Declaração de Práticas de Certificação

esFIRMA

Informação Geral

Controlo de documentos

Classificação de Segurança:	Público
Autor:	ESFIRMA
Versão:	1.20

Estatuto formal

Preparado por:	Revisto por:	Aprovado por:
Gabinete de Segurança Data: 02/05/2026	Gestor de Segurança Data: 02/05/2026	Comité de Segurança Data: 02/05/2026

Controlo de Versões

Ver	Descrição da mudança	Data
1.0	Criação de documentos	29/04/2016
1.1	Correções	02/06/2016
1.2	Análise do ETSI	19/05/2017
1.3	Revisão dos tipos de certificados	
1.4	Revisar Tipos de Certificados, Acrónimos e Definições	02/06/2017
1.5	Ajustes de referências regulamentares, mudança de nome, alteração de certificados 1.3.2, 1.3.3.1, 1.3.3.2, 1.4.1.8, 3.1.1.8, 4.3.1, 6.1.5, 9.2.1, 9.4, 9.6.2, 9.6.4	06/11/2017
1.6	6.1.1 Duração da TSA	20/06/2018
1.7	Correção relativamente à assinatura na emissão de certificados de software	08/08/2018
1.8	Adaptação devido a alterações regulamentares (Regulamento (UE) 910/2014 e Regulamento (UE) 2016/679) e revisão das secções de renovação.	13/11/2018
1.9	3.1.1.1 Esclarecimento sobre o segundo apelido opcional. 3.1.1.2 IdentificadorOrganizacional condicionado às Diretrizes do Fórum CA/Browser 3.1.1.4 Ajuste por Erros Tipográficos nas Descrições OID 3.1.1.7 CN do certificado opcional de VE do quartel-general	14/06/2019
1.10	Esclarecimentos diversos 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 RFC 3647 1.5.3. transferido para 1.5.2 Dados de Contacto da Organização 1.5.2 mudou para 1.5.3 Organização aprovando o documento "ACRÓNIMOS DEFINIÇÕES" passou para 1.6 Acrónimos e definições 4.4.2 Transferido para 4.4.1 Conduta que constitui aceitação do certificado 4.4.3 Mudança para 4.4.2 Publicação de Certificados 4.4.4 Avançado para 4.4.3 Notificação de Emissão a Terceiros Adicionado 4.6.1 Circunstâncias para Renovação de Certificado Adicionado 4.6.2 Quem pode pedir a renovação Adicionada a 4.6.3 Processamento de Pedidos de Renovação de Certificados Adicionada a 4.6.4 Notificação de Reemissão do Certificado ao Assinante Adendo 4.6.5 Conduta que constitui aceitação de um certificado de renovação Adicionado 4.6.6 Publicação do certificado de renovação pela CA Adicionada a 4.6.7 Notificação da emissão do certificado pela CA a outras entidades Adição do Procedimento 4.7.2 com nova identificação 4.7. Transferido para 4.7.3 Processamento de novos pedidos de chave de certificado 4.7.3 mudou para 4.7.4 Notificação da emissão do certificado renovado 4.7.4 Transferido para 4.7.5 Conduta que constitui aceitação do certificado 4.7.5 Transferido para 4.7.6 Publicação de Certificados 4.7.6 mudou para 4.7.7 Notificação da emissão a terceiros 4.11 mudou para 4.10 Certificado de Serviços de Verificação de Saúde 4.11.1 Transferido para 4.10.1 Características operacionais dos serviços 4.11.2 transferido para 4.10.2 Disponibilidade de serviços Adicionou as Funcionalidades Opcionais 4.10.3 A 4.10 foi transferida para a 4.11 Terminação da Subscrição 6.1.9 mudou para 6.1.7 Finalidades de utilização de chaves 6.2.9 Transferido para 6.2.9 Método de Desativação de Chave Privada 6.2.10 Transferido para 6.2.10 Método de Destruição de Chave Privada Adicionada 6.2.11 Classificação de Módulos Criptográficos Adicionado 6.4.3 Outros aspetos dos dados de ativação	08/06/2020

