Declaração de Práticas de Certificação

esFIRMA

Informação geral

Controle documental

Classificação de segurança:	Público
Autor:	ESFIRMA
Versão:	1.16

Estado formal

Preparado por:	Revisado por:	Aprovado por:
Oficina de segurança Data: 21/04/2023	Responsável de segurança Data: 21/04/2023	Comitê de segurança Data: 21/04/2023

Controle de versões

Ver	Descrição da mudança	Fechar
1.0	Criação do documento	29/04/2016
1.1	Subsanaciones	02/06/2016
1.2	Revisão ETSI	19/05/2017
1.3	Revisão de tipos de certificados	
1.4	Revisão de tipos de certificados, acrônimos e definições	02/06/2017
1.5	Ajustes referentes a normas, mudança de denominação, 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 do TSA	20/06/2018
1.7	Correção referente à assinatura na emissão de certificados de software	08/08/2018
1.8	Adaptação por mudança normativa (Regulamento (UE) 910/2014 e Regulamento (UE) 2016/679) e revisão dos parágrafos de renovação.	13/11/2018
1.9	3.1.1.1 Esclarecimento sobre o segundo sobrenome opcional. 3.1.1.2 OrganizationIdentifier condicionado a CA/Browser Forum Guidelines 3.1.1.4 Correção de erros tipográficos nas descrições dos OID 3.1.1.7 CN do certificado EV de sede opcional	14/06/2019
1.10	Várias clarificações em 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 com o RFC 3647 1.5.3. movido para 1.5.2 Dados de contato da organização 1.5.2 movido para 1.5.3 Organização que aprova o documento DEFINIÇÕES ACRÔNIMOS" movido para 1.6 Acrônimos e definições 4.4.2 movido a 4.4.1 Conducta que constituye aceptación del certificado 4.4.3 movido a 4.4.2 Publicação do certificado 4.4.4 movido para 4.4.3 Notificação da 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 do pedido de renovação de certificados Adicionado 4.6.4 Notificação de nova emissão de certificado ao assinante Adicionado 4.6.5 Conduta que constitua a aceitação de um certificado de renovação Adicionado 4.6.6 Publicação do certificado de renovação pela CA Adicionado 4.6.7 Notificação da emissão do certificado pela CA a outras entidades Adicionado 4.7.2 Procedimento com nova identificação 4.7. movido a 4.7.3 Processamento de solicitações de nova chave de certificado 4.7.3 movido a 4.7.4 Notificação da emissão do certificado renovado 4.7.4 movido a 4.7.5 Conduta que constitui aceitação do certificado 4.7.5 movido a 4.7.6 Publicação do certificado 4.7.6 movido para 4.7.7 Notificação da emissão a terceiros 4.11 movido para 4.10 Serviços de verificação do estado dos certificados 4.11.1 movido para 4.10.1 Características operacionais dos serviços 4.11.2 movido para 4.10.2 Disponibilidade dos serviços Adicionado 4.10.3 Características opcionais 4.10 movido a 4.11 Finalização da subscrição 6.1.9 movido para 6.1.7 Propósitos de uso de chaves 6.2.9 movido para 6.2.9 Método de desativação da chave privada 6.2.10 movido para 6.2.10 Método de destruição da chave privada Adicionado 6.2.11 Classificação do módulo criptográfico Adicionado 6.4.3 Outros aspectos dos dados de ativação	08/06/2020

	6.6.2.5 movido para 6.6.3 Avaliação da segurança do ciclo de vida 6.9 movido para 6.8 Fontes de Tempo Adicionado 7.1.7 Uso da extensão de restrições de política Adicionado 7.1.8 Qualificadores de política sintaxe e semântica Adicionado 7.1.9 Semântica de processamento para a extensão crítica de Políticas de certificado Adicionado 7.2.2 CRL e extensões CRL Adicionado 7.3.1 Número de versão Adicionado 7.3.2 Extensões OCSP Adicionado 9.4.1 Plano de privacidade Adicionado 9.4.2 Informação tratada como privada Adicionado 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 Adicionado 9.4.6 Divulgação em conformidade com um processo judicial ou administrativo Adicionado 9.4.7 Outras circunstâncias de divulgação de informação Adicionado 9.6.2 Representações e garantias do RA 9.6.2 movido para 9.6.3 Garantias oferecidas a assinantes e terceiros que confiam em certificados Adicionado 9.6.4 Obrigação e responsabilidade de terceiras partes 9.6.2 movido para 9.6.5 Obrigação e responsabilidade de outros participantes 9.6.3 movido a 9.7 Exoneração de responsabilidade 9.6.4 movido a 9.8 Limitação de responsabilidade em caso de perdas por transações 9.6.5 movido a 9.9 Indemnizações Adicionado 9.10. Prazo e Finalização Adicionado 9.10.1 Prazo Adicionado 9.10.2 Terminação Adicionado 9.10.3 Efeito da rescisão e sobrevivência Adicionado 9.11 Notificações individuais e comunicação com os participantes Adicionado 9.12 Modificações Adicionado 9.12.1 Procedimento de modificação Adicionado 9.12.2 Mecanismo de notificação e prazos Adicionado 9.12.3 Circunstâncias em que o OID deve ser alterado 9.6.10 movido para 9.13 Procedimento de resolução de conflitos 9.6.7 movido para 9.14 Legislação aplicável Adicionado 9.15 Conformidade com a Lei Aplicável Adicionado 9.16 Outras disposições Adicionado 9.16.1 Acordo completo Adicionado 9.16.2 Atribuição 9.6. movido a 9.16.3 Separabilidade Adicionado 9.16.4 Cumprimento (honorários advocatícios e isenção de taxas) 9.6.6 movido para 9.16.5 Força maior Adicionado 9.17 Outras disposições Incluem-se novos certificados: certificado de empregado público (Autenticação), certificado de empregado público com pseudônimo (Autenticação), certificado de pessoa física vinculada a entidade (Autenticação), certificado de pessoa física vinculada a entidade (ASSINATURA), certificado de pessoa física com pseudônimo vinculada a entidade (Autenticação), certificado de pessoa física com pseudônimo vinculada a entidade (ASSINATURA)	
1.11	Inclui novos certificados qualificados de selos eletrônicos O perfil do certificado de sede eletrônica é eliminado. Adaptação devido a mudança normativa (Lei 6/2020, de 11 de novembro, reguladora de determinados aspectos dos serviços eletrônicos de confiança).	03/05/2021

	No se adiciona en la seção 5.8 Término do Serviço do DPC o detalhe de como é fornecida a informação de estado dos certificados além do tempo de vida destes. As referências ao Ministério da Indústria, Energia e Turismo são atualizadas para o Ministério de Assuntos Econômicos e Transformação Digital.	
1.12	O ponto 5.2.1 é modificado mudando a denominação de "Administrador de Registro" para "Operador de Registro". Eliminam-se as referências ao CA/B Forum.	10/05/2021
1.13	Modificação ponto 5.8 Terminação do Serviço, de acordo com o Plano de Encerramento O ponto 4.9.1 é modificado incluindo o fim da certificação do QSCD Modificação do ponto 6.5.1, incluindo o fim da certificação DCCF. Eliminação da referência ao documento de segurança do esFIRMA da seção 6.6.2 (Operações de gerenciamento) Substituição de "política de segurança" por "sistema de gestão de segurança da informação" na seção 6.6.2 (Classificação e gestão de informações e ativos) O parágrafo 6.9 é adicionado de acordo com a ETSI TS 119 431-1: OVR-5.1-02 O ponto 9.6.4 é modificado, incluindo a Cadeia de Certificação como ponto de verificação. É adicionado o sistema de integração com DIR3 como meio para verificação da identidade da entidade (3.2.2) É adicionada a verificação do estado dos certificados da cadeia de certificação na seção 4.9.6.	18/07/2022
1.14	Informação do novo certificado de TSA	16/03/2023
1.15	Ajustes de informações sobre TSA e incorporação de selo de tempo não qualificado	31/03/2023
1.16	Novas restrições de comprimento dos elementos dos perfis de certificados Novos subperfis europeus de Pessoa física e Selo eletrônico Simplificação dos itens 3.2.2 e 3.2.3 Adiciona-se o parágrafo 4.5.3 para separar as informações e obrigações dos terceiros que confiam nos certificados. Diferenças e considerações entre as consultas de estado de revogação de um certificado através do OCSP e CRL 4.10.1	21/04/2023

Índice

1. Introdução

1.1 Apresentação

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

Os certificados emitidos são os seguintes:

- **De Funcionário Público (ASSINATURA)**
  - De Funcionário Público de nível médio
  - De Funcionário Público de nível Alto
- **De Funcionário Público (AUTENTICAÇÃO)**
  - De Funcionário Público de nível Alto
- **De Funcionário Público com pseudônimo (ASSINATURA)**
  - De Funcionário Público de nível médio
  - De Funcionário Público de nível Alto
- **De Funcionário Público com pseudônimo (AUTENTICAÇÃO)**
  - De Funcionário Público de nível Alto
- **De pessoa física vinculada a entidade (FIRMA)**
  - De pessoa física vinculada a entidade de nível médio
  - De pessoa física vinculada a entidade de nível Alto
- **De pessoa física vinculada a entidade (AUTENTICAÇÃO)**
  - De pessoa física vinculada a entidade de nível Alto
- **De pessoa física vinculada a entidade com pseudônimo (ASSINATURA)**
  - De pessoa física vinculada a entidade de nível médio
  - De pessoa física vinculada a entidade de nível Alto
- **De pessoa física vinculada a entidade com pseudônimo (AUTENTICAÇÃO)**
  - De pessoa física vinculada a entidade de nível Alto
- **De Selo de Órgão**
  - Selo de Órgão de nível Médio
- **De Selo Eletrônico para TSA/TSU**
  - De selo eletrônico para TSU em HSM
- **De Selo Eletrônico**
  - De selo eletrônico em software
  - De selo eletrônico com gerenciamento centralizado

1.2 Nome do documento e identificação

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

1.2.1 Identificadores de certificados

Número OID	Políticas de certificados
	De Funcionário Público (ASSINATURA)
1.3.6.1.4.1.47281.1.1.1	*De Empregado Público - Nível Alto em cartão*
1.3.6.1.4.1.47281.1.1.4	*De Funcionário Público - Nível Médio em HSM*
	De Funcionário Público (AUTENTICAÇÃO)
1.3.6.1.4.1.47281.1.1.5	*De Empregado Público - Nível Alto em cartão*
	De Funcionário Público com Pseudônimo (ASSINATURA)
1.3.6.1.4.1.47281.1.3.1	*De EP com pseudônimo - Nível Alto em Cartão*
1.3.6.1.4.1.47281.1.3.4	*De EP com pseudônimo - Nível Médio em HSM*
	De Funcionário Público com Pseudônimo (AUTENTICAÇÃO)
1.3.6.1.4.1.47281.1.3.5	*De EP com pseudônimo - Nível Alto em Cartão*
	De Pessoa Física vinculada a entidade (ASSINATURA)
1.3.6.1.4.1.47281.1.6.1	*De PF vinculada a entidad - Firma-e Qualificada, em Cartão*
1.3.6.1.4.1.47281.1.6.4	*De PF vinculada a entidad - Firma-e Centralizada*
	De Pessoa Física vinculada a entidade (AUTENTICAÇÃO)
1.3.6.1.4.1.47281.1.6.5	*De PF vinculada a entidade - em cartão*
	De Pessoa Física com pseudônimo vinculada a entidade (FIRMA)
1.3.6.1.4.1.47281.1.7.1	*De PF com pseudônimo vinculada a entidade - Firma-e Qualificada, em Cartão*

1.3.6.1.4.1.47281.1.7.4	*De PF com pseudônimo vinculada a entidade - Firma-e Centralizada*
	De Pessoa Física com pseudônimo, vinculada a entidade (AUTENTICAÇÃO)
1.3.6.1.4.1.47281.1.7.5	*De PF com pseudônimo, vinculada a entidade - no cartão*
	De Selo de Órgão
1.3.6.1.4.1.47281.1.2.2	*De Selo de Órgão - Nível Médio em software*
1.3.6.1.4.1.47281.1.2.4	*De Selo de Órgão - Nível Médio em HSM*
	De Selo Eletrônico para TSA/TSU
1.3.6.1.4.1.47281.1.5.1	*De Sello-e para TSA/TSU em HSM*
1.3.6.1.4.1.47281.1.5.2	*De Selo-e qualificado para TSA/TSU em HSM*
	De Selo Eletrônico
1.3.6.1.4.1.47281.1.8.2	*De Selo Eletrônico em software*
1.3.6.1.4.1.47281.1.8.4	*De Selo eletrônico centralizado*

Em caso de contradição entre esta Declaração de Práticas de Certificação e outros documentos de práticas e procedimentos da esFIRMA, prevalecerá o estabelecido nesta Declaração de Práticas.

Este documento está estruturado de acordo com o IETF RFC 3647.

1.3 Participantes nos serviços de certificação

1.3.1. Prestador de serviços de certificação

O provedor de serviços de certificação é a pessoa física ou jurídica que emite e gerencia certificados para entidades finais, usando uma Autoridade de Certificação ou fornecendo outros serviços relacionados à assinatura eletrônica.

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (ANTERIOR AULOCE SA), doravante denominada ESPUBLICO, com sede na Calle Bari 39 (Edif. Binary Building), C.P. 50.197, em Zaragoza, CIF A-50.878.842, registrada no Registro Mercantil de Zaragoza no volume 2.649, Folio 215, folha Z-28722, e que opera sob o nome comercial esFIRMA, nome comercial que será utilizado ao longo deste documento para designá-la, é um prestador de serviços de certificação que atua de acordo com o disposto no regime de obrigações e responsabilidades do Regulamento (UE) 910/2014, da Lei 6/2020, de 11 de novembro, reguladora de determinados aspectos dos serviços eletrônicos de confiança, Lei Orgânica 3/2018, de 5 de dezembro, de Proteção de Dados Pessoais e garantia dos direitos digitais e as normas técnicas do ETSI aplicáveis à emissão e gestão 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 de seus serviços.

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

esFIRMA AC raíz 2

Trata-se da entidade de certificação raiz da hierarquia que emite certificados para outras entidades de certificação, e cujo certificado de chave pública foi autoassinado.

Dados de identificação:

CN:	ESFIRMA AC RAIZ 2
Huella 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 desde:	2017-11-02T12:52:43Z
Válido até:	2042-11-02T12:52:43Z
Comprimento da chave RSA:	4.096 bits

esFIRMA AC AAPP 2

Trata-se da autoridade de certificação dentro da hierarquia que emite os certificados para as entidades finais, e cujo certificado de chave pública foi assinado digitalmente por "esFIRMA AC RAIZ 2".

Dados de identificação:

CN:	ESFIRMA AC AAPP 2
Huella 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 desde:	2017-11-02T13:12:47Z
Válido até:	2030-11-02T13:12:47Z
Comprimento da chave RSA:	4.096 bits

Plataforma de Administração Eletrônica

Trata-se da plataforma de gerenciamento do ciclo de vida do certificado exclusivamente para sua solicitação, aprovação, emissão e revogação.

Para obter informações completas sobre as funcionalidades da Plataforma de Administração Eletrônica nos serviços de certificação, consulte a documentação correspondente.

1.3.2 Autoridades de Registro

Uma autoridade de registro realiza tarefas de verificação e identificação dos solicitantes dos certificados.

Em geral, o próprio provedor do serviço de certificação atua como autoridade de registro da identidade dos assinantes de certificados.

Também são autoridades de registro dos certificados sujeitos a esta Declaração de Práticas de Certificação, devido à sua condição de certificados corporativos, as unidades

designadas para esta função pelos subscritores dos certificados, como a Secretaria da corporação, o departamento de pessoal ou o Representante legal da Administração, uma vez que dispõem dos registros autênticos sobre a vinculação dos signatários com o subscritor.

As funções de registro dos subscritores são realizadas por delegação e de acordo com as instruções do prestador de serviços de certificação, nos termos definidos pelo Regulamento (UE) 910/2014 e pela Lei 6/2020, de 11 de novembro, reguladora de determinados aspetos dos serviços eletrónicos de confiança, e sob a 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 uso de certificados digitais, para os fins de identificação e assinatura eletrônica.

As seguintes entidades serão as entidades finais dos serviços de certificação da esFIRMA:

1. Assinantes do serviço de certificação.
2. Firmantes.
3. Partes usuárias.

1.3.4 Partes usuárias

As partes usuárias são as pessoas e organizações que recebem assinaturas digitais e certificados digitais.

Como etapa prévia para confiar nos certificados, as partes usuárias devem verificá-los, conforme estabelecido nesta declaração de práticas de certificação e nas correspondentes instruções disponíveis no site da Entidade de Certificação.

1.3.5 Outros participantes

Assinantes do serviço de certificação

Os subscritores do serviço de certificação são as administrações públicas ou entidades que os adquirem da esFIRMA para uso em seu ambiente corporativo ou organizacional, e estão identificados nos certificados.

O assinante do serviço de certificação adquire uma licença de uso do certificado, para uso próprio - certificados de selo eletrônico - ou para facilitar a certificação da identidade de uma pessoa específica devidamente autorizada para várias ações no âmbito organizacional do assinante - certificados de assinatura eletrônica. Neste último caso, essa pessoa é identificada no certificado, conforme disposto no próximo parágrafo.

O assinante do serviço de certificação é, portanto, o cliente do provedor de serviços de certificação, de acordo com a legislação comercial, e tem os direitos e obrigações definidos pelo provedor de serviços de certificação, que são adicionais e entendidos sem prejuízo dos direitos e obrigações dos signatários, conforme autorizado e regulamentado pelas normas técnicas europeias aplicáveis à emissão de certificados eletrônicos qualificados, especialmente na ETSI EN 319 411-2, seções 5.4.2 e 6.3.4.e)

Firmantes

Os signatários são pessoas físicas que possuem exclusivamente ou controlam exclusivamente, de acordo com o regime de obrigações e responsabilidades do Regulamento (UE) 910/2014 e da Lei 6/2020, de 11 de novembro, que regula determinados aspectos dos serviços eletrônicos de confiança, as chaves de assinatura digital para identificação e assinatura eletrônica avançada ou qualificada; geralmente sendo os titulares ou membros dos órgãos administrativos, nos certificados de assinatura eletrônica do órgão, pessoas a serviço das Administrações Públicas, nos certificados de funcionário público ou pessoas que pertencem a uma entidade, nos certificados de pessoa física vinculada.

Os signatários estão devidamente autorizados pelo assinante e devidamente identificados no certificado pelo seu nome completo, número de identificação fiscal válido na jurisdição de emissão do certificado ou pelo pseudônimo correspondente nos certificados desse tipo.

Dada a existência de certificados para usos diferentes da assinatura eletrônica, como a identificação, também é utilizado o termo mais genérico de "pessoa física identificada no certificado", sempre com pleno respeito ao cumprimento da legislação de assinatura eletrônica em relação aos direitos e obrigações do signatário.

1.4 Uso dos certificados

Esta seção lista as aplicações para as quais cada tipo de certificado pode ser usado, estabelece limitações para certas aplicações e proíbe certas aplicações dos certificados.

1.4.1 Usos permitidos para os certificados

Os usos permitidos indicados nos diferentes campos dos perfis de certificados, visíveis no site https://www.esfirma.com, devem ser levados em consideração

Certificado de Funcionário Público de alto nível em Cartão

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.1.1	Na hierarquia da AC 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 de pessoa física de funcionário público de alto nível são certificados qualificados de acordo com o artigo 28 e o Anexo I do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, e cumprem as disposições da regulamentação técnica identificada pela referência ETSI EN 319 411-2.

Estes certificados são emitidos para funcionários públicos para identificá-los como pessoas a serviço da Administração, órgão, entidade de direito público ou outra entidade, vinculando-os a ela, cumprindo os requisitos estabelecidos no artigo 43 da Lei 40/2015,

de 1 de outubro, do Regime Jurídico do Setor Público, para a assinatura eletrônica do pessoal ao serviço das Administrações Públicas.

Os certificados de pessoa física de funcionários públicos de alto nível funcionam com um dispositivo seguro de criação de assinatura de acordo com o Anexo II do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014.

Da mesma forma, os certificados de pessoa física de nível alto para funcionários públicos são emitidos de acordo com os níveis de garantia alta dos perfis de certificado estabelecidos no ponto 10 do documento "Perfis de Certificados Eletrônicos" da Secretaria de Estado de Digitalização e Inteligência Artificial do Ministério de Assuntos Econômicos e Transformação Digital.

Estes certificados garantem a identidade do assinante e do signatário, e permitem a geração da "assinatura eletrônica qualificada"; isto é, a assinatura eletrônica avançada que se baseia em um certificado qualificado e que foi gerada usando um dispositivo qualificado, portanto, de acordo com o que estabelece o artigo 25.2 do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, terá um efeito jurídico equivalente ao de uma firma manuscrita.

Também podem ser usados em aplicações que não exigem a assinatura eletrônica equivalente à assinatura escrita, como as aplicações indicadas abaixo:

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

esFIRMA não oferece serviços de cópia de segurança ou recuperação de chaves. Portanto, esFIRMA não será responsável em nenhum caso 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" está ativado e, portanto, permite realizar as seguintes funções:

a. Compromisso com o conteúdo (Compromisso de conteúdo, para realizar a função de assinatura eletrônica)

b) No campo "Qualified Certificate Statements" 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 ao Usuário" descreve o uso deste certificado.

Certificado de Funcionário Público de nível médio em HSM

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.1.4	Na hierarquia da AC 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 pessoa física de nível médio de funcionário público são certificados qualificados de acordo com o artigo 28 e o Anexo I do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, e cumprem as disposições da regulamentação técnica identificada pela referência ETSI EN 319 411-2.

Estes certificados são emitidos para funcionários públicos para identificá-los como pessoas a serviço da Administração, organismo, entidade de direito público ou outra entidade, vinculando-os a esta, cumprindo os requisitos estabelecidos em o artigo 43 da Lei 40/2015, de 1 de outubro, do Regime Jurídico do Setor Público, para a assinatura eletrônica do pessoal ao serviço das Administrações Públicas.

Os certificados de pessoa física de funcionários públicos de nível médio são gerenciados de forma centralizada.

Os certificados de pessoa física de nível médio de funcionários públicos são emitidos de acordo com os níveis de garantia média dos perfis de certificados estabelecidos no ponto 10 do documento "Perfis de Certificados Eletrônicos" da Secretaria de Estado de Digitalização e Inteligência Artificial do Ministério de Assuntos Econômicos e Transformação Digital.

Estes certificados garantem a identidade do assinante e da pessoa indicada no certificado, e permitem a geração da "assinatura eletrônica avançada baseada em certificado eletrônico qualificado".

Também podem ser usados em aplicações que não exigem a assinatura eletrônica equivalente à assinatura escrita, como as aplicações indicadas abaixo:

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

esFIRMA não oferece serviços de cópia de segurança ou recuperação de chaves. Portanto, esFIRMA não será responsável em nenhum caso 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" está ativado, permitindo-nos realizar as seguintes funções:
    a. Compromisso com o conteúdo (Compromisso de conteúdo, para realizar a função de assinatura eletrônica)

b) No campo "Qualified Certificate Statements" 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 ao Usuário" descreve o uso deste certificado.

Certificado de Funcionário Público de alto nível em cartão para autenticação

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.1.5	Na hierarquia da AC esFIRMA
0.4.0.2042.1.2	De acordo com a política NCP+
2.16.724.1.3.5.7.1	Funcionário público espanhol de alto nível

Estes certificados são certificados emitidos de acordo com a política de certificados normalizados (NCP+) e cumprem com o estabelecido pela normativa técnica identificada com a referência ETSI EN 319 411-1.

