, quando ocorrer qualquer uma das seguintes causas:

- Incumprimento das obrigações do terceiro que invoca a certidão.
- Recurso imprudente a um certificado, consoante as circunstâncias.
- Não verificação do estado de um certificado, para determinar que não é está suspensa ou revogada.
- Não verificação de todas as medidas de segurança prescritas no DCP ou outras regras aplicáveis.

A ESFIRMA não será responsável pelos danos causados nos termos indicados no artigo 11.º da Lei n.º 6/2020, de 11 de novembro, que regula determinados aspetos dos serviços de confiança eletrónicos.