	6.6.2.5 Transferido para 6.6.3 Avaliação de Segurança ao Longo do Ciclo de Vida 6.9 mudou para 6.8 Fontes de Tempo Adicionada a 7.1.7 Usando a Extensão de Restrições de Política Adicionado 7.1.8 Qualificadores de Política, Sintaxe e Semântica Adicionada a 7.1.9 Semântica de Processamento para Extensão Crítica das Políticas de Certificados Adicionadas as extensões CRL 7.2.2 e CRL Número de Versão 7.3.1 Adicionado Adicionadas as extensões OCSP 7.3.2 Adição do Plano de Privacidade 9.4.1 Adicionada a 9.4.2 Informação tratada como privada Adicionada a 9.4.3 Informação Não Considerada Privada Adicionada a 9.4.4 Responsabilidade de Proteger a Informação Privada Adicionado 9.4.5 Aviso e Consentimento para Uso de Informação Privada Adicionado 9.4.6 Divulgação ao abrigo de processos judiciais ou administrativos Adicionado 9.4.7 Outras Circunstâncias de Divulgação de Informação Adicionadas representações e garantias de RA 9.6.2 9.6.2 Passou para 9.6.3 Garantias oferecidas a subscritores e terceiros com base em certificados Acrescentou 9.6.4 Obrigação e Responsabilidade de Terceiros 9.6.2 mudou para 9.6.5 Obrigação e Responsabilidade dos Outros Participantes 9.6.3 movido para 9.7 Aviso legal 9.6.4 mudou para 9.8 Limitação de responsabilidade em caso de perdas de transação 9.6.5 mudou para 9.9 Indemnizações Adicionei 9,10. Prazo e Conclusão Mandato Adicionado 9.10.1 Adicionado 9.10.2 Conclusão Adicionado 9.10.3 Efeito de Terminação e Sobrevivência Adicionada 9.11 Notificações individuais e comunicação com os participantes Modificações adicionadas na 9.12 Procedimento de Alteração Adicionado 9.12.1 Adicionado 9.12.2 Mecanismo de notificação e prazos Adicionado 9.12.3 Circunstâncias em que o OID deve ser alterado 9.6.10 transferido para 9.13 Procedimento de Resolução de Litígios 9.6.7 transferido para 9.14 Legislação aplicável Adicionado 9.15 Conformidade com a Lei Aplicável Adicionado 9.16 Outras disposições Adicionado 9.16.1 Acordo Completo Atribuição adicionada a 9.16.2 9.6. mudou para 9.16.3 Separabilidade Adicionado 9.16.4 Conformidade (honorários de advogados e isenção de dever) 9.6.6 Transferido para 9.16.5 Força Maior Adicionado 9.17 Outras disposições Estão incluídos novos certificados: certificado de funcionário público (Autenticação), certificado de funcionário público com pseudónimo (Autenticação), certificado de pessoa física ligada à entidade (Autenticação), certificado de pessoa física ligada à entidade (FIRMA), certificado de pessoa física com pseudónimo ligado à entidade (Autenticação), certificado de pessoa física com pseudónimo ligado à entidade (FIRMA)	
1.11	Estão incluídos novos certificados eletrónicos qualificados O perfil do certificado do e-Office é eliminado. Adaptação devido a alterações regulamentares (Lei 6/2020, de 11 de novembro, que regula certos aspetos dos serviços eletrónicos de trust).	03/05/2021