Estes certificados são emitidos para funcionários públicos para identificá-los como pessoas a serviço da Administração, organismo, entidade de direito público ou outra entidade, vinculando-os a esta, cumprindo os requisitos estabelecidos em a Lei 40/2015, de 1 de outubro, de Regime Jurídico do Setor Público.

Estes certificados de pessoa física de nível alto para funcionários públicos são usados com um dispositivo seguro de criação de assinatura de acordo com o Anexo II do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014.

Os certificados de pessoa física de nível alto para funcionários públicos são emitidos de acordo com os níveis de garantia de segurança alta dos perfis de certificados estabelecidos no ponto 10 do documento "Perfis de Certificados Eletrônicos" da Secretaria de Estado de Digitalização e Inteligência Artificial do Ministério de Assuntos Econômicos e Transformação Digital.

Estes certificados garantem a identidade do assinante e da pessoa indicada no certificado, e permitem a autenticação desta última perante aplicações e sites web.

esFIRMA não oferece serviços de cópia de segurança ou recuperação de chaves. Portanto, esFIRMA não será responsável em nenhum caso 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" está ativado, permitindo-nos realizar as seguintes funções:
    a. Assinatura digital (para realizar a função de autenticação)

e) O campo "Aviso ao Usuário" descreve o uso deste certificado.

Certificado de Selo de Órgão de nível médio em software

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.2.2	Na hierarquia da AC 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 eletrônico de nível médio do órgão são certificados qualificados de acordo com o artigo 38 e o Anexo III do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, e cumprem as disposições da regulamentação técnica identificada pela referência ETSI EN 319 411-2.

Estes certificados são emitidos para identificação e autenticação do exercício de competência na atuação administrativa automatizada, de acordo com o artigo 42 da Lei 40/2015, de 1 de outubro, de Regime Jurídico do Setor Público.

Os certificados de selo eletrônico de nível médio são emitidos de acordo com os níveis de garantia média dos perfis de certificado estabelecidos no ponto 9 do documento "Perfis de Certificados Eletrônicos" da Secretaria de Estado de Digitalização e Inteligência Artificial do Ministério de Assuntos Econômicos e Transformação Digital.

Estes certificados garantem a identidade do assinante e da entidade pública incluída no certificado.

esFIRMA não oferece serviços de cópia de segurança ou recuperação de chaves. Portanto, esFIRMA não será responsável em nenhum caso 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" está ativado, permitindo-nos realizar as seguintes funções:
    a. Compromisso com o conteúdo (Compromisso de conteúdo, para realizar a função de assinatura eletrônica)

b) No campo "Qualified Certificate Statements" 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 ao Usuário" descreve o uso deste certificado.

Certificado de Selo de Órgão de nível médio em HSM

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.2.4	Na hierarquia da AC 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 eletrônico de nível médio do órgão são certificados qualificados de acordo com o artigo 38 e o Anexo III do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, e cumprem as disposições da regulamentação técnica identificada pela referência ETSI EN 319 411-2.

Estes certificados são emitidos para identificação e autenticação do exercício de competência na atuação administrativa automatizada, de acordo com o artigo 42 da Lei 40/2015, de 1 de outubro, de Regime Jurídico do Setor Público.

Os certificados de selo eletrônico de órgão de nível médio são gerenciados de forma centralizada.

Os certificados de selo eletrônico de nível médio são emitidos de acordo com os níveis de garantia média dos perfis de certificado estabelecidos no ponto 9 do documento "Perfis de Certificados Eletrônicos" da Secretaria de Estado de Digitalização e Inteligência Artificial do Ministério de Assuntos Econômicos e Transformação Digital.

Estes certificados garantem a identidade do assinante e da entidade pública incluída no certificado.

esFIRMA não oferece serviços de cópia de segurança ou recuperação de chaves. Portanto, esFIRMA não será responsável em nenhum caso 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" está ativado, permitindo-nos realizar as seguintes funções:
    a. Compromisso com o conteúdo (Compromisso de conteúdo, para realizar a função de assinatura eletrônica)

b) No campo "Qualified Certificate Statements" 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 ao Usuário" descreve o uso deste certificado.

Certificado de Funcionário Público com Pseudônimo de Nível Alto em Cartão

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.3.1	Na hierarquia da AC 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 pseudônimo de alto nível

Os certificados de pessoa física de funcionário público com pseudônimo de alto nível são certificados qualificados de acordo com o artigo 28 e o Anexo I do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, e cumprem as disposições da regulamentação técnica identificada pela referência ETSI EN 319 411-2.

Estes certificados são emitidos para funcionários públicos para identificá-los (por meio de um pseudônimo) como pessoas ao serviço da Administração, organismo, entidade de direito público ou outra entidade, vinculando-os com esta, cumprindo os requisitos estabelecidos no artigo 43 da Lei 40/2015, de 1 de outubro, do Regime Jurídico do Setor Público, para a assinatura eletrônica do pessoal ao serviço das Administrações Públicas.

Os certificados de pessoa física de funcionário público com pseudônimo de alto nível funcionam com um dispositivo seguro de criação de assinatura, de acordo com Anexo II do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014.

Além disso, os certificados de pessoa física de funcionários públicos com pseudônimo de alto nível são emitidos de acordo com os níveis de garantia alta dos perfis de certificados estabelecidos no ponto 11 do documento "Perfis de Certificados Eletrônicos" da Secretaria de Estado de Digitalização e Inteligência Artificial do Ministério de Assuntos Econômicos e Transformação Digital.

Estes certificados permitem a geração da "assinatura eletrônica qualificada"; isto é, a assinatura eletrônica avançada que se baseia em um certificado qualificado e que foi gerada usando um dispositivo qualificado, portanto, de acordo com o estabelecido no artigo 25.2 do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, terá um efeito jurídico equivalente ao de uma firma manuscrita.

Também podem ser usados em aplicações que não exigem a assinatura eletrônica equivalente à assinatura escrita, como as aplicações indicadas abaixo:

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

esFIRMA não oferece serviços de cópia de segurança ou recuperação de chaves. Portanto, esFIRMA não será responsável em nenhum caso 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" está ativado e, portanto, permite realizar as seguintes funções:
    a. Compromisso com o conteúdo (Compromisso de conteúdo, para realizar a função de assinatura eletrônica)

b) No campo "Qualified Certificate Statements" 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 ao Usuário" descreve o uso deste certificado.

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

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.3.4	Na hierarquia da AC 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 pseudônimo de nível médio

Os certificados de pessoa física de funcionário público com pseudônimo de nível médio são certificados qualificados de acordo com o artigo 28 e o Anexo I do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, e cumprem as disposições da regulamentação técnica identificada pela referência ETSI EN 319 411-2.

Estes certificados são emitidos para funcionários públicos para identificá-los (por meio de um pseudônimo) como pessoas a serviço da Administração, órgão, entidade de direito público ou outra entidade, vinculando-os a esta, cumprindo os requisitos estabelecidos em o artigo 43 da Lei 40/2015, de 1 de outubro, do Regime Jurídico do Setor Público, para a assinatura eletrônica do pessoal ao serviço das Administrações Públicas.

Os certificados de pessoa física de funcionário público com pseudônimo de nível médio são gerenciados de forma centralizada.

Os certificados de pessoa física de funcionários públicos com pseudônimo de nível médio são emitidos de acordo com os níveis de garantia média dos perfis de certificados estabelecidos no ponto 11 do documento "Perfis de Certificados Eletrônicos" da Secretaria de Estado de Digitalização e Inteligência Artificial do Ministério de Assuntos Econômicos e Transformação Digital.

Estes certificados permitem a geração da "assinatura eletrônica avançada baseada em certificado eletrônico qualificado".

Também podem ser usados em aplicações que não exigem a assinatura eletrônica equivalente à assinatura escrita, como as aplicações indicadas abaixo:

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

esFIRMA não oferece serviços de cópia de segurança ou recuperação de chaves. Portanto, esFIRMA não será responsável em nenhum caso 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" está ativado, permitindo-nos realizar as seguintes funções:
    a. Compromisso com o conteúdo (Compromisso de conteúdo, para realizar a função de assinatura eletrônica)

b) No campo "Qualified Certificate Statements" 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 ao Usuário" descreve o uso deste certificado.

Certificado de Funcionário Público com pseudônimo, nível alto em cartão para autenticação

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.3.5	Na hierarquia da AC esFIRMA
0.4.0.2042.1.2	De acordo com a política NCP+
2.16.724.1.3.5.4.1	Funcionário público espanhol com pseudônimo de nível alto

Estes certificados são certificados emitidos de acordo com a política de certificados normalizados (NCP+) e cumprem com o estabelecido pela normativa técnica identificada com a referência ETSI EN 319 411-1.

Estes certificados são emitidos para funcionários públicos para identificá-los (por meio de um pseudônimo) como pessoas a serviço da Administração, órgão, entidade de direito público ou outra entidade, vinculando-os a esta, cumprindo os requisitos estabelecidos em a Lei 40/2015, de 1 de outubro, de Regime Jurídico do Setor Público.

Estes certificados de pessoa física de funcionário público com pseudônimo de alto nível funcionam com dispositivo seguro de criação de assinatura de acordo com o Anexo II do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014.

Os certificados de pessoa física de funcionário público com pseudônimo de alto nível são emitidos de acordo com os níveis de garantia alta dos perfis de certificados estabelecidos no ponto 11 do documento "Perfis de Certificados Eletrônicos" da Secretaria de Estado

de Digitalização e Inteligência Artificial do Ministério de Assuntos Econômicos e Transformação Digital.

Estes certificados garantem a identidade do assinante e da pessoa indicada no certificado, e permitem a autenticação desta última perante aplicações e sites web.

esFIRMA não oferece serviços de cópia de segurança ou recuperação de chaves. Portanto, esFIRMA não será responsável em nenhum caso 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" está ativado, permitindo-nos realizar as seguintes funções:
    a. Assinatura digital (para realizar a função de autenticação)

g) O campo "Aviso ao Usuário" descreve o uso deste certificado.

Certificado de Selo eletrônico qualificado de TSA/TSU

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.5.2	Na hierarquia da AC esFIRMA
0.4.0.194112.1.1	De acordo com a política QCP-l

Os certificados de selo eletrônico de TSA/TSU são certificados qualificados de acordo com o artigo 38 e o Anexo III do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, e cumprem as disposições da regulamentação técnica identificada pelas referências ETSI EN 319 421 e ETSI EN 319 422.

Este certificado permite que Unidades de Carimbo de Tempo ou TSU emitam carimbos de tempo quando recebem uma solicitação de acordo com as especificações do RFC3161.

As chaves são geradas em um dispositivo HSM.

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

a) O campo "uso da chave" está ativado, permitindo-nos realizar as seguintes funções:
    a. Content Commitment
b) O campo "extend key usage" tem a função ativada:
    a. TimeStamping
c) No campo "Qualified Certificate Statements" aparece a seguinte declaração:
    a. QcCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.
d) O campo "User Notice" descreve o uso 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:

- São estabelecidos controles para garantir a cessação do uso da chave privada antes da expiração de sua validade.
- Em caso de mudança de certificado, as chaves associadas serão destruídas conforme descrito no ciclo de vida.
- As chaves privadas são destruídas uma vez expirado o tempo de uso definido, sua substituição, revogação ou outras causas.
- A destruição é realizada de tal forma que a chave privada não possa ser recuperada, seguindo o procedimento estabelecido pelo fabricante do módulo criptográfico que as armazena.
- Para validação a longo prazo dos selos de tempo, pode-se utilizar a Última CRL emitida pela esFIRMA, seguindo os guias fornecidos. No momento da verificação, pode ser considerado válido se, no momento da data do selo de tempo, a chave privada não foi comprometida, o algoritmo de impressão digital não apresentava colisões e os algoritmos utilizados estavam fora do alcance dos ataques criptográficos do momento.

Certificado de Carimbo do Tempo Eletrônico de TSA/TSU

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.5.1	Na hierarquia da AC esFIRMA
0.4.0.194112.1.1	De acordo com a política QCP-l

Este certificado permite que Unidades de Carimbo de Tempo ou TSU emitam carimbos de tempo quando recebem uma solicitação de acordo com as especificações do RFC3161.

As chaves são geradas em um dispositivo HSM.

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

f) O campo "uso da chave" está ativado, permitindo-nos realizar as seguintes funções:
   a. Content Commitment

g) O campo "extend key usage" tem a função ativada:
   a. TimeStamping

h) O campo "User Notice" descreve o uso 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:

- São estabelecidos controles para garantir a cessação do uso da chave privada antes da expiração de sua validade.
- Em caso de mudança de certificado, as chaves associadas serão destruídas conforme descrito no ciclo de vida.
- As chaves privadas são destruídas uma vez expirado o tempo de uso definido, sua substituição, revogação ou outras causas.
- A destruição é realizada de tal forma que a chave privada não possa ser recuperada, seguindo o procedimento estabelecido pelo fabricante do módulo criptográfico que as armazena.
- Para validação a longo prazo dos selos de tempo, pode-se utilizar a Última CRL emitida pela esFIRMA, seguindo os guias fornecidos. No momento da verificação, pode ser considerado válido se, no momento da data do selo de tempo, a chave privada não foi comprometida, o algoritmo de impressão digital não apresentava

colisões e os algoritmos utilizados estavam fora do alcance dos ataques criptográficos do momento.

Certificado de pessoa física vinculada, em cartão para assinatura

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.6.1	Na hierarquia da AC esFIRMA
0.4.0.194112.1.2	De acordo com a política QCP-n-qscd

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

Estes certificados funcionam com dispositivo seguro de criação de assinatura, de acordo com o Anexo II do Regulamento (UE) 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 eletrônica qualificada"; isto é, a assinatura eletrônica avançada que se baseia em um certificado qualificado e que foi gerada usando um dispositivo qualificado, portanto, de acordo com o que estabelece o artigo 25.2 do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, terá um efeito jurídico equivalente ao de uma firma manuscrita.

Também podem ser usados em aplicações que não exigem a assinatura eletrônica equivalente à assinatura escrita, como as aplicações indicadas abaixo:

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

esFIRMA não oferece serviços de cópia de segurança ou recuperação de chaves. Portanto, esFIRMA não será responsável em nenhum caso 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" está ativado e, portanto, permite realizar as seguintes funções:
    a. Compromisso com o conteúdo (Compromisso de conteúdo, para realizar a função de assinatura eletrônica)

e) No campo "Qualified Certificate Statements" 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 "User Notice" descreve o uso deste certificado. Opcional

Certificado de pessoa física vinculada, centralizado, para assinatura

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.6.4	Na hierarquia da AC esFIRMA
0.4.0.194112.1.0	De acordo com a política QCP-n

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

Estes certificados são gerenciados de forma centralizada.

Estes certificados garantem a identidade do assinante e da pessoa indicada no certificado, e permitem a geração da "assinatura eletrônica avançada baseada em certificado eletrônico qualificado".

Também podem ser usados em aplicações que não exigem a assinatura eletrônica equivalente à assinatura escrita, como as aplicações indicadas abaixo:

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

esFIRMA não oferece serviços de cópia de segurança ou recuperação de chaves. Portanto, esFIRMA não será responsável em nenhum caso 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" está ativado, permitindo-nos realizar as seguintes funções:
    a. Compromisso com o conteúdo (Compromisso de conteúdo, para realizar a função de assinatura eletrônica)

i) No campo "Qualified Certificate Statements" aparece a seguinte declaração:
    a. qCCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.
j) O campo "User Notice" descreve o uso deste certificado. Opcional

Certificado de pessoa física vinculada, em cartão para autenticação

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.6.5	Na hierarquia da AC esFIRMA
0.4.0.2042.1.2	De acordo com a política NCP+

Estes certificados são certificados emitidos de acordo com a política de certificados normalizados (NCP+) e cumprem com o estabelecido pela normativa técnica identificada com a referência ETSI EN 319 411-1.

Estes certificados funcionam com dispositivo seguro de criação de assinatura, de acordo com o Anexo II do Regulamento (UE) 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 desta última perante aplicações e sites web.

esFIRMA não oferece serviços de cópia de segurança ou recuperação de chaves. Portanto, esFIRMA não será responsável em nenhum caso 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" está ativado, permitindo-nos realizar as seguintes funções:
   a. Assinatura digital (para realizar a função de autenticação)

l) O campo "User Notice" descreve o uso deste certificado. Opcional

Certificado de pessoa física vinculada, com pseudônimo, em cartão para assinatura

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.7.1	Na hierarquia da AC esFIRMA
0.4.0.194112.1.2	De acordo com a política QCP-n-qscd

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

Estes certificados funcionam com dispositivo seguro de criação de assinatura, de acordo com o Anexo II do Regulamento (UE) 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 por meio de um pseudônimo.
Estes certificados permitem a geração da "assinatura eletrônica qualificada"; isto é, a assinatura eletrônica avançada que se baseia em um certificado qualificado e que foi gerada usando um dispositivo qualificado, portanto, de acordo com o que estabelece o artigo 25.2 do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, terá um efeito jurídico equivalente ao de uma firma manuscrita.

Também podem ser usados em aplicações que não exigem a assinatura eletrônica equivalente à assinatura escrita, como as aplicações indicadas abaixo:

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

esFIRMA não oferece serviços de cópia de segurança ou recuperação de chaves. Portanto, esFIRMA não será responsável em nenhum caso 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" está ativado e, portanto, permite realizar as seguintes funções:
    a. Compromisso com o conteúdo (Compromisso de conteúdo, para realizar a função de assinatura eletrônica)

h) No campo "Qualified Certificate Statements" 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 "User Notice" descreve o uso deste certificado. Opcional

Certificado de pessoa física vinculada, com pseudônimo, centralizado, para assinatura

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.6.4	Na hierarquia da AC esFIRMA
0.4.0.194112.1.0	De acordo com a política QCP-n

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

Estes certificados são gerenciados de forma centralizada.
Estes certificados garantem a identidade do assinante.
Estes certificados garantem a identidade do signatário por meio de um pseudônimo.
Estes certificados permitem a geração da "assinatura eletrônica avançada baseada em certificado eletrônico qualificado".

Também podem ser usados em aplicações que não exigem a assinatura eletrônica equivalente à assinatura escrita, como as aplicações indicadas abaixo:

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

esFIRMA não oferece serviços de cópia de segurança ou recuperação de chaves. Portanto, esFIRMA não será responsável em nenhum caso 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" está ativado, permitindo-nos realizar as seguintes funções:
    a. Compromisso com o conteúdo (Compromisso de conteúdo, para realizar a função de assinatura eletrônica)

n) No campo "Qualified Certificate Statements" aparece a seguinte declaração:
    a. qCCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.

o) O campo "User Notice" descreve o uso deste certificado. Opcional

Certificado de pessoa física vinculada, com pseudônimo, em cartão para autenticação

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.7.5	Na hierarquia da AC esFIRMA
0.4.0.2042.1.2	De acordo com a política NCP+

Estes certificados são certificados emitidos de acordo com a política de certificados normalizados (NCP+) e cumprem com o estabelecido pela normativa técnica identificada com a referência ETSI EN 319 411-1.

Estes certificados funcionam com dispositivo seguro de criação de assinatura, de acordo com o Anexo II do Regulamento (UE) 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 por meio de um pseudônimo.
Estes certificados permitem a autenticação desta última perante aplicações e sites web.

esFIRMA não oferece serviços de cópia de segurança ou recuperação de chaves. Portanto, esFIRMA não será responsável em nenhum caso 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" está ativado, permitindo-nos realizar as seguintes funções:
    a. Assinatura digital (para realizar a função de autenticação)

q) O campo "User Notice" descreve o uso deste certificado. Opcional

Certificado de Selo Eletrônico em software

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.8.2	Na hierarquia da AC esFIRMA
0.4.0.194112.1.1	De acordo com a política QCP-l

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

esFIRMA não oferece serviços de cópia de segurança ou recuperação de chaves. Portanto, esFIRMA não será responsável em nenhum caso 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" está ativado, permitindo-nos realizar as seguintes funções:
    a. Assinatura digital (para a função de autenticação)
    b. Compromisso com o conteúdo (Content commitment, para realizar a função de assinatura eletrônica)
    c. Cifragem de chaves

b) No campo "Qualified Certificate Statements" 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 ao Usuário" descreve o uso deste certificado.Opcional

Certificado de Selo Eletrônico com gerenciamento centralizado

Este certificado dispõe dos seguintes OIDs:

1.3.6.1.4.1.47281.1.8.4	Na hierarquia da AC esFIRMA
0.4.0.194112.1.1	De acordo com a política QCP-l

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

Estes certificados são gerenciados de forma centralizada.

esFIRMA não oferece serviços de cópia de segurança ou recuperação de chaves. Portanto, esFIRMA não será responsável em nenhum caso 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" está ativado, permitindo-nos realizar as seguintes funções:
    a. Compromisso com o conteúdo (Content commitment, para realizar a função de assinatura eletrônica)

e) No campo "Qualified Certificate Statements" 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 ao Usuário" descreve o uso deste certificado.Opcional

1.4.2 Limites e proibições de uso dos certificados

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

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

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

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

Os limites indicados nos vários campos dos perfis de certificados, visíveis no site da esFIRMA https://www.esfirma.com, devem ser levados em consideração

O uso dos certificados digitais de forma que viole esta 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 fins legais apropriados, e isenta a esFIRMA de qualquer responsabilidade por esse uso indevido, seja do signatário ou de terceiros.

esFIRMA não tem autorização de acesso nem obrigação legal de supervisionar os dados sobre os quais se pode aplicar o uso de uma chave certificada. Portanto, e como consequência desta impossibilidade técnica de acessar o conteúdo da mensagem, não é possível por parte de esFIRMA emitir avaliação alguma sobre dito conteúdo, assumindo, portanto, o subscritor, o signatário ou a pessoa responsável pela custódia, qualquer responsabilidade decorrente do conteúdo associado ao uso de um certificado.

Da mesma forma, o subscritor, o signatário ou a pessoa responsável pela custódia serão responsáveis por qualquer responsabilidade que possa surgir do uso do mesmo fora dos limites e condições de uso estabelecidos nesta DPC, nos documentos jurídicos vinculativos de cada certificado, nos contratos ou acordos com as entidades de registro ou com seus subscritores, bem como de qualquer outro uso indevido do mesmo decorrente desta seção ou que possa ser interpretado como tal de acordo com a legislação vigente.

Os certificados são usados exclusivamente a partir da Plataforma de Administração Eletrônica ou suas extensões e complementos disponibilizados pela empresa ESPUBLICO ao assinante.

1.5 Administração da política

1.5.1 Organização que administra o documento

Oficina de Segurança da ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)
CALLE BARI 39 (Edif. Binary Building)
50197 - ZARAGOZA
(+34) 976300110

Identificação Registro	Registro Comercial de Zaragoza
Desculpe, "Tomo" pode ter vários significados em português. Poderia fornecer mais contexto ou informações para que eu possa fornecer uma tradução precisa?	2649
Folio	215
Hoja	Z-28722
CIF	A-50.878.842

1.5.2 Dados de contato da organização

ESPÚBLICO SERVIÇOS PARA A ADMINISTRAÇÃO SA (esFIRMA)
CALLE BARI 39 (Edif. Binary Building)
50197 - ZARAGOZA
(+34) 976300110

1.5.3 Organização que aprova o documento

Comitê de Segurança de ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)

O comitê de segurança da esFIRMA, composto pelo seu Presidente, pelo Responsável de Informação e Serviço e pelo Responsável de Segurança da esFirma, é responsável pela aprovação desta Declaração de Práticas.

Tanto as funções quanto os membros desse Comitê estão definidos na Política de Segurança da esFirma.