	A Secção 5.8 Cessação do Serviço DPC acrescenta detalhes sobre como a informação de estado dos certificados é fornecida para além da sua vigência. As referências ao Ministério da Indústria, Energia e Turismo são atualizadas pelo Ministério dos Assuntos Económicos e Transformação Digital.	
1.12	O Ponto 5.2.1 é alterado alterando o nome de "Administrador do Registo" para "Operador do Registo". As referências ao fórum CA/B são removidas.	10/05/2021
1.13	Ponto de Modificação 5.8 Rescisão de Serviço, de acordo com o Plano de Rescisão A Secção 4.9.1 é alterada para incluir o fim da certificação QSCD Modificação ponto 6.5.1, incluindo o fim da certificação DCCF. Remoção da referência ao documento de segurança da esFIRMA da secção 6.6.2 (Operações de gestão) Substituindo "política de segurança" por "sistema de gestão de segurança da informação" na secção 6.6.2 (Classificação e gestão de informação e propriedade) A Secção 6.9 é adicionada em conformidade com o 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. O sistema de integração com o DIR3 é adicionado como forma de verificar a identidade da entidade (3.2.2) A verificação do estado dos certificados na cadeia de certificação é adicionada na secção 4.9.6.	18/07/2022
1.14	Novas Informações sobre o Certificado TSA	16/03/2023
1.15	Configurações, informações sobre a TSA e incorporação de carimbo temporal não qualificado	31/03/2023
1.16	Novas Restrições de Comprimento dos Elementos do Perfil do Certificado Novos subperfis europeus para Pessoas Naturais e Selo Eletrónico Simplificação das secções 3.2.2 e 3.2.3 A Secção 4.5.3 é acrescentada para separar a informação e as obrigações de terceiros que dependem de certificados. Diferenças e Considerações Entre Consultas de Estado de Revogação de Certificados que Utilizam OCSP e CRL 4.10.1	21/04/2023
1.17	A possibilidade de transferir a gestão dos certificados emitidos para outro prestador em caso de cessação do serviço é eliminada na secção 5.8.	10/02/2024
1.18	O tempo máximo está incluído entre a validação de identidade e a emissão do certificado (secção 3.2.3.2) Um processo excecional está incluído no caso de não conseguir confirmar o pedido de revogação em menos de 24 horas (secção 4.9.5) Nova secção 1.4.3. Emissão de certificados de teste	26/07/2024
1.19	Revisão da secção 9.11	17/03/2025
1.20	Modificação das secções 5.8 e 9.11. O FIPS 140-3 Nível 3 é adicionado pela TSA. Alteração ao ponto 5.8 Cessação do Serviço, em conformidade com o Plano de Cessação	02/05/2026

Índice

1. Introdução....16
1.1 Apresentação....16
1.2 Nome e identificação do documento....17
1.2.1 Identificadores de Certificados....17
1.3 Participantes nos serviços de certificação....19
1.3.1. Prestador de serviços de certificação....19
Raiz enFIRMA AC 2....19
SIGNATURE AC AAPP 2....20
Plataforma de Administração Eletrónica....20
1.3.2 Autoridades de Registo....20
1.3.3 Entidades Finais....21
1.3.4 Partidos Utilizadores....21
1.3.5 Outros participantes....22
Signatários....22
1.4 Utilização de certificados....23
1.4.1 Utilizações Permitidas para Certificados....23
Certificado de Funcionário Público de Alto Nível no Cartão....23
Certificado de Funcionário Público ao nível intermédio na HSM....25
Certificado de Funcionário Público de Alto Nível no cartão para autenticação....27
Certificado de Selo de Órgão de nível médio em software....28
Certificado de Selo de Órgão ao nível intermédio em HSM....29
Certificado de Funcionário Público com Pseudónimo de Alto Nível no Cartão....30
Certificado de Funcionário Público com pseudónimo de nível intermédio, na HSM....32
Certificado de Funcionário Público com pseudónimo, nível superior no cartão para autenticação....34

Certificado de Selo Eletrónico Qualificado pela TSA/TSU 35
Certificado de Selo Eletrónico TSA/TSU 37
Certificado de pessoa física ligada, no cartão para assinatura 38
Certificado de uma pessoa física ligada, centralizado, para assinatura 39
Certificado de pessoa física ligada, no cartão para autenticação 41
Certificado de uma pessoa física ligada, com pseudónimo, num cartão para assinatura 41
Certificado de uma pessoa física ligada, com pseudónimo, centralizado, para assinatura 43
Certificado de uma pessoa física ligada, com pseudónimo, num cartão para autenticação 44
Certificado de Selo Eletrónico em software 45
Certificado de Selo Eletrónico com gestão centralizada 46
1.4.2 Limites e proibições ao uso de certificados 47
1.4.3 Emissão de certificados de teste 48
1.5 Gestão de Políticas 48
1.5.1 Organização que administra o documento 49
1.5.2 Contactos da organização 49
1.5.3 Organização aprovando o documento 49
1.5.4 Procedimentos de gestão documental 49
1.6 Siglas e definições 51
1.6.1. Siglas 51
1.6.2 Definições 54
2. Publicação de informações e depósito de certificados 56
2.1 Depósito do certificado 56
2.2 Publicação de informações de certificação 56
2.3 Frequência de publicação 56
2.4 Controlo de Acesso 57
3. Identificação e autenticação 58
3.1 Registo inicial 58
3.1.1 Tipos de nomes 58