1.5.4 Procedimentos de gestão do documento

O sistema documental e de organização da esFIRMA garante, por meio da existência e aplicação dos procedimentos correspondentes, a manutenção adequada deste documento e das especificações de serviço relacionadas a ele.

A esFIRMA realiza revisões deste documento, no mínimo, anualmente ou quando exigido por mudanças nas diretrizes e documentos que deve cumprir.

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

O Escritório de Segurança é responsável pela redação, manutenção e administração do DPC, textos de divulgação (PDS), folhas de entrega e aceitação e o restante da documentação jurídica (acordos, contratos, etc.) do esFirma.

Sempre que houver mudanças significativas na gestão dos certificados definidos nesta DPC, uma nova revisão deste documento é criada, que consta na tabela inicial de "controle de versões" dentro da seção de "informações gerais".

A atuação do Escritório de Segurança ocorre a pedido do seu responsável, de acordo com as necessidades que surgirem.

esFirma pode realizar alterações que não exijam notificação quando não afetarem diretamente os direitos dos signatários e subscritores dos certificados ou dos subscritores dos selos.
Quando a esFirma for introduzir alterações que modifiquem os direitos dos signatários e subscritores dos certificados e dos subscritores de selos, deverá notificá-los publicamente para que apresentem seus comentários ao Escritório de Segurança durante os 15 dias seguintes à publicação das futuras alterações.

Para notificar publicamente as mudanças ocorridas, elas serão publicadas na seção "documentação" no site https://www.esfirma.com

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

1.6 Acrônimos e definições

1.6.1. Acrónimos

AC (sem contexto, pode significar várias coisas em português)*ou também CA*)	*Autoridade Certificadora* Autoridade de Certificação
AR (também conhecido como RA)	*Registration Authority* Autoridade de Registro
CPD	Centro de Processamento de Dados
CPS (também conhecido como DPC)	*Certification Practice Statement*. Declaração de Práticas de Certificação
CRL (ou também LRC)	*Lista de Revogação de Certificados.* Lista de certificados revogados
DN	*Distinguished Name.* Nome distintivo dentro do certificado digital
DNI	Documento Nacional de Identidade
ETSI EN	*European Telecommunications Standards Institute - Norma Europeia.*
EV (para SSL)	*Extended Validation* Validação estendida em certificados SSL.
FIPS	*Federal Information Processing Standard Publication*
HSM	*Módulo de Segurança de Hardware* Módulo de segurança em Hardware
IETF	*Internet Engineering Task Force*
NIF	Número de Identificação Fiscal
NTP	*Network Time Protocol* Protocolo de tempo em rede.

OCSP	*Online Certificate Status Protocol.* Protocolo de acesso ao estado dos certificados
OID	*Object Identifier*. Identificador de objeto
PDS	*Declarações de divulgação do PKI* Texto de Divulgação de PKI.
PIN	*Personal Identification Number*. Número de identificação pessoal
PKI	*Infraestrutura de Chave Pública (Public Key Infrastructure)*. Infraestrutura de chave pública
QSCD (também conhecido como DCCF)	*Dispositivo de Criação de Assinatura/Selo Eletrônico Qualificado.* Dispositivo qualificado de criação de assinatura/selos
QCP	*Política de Certificado Qualificado* Política de certificados qualificados
QCP-n	*Política de Certificado Qualificado - pessoa natural* Política de certificados qualificados para pessoas físicas.
QCP-l	*Política de Certificado Qualificado - pessoa jurídica* Política de certificados qualificados para pessoas jurídicas.
QCP-n-qscd	*Qualified Certificate Policy-natural person-qscd* Política de certificados qualificados para pessoas físicas em dispositivo qualificado de assinatura/selo
QCP-l-qscd	*Qualified Certificate Policy-legal person-qscd* Política de certificados qualificados para pessoas jurídicas com dispositivo qualificado de assinatura/selo
RFC	*Request for Comments* Documento RFC
RSA	Rivest-Shamir-Adleman. Tipo de algoritmo de cifragem
SHA	*Secure Hash Algorithm.* Algoritmo seguro de Hash
SSL	*Secure Sockets Layer.* Protocolo projetado pela Netscape e convertido em padrão da rede, permite a

	transmissão de informações criptografadas entre um navegador da Internet e um servidor.
TCP/IP	*Transmission Control Protocol/Internet Protocol (TCP/IP)*. Sistema de protocolos, definidos no âmbito da IEFT.
TSA	*Time Stamping Authority* Autoridade de Carimbo do Tempo Eletrônico
TSU	*Time Stamping Unit* Unidade de Carimbo de Tempo.
UTC	*Tempo Universal Coordenado (UTC)* Tempo Universal Coordenado
VPN	*Virtual Private Network.* Rede privada virtual

1.6.2 Definições

Autoridade de Certificação	*É a entidade responsável pela emissão e gestão dos certificados digitais.*
Autoridade de Registro	*Entidade responsável pela gestão de solicitações, identificação e registro de solicitantes de um certificado. Pode fazer parte da Autoridade de Certificação ou ser externa.*
Certificado	*Arquivo que associa a chave pública com alguns dados identificativos do Sujeito/Signatário e é assinado pela AC.*
Clave pública	*Valor matemático conhecido publicamente e usado para a verificação de uma assinatura digital ou a criptografia de dados.*
Clave privada	*Valor matemático conhecido apenas pelo Sujeito/Signatário e usado para a criação de uma assinatura digital ou a decodificação de dados.* *A chave privada da AC será usada para assinar certificados e CRL's.* *A chave privada do serviço TSA será usada para assinar os carimbos de tempo.*
CPS	*Conjunto de práticas adotadas por uma Autoridade de Certificação para a emissão de certificados em conformidade com uma política de certificação específica.*
CRL	*Arquivo que contém uma lista dos certificados que foram revogados em um período de tempo determinado e que é assinada pela AC.*
Dados de Ativação	*Dados privados, como PINs ou senhas usados para ativar a chave privada*
DCCF	*Dispositivo Qualificado de criação de assinatura. Elemento de software ou 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.*
Firma digital	*O resultado da transformação de uma mensagem, ou qualquer tipo de dado, pela aplicação da chave privada em conjunto com alguns algoritmos conhecidos, garantindo assim:*

	a) que os dados não foram modificados (integridade) *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 de origem)*
OID	*Identificador numérico único registrado sob a padronização ISO e referido a um objeto ou classe de objeto determinado.*
Par de chaves	*Conjunto formado pela chave pública e privada, ambas relacionadas matematicamente entre si.*
PKI	*Conjunto de elementos hardware, software, recursos humanos, procedimentos, etc., que compõem um sistema baseado na criação e gestão de certificados de chave pública.*
Solicitante	*No contexto deste documento, o requerente será uma pessoa física autorizada com um poder especial para realizar determinados procedimentos em nome e representação da entidade.*
Assinante	*No contexto deste documento, a pessoa jurídica proprietária do certificado (a nível corporativo)*
Sujeito/Firmante	*No contexto deste documento, a pessoa física cuja chave pública é certificada pela AC e possui, ou tem acesso exclusivo a, uma chave privada válida para gerar assinaturas digitais.*
Parte Usuária	*No contexto deste documento, pessoa que confia voluntariamente no certificado digital e o utiliza como meio de comprovação da autenticidade e integridade do documento assinado*

2. Publicação de informações e depósito de certificados

2.1 Depósito de certificados

A esFIRMA dispõe de um Depósito de certificados, no qual são publicadas as informações relativas aos serviços de certificação:

https://www.esfirma.com

Este serviço está disponível 24 horas por dia, 7 dias por semana e, em caso de falha do sistema fora do controle da esFIRMA, ela fará todos os esforços para que o serviço esteja disponível novamente dentro do prazo estabelecido na seção 5.7.4 desta Declaração de Práticas de Certificação.

2.2 Publicação de informações de certificação

esFIRMA publica as seguintes informações no seu Depósito:

- As listas de certificados revogados e outras informações de estado de revogação dos certificados.
- As políticas de certificados aplicáveis.
- A Declaração de Práticas de Certificação.
- Os textos de divulgação (PKI Disclosure Statements - PDS), pelo menos em espanhol e em inglês.

2.3 Frequência de publicação

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

As alterações na Declaração de Práticas de Certificação são regidas pelo estabelecido na seção 1.5 deste documento.

As informações de status de revogação de certificados são publicadas de acordo com o estabelecido nas seções 4.9.7 e 4.9.8 desta Declaração de Práticas de Certificação.

2.4 Controle de acesso

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

esFIRMA emprega sistemas fiáveis para o Depósito, de modo que:

- Apenas as pessoas autorizadas podem fazer anotações e modificações.
- É possível verificar a autenticidade da informação.
- Qualquer mudança técnica que afete os requisitos de segurança pode ser detectada.

3. Identificação e autenticação

3.1 Registro inicial

3.1.1 Tipos de nomes

Todos os certificados contêm um nome diferenciado X.501 no campo *Assunto*, incluindo um componente *Common Name* (CN), referente à identidade do assinante e da pessoa física identificada no certificado, bem como várias informações adicionais de identidade no campo *SubjectAlternativeName*.

Os nomes contidos nos certificados são os seguintes.

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

País (C)	ES
Organization (O)	Denominação (nome "oficial") da Administração, organismo, entidade de direito público ou outra entidade subscritora do certificado, à qual o empregado está vinculado
organizationalUnitName (OU)	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Sobrenome	Primeiro e segundo (opcional) sobrenome, de acordo com o documento de identidade (DNI / Passaporte)
Given Name	Nome próprio, de acordo com o documento de identidade (DNI/Passaporte)
Serial Number	DNI/NIE do empregado
Common Name (CN)	Nome Apelido1 Apelido2 - NIF do funcionário
Tipo de certificado OID: 2.16.724.1.3.5.7.1.1	CERTIFICADO QUALIFICADO DE ASSINATURA DE FUNCIONÁRIO PÚBLICO DE ALTO NÍVEL
Nome da entidade subscritora OID: 2.16.724.1.3.5.7.1.2	Nome da entidade subscritora
NIF da entidade subscritora OID: 2.16.724.1.3.5.7.1.3	NIF entidad subscription
DNI/NIE do responsável OID: 2.16.724.1.3.5.7.1.4	DNI ou NIE do responsável

Nome próprio OID: 2.16.724.1.3.5.7.1.6	Nome próprio do responsável pelo certificado
Primer apellido OID: 2.16.724.1.3.5.7.1.7	Sobrenome do responsável pelo certificado
Segundo sobrenome OID: 2.16.724.1.3.5.7.1.8	Segundo sobrenome do responsável pelo certificado. Opcional.
Correo electrónico OID: 2.16.724.1.3.5.7.1.9	E-mail do responsável pelo certificado. Opcional.

3.1.1.2 Certificado de assinatura de funcionário público, nível médio, em HSM

País (C)	ES
Organization (O)	Denominação (nome "oficial") da Administração, organismo ou entidade de direito público subscritora do certificado, à qual o empregado está vinculado
organizationalUnitName (OU)	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Sobrenome	Primeiro e segundo (opcional) sobrenome, de acordo com o documento de identidade (DNI / Passaporte)
Given Name	Nome próprio, de acordo com o documento de identidade (DNI/Passaporte)
Serial Number	DNI/NIE do empregado
Common Name (CN)	Nome Apelido1 Apelido2 - NIF do funcionário
Tipo de certificado OID: 2.16.724.1.3.5.7.2.1	CERTIFICADO ELETRÔNICO DE EMPREGADO PÚBLICO DE NÍVEL MÉDIO
Nome da entidade subscritora OID: 2.16.724.1.3.5.7.2.2	Nome da entidade subscritora
NIF da entidade subscritora OID: 2.16.724.1.3.5.7.2.3	NIF da entidade subscritora
DNI/NIE do responsável OID: 2.16.724.1.3.5.7.2.4	DNI ou NIE do responsável
Número de autenticação pessoal OID: 2.16.724.1.3.5.7.2.5	NRP ou NIP do responsável pelo assinante do certificado
Nome próprio OID: 2.16.724.1.3.5.7.2.6	Nome próprio do responsável pelo certificado

Primer apellido OID: 2.16.724.1.3.5.7.2.7	Sobrenome do responsável pelo certificado
Segundo sobrenome OID: 2.16.724.1.3.5.7.2.8	Segundo sobrenome do responsável pelo certificado. Opcional.
Correo electrónico OID: 2.16.724.1.3.5.7.2.9	Endereço de e-mail do responsável pelo certificado. Opcional.

3.1.1.3 Certificado de autenticação de funcionário público, nível alto, em cartão

País (C)	ES
Organization (O)	Denominação (nome "oficial") da Administração, organismo, entidade de direito público ou outra entidade subscritora do certificado, à qual o empregado está vinculado
organizationalUnitName (OU)	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Sobrenome	Primeiro e segundo (opcional) sobrenome, de acordo com o documento de identidade (DNI / Passaporte)
Given Name	Nome próprio, de acordo com o documento de identidade (DNI/Passaporte)
Serial Number	DNI/NIE do empregado
Common Name (CN)	Nome Apelido1 Apelido2 - NIF do funcionário
Tipo de certificado OID: 2.16.724.1.3.5.7.1.1	CERTIFICADO ELETRÔNICO DE EMPREGADO PÚBLICO DE ALTO NÍVEL DE AUTENTICAÇÃO
Nome da entidade subscritora OID: 2.16.724.1.3.5.7.1.2	Nome da entidade subscritora
NIF da entidade subscritora OID: 2.16.724.1.3.5.7.1.3	NIF entidad subscription
DNI/NIE do responsável OID: 2.16.724.1.3.5.7.1.4	DNI ou NIE do responsável
Nome próprio OID: 2.16.724.1.3.5.7.1.6	Nome próprio do responsável pelo certificado
Primer apellido OID: 2.16.724.1.3.5.7.1.7	Sobrenome do responsável pelo certificado
Segundo sobrenome OID: 2.16.724.1.3.5.7.1.8	Segundo sobrenome do responsável pelo certificado. Opcional.

Correo electrónico 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 médio, em software

País (C)	ES
Organization (O)	Denominação (nome "oficial" da organização) do assinante
organizationalUnitName (OU)	SELLO ELETRÔNICO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Serial Number	DNI/NIE da organização subscritora
Common Name (CN)	Denominação do sistema ou aplicação de processo automático.
Tipo de certificado OID: 2.16.724.1.3.5.6.2.1	SELLO ELETRÔNICO DE NÍVEL MÉDIO
Nome da entidade subscritora OID: 2.16.724.1.3.5.6.2.2	Nome da entidade subscritora
NIF da entidade subscritora OID: 2.16.724.1.3.5.6.2.3	NIF da entidade subscritora
Denominação do sistema OID: 2.16.724.1.3.5.6.2.5	Denominação do sistema
Correo electrónico OID: 2.16.724.1.3.5.6.2.9	E-mail do responsável pelo selo

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

País (C)	ES
Organization (O)	Denominação (nome "oficial" da organização) do assinante
organizationalUnitName (OU)	SELLO ELETRÔNICO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Serial Number	DNI/NIE da organização subscritora
Common Name (CN)	Denominação do sistema ou aplicação de processo automático.

Tipo de certificado OID: 2.16.724.1.3.5.6.2.1	SELLO ELETRÔNICO DE NÍVEL MÉDIO
Nome da entidade subscritora OID: 2.16.724.1.3.5.6.2.2	Nome da entidade subscritora
NIF da entidade subscritora OID: 2.16.724.1.3.5.6.2.3	NIF da entidade subscritora
Denominação do sistema OID: 2.16.724.1.3.5.6.2.5	Denominação do sistema

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

País (C)	ES
Organization (O)	Denominação (nome "oficial") da Administração, organismo ou entidade de direito público subscritora do certificado, à qual o empregado está vinculado
organizationalUnitName (OU)	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO COM PSEUDÔNIMO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Pseudônimo	Pseudônimo obrigatório de acordo com a ETSI EN 319 412-2 para este tipo de certificados
Common Name (CN)	Seudônimo e o Organismo
Tipo de certificado OID: 2.16.724.1.3.5.4.1.1	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO COM PSEUDÔNIMO DE ALTO NÍVEL
Nome da entidade subscritora OID: 2.16.724.1.3.5.4.1.2	Nome da entidade subscritora
NIF da entidade subscritora OID: 2.16.724.1.3.5.4.1.3	NIF da entidade subscritora
Seudônimo OID: 2.16.724.1.3.5.4.1.12	Pseudônimo usado pelo signatário e autorizado pelo assinante

3.1.1.7 Certificado de assinatura de funcionário público com pseudônimo, nível médio, em HSM

País (C)	ES
Organization (O)	Denominação (nome "oficial") da Administração, organismo ou entidade de direito público subscritora do certificado, à qual o empregado está vinculado

organizationalUnitName (OU)	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO COM PSEUDÔNIMO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Pseudônimo	Pseudônimo obrigatório de acordo com a ETSI EN 319 412-2 para este tipo de certificados
Common Name (CN)	Seudônimo e o Organismo
Tipo de certificado OID: 2.16.724.1.3.5.4.2.1	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO COM PSEUDÔNIMO DE NÍVEL MÉDIO
Nome da entidade subscritora OID: 2.16.724.1.3.5.4.2.2	Nome da entidade subscritora
NIF da entidade subscritora OID: 2.16.724.1.3.5.4.2.3	NIF da entidade subscritora
Seudônimo OID: 2.16.724.1.3.5.4.2.12	Pseudônimo usado pelo signatário e autorizado pelo assinante

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

País (C)	ES
Organization (O)	Denominação (nome "oficial") da Administração, organismo, entidade de direito público ou outra entidade subscritora do certificado, à qual o empregado está vinculado
organizationalUnitName (OU)	CERTIFICADO ELETRÔNICO DE FUNCIONÁRIO PÚBLICO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
pseudônimo	Seudônimo obrigatório de acordo com a ETSI EN 319 412-2
Common Name (CN)	Puesto ou cargo ou "SEUDÔNIMO" - NÚMERO IDENTIFICATIVO - NOME OFICIAL DO ORGANISMO
Tipo de certificado OID: 2.16.724.1.3.5.4.1.1	CERTIFICADO DE AUTENTICAÇÃO DE FUNCIONÁRIO PÚBLICO COM PSEUDÔNIMO
Nome da entidade subscritora OID: 2.16.724.1.3.5.4.1.2	Nome da entidade subscritora
NIF da entidade subscritora OID: 2.16.724.1.3.5.4.1.3	NIF da entidade subscritora

3.1.1.9 Certificado de selo eletrônico de TSA/TSU

País (C)	ES
Organization (O)	Denominação (nome "oficial" da organização) do assinante
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Common Name (CN)	Denominação da TSU

3.1.1.10 Certificado de assinatura de pessoa física vinculada, em cartão

Subperfil Espanha:

País (C)	ES
Organization (O)	Denominação (nome "oficial") da entidade subscritora do certificado, à qual o funcionário está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Sobrenome	Primeiro e segundo (opcional) sobrenome, de acordo com o documento de identidade (DNI / Passaporte)
Given Name	Nome próprio, de acordo com o documento de identidade (DNI/Passaporte)
Serial Number	DNI/NIE da pessoa física
Common Name (CN)	Apellido1 Apellido2 Nome - NIF pessoa física (ASSINATURA)
Tipo de certificado OID: 1.3.6.1.4.1.47281.0.7.1	CERTIFICADO DE PESSOA FÍSICA VINCULADA A ENTIDADE
Nome da entidade subscritora OID: 1.3.6.1.4.1.47281.0.7.2	Nome da entidade subscritora
NIF da entidade subscritora OID: 1.3.6.1.4.1.47281.0.7.3	NIF entidad subscription
DNI/NIE do responsável OID: 1.3.6.1.4.1.47281.0.7.4	DNI ou NIE do responsável
Nome próprio OID: 1.3.6.1.4.1.47281.0.7.6	Nome próprio do responsável pelo certificado
Primer apellido OID: 1.3.6.1.4.1.47281.0.7.7	Sobrenome do responsável pelo certificado
Segundo sobrenome OID: 1.3.6.1.4.1.47281.0.7.8	Segundo sobrenome do responsável pelo certificado. Opcional.

Correo electrónico OID: 1.3.6.1.4.1.47281.0.7.9	E-mail do responsável pelo certificado. Opcional.

Subperfil Europa:

País (C)	País
Organization (O)	Denominação (nome "oficial") da entidade subscritora do certificado, à qual o funcionário está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Sobrenome	Primeiro e segundo (opcional) sobrenome, de acordo com o documento de identidade
Given Name	Nome próprio, de acordo com o documento de identidade
Serial Number	Número do documento de identidade da pessoa física
Common Name (CN)	Sobrenome1 Sobrenome2 Nome - num 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 com a organização do sujeito
Identificador da entidade assinante OID: 1.3.6.1.4.1.47281.0.19.3	Corresponde com o organizationIdentifier do sujeito
Identificador do responsável OID: 1.3.6.1.4.1.47281.0.19.4	DNI ou NIE do responsável
Nome próprio OID: 1.3.6.1.4.1.47281.0.19.6	Nome próprio do responsável pelo certificado
Primer apellido OID: 1.3.6.1.4.1.47281.0.19.7	Sobrenome do responsável pelo certificado
Segundo sobrenome OID: 1.3.6.1.4.1.47281.0.19.8	Segundo sobrenome do responsável pelo certificado. Opcional.
Unidade da entidade subscritora OID: 1.3.6.1.4.1.47281.0.19.10	Corresponde com OrganizationUnit do sujeito. Opcional

3.1.1.11 Certificado de assinatura de pessoa física vinculada, em HSM

Subperfil Espanha:

País (C)	ES

Organization (O)	Denominação (nome "oficial") da entidade subscritora, à qual o funcionário está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Sobrenome	Primeiro e segundo (opcional) sobrenome, de acordo com o documento de identidade (DNI / Passaporte)
Given Name	Nome próprio, de acordo com o documento de identidade (DNI/Passaporte)
Serial Number	DNI/NIE do empregado
Common Name (CN)	Apellido1 Apellido2 Nome - NIF pessoa física
Tipo de certificado OID: 1.3.6.1.4.1.47281.0.7.1	CERTIFICADO DE PESSOA FÍSICA VINCULADA A ENTIDADE
Nome da entidade subscritora OID: 1.3.6.1.4.1.47281.0.7.2	Nome da entidade subscritora
NIF da entidade subscritora OID: 1.3.6.1.4.1.47281.0.7.3	NIF entidad subscription
DNI/NIE do responsável OID: 1.3.6.1.4.1.47281.0.7.4	DNI ou NIE do responsável
Nome próprio OID: 1.3.6.1.4.1.47281.0.7.6	Nome próprio do responsável pelo certificado
Primer apellido OID: 1.3.6.1.4.1.47281.0.7.7	Sobrenome do responsável pelo certificado
Segundo sobrenome OID: 1.3.6.1.4.1.47281.0.7.8	Segundo sobrenome do responsável pelo certificado. Opcional.
Correo electrónico OID: 1.3.6.1.4.1.47281.0.7.9	E-mail do responsável pelo certificado. Opcional.

Subperfil Europa:

País (C)	País
Organization (O)	Denominação (nome "oficial") da entidade subscritora do certificado, à qual o funcionário está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Sobrenome	Primeiro e segundo (opcional) sobrenome, de acordo com o documento de identidade
Given Name	Nome próprio, de acordo com o documento de identidade
Serial Number	Número do documento de identidade da pessoa física

Common Name (CN)	Sobrenome1 Sobrenome2 Nome - num documento
Nome próprio OID: 1.3.6.1.4.1.47281.0.19.6	Nome do responsável pelo certificado, corresponde a Given Name
Primer apellido OID: 1.3.6.1.4.1.47281.0.19.7	Sobrenome do responsável pelo certificado
Segundo sobrenome OID: 1.3.6.1.4.1.47281.0.19.8	Segundo sobrenome do responsável pelo certificado. Opcional.

3.1.1.12 Certificado de autenticação de pessoa física vinculada, em cartão

Subperfil Espanha:

País (C)	ES
Organization (O)	Denominação (nome "oficial") da entidade subscritora do certificado, à qual o funcionário está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Sobrenome	Primeiro e segundo (opcional) sobrenome, de acordo com o documento de identidade (DNI / Passaporte)
Given Name	Nome próprio, de acordo com o documento de identidade (DNI/Passaporte)
Serial Number	DNI/NIE do empregado
Common Name (CN)	Apellido1 Apellido2 Nome - NIF pessoa física (AUTENTICAÇÃO)
Tipo de certificado OID: 1.3.6.1.4.1.47281.0.7.1	CERTIFICADO DE PESSOA FÍSICA VINCULADA A ENTIDADE
Nome da entidade subscritora OID: 1.3.6.1.4.1.47281.0.7.2	Nome da entidade subscritora
NIF da entidade subscritora OID: 1.3.6.1.4.1.47281.0.7.3	NIF entidad subscription
DNI/NIE do responsável OID: 1.3.6.1.4.1.47281.0.7.4	Corresponde com SerialNumber do sujeito
Nome próprio OID: 1.3.6.1.4.1.47281.0.7.6	Nome próprio do responsável pelo certificado
Primer apellido OID: 1.3.6.1.4.1.47281.0.7.7	Sobrenome do responsável pelo certificado

Segundo sobrenome OID: 1.3.6.1.4.1.47281.0.7.8	Segundo sobrenome do responsável pelo certificado. Opcional.
Correo electrónico OID: 1.3.6.1.4.1.47281.0.7.9	E-mail do responsável pelo certificado. Opcional.

Subperfil Europa:

País (C)	País
Organization (O)	Denominação (nome "oficial") da entidade subscritora do certificado, à qual o funcionário está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Sobrenome	Primeiro e segundo (opcional) sobrenome, de acordo com o documento de identidade
Given Name	Nome próprio, de acordo com o documento de identidade
Serial Number	Número do documento de identidade da pessoa física
Common Name (CN)	Sobrenome1 Sobrenome2 Nome - num documento (AUTENTICAÇÃO)
Nome próprio OID: 1.3.6.1.4.1.47281.0.19.6	Nome do responsável pelo certificado, corresponde a Given Name
Primer apellido OID: 1.3.6.1.4.1.47281.0.19.7	Sobrenome do responsável pelo certificado
Segundo sobrenome OID: 1.3.6.1.4.1.47281.0.19.8	Segundo sobrenome do responsável pelo certificado. Opcional.

3.1.1.13 Certificado de assinatura de pessoa física vinculada, em cartão, com pseudônimo

Subperfil Espanha:

País (C)	ES
Organization (O)	Denominação (nome "oficial") da entidade subscritora do certificado, à qual o funcionário está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
pseudônimo	Seudônimo obrigatório de acordo com a ETSI EN 319 412-2
Common Name (CN)	Puesto ou "SEUDÔNIMO" - NÚMERO IDENTIFICATIVO - NOME DA ENTIDADE

Subperfil Europa:

País (C)	País
Organization (O)	Denominação (nome "oficial") da entidade subscritora do certificado, à qual o funcionário está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
pseudônimo	Seudônimo obrigatório de acordo com a ETSI EN 319 412-2
Common Name (CN)	PSEUDÔNIMO - NOME ENTIDADE

3.1.1.14 Certificado de assinatura de pessoa física vinculada, em HSM

Subperfil Espanha:

País (C)	ES
Organization (O)	Denominação (nome "oficial") da entidade subscritora, à qual o funcionário está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
pseudônimo	Seudônimo obrigatório de acordo com a ETSI EN 319 412-2
Common Name (CN)	Puesto ou "SEUDÔNIMO" - NÚMERO IDENTIFICATIVO - NOME DA ENTIDADE

Subperfil Europa:

País (C)	País
Organization (O)	Denominação (nome "oficial") da entidade subscritora do certificado, à qual o funcionário está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
pseudônimo	Seudônimo obrigatório de acordo com a ETSI EN 319 412-2
Common Name (CN)	PSEUDÔNIMO - NOME ENTIDADE

3.1.1.15 Certificado de autenticação de pessoa física vinculada, em cartão, com pseudônimo

Subperfil Espanha:

País (C)	ES

Organization (O)	Denominação (nome "oficial") da entidade subscritora do certificado, à qual o funcionário está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Common Name (CN)	Puesto ou "SEUDÔNIMO" - NÚMERO IDENTIFICATIVO - NOME DA ENTIDADE

Subperfil Europa:

País (C)	País
Organization (O)	Denominação (nome "oficial") da entidade subscritora do certificado, à qual o funcionário está vinculado
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
pseudônimo	Seudônimo obrigatório de acordo com a ETSI EN 319 412-2
Common Name (CN)	PSEUDÔNIMO - NOME ENTIDADE

3.1.1.16 Certificado de selo eletrônico, em software

Subperfil Espanha:

País (C)	ES
Organization (O)	Denominação (nome "oficial" da organização) do assinante
organizationalUnitName (OU)	SELLO ELETRÔNICO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Serial Number	DNI/NIE da organização subscritora
Common Name (CN)	Denominação do sistema ou aplicação de processo automático.

Subperfil Europa:

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

Serial Number	Identificação da organização subscritora (legalPersonSemanticsIdentifier)

3.1.1.17 Certificado de selo eletrônico com gerenciamento centralizado

Subperfil Espanha:

País (C)	ES
Organization (O)	Denominação (nome "oficial" da organização) do assinante
organizationalUnitName (OU)	SELLO ELETRÔNICO
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Serial Number	DNI/NIE da organização subscritora
Common Name (CN)	Denominação do sistema ou aplicação de processo automático.

Subperfil Europa:

País (C)	País
Organization (O)	Denominação (nome "oficial" da organização) do assinante
organizationIdentifier	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Serial Number	Identificação da organização subscritora (legalPersonSemanticsIdentifier)

3.1.2. Significado dos nomes

Os nomes contidos nos campos *SubjectName* y *SubjectAlternativeName* os certificados são compreensíveis em linguagem natural, de acordo com o estabelecido na seção anterior.

3.1.3 Uso de anônimos e pseudônimos

Em nenhum caso podem ser utilizados pseudônimos para identificar uma entidade/empresa/organização, e em nenhum caso são emitidos certificados anônimos, exceto quando, por razões de segurança pública, os sistemas de assinatura eletrônica possam se referir apenas ao número de identificação profissional do funcionário público.

3.1.4 Interpretação de formatos de nomes

Os formatos de nomes serão interpretados de acordo com a lei do país de estabelecimento do assinante, em seus próprios termos.

O campo "país" será sempre Espanha, uma vez que os certificados são emitidos exclusivamente para as Administrações Públicas espanholas.

O certificado mostra a relação entre uma pessoa física e a Administração, organismo, entidade de direito público ou outra entidade com a qual está vinculada, independentemente da nacionalidade da pessoa física. Isso decorre da natureza corporativa do certificado, do qual a corporação é o subscritor e a pessoa física vinculada é a pessoa autorizada a usá-lo.

Nos certificados emitidos para assinantes espanhóis, o campo "número de série" deve incluir o NIF do signatário, para que o certificado seja aceito para a realização de procedimentos com as Administrações espanholas.

3.1.5 Unicidade dos nomes

Os nomes dos subscritores de certificados serão únicos para cada política de certificado da esFIRMA.

Não é possível atribuir um nome de assinante que já tenha sido usado a um assinante diferente, situação que, em princípio, não deve ocorrer, graças à presença do Número de Identificação Fiscal, ou equivalente, no esquema de nomes.

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

- Número de Identificação Fiscal (NIF) ou outro identificador legalmente válido da pessoa física.
- Número de Identificação Fiscal (NIF) ou outro identificador legalmente válido do subscritor.
- Tipo de Certificado (Campo descrição do certificado).

3.1.6 Resolução de conflitos relativos a nomes

Os requerentes de certificados não incluirão nomes nas solicitações que possam implicar em violação, por parte do futuro assinante, dos direitos de terceiros.

esFIRMA não será obrigada a determinar previamente se um solicitante de certificados tem direitos de propriedade industrial sobre o nome que aparece em uma solicitação de certificado, mas em princípio procederá a certificá-lo.

Da mesma forma, não atuará como árbitro ou mediador, nem de qualquer outra forma deverá resolver qualquer disputa relacionada à propriedade de nomes de pessoas ou organizações, nomes de domínio, marcas ou nomes comerciais.

No entanto, se receber uma notificação sobre um conflito de nomes, de acordo com a legislação do país do assinante, poderá tomar as medidas apropriadas para bloquear ou retirar o certificado emitido.

Em todo caso, o provedor de serviços de certificação reserva-se o direito de recusar um pedido de certificado devido a um conflito de nomes.

Qualquer controvérsia ou conflito decorrente do presente documento será definitivamente resolvido por meio de arbitragem de direito de um árbitro, no âmbito da Corte Espanhola de Arbitragem, de acordo com seu Regulamento e Estatuto, que é encarregada da administração da arbitragem e da nomeação do árbitro ou tribunal arbitral. As partes registram seu compromisso de cumprir a sentença que é emitida no documento contratual que formaliza o serviço.

3.2 Validação inicial da identidade

A identidade dos assinantes de certificados é estabelecida no momento da assinatura do contrato entre esFIRMA e o assinante ou antes da ativação do serviço de esFIRMA, momento em que é verificada a existência do assinante e da documentação justificativa de sua identidade, cargo e/ou condição em que assina e seu endereço, de acordo com o indicado na regulamentação do direito administrativo que seja aplicável.

A identidade das pessoas físicas identificadas nos certificados é validada por meio dos registros corporativos da Administração, órgão, entidade de direito público ou outra entidade subscritora dos certificados. O subscritor produzirá uma certificação dos dados necessários e a enviará para a esFIRMA, pelos meios que esta habilite, para o registro da identidade dos signatários. Quando o subscritor não tiver Secretaria, essa certificação será emitida pelo Responsável pelo serviço de certificação designado.

O responsável pelo tratamento dos dados pessoais de cada Administração, organismo, entidade de direito público ou outra entidade é cada uma delas, sendo a esFIRMA 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 de confiança "esFIRMA" e da empresa ESPUBLICO[1].

3.2.1 Prova de posse da chave privada

A posse da chave privada é comprovada pelo procedimento confiável de entrega e aceitação do certificado pelo signatário a partir da Plataforma de Administração Eletrônica, ao assinar a folha de aceitação, e seu uso nessa plataforma.

1. 3.2.2 Identificação da entidade

Nas Administrações Públicas, não é exigida a documentação comprovativa da existência da administração pública, organismo ou entidade de direito público, uma vez que essa identidade faz parte do âmbito corporativo da Administração Geral do Estado ou de outras AAPP do Estado.

EsFIRMA verifica a existência de cada Administração Pública, organismo ou entidade de direito público, quando necessário, perante o inventário de entidades do setor público do Ministério da Fazenda e Função Pública em , perante um Boletim Oficial de seu âmbito

[1] Ap 6.2.2.q) de ETSI EN 319 411-1

ou mediante a integração com o Sistema de Diretório Comum (DIR3).https://www.hacienda.gob.es/es-ES/CDI/Paginas/Inventario/Inventario.aspx

No caso de a entidade não fazer parte do âmbito corporativo da Administração Geral do Estado ou de outras AAPP do Estado, ESFIRMA verificará a existência da entidade por meio de os documentos ou consulta de registros públicos pertinentes conforme indicado na regulamentação de direito administrativo que seja aplicável.

As pessoas físicas com capacidade de agir em nome de uma Administração, organismo, entidade de direito público ou outra entidade subscritora dos certificados, poderão atuar como representantes das mesmas em relação ao previsto nesta DPC, desde que exista uma situação prévia de representação legal ou voluntária entre a pessoa física e a Administração, organismo, entidade de direito público ou outra entidade subscritora dos certificados, que exige seu reconhecimento por esFIRMA, o qual será realizado por meio de um dos seguintes procedimentos:

1. No caso de a pessoa que ocupe o cargo de Secretário ter a faculdade de fé pública, serão coletados e verificados os seguintes documentos:
    a. Certificado do Secretário no qual se nomeia o representante legal, com os seguintes dados:
        i. Nome e sobrenome 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. No caso de a pessoa que ocupa o cargo de Secretário não ter a faculdade de fé pública, serão coletados e verificados os seguintes documentos:
    a. Um certificado do Secretário da nomeação do representante legal no qual constam os seguintes dados:
        i. Dados do representante:
            1. Nome e sobrenome do representante legal
            2. Documento: NIF do representante
        ii. Dados da entidade que representa:
            1. CIF

2. Nome
3. Endereço postal

iii. Informação sobre a validade da representação

b. Documentação oficial que permita comprovar os dados relativos à representação ou à capacidade de atuação que detém o representante legal.

c. Todos os documentos necessários para comprovar os extremos citados de maneira inequívoca, de acordo com o indicado na regulamentação de direito administrativo aplicável, e sua inscrição no registro público correspondente, se assim for exigível.

Após a verificação da documentação coletada, o Representante legal procederá à assinatura do contrato de prestação de serviços de certificação entre esFIRMA (ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA) e a entidade por meio da qual são reguladas as condições sob as quais a ESFIRMA prestará os serviços de certificação à entidade, que se constitui como Autoridade de Registro, nomeando os Operadores autorizados para exercer as funções correspondentes à RA.

Uma vez assinados eletronicamente os documentos, as funções de RA serão ativadas para os usuários da entidade que constem no contrato como operadores autorizados para desempenhar essa função.

3.2.3 Autenticação da identidade de uma pessoa física

Esta seção descreve os métodos de verificação da identidade de uma pessoa física identificada em um certificado.

O procedimento para solicitar e gerar certificados é realizado através de um procedimento eletrônico na Plataforma de Administração Eletrônica à disposição do assinante e dos signatários.

O procedimento eletrônico para emitir um certificado para uma pessoa física seguirá os seguintes passos e os seguintes documentos serão gerados:

1. Solicitação da pessoa física através da Plataforma de Administração Eletrônica (com seu respectivo registro de entrada e abertura de processo).

2. Um certificado em que o Operador de Verificação atesta a ligação entre o requerente e a entidade.
3. Ordem de emissão assinada pelo Operador de autorização da entidade, que é registrada na saída e notificada à ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (anexando cópia do certificado e do pedido do usuário).

O procedimento eletrônico para emitir um certificado de selo eletrônico seguirá os seguintes passos e os seguintes documentos serão gerados:

1. Ordem de emissão do Representante legal através da Plataforma de Administração Eletrônica (com seu respectivo registro de entrada e abertura de processo). Para apresentar tal solicitação, o Representante legal deverá se identificar na plataforma utilizando meios de identificação eletrônica, para os quais tenha sido garantida a presença da pessoa física de acordo com o artigo 8 do Regulamento eIDAS em relação aos níveis de segurança "substancial" ou "alto".

3.2.3.1 Nos certificados

A informação de identificação das pessoas físicas identificadas nos certificados é validada comparando a informação da solicitação da Administração, organismo, entidade de direito público ou outra entidade subscritora dos certificados, com os registros da Administração, organismo, entidade de direito público ou outra entidade a que está vinculado, gerados conforme indicado no ponto 3.2 desta DPC, assegurando a correção da informação a certificar.

3.2.3.2 Necessidade de presença pessoal

Para realizar o pedido dos certificados, não é necessário a presença física direta devido à relação já comprovada entre a pessoa física e a Administração, organismo, entidade de direito público ou outra entidade à qual está vinculada. Essa comprovação é refletida na validação do pedido pelo Operador de verificação autorizado pelo assinante, que registra a identificação presencial e única do signatário.

Para aceitar o certificado, não é necessária a presença física direta do signatário, pois isso pode ser feito por meio de assinatura eletrônica avançada. Durante este procedimento, a identidade da pessoa física identificada no certificado é confirmada.

3.2.3.3 Vinculação da pessoa física

A justificação documental da vinculação de uma pessoa física identificada em um certificado com a Administração, organismo, entidade de direito público ou outra entidade é dada pela sua presença nos Registros de Pessoal da Administração, organismo, entidade de direito público ou outra entidade à qual a pessoa física está vinculada.

3.2.4 Informação de assinante não verificada

esFIRMA não inclui nenhuma informação de assinante não verificada nos certificados.

3.2.5 Critérios de interoperabilidade

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

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

3.3 Identificação e autenticação de solicitações de renovação

3.3.1 Validação para renovação rotineira de certificados

esFirma não realiza renovações de certificados. esFirma emitirá um novo certificado, seguindo o procedimento de solicitação registrado na Plataforma de Administração Eletrônica.

3.3.2 Identificação e autenticação de renovação após revogação

esFIRMA não realiza renovações de certificados.

3.4 Identificação e autenticação do pedido de revogação

A esFIRMA autentica as solicitações e relatórios relacionados com a revogação de um certificado, verificando se provêm de uma pessoa autorizada.
Os métodos aceitáveis para essa verificação são os seguintes:

- O envio de um pedido de revogação por parte do assinante ou da pessoa física identificada no certificado, assinado eletronicamente.
- O uso da "frase de verificação de identidade", ou de outros métodos de autenticação pessoal, que consiste em informações que apenas a pessoa física identificada no certificado conhece, e que lhe permite revogar automaticamente o seu certificado.
- A apresentação física em um escritório da entidade assinante.
- Outros meios de comunicação, como o telefone, quando houver garantias razoáveis da identidade do solicitante da revogação, a critério da esFIRMA.

esFIRMA não realiza suspensões de certificados. As solicitações de suspensão são tratadas como solicitações de revogação.

4. Requisitos de operação do ciclo de vida dos certificados

4.1 Solicitação de certificado

4.1.1 Legitimação para solicitar a emissão

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

Além disso, antes da emissão e entrega de um certificado, há uma solicitação de certificados em um formulário de solicitação de certificados através da Plataforma de Administração Eletrônica.

Existe uma autorização do assinante para que o solicitante possa realizar a solicitação, que é formalizada juridicamente por meio de um formulário de solicitação de certificados assinado pelo solicitante em nome da Administração, órgão, entidade de direito público ou outra entidade.

4.1.2 Procedimento de registro e responsabilidades

esFIRMA recebe solicitações de certificados, feitas por Administrações, organismos, entidades de direito público ou outras entidades.

As solicitações são realizadas por meio de um documento em formato eletrônico, preenchido pela Administração, organismo, entidade de direito público ou outra entidade, cujo destinatário é o esFIRMA, que incluirá os dados das pessoas às quais os certificados serão emitidos. A solicitação será feita pelo operador autorizado pelo assinante (responsável pela certificação) e que foi identificado no contrato entre este assinante e o esFIRMA.

A solicitação deve ser acompanhada de documentação justificativa da identidade e outras circunstâncias da pessoa física identificada no certificado, de acordo com o estabelecido na seção 3.2.3. Também deve ser fornecido um endereço físico, ou outros dados, que permitam entrar em contato com a pessoa física identificada no certificado.

4.2 Processamento do pedido de certificação

4.2.1 Execução das funções de identificação e autenticação

Uma vez recebido um pedido de certificado, a esFIRMA garante que os pedidos de certificado sejam completos, precisos e devidamente autorizados antes de processá-los.

Caso afirmativo, esFIRMA verifica a informação fornecida, verificando se os requisitos descritos na seção 3.2 foram cumpridos corretamente.

A documentação justificativa da aprovação da solicitação deve ser mantida, devidamente registrada e com garantias de segurança e integridade, pelo prazo de 15 anos a partir da extinção do certificado ou da conclusão do serviço prestado, mesmo em caso de perda antecipada de validade por revogação, uma vez que os certificados são qualificados.

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 domínios e os critérios de mitigação de riscos próprios da esFIRMA.

4.2.2 Aprovação ou rejeição do pedido

esFIRMA aprova o pedido do certificado e procede à sua emissão e entrega, após a solicitação que ocorre na Plataforma de Administração Eletrônica.

Em caso de suspeita de que a informação não é correta ou pode afetar a reputação da Entidade de Certificação ou dos assinantes, a esFIRMA negará o pedido ou interromperá sua aprovação até que sejam realizadas as verificações complementares que considere apropriadas.

Caso as verificações adicionais não revelem a correção das informações a serem verificadas, a esFIRMA negará definitivamente a solicitação.

esFIRMA notifica ao solicitante a aprovação ou negação da solicitação.

esFIRMA poderá automatizar os procedimentos de verificação da correção das informações que serão contidas nos certificados e de aprovação das solicitações.

4.2.3 Prazo para resolver a solicitação

O esFIRMA atende as solicitações de certificados por ordem de chegada, em um prazo razoável, podendo ser especificada uma garantia de prazo máximo no contrato de emissão de certificados.

As solicitações permanecem ativas até sua aprovação ou rejeição.

4.3 Emissão do certificado

4.3.1 Ações da CA 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, por meio do envio de um link para o dispositivo móvel e/ou endereço de e-mail designado pelo assinante na solicitação de certificados, de acordo com o procedimento indicado na seção 4.4.2 ou por meio do sistema de mensagens da Plataforma de Administração Eletrônica.

Durante o processo, esFIRMA:

- Protege a confidencialidade e integridade dos dados de registro que possui.
- Utiliza sistemas e produtos confiáveis que estejam protegidos contra qualquer alteração e que garantam a segurança técnica e, se for o caso, criptográfica dos processos de certificação aos quais servem de suporte.
- Gera o par de chaves, através de um procedimento de geração de certificados vinculado de forma segura com o procedimento de geração de chaves.
- Utiliza um procedimento de geração de certificados que vincula de forma segura o certificado com as informações de registro, incluindo a chave pública certificada.
- Assegura-se de que o certificado é emitido por sistemas que utilizem proteção contra falsificação e que garantam a confidencialidade das chaves durante o processo de geração dessas chaves.
- Inclui no certificado as informações estabelecidas no anexo 1 do Regulamento (UE) 910/2014, de acordo com o estabelecido nas seções 3.1.1 e 7.1.
- Indica a data e hora em que um certificado foi emitido.

4.3.2 Notificação da emissão ao assinante

esFIRMA notifica a emissão do certificado à Administração, organismo, entidade de direito público ou outra entidade subscritora do certificado, e à pessoa física identificada no certificado, através de seus endereços de e-mail, já incluídos nas informações da Plataforma de Administração Eletrônica.

4.4 Entrega e aceitação do certificado

Durante este processo, esFIRMA deve realizar as seguintes ações:

- Definitivamente comprovar a identidade da pessoa física identificada no certificado, com a colaboração da Administração, organismo, entidade de direito público ou outra entidade de acordo com o estabelecido nas seções 3.2.2, 3.2.3 e 4.3.1.

- Entregar a folha de entrega e aceitação do certificado à pessoa física identificada nela, que contém os seguintes conteúdos mínimos:
    - Informações básicas sobre o uso do certificado, incluindo especialmente informações sobre o provedor de serviços de certificação e a Declaração de Práticas de Certificação aplicável, como suas obrigações, poderes e responsabilidades
    - Informação sobre o certificado.
    - Reconhecimento, por parte do signatário, de receber o certificado e a aceitação dos elementos mencionados.
    - Regime de obrigações do signatário.
    - Responsabilidade do signatário.
    - Método de imputação exclusiva ao signatário, sua chave privada e seus dados de ativação do certificado, de acordo com o estabelecido nas seções 6.2 e 6.4.
    - A data do ato de entrega e aceitação.
- Obter a assinatura, escrita ou eletrônica, da pessoa identificada no certificado.