3.1.1.1 Certificado de assinatura do funcionário público, de alto nível, no cartão 58

3.1.1.2 Certificado de assinatura do funcionário público, nível intermédio, no HSM 59

3.1.1.3 Certificado de autenticação de funcionário público, de alto nível, no cartão.....60

3.1.1.4 Certificado de selo de órgão, nível intermédio, em software.....61

3.1.1.5 Certificado de selo de órgão, nível intermédio, em HSM 61

3.1.1.6 Certificado de assinatura de funcionário público com pseudónimo, de alto nível, num cartão.....62

3.1.1.7 Certificado de assinatura do funcionário público com pseudónimo, nível intermédio, no HSM 62

3.1.1.8 Certificado de autenticação de funcionário público, com pseudónimo, de alto nível, no cartão.....63

3.1.1.9 Certificado de Selo Eletrónico TSA/TSU 63

3.1.1.10 Certificado de assinatura de pessoa física relacionada, num cartão 64

3.1.1.11 Certificado de assinatura de pessoa física relacionada, no HSM.....65

3.1.1.12 Certificado de autenticação da pessoa física ligada, no cartão 67

3.1.1.13 Certificado de assinatura de uma pessoa física ligada, num cartão, com pseudónimo.....68

3.1.1.14 Certificado de assinatura de pessoa física relacionada, na HSM 69

3.1.1.15 Certificado de autenticação de uma pessoa física ligada, em cartão, com pseudónimo.....69

3.1.1.16 Certificado de selo eletrónico, em software 70

3.1.1.17 Certificado eletrónico de selo com gestão centralizada 70

3.1.2. Significado dos nomes.....71

3.1.3 Uso de anónimos e pseudónimos.....71

3.1.4 Interpretação dos Formatos dos Nomes 71

3.1.5 Unicidade dos nomes.....72

3.1.6 Resolução de disputas de nomeação.....72

3.2 Validação inicial de identidade 73

3.2.1 Prova de Posse de Chave Privada 74
3.2.2 Identificação da entidade 74
3.2.3 Autenticação da identidade de uma pessoa natural 76
3.2.3.1 Em certificados 77
3.2.3.2 Necessidade de presença pessoal 77
3.2.3.3 Relação da pessoa física 77
3.2.4 Informação não verificada do assinante 78
3.2.5 Critérios de interoperabilidade 78
3.3 Identificação e autenticação de pedidos de renovação 78
3.3.1 Validação para renovação rotineira de certificados 78
3.3.2 Identificação e Autenticação da Renovação após a Revogação 78
3.4 Identificação e autenticação do pedido de revogação 78
4. Requisitos de Operação do Ciclo de Vida do Certificado 79
4.1 Candidatura ao Certificado 79
4.1.1 Legitimidade para solicitar a emissão 79
4.1.2 Procedimento de registo e responsabilidades 79
4.2 Processamento da candidatura à certificação 80
4.2.1 Execução das funções de identificação e autenticação 80
4.2.2 Aprovação ou rejeição da candidatura 80
4.2.3 Prazo para resolver a candidatura 81
4.3 Emissão do certificado 81
4.3.1 Ações da AC durante o processo de emissão 81
4.3.2 Notificação do problema ao assinante 82
4.4 Entrega e aceitação do certificado 82
4.4.1 Conduta que constitui aceitação do certificado 83
4.4.2 Publicação do certificado 84
4.4.3 Notificação da questão a terceiros 84
4.5 Utilização do Par de Chaves e do Certificado 84
4.5.1 Utilização pelo subscritor ou signatário 84
4.5.2 Utilização pelo Assinante 85
4.5.3 Utilização pelo certificado com base em terceiros 86
4.6. Renovação de certificados 87
4.6.1 Circunstâncias para a Renovação do Certificado 87
4.6.2 Quem pode pedir a renovação 87