Quando necessário, a Administração, organismo, entidade de direito público ou outra entidade colabora nesses processos, devendo registrar documentalmente os atos anteriores e conservar os documentos originais mencionados (folhas de entrega e aceitação), enviando uma cópia eletrônica para esFIRMA, bem como os originais quando esFIRMA precisar de acesso aos mesmos.

4.4.1 Comportamento 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 aceitá-lo por meio do envio de um link para o dispositivo móvel e/ou endereço de e-mail designado pelo assinante no pedido de certificados ou por meio do sistema de mensagens da Plataforma de Administração Eletrônica.

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

Nos certificados emitidos em cartão, estes são enviados ao responsável pela certificação do assinante, e os correspondentes PIN são enviados diretamente para o endereço postal do signatário.

Além disso, a aceitação do certificado pela pessoa física identificada no certificado é feita por meio da assinatura do termo de entrega e aceitação, através da Plataforma de Administração Eletrônica.

4.4.2 Publicação do certificado

No caso do certificado de TSA/TSU, a esFIRMA publica-o em seu site.

4.4.3 Notificação da emissão a terceiros

esFIRMA não realiza nenhuma notificação da emissão a terceiras entidades.

4.5 Uso do par de chaves e do certificado

4.5.1 Uso pelo assinante ou signatário

esFIRMA obriga ao seguinte:

- Facilitar a esFIRMA informação completa e adequada, de acordo com os requisitos desta Declaração de Práticas de Certificação, especialmente no que diz respeito ao procedimento de aceitação.
- Manifestar o seu consentimento prévio para a emissão e entrega de um certificado.
- Usar o certificado de acordo com o estabelecido na seção 1.4.
- Quando o certificado funcionar em conjunto com um DCCF, reconhecer sua capacidade de produção de assinaturas eletrônicas qualificadas, isto é, equivalentes a assinaturas manuscritas, bem como outros tipos de assinaturas eletrônicas e mecanismos de criptografia de informações.
- Ser especialmente diligente na guarda da sua chave privada, a fim de evitar usos não autorizados, de acordo com o estabelecido nas seções 6.1, 6.2 e 6.4.
- Comunicar à esFIRMA e a qualquer pessoa que acredite poder confiar no certificado, sem atrasos injustificados:

  - A perda, roubo ou comprometimento potencial da sua chave privada.
  - A perda de controle sobre sua chave privada, devido à comprometimento dos dados de ativação (por exemplo, o código PIN) ou por qualquer outra causa.
  - As imprecisões ou alterações no conteúdo do certificado que o assinante conheça ou possa conhecer.
- Parar de usar a chave privada após o período indicado na seção 6.3.2.
- Que todas as informações fornecidas pelo signatário contidas no certificado estão corretas.
- Que o certificado é usado exclusivamente para fins legais e autorizados, de acordo com a Declaração de Práticas de Certificação.
- Que nenhuma pessoa não autorizada teve acesso à chave privada do certificado, e que é o único responsável pelos danos causados pelo seu incumprimento do dever de proteger a chave privada.
- Que o signatário 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 nenhum certificado (ou qualquer outro formato de chave pública certificada), nem Lista de Revogação de Certificados, nem título de provedor de serviços de certificação ou em qualquer outro caso.

4.5.2 Uso pelo assinante

esFIRMA obriga contratualmente o subscritor a:

- Fornecer à Entidade de Certificação informações completas e adequadas, de acordo com os requisitos desta Declaração de Práticas de Certificação, especialmente no que diz respeito ao procedimento de aceitação.
- Manifestar o seu consentimento prévio para a emissão e entrega de um certificado.
- Usar o certificado de acordo com o estabelecido na seção 1.4.
- Comunicar à esFIRMA e a qualquer pessoa que o assinante acredite que possa confiar no certificado, sem atrasos injustificáveis:
  - A perda, roubo ou comprometimento potencial da sua chave privada.

  - A perda de controle sobre sua chave privada, devido à comprometimento dos dados de ativação (por exemplo, o código PIN) ou por qualquer outra causa.
  - As imprecisões ou alterações no conteúdo do certificado que o assinante conheça ou possa conhecer.
  - A perda, a alteração, o uso não autorizado, o roubo ou a violação, quando existente, do cartão.
- Transmitir às pessoas físicas identificadas no certificado o cumprimento das obrigações específicas dos mesmos e estabelecer mecanismos para garantir o cumprimento efetivo das mesmas.
- Não monitorizar, manipular ou realizar atos de engenharia reversa sobre a implementação técnica dos serviços de certificação da esFIRMA, sem permissão prévia por escrito.
- Não comprometer a segurança dos serviços de certificação do provedor de serviços de certificação da esFIRMA, sem permissão prévia por escrito.
- Que todas as declarações feitas na solicitação estão corretas.
- Que todas as informações fornecidas pelo assinante contidas no certificado estão corretas.
- Que o certificado é usado exclusivamente para fins legais e autorizados, de acordo com a Declaração de Práticas de Certificação.
- Que nenhuma pessoa não autorizada teve acesso à chave privada do certificado, e que é o único responsável pelos danos causados pelo seu incumprimento 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 nenhum certificado (ou qualquer outro formato de chave pública certificada), nem Lista de Revogação de Certificados, nem título de provedor de serviços de certificação ou em qualquer outro caso.

4.5.3 Uso pelo terceiro que confia em certificados

esFIRMA informa ao terceiro que confia em certificados que o mesmo deve assumir as seguintes obrigações:

- Consultar de forma independente se o certificado é apropriado para o uso pretendido.

- Verificar a validade, suspensão ou revogação dos certificados emitidos, para o qual utilizará informações sobre o estado dos certificados.
- Verificar todos os certificados da hierarquia de certificados, antes de confiar na assinatura digital ou em algum dos certificados da hierarquia.
- Reconhecer que para ser considerado certificado qualificado deve estar incluído na Lista de Confiança nacional (Trusted List).
- Reconhecer que as assinaturas eletrônicas verificadas, produzidas em um dispositivo qualificado de criação de assinatura (DCCF), têm a consideração legal de assinaturas eletrônicas qualificadas; isto é, equivalentes a assinaturas manuscritas, bem como que o certificado permite a criação de outros tipos de assinaturas eletrônicas e mecanismos de criptografia.
- Ter em mente quaisquer limitações no uso do certificado, independentemente de estar no próprio certificado ou no contrato de terceiro que confia no certificado.
- Ter em conta qualquer precaução estabelecida em um contrato ou em outro instrumento, independentemente de sua natureza jurídica.
- Não monitorizar, manipular ou realizar atos de engenharia reversa sobre a implementação técnica dos serviços de certificação da esFIRMA, sem permissão prévia por escrito.
- Não comprometer a segurança dos serviços de certificação da esFIRMA, sem permissão prévia por escrito.

esFIRMA informa ao terceiro que confia em certificados que o mesmo deve assumir as seguintes responsabilidades:

- Que tem informação suficiente para tomar uma decisão informada sobre confiar ou não no certificado.
- Que é o único responsável por confiar ou não na informação contida no certificado.
- Que será o único responsável se não cumprir suas obrigações como terceiro que confia no certificado.

4.6. Renovação de certificados

esFIRMA não realiza renovação de certificados. esFirma emitirá um novo certificado, seguindo o procedimento de solicitação registrado na Plataforma de Administração Eletrônica.

4.6.1 Circunstâncias para a renovação do certificado

Não se aplica.

4.6.2 Quem pode solicitar uma renovação

Não se aplica.

4.6.3 Processamento da solicitação de renovação de certificados

Não se aplica.

4.6.4 Notificação de nova emissão de certificado ao assinante

Não se aplica.

4.6.5 Comportamento que constitua a aceitação de um certificado de renovação

Não se aplica.

4.6.6 Publicação do certificado de renovação pela CA

Não se aplica.

4.6.7 Notificação da emissão do certificado pela CA para outras entidades

Não se aplica.

4.7 Renovação de chaves e certificados

4.7.1 Quem pode solicitar o certificado de uma nova chave pública

Não se aplica.

4.7.2 Procedimento com nova identificação

Não se aplica.

4.7.3 Processamento de solicitações de nova chave de certificado

esFIRMA advertirá o subscritor da necessidade de proceder a uma nova identificação do signatário e assinatura da folha de aceitação, nos casos em que seja necessário devido ao transcurso do prazo legal de identificação de 5 anos.

A referida personificação e identificação serão realizadas de acordo com o indicado na seção 3.2.

A assinatura do termo de aceitação será realizada de acordo com o indicado na seção 4.4.2.

4.7.4 Notificação da emissão do certificado renovado

Não se aplica por não haver renovações.

4.7.5 Comportamento que constitui aceitação do certificado

Não se aplica.

4.7.6 Publicação do certificado

Não se aplica.

4.7.7 Notificação da emissão a terceiros

esFIRMA não realiza nenhuma notificação da emissão a terceiras entidades.

4.8 Modificação de certificados

A modificação de certificados será tratada como uma nova emissão de certificado, aplicando-se o descrito nas seções 4.1, 4.2, 4.3 e 4.4.

4.9 Revogação e suspensão de certificados

4.9.1 Causas de revogação de certificados

esFIRMA extinguirá a validade dos certificados eletrônicos por revogação quando ocorrer uma das seguintes causas:

1) Circunstâncias que afetam as informações contidas no certificado:
   a) Modificação de algum dos dados contidos no certificado, após a emissão correspondente do certificado que inclui as modificações.
   b) Descoberta de que alguns dos dados contidos no pedido 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 prestador de serviços de certificação que emitiu o certificado, desde que afete a confiabilidade dos certificados emitidos a partir desse incidente.
   b) Infringimento, por meio da esFIRMA, dos requisitos previstos nos procedimentos de gestão de certificados, estabelecidos nesta Declaração de Práticas de Certificação.
   c) Comprometimento ou suspeita de comprometimento da segurança da chave ou do certificado emitido.
   d) Acesso ou uso não autorizado, por terceiros, da chave privada correspondente à chave pública contida no certificado.
   e) O uso irregular do certificado pela pessoa física identificada no certificado, ou a falta de diligência na guarda da chave privada.

3) Circunstâncias que afetam o assinante ou a pessoa física identificada no certificado:
   a) Finalização da relação jurídica de prestação de serviços entre esFIRMA e o assinante.

b) Modificação ou extinção da relação jurídica subjacente ou causa que provocou a emissão do certificado à pessoa física identificada no certificado.

c) Infringência pelo solicitante do certificado dos requisitos preestabelecidos para a solicitação do mesmo.

d) Infringência pelo assinante ou pela pessoa identificada no certificado, de suas obrigações, responsabilidades e garantias, estabelecidas no documento jurídico correspondente.

e) A incapacidade sobrevenida ou o falecimento do detentor das chaves.

f) A extinção da pessoa jurídica subscritora do certificado, bem como o fim da autorização do subscritor ao detentor das chaves ou o término da relação entre subscritor e pessoa identificada no certificado.

g) Pedido de revogação do certificado pelo assinante, de acordo com o estabelecido na seção 3.4.

4) Outras circunstâncias:

a) O término do serviço de certificação da esFIRMA, de acordo com o estabelecido na seção 5.8.

b) O uso do certificado que seja prejudicial e contínuo para a esFIRMA. Neste caso, considera-se que o uso é prejudicial com base nos seguintes critérios:
   - A natureza e o número de reclamações recebidas.
   - A identidade das entidades que apresentam as queixas.
   - A legislação relevante em vigor em cada momento.
   - A resposta do assinante ou da pessoa identificada no certificado às reclamações recebidas.

c) Pérdida de certificação de algum dos dispositivos qualificados de criação de assinatura que estivesse utilizando esFIRMA na qualidade de Prestador Qualificado de Serviços de Confiança,

4.9.2 Legitimação para solicitar a revogação

É possível solicitar a revogação de um certificado:

- A pessoa identificada no certificado, através de um pedido dirigido à esFIRMA ou ao subscritor.
- O titular do certificado, através de uma solicitação dirigida à esFIRMA.

4.9.3 Procedimentos de solicitação de revogação

O pedido de revogação incluirá as seguintes informações:

- Data de solicitação de revogação.
- Identidade do assinante ou do signatário.
- Razão detalhada para a solicitação de revogação.

O pedido deve ser autenticado, por meio de esFIRMA, de acordo com os requisitos estabelecidos na seção 3.4 desta política, antes de prosseguir com a revogação.

esFIRMA poderá incluir qualquer outro requisito para a confirmação das solicitações de revogação[2].

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

Caso o destinatário de uma solicitação de revogação por parte de uma pessoa física identificada no certificado seja a entidade assinante, uma vez autenticada a solicitação, esta deve enviar uma solicitação nesse sentido para a esFIRMA.

O pedido de revogação será processado após o recebimento e o assinante e a pessoa física identificada no certificado serão informados sobre a mudança de status do certificado revogado.

esFIRMA não reativa o certificado uma vez que tenha sido revogado.

Existe um serviço 24/7 disponível no número de telefone +34 976 579 516, para solicitar a revogação dos certificados. A comunicação é gravada e registrada, para ser..
utilizado como suporte e garantia de aceitação da revogação solicitada.

[2] Ap 6.2.4.a) iii) de ETSI EN 319 411-1

4.9.4 Prazo temporal para solicitação de revogação

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

4.9.5 Prazo temporal de processamento do pedido

A revogação ocorrerá imediatamente após ser recebida, dentro do horário normal de operação da esFIRMA, e não excederá 60 minutos[4].

4.9.6 Obrigação de consulta de informações de revogação de certificados por terceiros

Os terceiros devem verificar o estado dos certificados nos quais desejam confiar.

Um método pelo qual se pode verificar o estado dos certificados é consultando a Lista de Revogação de Certificados mais recente emitida pela Entidade de Certificação de esFIRMA.

As Listas de Revogação de Certificados são publicadas no Repositório da Entidade de Certificação, bem como nos seguintes endereços da web, indicados dentro dos certificados:

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

- *CA INTERMEDIÁRIO:*
  - https://crls1.esfirma.com/acaapp/acaapp2.crl
  - https://crls2.esfirma.com/acaapp/acaapp2.crl

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

[3] Ap 6.2.4.a) vi) de ETSI EN 319 411-1

[4] Ap 6.2.4.a) vii) de ETSI EN 319 411-1

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

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

A CRL indica o momento programado para a emissão de uma nova CRL, embora seja possível emitir uma CRL antes do prazo indicado na CRL anterior, para refletir revogações.

A CRL mantém obrigatoriamente o certificado revogado ou suspenso até que expire.

4.9.8 Prazo máximo de publicação de CRLs

As CRLs são publicadas no Depósito em um período imediato razoável após sua geração, que em nenhum caso excede alguns minutos.

4.9.9 Disponibilidade de serviços de verificação online do estado dos certificados

esFIRMA informa sobre o estado de revogação dos certificados, por meio do protocolo OCSP, que permite conhecer o estado de validade dos certificados online nos seguintes endereços:

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

Em caso de falha dos sistemas de verificação de estado de certificados por causas fora do controle da esFIRMA, esta deverá fazer o melhor possível para garantir que este serviço permaneça inativo pelo menor tempo possível, que não poderá exceder um dia.

esFIRMA fornece informações a terceiros que confiam em certificados sobre o funcionamento do serviço de informações de estado de certificados.

Os serviços de verificação do estado dos certificados são de uso gratuito[5].

[5] Ap 6.3.10 de ETSI EN 319 411-2

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

4.9.10 Obrigação de consulta de serviços de verificação de estado de certificados

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

esFIRMA admite o método GET para OCSP.

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

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

Para conhecer o estado dos Certificados de AC subordinados, as informações fornecidas através do OCSP são atualizadas pelo menos a cada seis meses e dentro de 24 horas após a revogação de um Certificado de AC subordinada.

Se o respondedor OCSP receber uma solicitação de estado de um certificado que não foi emitido, ele retornará *revogado, certificateHold 1 de janeiro de 1970*, registrando essas solicitações como parte dos procedimentos de resposta de segurança da esFIRMA.

4.9.11 Outras formas de informação de revogação de certificados

Alternativamente, terceiros que confiam em certificados poderão verificar o estado de revogação dos certificados consultando as CRLs mais recentes emitidas pela esFIRMA. Elas estão publicadas no site da esFIRMA, bem como nos endereços da web indicados nos certificados.

esFIRMA não delega suas respostas OCSP por meio de OCSP stapling.

[6] Ap 6.3.10.b) de ETSI EN 319 411-2

4.9.12 Requisitos especiales en caso de compromiso de la clave privada

O comprometimento da chave privada do esFIRMA é notificado a todos os participantes dos serviços de certificação, na medida do possível, por meio da publicação deste fato no site do esFIRMA, bem como, se considerado necessário, em outros meios de comunicação, inclusive em papel.

4.9.13 Causas de suspensão de certificados

esFIRMA não realiza suspensão de certificados.

4.9.14 Pedido de suspensão

esFIRMA não realiza suspensão de certificados

4.9.15 Procedimentos para solicitação de suspensão

esFIRMA não realiza suspensão de certificados.

4.9.16 Período máximo de suspensão

esFIRMA não realiza suspensão de certificados.

4.10 Serviços de verificação do estado dos certificados

4.10.1 Características operacionais dos serviços

Os serviços de verificação do estado dos certificados são fornecidos por meio de uma interface de consulta web, no site https://www.esfirma.com

Também podem ser verificados através do acesso ao serviço OCSP nos endereços da web indicados na seção 4.9.9

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

Diferenças e considerações entre as consultas de estado de revogação de um certificado por meio de OCSP e CRL:

- Tanto OCSP como CRL mostram as informações mais recentes sobre o estado 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 ambos os métodos. Eventualmente, o estado de revogação de um certificado não expirado é o mesmo em consulta via OCSP e CRL.
- As CRL não incluem certificados revogados que já expiraram, enquanto que o OCSP inclui essa informação. Ao adicionar certificados expirados a uma CRL, aumenta-se o tempo necessário para verificar a validade dos certificados, já que a lista é maior e leva mais tempo para baixar e processar. Além disso, ocorre um crescimento indefinido nas CRL até o fim da validade do emissor.
- EsFIRMA emite uma Última CRL, que se refere à última CRL emitida antes de o certificado emissor das CRL deixar de ter validade por expiração, revogação ou outros casos. Esta CRL juntamente com um arquivo de assinatura LTA é utilizada para verificar se um certificado era válido ou não em um determinado momento. Se não for possível validar a Última CRL, deve-se assumir que o certificado é inválido. Uma vez verificada a Última CRL, deverá ser verificado o estado do certificado na CRL.
- OCSP requer conexão em tempo real com a autoridade de certificação para obter o status de revogação, enquanto as CRL podem ser baixadas e armazenadas localmente para uso offline.
- OCSP pode ser menos privado que as CRL, já que 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 do estado dos certificados e o serviço de carimbo de tempo estão disponíveis 24 horas por dia, 7 dias por semana, durante todo o ano, exceto por paradas programadas.

Os serviços de verificação do estado dos certificados são gratuitos.

4.10.3 Características opcionais

Não se aplica.

4.11 Finalização da subscrição

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

4.12 Depósito e recuperação de chaves

4.12.1 Política e práticas de depósito e recuperação de chaves

esFIRMA não presta serviços de depósito e recuperação de chaves.

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

Sem estipulação.

5. Controles de segurança física, de gestão e de operações

5.1 Controles de segurança física

A esFIRMA estabeleceu controles de segurança física e ambiental para proteger os recursos das instalações onde se encontram os sistemas, os próprios sistemas e os equipamentos empregados para as operações de registro e aprovação das solicitações, geração técnica dos certificados e a gestão do hardware criptográfico.

Especificamente, a política de segurança física e ambiental aplicável aos serviços de geração de certificados, dispositivos criptográficos e gestão de revogação estabeleceu prescrições para as seguintes contingências:

- Controles de acesso físico.
- Proteção contra desastres naturais.
- Medidas de proteção contra incêndios.
- Falha dos sistemas de suporte (energia eletrônica, telecomunicações, etc.)
- Derrubada da estrutura.
- Inundações.
- Proteção antirroubo.
- Saída não autorizada de equipamentos, informações, suportes e aplicativos relativos a componentes utilizados para os serviços do provedor de serviços de certificação.

Essas medidas são aplicáveis às instalações onde os certificados são produzidos sob a total responsabilidade da esFIRMA, que os fornece a partir de suas instalações de alta segurança, tanto principais como, quando necessário, de operação em contingência, que são devidamente auditadas periodicamente.

As instalações contam com sistemas de manutenção preventiva e corretiva com assistência 24h-365 dias por ano, com assistência nas 24 horas seguintes à notificação.

5.1.1 Localização e construção das instalações

A proteção física é alcançada através da criação de perímetros de segurança claramente definidos em torno dos serviços. A qualidade e solidez dos materiais de construção das instalações garantem níveis adequados de proteção contra intrusões por força bruta e estão localizadas em uma área de baixo risco de desastres e permitem acesso rápido.

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

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

esFIRMA dispõe de instalações que protegem fisicamente a prestação dos serviços de aprovação de solicitações de certificados e de gestão de revogação, do comprometimento causado por acesso não autorizado aos sistemas ou aos dados, assim como à divulgação dos mesmos

5.1.2 Acesso físico

O CPD onde está localizada a AC da esFIRMA possui a classificação TIER IV.

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

- Está limitado a pessoal expressamente autorizado, com identificação no momento do acesso e registro do mesmo, incluindo filmagem por circuito fechado de televisão e seu arquivo.

- O acesso às salas é feito com leitores de cartão de identificação.

- Para acessar o RAC onde os processos criptográficos estão localizados, é necessário a autorização prévia da esFIRMA aos administradores do serviço de hospedagem que possuem a chave para abrir a jaula.

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 gerador elétrico.

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 área de baixo risco de inundação.

As salas onde os equipamentos de informática são alojados possuem um sistema de detecção de umidade.

5.1.5 Prevenção e proteção contra incêndios

As instalações e ativos da esFIRMA contam com sistemas automáticos de detecção e extinção de incêndios.

5.1.6 Armazenamento de mídias

Apenas pessoal autorizado tem acesso aos meios de armazenamento.

A informação de classificação mais alta é armazenada em uma caixa de segurança fora das instalações do Centro de Processamento de Dados.

5.1.7 Tratamento de resíduos

A eliminação de suportes, tanto em papel como magnéticos, é realizada por mecanismos que garantam a impossibilidade de recuperação da informação.

No caso de suportes magnéticos, é realizado o formato, a exclusão permanente ou a destruição física do suporte, por meio de software especializado que realiza um mínimo de 3 passagens de exclusão e com padrões de exclusão variáveis.

No caso de documentação em papel, por meio de trituradoras ou em cestos de lixo designados para esse fim, para posterior destruição sob controle.

5.1.8 Cópia de backup fora das instalações

esFIRMA utiliza um depósito externo seguro para a guarda de documentos, dispositivos magnéticos e eletrônicos que são independentes do centro de operações.

São necessárias pelo menos duas pessoas autorizadas expressamente para acessar, depositar ou retirar dispositivos.

5.2 Controles de procedimentos

esFIRMA garante que seus sistemas operam de forma segura, para isso estabeleceu e implementou procedimentos para as funções que afetam a prestação de 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 Funções confiáveis

esFIRMA identificou, de acordo com sua política de segurança, as seguintes funções ou papéis como confiáveis:

- **Auditor Interno:** Responsável pelo cumprimento dos procedimentos operacionais. Trata-se de uma pessoa externa ao departamento de Sistemas de Informação. As tarefas de Auditor interno são incompatíveis no tempo com as tarefas de Certificação e incompatíveis com Sistemas. Essas funções estarão subordinadas à chefia de operações, reportando tanto a ela quanto à direção técnica.