4.6.3 Processamento do Pedido de Renovação de Certificado 88
4.6.4 Notificação da emissão de novo certificado ao assinante 88
4.6.5 Conduta que constitui aceitação de um certificado de renovação 88
4.6.6 Publicação do certificado de renovação pela CA 88
4.6.7 Notificação da emissão do certificado pela CA a outras entidades 88
4.7 Renovação de Chaves e Certificados 88
4.7.1 Quem pode solicitar o certificado de uma nova chave pública 88
4.7.2 Procedimento com nova identificação 88
4.7.3 Processamento de Novos Pedidos de Chave de Certificado 88
4.7.4 Notificação da emissão do certificado renovado 89
4.7.5 Conduta que constitui aceitação do certificado 89
4.7.6 Publicação do certificado 89
4.7.7 Notificação da emissão a terceiros 89
4.8 Modificação de certificados 89
4.9 Revogação e suspensão de certificados 89
4.9.1 Causas para revogação de certificados 89
4.9.2 Legitimidade para solicitar revogação 91
4.9.3 Procedimentos de Pedido de Revogação 91
4.9.4 Prazo para pedido de revogação 92
4.9.5 Prazo para o Processamento de Candidaturas 92
4.9.6 Obrigação de consultar informações sobre a revogação de certificados por terceiros 93
4.9.7 Frequência de emissão de listas de revogação de certificados (CRLs) 93
4.9.8 Prazo Máximo de Publicação para CRLs 94
4.9.9 Disponibilidade de Serviços de Verificação de Saúde com Certificado Online 94
4.9.10 Obrigação de consultar os serviços de verificação de saúde certificado 94
4.9.11 Outras formas de informação sobre revogação de certificados 95
4.9.12 Requisitos especiais em caso de comprometimento de chave privada 95
4.9.13 Causas para suspensão de certificados 95
4.9.14 Pedido de suspensão 96
4.9.15 Procedimentos para o pedido de suspensão 96
4.9.16 Período Máximo de Suspensão 96
4.10 Certificados de Serviços de Verificação de Saúde 96
4.10.1 Características operacionais dos serviços 96
4.10.2 Disponibilidade de Serviços 97

4.10.3 Funcionalidades Opcionais 97
4.11 Cessação da Subscrição 97
4.12 Depósito de Chave e Recuperação 97
4.12.1 Política e Práticas de Depósito e Recuperação de Chaves 97
4.12.2 Política e Práticas de Envolvimento e Recuperação de Chaves de Sessão 98
5. Controlos de segurança física, de gestão e operacionais 99
5.1 Controlos de Segurança Física 99
5.1.1 Localização e construção das instalações 100
5.1.2 Acesso Físico 100
5.1.3 Eletricidade e ar condicionado 101
5.1.4 Exposição à água 101
5.1.5 Prevenção e proteção contra incêndios 101
5.1.6 Armazenamento de Media 101
5.1.7 Tratamento de resíduos 101
5.1.8 Backup fora do local 102
5.2 Controlos Procedurais 102
5.2.1 Funcionalidades Fiáveis 102
5.2.2 Número de pessoas por tarefa 103
5.2.3 Identificação e autenticação para cada função 103
5.2.4 Papéis que Exigem Separação de Funções 104
5.2.5 Sistema de Gestão de PKI 104
5.3 Verificações de pessoal 104
5.3.1 Histórico, qualificações, experiência e requisitos de autorização 104
5.3.2 Procedimentos de Investigação do Histórico 105
5.3.3 Requisitos de Formação 106
5.3.4 Requisitos e frequência das atualizações de formação 106
5.3.5 Sequência e frequência de rotatividade de trabalho 106
5.3.6 Penalizações por Ações Não Autorizadas 107
5.3.7 Requisitos para a contratação de profissionais 107
5.3.8 Fornecimento de documentação ao pessoal 107
5.4 Procedimentos de auditoria de segurança 107
5.4.1 Tipos de Eventos Registados 107
5.4.2 Frequência do Processamento dos Registos de Auditoria 109