- **Administrador de Sistemas**Responsável pelo correto funcionamento do hardware e software de suporte da plataforma de certificação
- **Administrador de AC**: Responsável pelas ações a serem executadas com o material criptográfico, ou com a realização de alguma função que envolva a ativação das chaves privadas das autoridades de certificação descritas neste documento, ou de qualquer um de seus elementos.
- **Operador de AC:** Responsável necessário, juntamente com o Administrador de CA, pela custódia do material de ativação das chaves criptográficas, também responsável pelas operações de cópia de backup e manutenção do AC.
- **Operador de Registro:** Pessoa responsável por aprovar as solicitações de certificação feitas pelo assinante.
- **Responsável de Segurança**Encarregado de coordenar, controlar e fazer cumprir as medidas de segurança definidas pelas políticas de segurança da esFIRMA. Deve cuidar dos aspectos relacionados à segurança da informação: lógica, física, redes, organizacional, etc.
- **Responsável de Informação e Serviço**Define os requisitos de informação e serviços em matéria de segurança. Este papel tem a responsabilidade final do uso que é feito da informação e dos serviços e, portanto, do seu nível de proteção.
- **Especialista em Validação**: Responsável pela validação das solicitações de certificados.
- **Oficial de Revogação:** Responsável pela operação de mudança de estado dos certificados.

As pessoas que ocupam os cargos anteriores estão sujeitas a procedimentos específicos de investigação e controle.

5.2.2 Número de pessoas por tarefa

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

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 o seu papel, garantindo assim que nenhuma pessoa tenha acesso a recursos não atribuídos.

O acesso aos recursos é realizado dependendo do ativo por meio de cartões criptográficos e códigos de ativação.

5.2.4 Funções que exigem separação de tarefas

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

- Emissão e revogação de certificados, e acesso ao repositório.
- Geração, emissão e revogação de certificados da Autoridade Certificadora.
- Implementação da Entidade de Certificação em produção.

5.2.5 Sistema de gestão PKI

O sistema de PKI é composto pelos seguintes módulos:

- Componente/módulo de gestão da Autoridade de Certificação Subordinada.
- Componente/módulo de gestão da Autoridade de Registro.
- Componente/módulo de gestão de solicitações.
- Componente/módulo de gestão de chaves (HSM).
- Componente/módulo de bases de dados.
- Componente/módulo de gestão de CRL.
- Componente/módulo de gestão do serviço de OCSP.
- Componente/módulo de gestão da Autoridade de Carimbo de Tempo (TSA)

5.3 Controles de pessoal

5.3.1 Requisitos de histórico, qualificações, experiência e autorização

Todo o pessoal que realiza tarefas qualificadas como confiáveis, trabalha há pelo menos um ano no centro de produção e possui contratos de trabalho fixos.

Todo o pessoal está qualificado e foi instruído adequadamente para realizar as operações que lhe foram atribuídas.

O pessoal em cargos de confiança não tem interesses pessoais que entrem em conflito com o desenvolvimento da função que lhe foi confiada.

esFIRMA garante que o pessoal de registro é confiável para realizar as tarefas de registro.

O Operador de Registro realizou um curso de preparação para a realização das tarefas de validação das solicitações.

Em geral, a esFIRMA removerá de suas funções de confiança um funcionário quando se tiver conhecimento da existência da comissão de algum fato criminoso que possa afetar o desempenho de suas funções.
esFIRMA não designará uma pessoa não apta para o cargo como responsável por um site confiável ou de gestão, especialmente se tiver sido condenada por um crime ou delito que afete sua aptidão para o cargo.

5.3.2 Procedimentos de investigação de histórico

esFIRMA realiza comprovações sobre os antecedentes dos possíveis funcionários antes de sua contratação ou de seu acesso ao cargo de trabalho.

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

A pesquisa será repetida com uma periodicidade suficiente.

Todas as verificações são realizadas até onde a legislação aplicável permitir. Os motivos que podem levar à rejeição do candidato a um cargo confiável são os seguintes:

- Falsidades na solicitação de trabalho, feitas pelo candidato.
- Referências profissionais muito negativas ou pouco confiáveis em relação ao candidato.

Na solicitação para o cargo de trabalho, é informado sobre a necessidade de se submeter a uma investigação prévia, sendo avisado que a recusa em se submeter à investigação implicará na rejeição da solicitação.

5.3.3 Requisitos de formação

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

A formação inclui, pelo menos, os seguintes conteúdos:

- Princípios e mecanismos de segurança da hierarquia de certificação, bem como o ambiente do usuário da pessoa a ser treinada.
- Tarefas que a pessoa deve realizar.
- Políticas e procedimentos de segurança da esFIRMA. Uso e operação de equipamentos e aplicativos instalados.
- Gestão e tratamento de incidentes e compromissos de segurança.
- Procedimentos de continuidade de negócio e emergência.
- Procedimento de gestão e segurança em relação ao tratamento de dados pessoais.

5.3.4 Requisitos e frequência de atualização formativa

esFIRMA atualiza a formação do pessoal de acordo com as necessidades e com frequência suficiente para desempenhar suas funções de forma competente e satisfatória, especialmente quando forem realizadas modificações substanciais nas tarefas de certificação

5.3.5 Sequência e frequência de rotação de trabalho

Não aplicável.

5.3.6 Sanções para ações não autorizadas

esFIRMA dispõe de um sistema sancionatório, para depurar as responsabilidades derivadas de ações não autorizadas, adequado à legislação laboral aplicável e, em especial, coordenado com o sistema sancionatório do convênio coletivo que resulte de aplicação ao pessoal.

As ações disciplinares incluem a suspensão e a demissão da pessoa responsável pela ação prejudicial, de forma proporcional à gravidade da ação não autorizada.

5.3.7 Requisitos de contratação de profissionais

Os funcionários contratados para realizar tarefas confiáveis assinam previamente as cláusulas de confidencialidade e os requisitos operacionais utilizados pela esFIRMA. Qualquer ação que comprometa a segurança dos processos aceitos pode, uma vez avaliada, resultar no término do contrato de trabalho.

No caso em que todos ou parte dos serviços de certificação sejam operados por terceiros, os controles e previsões realizados nesta seção, ou em outras partes do DPC, serão aplicados e cumpridos pelo terceiro que realiza as funções de operação dos serviços de certificação, no entanto, a entidade de certificação será responsável em todo caso pela efetiva execução. Esses aspectos são concretizados no instrumento jurídico utilizado para acordar a prestação dos serviços de certificação por terceiro distinto da esFIRMA.

5.3.8 Fornecimento de documentação ao pessoal

O provedor de serviços de certificação fornecerá a documentação necessária estritamente ao seu pessoal em cada momento, a fim de realizar seu trabalho de forma competente e satisfatória.

5.4 Procedimentos de auditoria de segurança

5.4.1 Tipos de eventos registrados

esFIRMA produz e armazena registro, pelo menos, dos seguintes eventos relacionados à segurança da entidade:

- Ligar e desligar o sistema.
- Tentativas de criação, exclusão, estabelecimento de senhas ou mudança de privilégios.
- Intentos de início e fim de sessão.
- Tentativas de acesso não autorizado ao sistema da AC através da rede.
- Tentativas de acesso não autorizado ao sistema de arquivos.
- Acesso físico aos logs.
- Alterações na configuração e manutenção do sistema.
- Registros das aplicações da AC.
- Ligar e desligar a aplicação da AC.
- Alterações nos detalhes da AC e/ou suas chaves.
- Alterações na criação de políticas de certificados.
- Geração de chaves próprias.
- Criação e revogação de certificados.
- Registros da destruição dos meios que contêm as chaves, dados de ativação.
- Eventos relacionados com o ciclo de vida do módulo criptográfico, como receção, uso e desinstalação do mesmo.
- As atividades dos firewalls e roteadores[7]
- A cerimônia de geração de chaves e os bancos de dados de gerenciamento de chaves.
- Registros de acesso físico.
- Mantenimentos e mudanças de configuração do sistema.
- Alterações no pessoal.
- Informes de compromissos e discrepâncias.
- Registros da destruição de material que contenha informações de chaves, dados de ativação ou informações pessoais do assinante, no caso de certificados individuais, ou da pessoa física identificada no certificado, no caso de certificados de organização.
- Posse de dados de ativação, para operações com a chave privada da Entidade de Certificação.

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

- Relatórios completos das tentativas de intrusão física nas infraestruturas que dão suporte à emissão e gestão de certificados.

As entradas do registro incluem os seguintes elementos:

- Data e hora da entrada.
- Número de série ou sequência da entrada, nos registros automáticos.
- Identidade da entidade que entra no registro.
- Tipo de entrada.

Todos os eventos relacionados à preparação dos dispositivos qualificados de criação de assinaturas usados pelos signatários ou guardiões são registrados[8].

5.4.2 Frequência de tratamento de registros de auditoria

esFIRMA revisa seus logs quando ocorre um alerta do sistema motivado pela existência de algum incidente.

O processamento dos registros de auditoria envolve uma revisão dos registros que inclui a verificação de que eles não foram manipulados, uma breve inspeção de todas as entradas do registro e uma investigação mais profunda de qualquer alerta ou irregularidade nos registros. As ações realizadas a partir da revisão de auditoria são documentadas.

esFIRMA mantém um sistema que permite garantir:

- Espaço suficiente para armazenamento de logs
- Que os arquivos de logs não sejam reescritos.
- Que a informação armazenada inclui no mínimo: 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 em um banco de dados para posterior exploração.

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

5.4.3 Período de conservação de registros de auditoria

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

esFIRMA coloca esses registros de auditoria à disposição do seu Auditor Qualificado, mediante solicitação.

5.4.4 Proteção dos registros de auditoria

Os logs dos sistemas:

- Estão protegidos contra manipulação, exclusão ou remoção[9] através da assinatura dos arquivos que os contêm.
- São armazenados em dispositivos à prova de fogo.
- Protege-se a disponibilidade armazenando-a em instalações externas ao centro onde a AC está localizada.

O acesso aos arquivos de logs é reservado apenas para pessoas autorizadas. Além disso, os dispositivos são manuseados em todos os momentos por pessoal autorizado.
Existe um procedimento interno onde são detalhados os processos de gestão dos dispositivos que contêm dados de logs de auditoria.

5.4.5 Procedimentos de cópia de backup

esFIRMA dispõe de um procedimento adequado de backup, de modo que, em caso de perda ou destruição de arquivos relevantes, as correspondentes cópias de backup dos logs estejam disponíveis em um curto período de tempo.

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

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

5.4.6 Localização do sistema de armazenamento de registros de auditoria

As informações de auditoria de eventos são coletadas internamente e de forma automatizada pelo sistema operacional, comunicações de rede e pelo software de gerenciamento de certificados, além dos dados gerados manualmente, que serão armazenados pelo pessoal devidamente autorizado. Tudo isso compõe o sistema de registro de auditoria.

5.4.7 Notificação do evento de auditoria ao causador do evento

Quando o sistema de registro de auditoria registra um evento, não é necessário enviar uma notificação ao indivíduo, organização, dispositivo ou aplicação que causou o evento.

5.4.8 Análise de vulnerabilidades

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

As análises de vulnerabilidade devem ser executadas, revisadas e avaliadas 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 anual de riscos.

5.5. Arquivos de informações

esFIRMA, garante que todas as informações relativas aos certificados são mantidas por um período de tempo apropriado, conforme estabelecido na seção 5.5.2 desta política.

5.5.1 Tipos de registros arquivados

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

- 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
- Solicitações de emissão e revogação de certificados, incluindo todos os relatórios relacionados ao processo de revogação[10].
- Todas as eleições específicas que o signatário ou o assinante disponha durante o acordo de assinatura[11].
- Tipo de documento apresentado na solicitação do certificado.
- Identidade da Entidade de Registro que aceita a solicitação de certificado.
- Número de identificação único fornecido pelo documento anterior.
- Todos os certificados emitidos ou publicados.
- CRLs emitidas ou registros do estado dos certificados gerados.
- O histórico de chaves geradas.
- As comunicações entre os elementos da PKI.
- Políticas e Práticas de Certificação
- Todos os dados de auditoria identificados na seção 5.4
- Informação de solicitações de certificação.
- Documentação fornecida para justificar as solicitações de certificação.
- Informação do ciclo de vida do certificado.

esFIRMA é responsável pelo correto arquivo de todo este material.

5.5.2 Período de conservação de registros

esFIRMA arquiva os registros especificados anteriormente por pelo menos 15 anos.

5.5.3 Proteção do arquivo

esFIRMA protege o arquivo de forma que apenas pessoas devidamente autorizadas possam obter acesso ao mesmo. O arquivo é protegido contra visualização, modificação,

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

[11] Ap 6.4.5.c) iv) de ETSI EN 319 411-1

exclusão ou qualquer outra manipulação mediante o seu armazenamento em um sistema confiável.

esFIRMA assegura a correta proteção dos arquivos por meio da designação de pessoal qualificado para seu tratamento e armazenamento em caixas de segurança à prova de fogo e instalações externas.

5.5.4 Procedimentos de cópia de backup

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

esFIRMA, no mínimo, realiza cópias de backup incrementais diárias de todos os seus documentos eletrônicos e realiza cópias de backup completas semanalmente para casos de recuperação de dados.

Além disso, a esFIRMA (ou as organizações que realizam a função de registro) mantêm uma cópia dos documentos em papel em um local seguro diferente das instalações da própria Entidade de Certificação.

5.5.5 Requisitos de selagem de data e hora

Os registros são datados com uma fonte confiável via NTP.

esFIRMA dispõe de um procedimento onde descreve a configuração de tempos dos equipamentos utilizados na emissão de certificados.
O horário utilizado para registrar os eventos do registro de auditoria deve ser sincronizado com o UTC, pelo menos, uma vez por dia[12].

Não é necessário que esta informação esteja assinada digitalmente.

[12] Ap 7.10.d) de la ETSI EN 319 401

5.5.6 Localização do sistema de arquivos

A esFIRMA dispõe de um sistema centralizado de coleta de informações sobre a atividade dos equipamentos envolvidos no serviço de gerenciamento de certificados.

5.5.7 Procedimentos de obtenção e verificação de informações de arquivo

O esFIRMA possui um procedimento que descreve o processo para verificar se as informações arquivadas estão corretas e acessíveis.

5.6 Renovação de chaves

Antes que o uso da chave privada do AC/SUBCA/TSA expire, uma troca de chaves será realizada. O antigo AC/SUBCA e sua chave privada serão usados apenas para assinar CRLs enquanto houver certificados ativos emitidos por esse AC/SUBCA. Será gerado um novo AC/SUBCA/TSA com uma nova chave privada e um novo DN. A chave privada do TSA será destruída.

A mudança de chaves do assinante é realizada através da realização de um novo processo de emissão.

5.7 Compromisso de chaves e recuperação de desastres

5.7.1 Procedimentos de gestão de incidentes e compromissos

São armazenadas cópias de segurança das seguintes informações em instalações de armazenamento externo à esFIRMA, que são disponibilizadas em caso de comprometimento ou desastre: dados técnicos de solicitação de certificados, dados de auditoria e registros de banco de dados de todos os certificados emitidos.

As cópias de segurança das chaves privadas do esFIRMA são geradas e mantidas de acordo com o estabelecido na seção 6.2.4

5.7.2 Corrupção de recursos, aplicativos ou dados

Quando ocorrer um evento de corrupção de recursos, aplicativos ou dados, o incidente será comunicado à segurança e os procedimentos de gerenciamento apropriados serão iniciados, que incluem escalonamento, investigação e resposta ao incidente. Se necessário, os procedimentos de comprometimento de chaves ou recuperação de desastres do esFIRMA serão iniciados.

5.7.3 Compromisso da chave privada da entidade

Em caso de suspeita ou conhecimento do comprometimento do esFIRMA, os procedimentos de comprometimento de chaves serão ativados, liderados por uma equipe de resposta que avaliará a situação, desenvolverá um plano de ação, que será executado sob a aprovação da direção da Entidade de Certificação.

Em caso de comprometimento da chave privada de esFIRMA, pode ocorrer que os estados dos certificados e dos processos de revogação usando essa chave não sejam válidos[13]. Em qualquer caso, todos os certificados ativos serão revogados, gerando posteriormente uma última CRL na qual serão incluídos todos os certificados revogados, estejam ou não expirados. As instruções para a validação de um certificado ou carimbo do tempo serão publicadas no site da esFIRMA.

esFIRMA desenvolveu um Plano de contingência para recuperar os sistemas críticos, se necessário, em um centro de dados alternativo.

O caso de comprometimento da chave raiz deve ser tratado como um caso separado no processo de contingência e continuidade de negócios. Esse incidente afeta, no caso de substituição das chaves, o reconhecimento por diferentes aplicativos e serviços privados e públicos. A recuperação da efetividade 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, mas não seu reconhecimento por terceiros.

13 Ap 6.4.8.g) ii) de ETSI EN 319 411-1

Qualquer falha na realização dos objetivos estabelecidos por este Plano de contingência será tratada como razoavelmente inevitável, a menos que essa falha seja devido a uma violação das obrigações do AC para implementar esses processos.

5.7.4 Continuidade dos negócios após um desastre

esFIRMA restabelecerá os serviços críticos (suspensão e revogação, e publicação de informações de estado de certificados) de acordo com o Plano de Continuidade de Negócios existente.
A esFIRMA possui um centro alternativo, se necessário, para colocar em operação os sistemas de certificação descritos no plano de continuidade de negócios.

Tanto o serviço de gestão de revogações quanto o serviço de consulta são considerados serviços críticos e constam no Plano de Continuidade de Negócios da esFIRMA.

5.8 Terminação do serviço

esFIRMA assegura que as possíveis interrupções para os assinantes e terceiros são mínimas como resultado da cessação dos serviços do prestador de serviços de certificação e, em particular, garantem a manutenção contínua dos registros necessários para fornecer evidências de certificação em caso de investigação civil ou criminal.

Antes de terminar seus serviços, a esFIRMA desenvolve um Plano de término, com as seguintes disposições:

- Fornecerá os fundos necessários para continuar a conclusão das atividades de revogação.
- Comunicará ao Ministério de Assuntos Econômicos e Transformação Digital, com uma antecedência mínima de 2 meses, o encerramento de sua atividade e o destino dos certificados, especificando se a gestão será transferida e para quem, ou se a vigência será extinta.
- Também comunicará ao Ministério de Assuntos Econômicos e Transformação Digital a abertura de qualquer processo concursal que seja iniciado contra a esFIRMA, bem como qualquer outra circunstância relevante que possa impedir a continuação da atividade.

- Informará a todos os Signatários/Assinantes, Terceiros que confiam e outras AC's com as quais tenha acordos ou outro tipo de relação sobre a cessação com uma antecedência mínima de 6 meses.
- Transferirá a gestão dos certificados válidos para terceiros provedores sempre que haja consentimento dos titulares ou, caso contrário, procederá à extinção da sua validade (contido nos pontos b) e c) da comunicação do ponto 1.1).
- Transferirá as obrigações da ESFIRMA ao novo provedor que será responsável: pela gestão dos certificados, manutenção das informações de registro de dados e manutenção do estado do processo de revogação e dos arquivos de registro de eventos durante seus respectivos períodos de tempo, indicados aos assinantes, usuários e partes que confiam nos certificados.
- Serão informadas as características do novo provedor para o qual a ESFIRMA transfere a gestão dos certificados.
- Revogará todas as autorizações concedidas a entidades subcontratadas para atuar em nome da AC no processo de emissão de certificados.
- As chaves privadas da AC serão destruídas ou desabilitadas para uso.
- Os certificados das Unidades de Carimbo de Tempo (TSU) serão revogados.
- Todos os certificados ativos e o sistema de verificação e revogação serão mantidos até a extinção de todos os certificados emitidos durante 15 anos. Para isso, será emitida uma última CRL que incluirá todos os certificados revogados, expirados ou não, estabelecendo os meios necessários para garantir sua conservação a longo prazo.

6. Controles de segurança técnica

6.1 Geração e instalação do par de chaves

6.1.1 Geração do par de chaves

O par de chaves da entidade de certificação intermediária "ESFIRMA AC AAPP 2" é criado pela entidade de certificação raiz "ESFIRMA AC RAIZ 2" de acordo com os procedimentos de cerimônia da esFIRMA, dentro do perímetro de alta segurança destinado a essa tarefa.

As atividades realizadas durante a cerimônia de geração de chaves foram registradas, datadas e assinadas por todos os indivíduos participantes, na presença de um Auditor CISA. Esses registros são mantidos para fins de auditoria e monitoramento por um período apropriado determinado pela esFIRMA.

Para a geração da chave das entidades de certificação raiz e intermediária, são utilizados dispositivos com as certificações Common Criteria EAL 4+ ou FIPS 140-2 Nível 3.

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

Mais informações nos seguintes locais dos PDS:

CERTIFICADO	PDS
De Funcionário Público (ASSINATURA)	Español: https://esfirma.com/doc-pki/PDS-V2.0/PDS-AAPP-ES.pdf Inglês:

CERTIFICADO	PDS
	https://esfirma.com/doc-pki/PDS-V2.0/PDS-AAPP-EN.pdf
De Empleado Público - Nível Alto 1.3.6.1.4.1.47281.1.1.1	
De Empleado Público – Nivel Medio 1.3.6.1.4.1.47281.1.1.4	
De Funcionário Público (AUTENTICAÇÃO)	
De Empleado Público - Nível Alto 1.3.6.1.4.1.47281.1.1.5	
De Funcionário Público com Pseudônimo (ASSINATURA)	
De EP com Pseudônimo - Nível Alto 1.3.6.1.4.1.47281.1.3.1	
De EP com Pseudônimo - Nível Médio 1.3.6.1.4.1.47281.1.3.4	
De Funcionário Público com Pseudônimo (AUTENTICAÇÃO)	
De Empleado Público com Seudónimo – 1.3.6.1.4.1.47281.1.3.5	
De Selo de Órgão	
De Sello de Órgano – Nível Médio 1.3.6.1.4.1.47281.1.2.2	
De Selo de Órgão - Nível Médio centralizado *1.3.6.1.4.1.47281.1.2.4*	
De Pessoa Física vinculada a entidade (ASSINATURA)	Español: https://esfirma.com/doc-pki/PDS-V2.0/PDS-PFV-ES.pdf Inglês: https://esfirma.com/doc-pki/PDS-V2.0/PDS-PFV-EN.pdf
De PF vinculada a entidad – F. Cualificada 1.3.6.1.4.1.47281.1.6.1	
De PF vinculada a entidad – F. Centralizada 1.3.6.1.4.1.47281.1.6.4	
De Pessoa Física vinculada a entidade (AUTENTICAÇÃO)	
De PF vinculada a entidad	

CERTIFICADO	PDS
1.3.6.1.4.1.47281.1.6.5	
De Pessoa Física com pseudônimo vinculada a entidade (FIRMA)	
De PF con seudónimo vinculada a entidad – Firma Cualificada 1.3.6.1.4.1.47281.1.7.1	
De PF con seudónimo vinculada a entidad – Firma Centralizada 1.3.6.1.4.1.47281.1.7.4	
De Pessoa Física com pseudônimo, vinculada a entidade (AUTENTICAÇÃO)	
De PF com pseudônimo, vinculada a entidade 1.3.6.1.4.1.47281.1.7.5	
De Selo Eletrônico	
De Selo Eletrônico em software 1.3.6.1.4.1.47281.1.8.2	
De Selo eletrônico centralizado 1.3.6.1.4.1.47281.1.8.4	
De Selo Eletrônico para TSA/TSU	Español: https://esfirma.com/doc-pki/PDS-V1.5/TSADS-ES.pdf Inglês: https://esfirma.com/doc-pki/PDS-V1.5/TSADS-EN.pdf
De Sello-e para TSA/TSU em HSM 1.3.6.1.4.1.47281.1.5.2	

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

Nos certificados gerados em HSM ou software, o assinante autoriza o signatário ou criador de selos a gerar suas chaves privada e pública, e solicita, em nome do signatário ou criador de selos, a emissão do certificado para esFIRMA.

esFIRMA nunca gera chaves em software para serem enviadas por canais inseguros ao signatário.