5.4.3 Período de Retenção dos Registos de Auditoria 109
5.4.4 Proteção dos Registos de Auditoria 110
5.4.5 Procedimentos de Backup 110
5.4.6 Localização do Sistema de Acumulação de Registos de Auditoria 110
5.4.7 Notificação do evento de auditoria à pessoa que o causou 111
5.4.8 Análise de Vulnerabilidades 111
5.5. Ficheiros de informação 111
5.5.1 Tipos de Registos Arquivados 111
5.5.2 Período de retenção de recordes 112
5.5.3 Proteção de ficheiros 112
5.5.4 Procedimentos de Backup 113
5.5.5 Requisitos de Marcação de Data e Hora 113
5.5.6 Localização do Sistema de Ficheiros 113
5.5.7 Procedimentos para Obtenção e Verificação de Informação de Arquivo 114
5.6 Renovação de chaves 114
5.7 Compromisso Chave e Recuperação em Desastres 114
5.7.1 Procedimentos para a gestão de incidentes e compromissos 114
5.7.2 Corrupção de Recursos, Aplicações ou Dados 114
5.7.3 Compromisso da chave privada da entidade 115
5.7.4 Continuidade dos Negócios Após um Desastre 115
5.8 Término do Serviço 116
6. Verificações técnicas de segurança 117
6.1 Geração e Instalação de Pares de Chaves 117
6.1.1 Geração de Pares de Chaves 117
6.1.2 Envio da Chave Privada ao Signatário 120
6.1.3 Envio da chave pública ao emissor do certificado 120
6.1.4 Distribuição da chave pública do fornecedor de serviços de certificação 120
6.1.5 Tamanhos das teclas 121
6.1.6 Geração de parâmetros de chave pública e verificação de qualidade 121
6.1.7 Finalidades do Uso de Teclas 121
6.2 Proteção de Chave Privada e Controlos de Módulos Criptográficos 122
6.2.1 Normas para Módulos Criptográficos 122
6.2.2 Controlo por mais do que uma pessoa (n de m) sobre a chave privada 122
6.2.3 Depósito de Chave Privada 122
6.2.4 Backup de Chave Privada 122

6.2.5 Arquivamento de Chave Privada 122
6.2.6 Introdução da chave privada no módulo criptográfico 123
6.2.7 Armazenamento de Chaves Privadas em Módulos Criptográficos 123
6.2.8 Método de Ativação de Chave Privada 123
6.2.9 Método de Desativação de Chave Privada 123
6.2.10 Método de Destruição de Chave Privada 123
6.2.11 Classificação do Módulo Criptográfico 124
6.3 Outros aspetos da gestão de pares de chaves 124
6.3.1 Ficheiro de Chave Pública 124
6.3.2 Períodos de utilização de chaves públicas e privadas 124
6.4 Dados de Ativação 125
6.4.1 Geração e instalação de dados de ativação 125
6.4.2 Proteção dos dados de ativação 125
6.4.3 Outros aspetos dos dados de ativação 125
6.5. Controlos de segurança informática 125
6.5.1 Requisitos técnicos específicos para segurança informática 126
6.5.2 Avaliação do nível de segurança informática 127
6.6 Controlos técnicos do ciclo de vida 127
6.6.1 Controlos de Desenvolvimento do Sistema 127
6.6.2 Controlos de Gestão de Segurança 127
Classificação e gestão de informação e ativos 127
Operações de gestão 128
Tratamento e segurança dos media 128
Gestão do sistema de acesso 129
6.6.3 Avaliação da Segurança ao Longo do Ciclo de Vida 130
6.7 Controlo de Segurança de Rede 130
6.8 Fontes Temporais 131
6.9 Algoritmos de assinatura e parâmetros do sistema centralizado de assinaturas 131
7. Perfis de Certificados, CRL e OCSP 132
7.1 Perfil de Certificado 132
7.1.1 Número de Versão 132
7.1.2 Prorrogações de Certificados 132
7.1.3 Identificadores de Objeto (OIDs) de Algoritmos 132
7.1.4 Formatação do Nome 133