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

6.1.2 Envio da chave privada ao signatário

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

Em certificados de software, a chave privada do signatário é criada no sistema de computador que o signatário usa ao solicitar o certificado, portanto, a chave privada é devidamente protegida dentro do sistema de computador do signatário.

6.1.3 Envio da chave pública ao emissor do certificado

O método de envio da chave pública ao 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, a esFIRMA garante que a chave pública enviada ao provedor de serviços de certificação vem de um par de chaves gerado por esse DCCF[14].

6.1.4 Distribuição da chave pública do provedor de serviços de certificação

As chaves do esFIRMA são comunicadas a terceiros que confiam em certificados, garantindo a integridade da chave e autenticando sua origem, por meio de sua publicação no Depósito.

Os usuários podem acessar o Depósito 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 dessa forma.

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

O certificado das AC raiz e subordinadas estarão disponíveis para os usuários na página da Web da esFIRMA.

6.1.5 Tamanhos de chaves

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

6.1.6 Geração de parâmetros de chave pública e verificação de qualidade

A chave pública da CA Root, da CA subordinada e dos certificados dos assinantes são codificados de acordo com o RFC 5280.

Qualidade dos parâmetros de chave pública

- Comprimento do Módulo = 4096
- Algoritmo de geração de chaves: rsagen1
- Funções criptográficas de resumo: SHA256.

Todas as chaves são geradas em equipamentos seguros, de acordo com o indicado na seção 6.1.1.

6.1.7 Propósitos de uso de chaves

Os usos das chaves para os certificados das AC são exclusivamente para a assinatura de certificados e CRLs.

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

6.2 Proteção da chave privada e controles dos módulos criptográficos

6.2.1 Padrões de módulos criptográficos

Em relação aos módulos que gerenciam as chaves do esFIRMA e dos assinantes de certificados de assinatura eletrônica, o nível exigido pelos padrões indicados nas seções anteriores é garantido.

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

É necessário um controle multi-pessoa para ativar a chave privada da AC. No caso desta DPC, há uma política específica **3 de 5** pessoas para a ativação das chaves.

Os dispositivos criptográficos são fisicamente protegidos conforme determinado neste documento.

6.2.3 Depósito da chave privada

esFIRMA não armazena cópias das chaves privadas dos signatários.

6.2.4 Cópia de backup da chave privada

esFIRMA realiza cópia de backup das chaves privadas das ACs que permitem sua recuperação em caso de desastre, perda ou deterioração das mesmas. Tanto a geração da cópia quanto a recuperação dela exigem pelo menos a participação de duas pessoas.

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

As chaves do signatário em hardware não podem ser copiadas, pois não podem sair do dispositivo criptográfico.

6.2.5 Arquivo da chave privada

As chaves privadas das AC 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. Será necessário pelo menos a colaboração de duas pessoas para recuperar a chave privada dos ACs no dispositivo criptográfico inicial.

6.2.6 Introdução da chave privada no módulo criptográfico

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

6.2.7 Armazenamento das chaves privadas nos módulos criptográficos

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

6.2.8 Método de ativação da chave privada

A chave privada do esFIRMA é ativada através da execução do correspondente procedimento de inicialização segura do módulo criptográfico, pelas pessoas indicadas na seção 6.2.2.

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

A ativação das chaves privadas da AC Intermediária é gerenciada com o mesmo processo de m de n que as chaves da AC.

6.2.9 Método de desativação da chave privada

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

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

6.2.10 Método de destruição da chave privada

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

Os dispositivos que armazenam qualquer parte das chaves privadas do esFIRMA serão fisicamente destruídos ou reiniciados em um nível inferior. Para a eliminação, os passos descritos no manual do administrador do equipamento criptográfico serão seguidos.

Finalmente, as cópias de segurança serão destruídas de forma segura.

As chaves do signatário em software podem ser destruídas através da sua exclusão, seguindo as instruções da aplicação que as contém.

As chaves do assinante em hardware podem ser destruídas por meio de um aplicativo de computador especial nas dependências das RAs ou da esFIRMA.

6.2.11 Classificação do módulo criptográfico

Os módulos criptográficos são submetidos aos controles de engenharia previstos nas normas indicadas ao longo desta seção.

Os algoritmos de geração de chaves utilizados são comumente aceitos para o uso da chave a que se destinam.

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

6.3 Outros aspectos de gestão do par de chaves

6.3.1 Arquivo da chave pública

A esFIRMA arquiva suas chaves públicas de forma rotineira, de acordo com o estabelecido na seção 5.5 deste documento.

6.3.2 Períodos de utilização de chaves pública e privada

Os períodos de utilização das chaves são determinados pela duração do certificado, após o qual não podem mais ser utilizados.

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 o estabelecido na seção 6.2.2 e os procedimentos de cerimônia de chaves.

A criação e distribuição desses dispositivos são registradas.

Além disso, esFIRMA gera de forma segura os dados de ativação.

6.4.2 Proteção de dados de ativação

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

O signatário do certificado é responsável pela proteção de sua chave privada, com uma senha o mais completa possível. O signatário deve lembrar dessa senha.

6.4.3 Outros aspectos dos dados de ativação

Não se aplica.

6.5. Controles de segurança da informática

A esFIRMA utiliza sistemas confiáveis para oferecer seus serviços de certificação. A esFIRMA realizou controles e auditorias de computação para estabelecer uma gestão adequada de seus ativos de informática com o nível de segurança exigido na gestão de sistemas de certificação eletrônica.

Os equipamentos utilizados são inicialmente configurados com os perfis de segurança adequados pela equipe de sistemas da esFIRMA, nos seguintes aspectos:

- Configuração de segurança do sistema operacional.
- Configuração de segurança de aplicativos.
- Dimensionamento correto do sistema.
- Configuração de usuários e permissões.
- Configuração de eventos de Log.
- Plano de backup e recuperação.
- Configuração do antivírus.
- Requisitos de tráfego de rede.

6.5.1 Requisitos técnicos específicos de segurança cibernética

Cada servidor de esFIRMA inclui as seguintes funcionalidades:

- Controle de acesso aos serviços da SubCA e gestão de privilégios.
- Imposição de separação de tarefas para a gestão de privilégios.
- Identificação e autenticação de funções associadas a identidades.
- Arquivo de histórico do assinante e da SubCA e dados de auditoria.
- Auditoria de eventos relativos a segurança.
- Auto-diagnóstico de segurança relacionado com os serviços da SubCA.
- Mecanismos de recuperação de chaves e do sistema da SubCA.

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

No caso em que a esFIRMA distribua dispositivos qualificados de criação de assinatura, verificará a todo momento que esses dispositivos continuam certificados como DCCF[15].

A verificação da certificação do DCCF é realizada durante todo o período de validade do certificado[16]. Se o DCCF perder sua certificação como tal, a esFIRMA procederá com a revogação dos certificados emitidos nesses DCCF, informando aos titulares dos mesmos.

[15] Ap 6.5.1.a) de ETSI 319 411-2

[16] Ap 6.5.1.c) de ETSI EN 319 411-2

esFIRMA exige autenticação com múltiplos fatores para todas as contas capazes de causar diretamente a emissão de certificados.

6.5.2 Avaliação do nível de segurança cibernética

As aplicações de autoridade de certificação e de registro utilizadas pela esFIRMA são confiáveis.

6.6 Controles técnicos do ciclo de vida

6.6.1 Controles de desenvolvimento de sistemas

As aplicações são desenvolvidas e implementadas pela esFIRMA de acordo com padrões de desenvolvimento e controle de mudanças.

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

6.6.2 Controles de gestión de segurança

esFIRMA desenvolve as atividades necessárias para a formação e conscientização dos funcionários em segurança. Os materiais utilizados para a formação e os documentos descritivos dos processos são atualizados após a aprovação por um grupo de gestão de segurança. Para realizar essa função, ele tem um plano de treinamento anual.

esFIRMA exige, mediante contrato, as medidas de segurança equivalentes a qualquer fornecedor externo envolvido nas tarefas de certificação.

Classificação e gestão de informações e bens

esFIRMA mantém um inventário de ativos e documentação e um procedimento para a gestão deste material para garantir seu uso.

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

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

Operações de gestão

A esFIRMA dispõe de um procedimento adequado de gestão e resposta a incidentes, por meio da implementação de um sistema de alertas e da geração de relatórios periódicos.

esFIRMA tem documentado todo o procedimento relativo às funções e responsabilidades do pessoal envolvido no controle e manipulação de elementos contidos no processo de certificação.

Tratamento dos suportes e segurança

Todos os suportes são tratados de forma segura de acordo com os requisitos de classificação da informação. Os suportes que contenham dados sensíveis são destruídos de forma segura se não forem mais necessários.

Planificação do sistema

O departamento de Sistemas da esFIRMA mantém um registro das capacidades dos equipamentos. Juntamente com a aplicação de controle de recursos de cada sistema, é possível prever uma possível redimensionamento.

Reporte de incidentes e resposta

esFIRMA dispõe de um procedimento para o acompanhamento de incidentes e sua resolução.

Procedimentos operacionais e responsabilidades

esFIRMA define atividades, atribuídas a pessoas com um papel de confiança, diferentes das pessoas encarregadas de realizar as operações diárias que não têm caráter de confidencialidade.

Gestão do sistema de acesso

esFIRMA realiza todos os esforços que razoavelmente estão ao seu alcance para confirmar que o sistema de acesso está limitado às pessoas autorizadas.

Em particular:

AC General

- Existem controles baseados em firewalls, antivírus e IDS em alta disponibilidade disponíveis.
- Os dados sensíveis são protegidos por meio de técnicas criptográficas ou controles de acesso com identificação forte.
- A esFIRMA dispõe de um procedimento documentado para gerenciamento de admissões e demissões de usuários e política de acesso detalhada em sua política de segurança.
- esFIRMA dispõe de procedimentos para garantir que as operações são realizadas respeitando a política de funções.
- Cada pessoa tem associada uma função para realizar as operações de certificação.
- A equipe da esFIRMA é responsável por suas ações através do compromisso de confidencialidade assinado com a empresa.

Geração do certificado

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

Gestão da revogação

A revogação será realizada por meio de autenticação forte às aplicações de um administrador autorizado. Os sistemas de logs gerarão as provas que garantem a não repudiação da ação realizada pelo administrador de esFIRMA.

Estado da revogação

A aplicação do estado de revogação possui um controle de acesso baseado em autenticação com certificados ou autenticação de duplo fator para evitar tentativas de modificação das informações do estado de revogação.

6.6.3 Avaliação da segurança do ciclo de vida

esFIRMA assegura que o hardware criptográfico usado para a assinatura de certificados não é manipulado durante o transporte, através da inspeção do material entregue.

O hardware criptográfico é transportado em suportes preparados para evitar qualquer manipulação.

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

O uso de hardware criptográfico para assinatura de certificados requer o envolvimento de pelo menos dois funcionários de confiança.

esFIRMA realiza testes de provas periódicas para garantir o correto funcionamento do dispositivo.

O dispositivo de hardware criptográfico é manipulado apenas por pessoal confiável.
A chave privada de assinatura da esFIRMA armazenada no hardware criptográfico será eliminada assim que o dispositivo for removido.

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

A esFIRMA possui um contrato de manutenção do dispositivo. As alterações ou atualizações são autorizadas pelo responsável pela segurança e são refletidas nas atas de trabalho correspondentes. Essas configurações serão realizadas por pelo menos duas pessoas confiáveis.

6.7 Controles de segurança de rede

esFIRMA protege o acesso físico aos dispositivos de gestão de rede e possui uma arquitetura que ordena o tráfego gerado com base em suas características de segurança, criando seções de rede claramente definidas. Essa divisão é realizada por meio do uso de firewalls.

A informação confidencial que é transferida por redes não seguras é criptografada usando protocolos SSL ou o sistema VPN com autenticação de duplo fator.

6.8 Fontes de Tempo

esFIRMA tem um procedimento de sincronização de tempo coordenado via NTP. O valor de tempo no TSU é rastreável até um valor de tempo distribuído por uma laboratório UTC(k), o ROA (Real Observatório da Armada) e mantém a precisão de relógio com pelo menos quatro fontes de tempo STRATUM-1.

6.9 Algoritmos de assinatura e parâmetros do sistema de assinatura centralizada

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) em Real Random Mode (hardware noise) segundo NIST SP 800-90A e teste contínuo de acordo com 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 do HSM utiliza o algoritmo ECDSA NIST-P256/secp256r1 (OID 1.2.840.10045.3.1.7) e requer 3 de 5 cartões para sua ativação e que foi gerada em uma cerimônia de inicialização de alta segurança. O PIN do usuário é derivado de um salt do servidor com o algoritmo PBKDF2-SHA1. O transporte do SAD (Signature Activation Data) do SIC (Signature Interaction Component) ao SAM (Signature Activation Module) é protegido por meio de AES-GCM com chave de 256 bits derivada de uma troca de chaves pelo algoritmo ECDH segundo NIST SP 800-56A. A chave do servidor está publicada no repositório web de esFirma, seção "Informação de segurança da

assinatura remota". O sistema permite gerar 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 certificados, CRL e OCSP

7.1 Perfil de certificado

Todos os certificados qualificados emitidos sob esta política cumprem o padrão X.509 versão 3, RFC 5280, RFC 3739 e as normas ETSI seguintes:

- ETSI EN 319 412-2 para certificados emitidos a pessoas físicas
- ETSI EN 319 412-3 para certificados emitidos a pessoas jurídicas
- ETSI EN 319 412-5 para a definição dos QCStatements dos certificados qualificados de acordo com o RD (EU) 910/2014.

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

7.1.1 Número de versão

esFIRMA emite certificados X.509 Versão 3

7.1.2 Extensões do certificado

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

7.1.3 Identificadores de objeto (OID) dos algoritmos

O identificador do objeto do algoritmo de assinatura é:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption
- 1.2.840.10045.4.3.2 sha256WithECDSA

O identificador do objeto do algoritmo de chave pública é:

- 1.2.840.113549.1.1.1 rsaEncryption
- 1.2.840.10045.3.1.7 NIST-P256/secp256r1
-

7.1.4 Formato de Nomes

Os certificados devem conter as informações necessárias para o seu uso, conforme determinado pela política correspondente.

A codificação do certificado segue a recomendação RFC 5280 "Certificado de infraestrutura de chave pública da Internet X.509 e Lista de revogação de certificados (CRL)
Ver perfis em https://www.esfirma.com

7.1.5 Restrição dos nomes

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

7.1.6 Identificador de objeto (OID) dos tipos de certificados

Todos os certificados incluem um identificador de política de certificados sob a qual foram emitidos, de acordo com a estrutura indicada no ponto 1.2.1

7.1.7 Uso da extensão de restrições de política

Não aplicável

7.1.8 Qualificadores de sintaxe e semântica de política

Não aplicável

7.1.9 Semântica de processamento para a extensão crítica de Políticas de certificado

A extensão "Certificate Policy" identifica a política que define as práticas que a esFIRMA associa explicitamente com o certificado. A extensão pode conter um qualificador de política. Ver 7.1.6

7.1.10 Restrições de comprimento dos elementos

Para todos os perfis, são estabelecidas as seguintes restrições de comprimento máximo em caracteres dos seguintes elementos:

Elemento	**Comprimento Máximo esFIRMA**	**Comprimento Base**	**Norma**
2.5.4.42 *(givenName,GN)*	**127**	32000***	RFC5280
2.5.4.10 (organizationName)	**256**	64	RFC5280
2.5.4.11 (organizationalUnitName)	**256**	32	RFC5280
2.5.4.4 (sobrenomes)	**256**	40	RFC5280
2.5.4.3 (commonName, CN)	**400**	64	RFC5280
2.5.4.5 (serialNumber,SN)	32*	32	RFC5280
2.5.4.97 (organizationIdentifier)	**32**	MAX**	X520
2.5.4.65 (pseudônimo)	**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 na RFC 5280 (desde que indicado na DPC) para os campos do subject indicados de acordo com o tipo de certificado (givenName, surname, pseudonym, commonName, organizationName e organizationalUnitName), mas não o restante dos campos. O comprimento destes campos é de acordo com a RFC 5280.
** MAX indica que o limite superior não está especificado (RFC5280 Apêndice B. Notas ASN1)
*** 32000 ub-name usado em vez de ub-givenname (16)

Os comprimentos máximos para o resto dos elementos estão especificados em RFC-5280

7.2 Perfil da lista de revogação de certificados

De acordo com o padrão IETF RFC 3280

7.2.1 Número de versão

As CRL emitidas pela esFIRMA são da versão 2.

7.2.2 CRL e extensões CRL

crlExtensions:

2.5.29.35 (Identificador de chave de autoridade)

2.5.29.20 (Número de CRL)

crlEntryExtensions

2.5.29.21 (ReasonCode)

7.3 Perfil OCSP

De acordo com o padrão IETF RFC 6960

7.3.1 Número de versão

Os OCSP emitidos pela esFIRMA são da versão 3.

7.3.2 Extensões OCSP

responseExtensions

Id: 1.3.6.1.5.5.7.48.1.2 (Extensão Nonce OCSP)

Critical: verdadeiro

8. Auditoria de conformidade

A esFIRMA comunicou o início de sua atividade como prestadora de serviços de certificação pelo Ministério de Assuntos Econômicos e Transformação Digital e está sujeita às revisões de controle que este organismo considere necessárias.

8.1 Frequência da auditoria de conformidade

A esFIRMA realiza uma auditoria de conformidade anualmente, além das auditorias internas que realiza sob seu próprio critério ou a qualquer momento, devido a uma suspeita de não conformidade com alguma medida de segurança.

esFIRMA supervisiona o cumprimento deste documento e controla estritamente a qualidade do seu serviço, realizando autoauditorias pelo menos trimestralmente em uma amostra selecionada aleatoriamente do maior de um certificado ou pelo menos três por cento dos certificados emitidos por ele durante o período que começa imediatamente após a autoauditoria anterior.

8.2 Identificação e qualificação do auditor

As auditorias são realizadas por uma empresa de auditoria externa independente que demonstra competência técnica e experiência em segurança da informação, 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 reconhecidas pelo seu prestígio com departamentos especializados na realização de auditorias informáticas, portanto, não há nenhum conflito de interesse que possa distorcer sua atuação em relação à esFIRMA.

8.4 Lista de elementos sujeitos a auditoria

A auditoria verifica em relação à esFIRMA:

a) Que a entidade possui um sistema de gestão que garante a qualidade do serviço prestado.
b) Que a entidade cumpre com os requisitos da DPC e outra documentação relacionada à emissão dos diferentes certificados digitais.
c) Que a DPC e demais documentação jurídica relacionada estão em conformidade com o acordado pela esFIRMA e com o estabelecido na regulamentação atual.
d) Que a entidade gerencia adequadamente seus sistemas de informação

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

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

8.5 Ações a serem tomadas como resultado de uma falta de conformidade

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

Se a esFIRMA for incapaz de desenvolver e/ou executar tal plano ou se as deficiências encontradas representarem uma ameaça imediata para a segurança ou integridade do sistema, deverá comunicá-lo imediatamente à alta direção da esFIRMA, que poderá executar as seguintes ações:

- Suspender temporariamente as operações.
- Revogar a chave da AC e regenerar a infraestrutura.
- Encerrar o serviço da AC.
- Outras ações complementares que sejam necessárias.

8.6 Tratamento dos relatórios de auditoria

Os relatórios de resultados da auditoria são entregues à alta direção da esFIRMA no prazo máximo de 15 dias após a realização da auditoria.

9. Requisitos comerciais e legais

9.1 Tarifas

9.1.1 Tarifa de emissão ou renovação de certificados

esFIRMA pode estabelecer uma taxa pela emissão dos certificados, da qual, se for o caso, os assinantes serão informados oportunamente.

9.1.2 Taxa de acesso a certificados

esFIRMA não estabeleceu nenhuma taxa pelo acesso aos certificados.

9.1.3 Taxa de acesso à informação do estado do certificado

esFIRMA não estabeleceu nenhuma taxa pelo acesso à informação do estado dos certificados.

9.1.4 Tarifas de outros serviços

Sem estipulação.

9.1.5 Política de reembolso

Sem estipulação.

9.2 Responsabilidade financeira

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

9.2.1 Cobertura de seguro

esFIRMA dispõe de uma garantia de cobertura de responsabilidade civil suficiente, através de um seguro de responsabilidade civil profissional que cumpre com o indicado no regime de obrigações e responsabilidades do Regulamento (UE) 910/2014, e com o artigo 9.3.b) da Lei 6/2020, de 11 de novembro, reguladora de determinados aspectos dos serviços eletrônicos de confiança, com um mínimo segurado de 3.000.000 de euros.

9.2.2 Outros ativos

Sem estipulação.

9.2.3 Cobertura de seguro para subscritores e terceiros que confiam em certificados

esFIRMA dispõe de uma garantia de cobertura de sua responsabilidade civil suficiente, por meio de um seguro de responsabilidade civil profissional que cumpre com o indicado no regime de obrigações e responsabilidades do Regulamento (UE) 910/2014, e com o artigo 9.3.b) da Lei 6/2020, de 11 de novembro, reguladora de determinados aspectos dos serviços eletrônicos de confiança com um mínimo segurado de 3.000.000 de euros.

9.3 Confidencialidade da informação

9.3.1 Informações confidenciais

As seguintes informações são mantidas confidenciais pela esFIRMA:

- Pedidos de certificados, aprovados ou negados, bem como qualquer outra informação pessoal obtida para a emissão e manutenção de certificados, exceto as informações indicadas na seção seguinte.
- Chaves privadas geradas e/ou armazenadas pelo provedor de serviços de certificação.
- Registros de transações, incluindo registros completos e registros de auditoria das transações.
- Registos de auditoria interna e externa, criados e/ou mantidos pela Entidade de Certificação e seus auditores.
- Planos de continuidade de negócio e de emergência.
- Política e planos de segurança.

- Documentação de operações e outros planos de operação, como arquivamento, monitoramento e similares.
- Toda outra informação identificada como "Confidencial".

9.3.2 Informações não confidenciais

A seguinte informação é considerada não confidencial:

- Os certificados emitidos ou em processo de emissão.
- A vinculação do assinante a um certificado emitido pela Autoridade de Certificação.
- O nome e sobrenome da pessoa física identificada no certificado, bem como qualquer outra circunstância ou dado pessoal do titular, no caso de ser significativo em função da finalidade do certificado.
- O endereço de e-mail da pessoa física identificada no certificado, ou o endereço de e-mail atribuído pelo assinante, no caso em que seja significativo em função da finalidade do certificado.
- Os usos e limites econômicos mencionados no certificado.
- O período de validade do certificado, bem como a data de emissão do certificado e a data de expiração.
- O número de série do certificado.
- Os diferentes estados ou situações do certificado e a data de início de cada um deles, em particular: pendente de geração e/ou entrega, válido, revogado, suspenso ou expirado e o motivo que causou a mudança de estado.
- As listas de revogação de certificados (CRLs), bem como as demais informações de estado de revogação.
- Qualquer outra informação que não esteja indicada na seção anterior.

9.3.3 Divulgação de informações de suspensão e revogação

Veja a seção anterior.

9.3.4 Divulgação legal de informações

esFIRMA divulga a informação confidencial apenas nos casos legalmente previstos.

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

esFIRMA indicará essas circunstâncias na política de privacidade prevista na seção 9.4.

9.3.5 Divulgação de informações mediante solicitação do titular

esFIRMA inclui, na política de privacidade prevista na seção 9.4, prescrições para permitir a divulgação das informações do assinante e, se for o caso, da pessoa física identificada no certificado, diretamente a eles ou a terceiros.

9.3.6 Outras circunstâncias de divulgação de informação

Sem estipulação.

9.4 Privacidade das informações pessoais

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

esFIRMA obtém os dados pessoais que constam nos arquivos por meio da captura de dados pelo ASSINANTE, que deve tê-los obtido legalmente de quem corresponda, nas condições previstas na regulamentação sobre assinatura eletrônica e proteção de dados pessoais.

[17] Apartado 7.10.c) de la ETSI EN 319 401

esFIRMA tem a condição de encarregado do tratamento de dados pessoais e, como tal, trata os dados única e exclusivamente para os fins que constam nesta Declaração de Práticas de Certificação de acordo com as instruções do responsável pelo tratamento, 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 qualidade de ENCARRAGADO DO TRATAMENTO*, que rege o contrato de prestação de serviços "Gestiona" entre o ASSINANTE e ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.

9.4.1 Plano de privacidade

A esFIRMA desenvolveu uma política de privacidade de acordo com o REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE, e com a Lei Orgânica 3/2018, de 5 de dezembro, de Proteção de Dados Pessoais e garantia dos direitos digitais, e documentou isso 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 qualidade de ENCARGADO DEL TRATAMIENTO"* que regula o contrato de prestação de serviços "Gestiona" entre o ASSINANTE e a ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A., os aspectos, procedimentos e medidas de segurança e organizacionais em conformidade com o regime de obrigações e responsabilidades contidas nas normas anteriores.

9.4.2 Informação tratada como privada

As informações pessoais sobre um indivíduo que não estão publicamente disponíveis em O conteúdo de um certificado ou CRL é considerado privado.

9.4.3 Informação não considerada privada

As informações pessoais sobre um indivíduo disponíveis nos conteúdos de um certificado ou CRL são consideradas não privadas, uma vez que são necessárias para a prestação do serviço contratado, sem prejuízo dos direitos correspondentes ao titular dos dados pessoais em virtude da legislação LOPD/RGPD.

9.4.4 Responsabilidade de proteger a informação privada

As informações confidenciais, de acordo com a regulamentação de proteção de dados pessoais, são protegidas contra perda, destruição, dano, falsificação e processamento ilícito ou não autorizado, de acordo com as prescrições estabelecidas neste documento, que estão alinhadas 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 físicas 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, de Proteção de Dados Pessoais e garantia dos direitos digitais.

9.4.5 Aviso e consentimento para uso de informações privadas

Antes de estabelecer uma relação contratual, os interessados serão oferecidos a Informações prévias sobre o tratamento de seus dados pessoais e o exercício de direitos serão fornecidas e, se necessário, será obtido o consentimento obrigatório para o tratamento diferenciado do tratamento principal para a prestação dos serviços contratados.

9.4.6 Divulgação em conformidade com um processo judicial ou administrativo

esFIRMA não divulga nem cede dados pessoais, exceto nos casos previstos nas seções 9.3.2 a 9.3.6, e na seção 5.8, em caso de término do serviço de certificação.

9.4.7 Outras circunstâncias de divulgação de informação

Não são cedidos dados pessoais a terceiros, exceto por obrigação legal.

9.5 Direitos de propriedade intelectual

9.5.1 Propriedade dos certificados e informações de revogação

Apenas a esFIRMA possui direitos de propriedade intelectual sobre os certificados que emite, sem prejuízo dos direitos dos subscritores, detentores de chaves e terceiros, aos quais concede uma licença não exclusiva para reproduzir e distribuir certificados, sem custo algum, desde que a reprodução seja completa e não altere nenhum elemento do

certificado, e seja necessária em relação a assinaturas digitais e/ou sistemas de criptografia dentro do âmbito de uso do certificado, e de acordo com a documentação que os vincula.

Adicionalmente, os certificados emitidos por esFIRMA contêm um aviso legal relativo à propriedade dos mesmos.

As mesmas regras se aplicam ao uso das informações de revogação dos certificados.

9.5.2 Propriedade da Declaração de Práticas de Certificação

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

9.5.3 Propriedade da informação relativa a nomes

O subscritor e, se for o caso, a pessoa física identificada no certificado, mantém todos os direitos, se existirem, sobre a marca, produto ou nome comercial contido no certificado.

O assinante é o proprietário do nome distintivo do certificado, formado pelas informações especificadas na seção 3.1.1

9.5.4 Propriedade de chaves

Os pares de chaves são propriedade dos signatários dos certificados.

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

9.6 Obrigações e responsabilidade civil

9.6.1 Obrigações da Entidade de Certificação "esFIRMA

esFIRMA garante, sob sua total responsabilidade, que cumpre com todos os requisitos estabelecidos na DPC, sendo o único responsável pelo cumprimento dos procedimentos

descritos, mesmo que uma parte ou a totalidade das operações sejam subcontratadas externamente.

esFIRMA presta os 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 assinante sobre os termos e condições relativos ao uso do certificado, seu preço e suas limitações de uso, por meio de um contrato de assinante que incorpora por referência os textos de divulgação (PDS) de cada um dos certificados adquiridos.

O documento de divulgação de texto, também conhecido como PDS, atende ao conteúdo do anexo A do ETSI EN 319 411-1 v1.1.1 (2016-02), que pode ser transmitido eletronicamente, usando um meio de comunicação durável no tempo e em linguagem compreensível.
esFIRMA comunica de forma permanente los cambios[18] produzir novas versões da sua documentação jurídica no seu site https://www.esfirma.com, como parte das suas obrigações

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

- Prescrições para cumprir o estabelecido nas seções 4.5.3, 9.2, 9.6.7, 9.6.8, 9.6.9 e 9.6.10.
- Indicação da política aplicável, com indicação de que os certificados não são emitidos ao público.
- Declaração de que as informações contidas no certificado estão corretas, exceto notificação em contrário pelo assinante.
- Consentimento para o armazenamento das informações utilizadas para o registro do assinante e para a transferência dessas informações a terceiros, no caso de encerramento das operações da Entidade de Certificação sem revogação de certificados válidos.

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

- Limites de uso do certificado, incluindo aqueles estabelecidos na seção 1.4.2
- Informações sobre como validar um certificado, incluindo o requisito de verificar o estado do certificado e as condições em que se pode confiar razoavelmente no certificado, que se aplica quando o assinante age como terceiro que confia no certificado.
- Forma como é garantida a responsabilidade patrimonial da Entidade de Certificação.
- Limitações de responsabilidade aplicáveis, incluindo os usos pelos quais a Entidade de Certificação aceita ou exclui sua responsabilidade.
- Período de arquivo de informação de solicitação de certificados.
- Período de arquivo de registros de auditoria.
- Procedimentos aplicáveis de resolução de disputas.
- Lei aplicável e jurisdição competente.
- Se a Entidade de Certificação foi declarada conforme com a política de certificação e, se for o caso, de acordo com qual sistema.

9.6.2. Obrigação e responsabilidade da RA

As AR são as entidades delegadas pela AC para realizar as tarefas de registro e aprovação de solicitações de certificados, portanto, a AR também é obrigada nos termos definidos nas Práticas de Certificação para a emissão de certificados, principalmente:

• Respeitar o disposto nesta CPS e nas correspondentes PDS.

• Proteger suas chaves privadas que serão usadas para o exercício de suas funções.

• Verificar a identidade dos Sujeitos/Assinantes e Solicitantes dos certificados quando necessário, comprovando definitivamente a identidade do Assinante, no caso de certificados individuais, ou do detentor das chaves, no caso de certificados de organização, de acordo com o estabelecido nas seções correspondentes deste documento.

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

• Fornecer ao Signatário, no caso de certificados individuais, ou ao futuro detentor de chaves, no caso de certificados de organização, acesso ao certificado.

• Entregar, se aplicável, o dispositivo criptográfico correspondente.

• Arquivar, pelo período estabelecido na legislação em vigor, os documentos fornecidos pelo solicitante ou signatário.

• Respeitar o disposto nos contratos assinados com a esFIRMA e com o Sujeito/Signatário.

• Informar a esFIRMA das causas de revogação, sempre que tomarem conhecimento.
• Fornecer informações básicas sobre a política e uso do certificado, incluindo especialmente informação sobre esFIRMA e a Declaração de Práticas de Certificação aplicável, assim como suas obrigações, faculdades e responsabilidades.
• Fornecer informações sobre o certificado e o dispositivo criptográfico.
• Coletar informações e evidências do titular do certificado e, se for o caso, do dispositivo criptográfico, e aceitação desses elementos.
• Informar sobre o método de atribuição exclusiva ao detentor da chave privada e seus dados de ativação do certificado e, se aplicável, do dispositivo criptográfico, de acordo com o estabelecido nas seções correspondentes deste documento.
Essas obrigações se aplicam mesmo nos casos de entidades delegadas por elas, como os pontos de verificação presencial (PVP).
As informações sobre o uso e responsabilidades do assinante são fornecidas através da aceitação das cláusulas de uso antes da confirmação do pedido do certificado e por meio de correio eletrônico.

As RA assinam um contrato de prestação de serviços com a esFIRMA, através do qual a esFIRMA delega as funções de registro nas RA, consistindo fundamentalmente em:
1.- Obrigações prévias à emissão de um certificado.
a) Informar adequadamente os solicitantes sobre a assinatura de suas obrigações e responsabilidades.
b) A adequada identificação dos solicitantes, que devem ser pessoas capacitadas ou autorizadas a solicitar um certificado digital.
c) A correta verificação da validade e vigência desses dados dos solicitantes e da Entidade, no caso de existir uma relação de vinculação ou representação.
d) Aceder à aplicação de Autoridade de Registro para gerenciar as solicitações e os certificados emitidos.
2.- Obrigações após a emissão do certificado.
a) Assinar os contratos de Prestação de Serviços de Certificação Digital com os solicitantes. Na maioria dos processos de emissão, este contrato é formalizado mediante a aceitação de condições nas páginas web que fazem parte do processo de emissão do certificado, não sendo possível realizar a emissão sem antes ter aceitado as condições de uso.
b) A manutenção dos certificados durante sua vigência (extinção, suspensão, revogação).

c) Arquivar as cópias da documentação apresentada e os contratos devidamente assinados pelos solicitantes em conformidade com as Políticas de Certificação publicadas pela esFIRMA e a legislação vigente.

Assim, as RA são responsáveis pelas consequências em caso de não cumprimento de suas funções de registro, e através das quais se comprometem a respeitar também as normas reguladoras internas da entidade certificadora esFIRMA (Políticas e CPS), que devem ser perfeitamente controladas pelas RA e que devem servir como manual de referência para elas.

Em caso de reclamação por um Sujeito, uma Entidade ou um usuário, a AC deverá fornecer a

Se for comprovado que a origem da reclamação se deve a um erro na validação ou verificação dos dados, a AC poderá, com base nos acordos assinados com as RA, fazer com que a RA responsável assuma as consequências, como prova de diligência.

Porque, embora legalmente a AC seja a pessoa jurídica responsável perante o Sujeito, uma Entidade ou Parte Usuária, e que para isso disponha de um seguro de responsabilidade civil, de acordo com o acordo em vigor, a RA tem como obrigação contratual "identificar e autenticar corretamente o Solicitante e, se for o caso, a Entidade correspondente", e, portanto, deverá responder perante a esFIRMA por seus descumprimentos.

Claro, não é intenção da esFIRMA transferir toda a responsabilidade para as RA em relação aos possíveis danos cuja origem seria o descumprimento das tarefas delegadas às RA. Por esta razão, assim como previsto para a AC, a RA está sujeita a um regime de controle que será exercido pela esFIRMA, não apenas por meio de controles de arquivos e procedimentos de conservação de arquivos assumidos pela RA, por meio da realização de auditorias para avaliar, entre outros, os recursos utilizados e o conhecimento e controle dos procedimentos operacionais para oferecer serviços de RA.

As RA deverão assumir as mesmas responsabilidades em caso de violações das mesmas entidades delegadas como por exemplo os pontos de verificação presencial (PVP), sem prejuízo do seu direito de repercutir contra elas.

9.6.3 Garantias oferecidas a assinantes e terceiros que confiam em certificados

esFIRMA, na documentação que a vincula com assinantes e terceiros que confiam em certificados, estabelece e rejeita garantias e limitações de responsabilidade aplicáveis.

esFIRMA, como mínimo, garante ao subscritor:

- Que não há erros de fato nas informações contidas nos certificados, conhecidos ou realizados pela Entidade de Certificação.
- Que não há erros de fato nas informações contidas nos certificados, devido à falta de diligência adequada na gestão do pedido de certificado ou na sua criação.
- Que os certificados atendem a todos os requisitos materiais estabelecidos na Declaração de Práticas de Certificação.
- Que os serviços de revogação e o uso do Depósito cumprem com todos os requisitos materiais estabelecidos na Declaração de Práticas de Certificação.

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

- Que a informação contida ou incorporada por referência no certificado está correta, exceto quando indicado o contrário.
- Que na aprovação do pedido de certificado e na emissão do certificado foram cumpridos todos os requisitos materiais estabelecidos na Declaração de Práticas de Certificação.
- A rapidez e segurança na prestação de serviços, especialmente nos serviços de revogação.

Adicionalmente, esFIRMA garantiza ao assinante e ao terceiro que confia no certificado:

- Que o certificado contém as informações que devem estar contidas em um certificado qualificado, de acordo com o anexo 1 do Regulamento (UE) 910/2014.
- Que, no caso em que as chaves privadas do assinante ou, se for o caso, da pessoa física identificada no certificado, sejam geradas, sua confidencialidade é mantida durante o processo.
- A responsabilidade da Entidade de Certificação, dentro dos limites estabelecidos. Em nenhum caso a ESFIRMA será responsável por caso fortuito e em caso de força maior.
- A chave privada da entidade de certificação utilizada para emitir certificados não foi comprometida, a menos que a esFIRMA tenha comunicado o contrário.
- Não originou nem introduziu declarações falsas ou incorretas nas informações de nenhum certificado, nem deixou de incluir informações necessárias

fornecidas pelo assinante e validadas pela esFIRMA, no momento da emissão do certificado.

- Todos os certificados cumprem os requisitos formais e de conteúdo desta Declaração de Práticas, incluindo todos os requisitos legais em vigor e aplicáveis.
- Fica vinculado pelos procedimentos operacionais e de segurança descritos nesta Declaração de Práticas.

9.6.4 Obrigação e responsabilidade de terceiros

Será obrigação da Parte Usuária cumprir com o disposto na normativa vigente e, além disso:

- Verificar a validade dos certificados e de toda a cadeia de certificação antes de realizar qualquer operação baseada nos mesmos. O esFIRMA possui vários mecanismos para realizar essa verificação, como o acesso a listas de certificados revogados ou a serviços de consulta online OCSP.
- Conhecer e sujeitar-se às garantias, limites e responsabilidades aplicáveis na aceitação e uso dos certificados em que confia, e aceitar sujeitar-se às mesmas.
- 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 Obrigação e responsabilidade de outros participantes

Não estipulado

9.7. Exclusão de garantia

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

- Não ter fornecido informações adequadas, iniciais ou posteriores como

- consequência de modificações das circunstâncias refletidas no certificado eletrônico, quando sua imprecisão não pôde ser detectada pelo provedor de serviços de certificação
- Ter incorrido em negligência em relação à conservação dos dados de criação de assinatura e sua confidencialidade.
- Não ter solicitado a revogação dos dados do certificado eletrônico em caso de dúvida sobre a manutenção da confidencialidade
- Ter usado a assinatura digital após o período de validade do certificado eletrônico ter expirado
- Ultrapassar os limites indicados no certificado eletrônico.
- Em comportamentos imputáveis ao Usuário, se este agir de forma negligente, ou seja, quando não verificar ou levar em conta as restrições que constam no certificado quanto aos seus possíveis usos e limite de valor das transações; ou quando não levar em conta o estado de validade do certificado
- Dos danos causados ao sujeito ou a terceiros que confiam na inexatidão dos dados contidos no certificado eletrônico, se estes foram comprovados por meio de documento público, registrado em um registro público, se exigido.
- Um uso inadequado ou fraudulento do certificado no caso em que o Sujeito/Titular o tenha cedido ou autorizado seu uso em favor de terceiros em virtude de um negócio jurídico, como mandato ou representação, sendo exclusiva responsabilidade do Sujeito/Titular o controle das chaves associadas ao seu certificado.

esFIRMA e suas RAs também não serão responsáveis em nenhum caso quando se encontrarem diante de qualquer uma dessas circunstâncias:

- Estado de Guerra, desastres naturais ou qualquer outro caso de Força Maior.
- Pelo uso dos certificados desde que exceda o disposto na regulamentação em vigor e nas Políticas de Certificação
- Pelo uso indevido ou fraudulento dos certificados ou CRLs emitidos pela AC
- Pelo uso da informação contida no Certificado ou no CRL.
- Pelo prejuízo causado durante o período de verificação das causas de revogação.
- Pelo conteúdo das mensagens ou documentos assinados ou criptografados digitalmente.
- Pela falta de recuperação de documentos criptografados com a chave pública do Sujeito.

9.8. Limitação de responsabilidade em caso de perdas por transações

O limite máximo permitido pelo esFIRMA em transações econômicas é de 0 (zero) euros.

9.9. Indenizações

Ver seção 9.2

9.10. Prazo e Finalização

9.10.1 Prazo

Ver seção 5.8

9.10.2 Terminação

Ver seção 5.8

9.10.3 Efeito da rescisão e sobrevivência

Ver seção 5.8

9.11. Notificações individuais e comunicação com os participantes

Qualquer notificação referente a esta CPS será feita por e-mail ou
por correio certificado dirigido a qualquer um dos endereços mencionados na seção dados de contato 1.5.2.

9.12. Emendas

9.12.1 Procedimento de modificação

A AC reserva-se o direito de modificar este documento por razões técnicas ou para refletir qualquer mudança nos procedimentos que tenham ocorrido devido a requisitos legais, regulatórios (eIDAS, órgãos de supervisão nacionais, etc.) ou como resultado da otimização do ciclo de trabalho. Cada nova versão desta CPS substitui todas as versões anteriores, que continuam, no entanto, aplicáveis aos certificados emitidos enquanto essas versões estavam em vigor e até a primeira data de vencimento desses certificados. Será publicada pelo menos uma atualização anual. Essas atualizações serão refletidas na tabela de versões no início do documento.

As alterações que podem ser feitas nesta CPS não exigem notificação, exceto se afetarem diretamente os direitos dos Sujeitos/Signatários dos certificados, caso em que poderão apresentar seus comentários à organização de administração de políticas dentro de 15 dias após a publicação.

9.12.2 Mecanismo de notificação y plazos

Todas as mudanças propostas nesta política serão imediatamente publicadas no site da esFIRMA. Neste mesmo documento, há uma seção de mudanças e versões onde é possível conhecer as mudanças ocorridas desde a sua criação e a data dessas modificações.

As alterações deste documento são comunicadas às autoridades e empresas terceiras que emitem certificados sob esta CPS, bem como aos auditores correspondentes. As alterações nesta CPS serão especialmente notificadas às autoridades de Supervisão Nacional.

Os Signatários/Subscritores e Terceiros afetados que confiam podem apresentar seus comentários à organização de administração de políticas dentro de 15 dias após o recebimento da notificação.

9.12.3 Circunstâncias em que o OID deve ser alterado

Não estipulado

9.13 Procedimento de resolução de conflitos

esFIRMA estabelece, no contrato de assinante, e no texto de divulgação ou PDS, os procedimentos de mediação e resolução de conflitos aplicáveis.

9.14. Legislação aplicável

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

9.15. Conformidade com a Lei Aplicável

Ver ponto 9.14

9.16. Outras disposições

9.16.1 Acordo completo

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

9.16.2 Atribuição

As partes desta DPC não podem ceder nenhum dos seus direitos ou obrigações sob ela ou acordos aplicáveis sem o consentimento por escrito da esFIRMA.

9.16.3 Separabilidade

esFIRMA estabelece, no contrato de assinante, e no texto de divulgação ou PDS, cláusulas de divisibilidade, sobrevivência, acordo integral e notificação:

- Em virtude da cláusula de divisibilidade, a invalidade de uma cláusula não afetará o restante do contrato.
- Em virtude da cláusula de sobrevivência, certas regras continuarão em vigor após a finalização da relação jurídica reguladora do serviço entre as partes. Para esse fim, a Entidade de Certificação garante que, pelo menos, os requisitos contidos nas seções 9.6.1 (Obrigações e responsabilidades), 8 (Auditoria de conformidade) e 9.3 (Confidencialidade) permaneçam em vigor após a rescisão do serviço e das condições gerais de emissão / uso.
- Em virtude da cláusula de acordo completo, entender-se-á que o documento jurídico regulador do serviço contém a vontade completa e todos os acordos entre as partes.

- Em virtude da cláusula de notificação, será estabelecido o procedimento pelo qual as partes notificam mutuamente os fatos.

9.16.4 Cumprimento (honorários advocatícios e isenção de taxas)

esFIRMA pode solicitar uma indemnização e honorários de advogados de uma parte por danos, perdas e despesas relacionadas com a conduta da referida parte. O fato de que esFIRMA não fazer cumprir uma disposição desta CPS não elimina o direito de esFIRMA de fazer cumprir as mesmas disposições posteriormente ou o direito de fazer cumprir qualquer outra disposição desta CPS. Para ser efetiva, qualquer renúncia deve estar por escrito e assinada por esFIRMA

9.16.5 Força maior

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

9.17 Outras disposições

9.17.1 Cláusula de indemnidad de suscriptor

esFIRMA inclui no contrato com o assinante uma cláusula pela qual o assinante se compromete a manter a Entidade de Certificação livre de qualquer dano decorrente de qualquer ação ou omissão que resulte em responsabilidade, dano ou perda, despesa de qualquer tipo, incluindo as judiciais e de representação legal em que possa incorrer, pela publicação e uso do certificado, quando ocorrer uma das seguintes causas:

- Falsidade ou declaração incorreta feita pelo usuário do certificado.
- Erro do usuário do certificado ao fornecer os dados da solicitação, se houve dolo ou negligência na ação ou omissão em relação à Entidade de Certificação ou a qualquer pessoa que confie no certificado.
- Negligência na proteção da chave privada, no uso de um sistema confiável ou na manutenção das precauções necessárias para evitar a comprometimento, perda, divulgação, modificação ou uso não autorizado dessa chave.
- Emprego pelo assinante de um nome (incluindo nomes comuns, endereço de e-mail e nomes de domínio), ou outras informações no certificado, que violem os direitos de propriedade intelectual ou industrial de terceiros.

9.17.2 Cláusula de indenização de terceiro que confia no certificado

esFIRMA inclui no texto de divulgação ou PDS, uma cláusula pela qual o terceiro que confia no certificado se compromete a manter a Entidade de Certificação livre de qualquer dano decorrente de qualquer ação ou omissão que resulte em responsabilidade, dano ou perda, despesa de qualquer tipo, incluindo as judiciais e de representação legal em que possa incorrer, pela publicação e uso do certificado, quando ocorrer alguma das seguintes causas:

- Incumprimento das obrigações do terceiro que confia no certificado.
- Confiança temerária em um certificado, de acordo com as circunstâncias.
- Falta de verificação do estado de um certificado, para determinar se ele não está suspenso ou revogado.

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

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

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