7.1.5 Restrição de nomes 133
7.1.6 Identificador de Objeto (OID) dos Tipos de Certificados 133
7.1.7 Utilização da Extensão de Restrições de Política 133
7.1.8 Qualificadores de Política, Sintaxe e Semântica 133
7.1.9 Processamento Semântico para Extensão Crítica de Políticas de Certificados 133
7.1.10 Restrições de Comprimento dos Elementos 133
7.2 Perfil da Lista de Revogação de Certificados 134
7.2.1 Número de Versão 134
7.2.2 CRL e extensões CRL 134
7.3 Perfil OCSP 135
7.3.1 Número de Versão 135
7.3.2 Extensões OCSP 135
8. Auditoria de conformidade 136
8.1 Frequência da Auditoria de Conformidade 136
8.2 Identificação e qualificação do auditor 136
8.3 Relação do auditor com a entidade auditada 136
8.4 Lista de itens sujeitos a auditoria 137
8.5 Ações a serem tomadas devido à falta de conformidade 137
8.6 Tratamento dos relatórios de auditoria 137
9. Requisitos Empresariais e Jurídicos 139
9.1 Taxas 139
9.1.1 Taxa de Emissão ou Renovação de Certificados 139
9.1.2 Taxa de Acesso ao Certificado 139
9.1.3 Taxa de Acesso à Informação sobre o Estado do Certificado 139
9.1.4 Taxas por Outros Serviços 139
9.1.5 Política de Retirada 139
9.2 Responsabilidade Financeira 139
9.2.1 Cobertura de Seguro 140
9.2.2 Outros ativos 140
9.3 Confidencialidade da Informação 140
9.3.1 Informação confidencial 140
9.3.2 Informação não confidencial 141
9.3.3 Divulgação de Informações de Suspensão e Revogação 141
9.3.4 Divulgação Legal de Informação 141
9.3.5 Divulgação de informações a pedido do proprietário 142

9.3.6 Outras Circunstâncias de Divulgação de Información 142
9.4 Privacidade das Informações Pessoais 142
9.4.1 Plano de Privacidade 143
9.4.2 Informação tratada como privada 143
9.4.3 Informação não considerada privada 143
9.4.4 Responsabilidade de Proteger a Informação Privada 144
9.4.5 Aviso e Consentimento para o Uso de Informação Privada 144
9.4.6 Divulgação ao abrigo de processos judiciais ou administrativos 144
9.4.7 Outras Circunstâncias de Divulgação de Informação 144
9.5 Direitos de Propriedade Intelectual 144
9.5.1 Propriedade de Certificados e Informações de Revogação 144
9.5.2 Propriedade da Declaração de Práticas de Certificação 145
9.5.3 Propriedade da Informação do Nome 145
9.5.4 Propriedade de Chaves 145
9.6 Obrigações e responsabilidade civil 145
9.6.1 Obrigações do Organismo de Certificação "esFIRMA" 146
9.6.2. Obrigação e Responsabilidade da RA 147
9.6.3 Garantias Oferecidas a Assinantes e Terceiros Com Base em Certificados 150
9.6.4 Responsabilidade e responsabilidade de terceiros 151
9.6.5 Responsabilidade e obrigação dos outros participantes 151
9.7. Renúncia da Garantia 151
9.8. Limitação de Responsabilidade por Perdas de Transação 153
9.9. Compensação 153
9.10. Período e Conclusão 153
9.10.1 Mandato 153
9.10.2 Rescisão 153
9.10.3 Efeito da terminação e sobrevivência 153
9.11. Comunicação com as partes interessadas e o órgão supervisor 153
9.12. Alterações 154
9.12.1 Procedimento de modificação 154
9.12.2 Mecanismo de notificação e prazos 154
9.12.3 Circunstâncias em que o OID deve ser alterado 155
9.13 Procedimento de resolução de litígios 155
9.14. Legislação aplicável 155
9.15. Conformidade com a Lei Aplicável 155

9.16. Outras disposições 155
9.16.1 Acordo Completo 155
9.16.2 Atribuição 156
9.16.3 Separabilidade 156
9.16.4 Conformidade (Honorários de Advogados e Renúncia) 156
9.16.5 Força Maior 156
9.17 Outras disposições 157
9.17.1 Cláusula de indemnização do assinante 157
9.17.2 Cláusula de indemnização de terceiros que se baseiam no certificado 157

1. Introdução

1.1 Apresentação

Este documento estabelece as práticas de certificação de assinatura eletrónica da esFIRMA.

Os certificados emitidos são os seguintes:

- **Funcionário Público (FIRMA)**
  - De Nível Intermédio de Funcionários Públicos
  - Funcionário Público de Alto Nível
- **Funcionário Público (AUTENTICAÇÃO)**
  - Funcionário Público de Alto Nível
- **De Funcionário Público com pseudónimo (FIRMA)**
  - De Nível Intermédio de Funcionários Públicos
  - Funcionário Público de Alto Nível
- **De Funcionário Público com pseudónimo (AUTENTICAÇÃO)**
  - Funcionário Público de Alto Nível
- **De uma pessoa física ligada a uma entidade (FIRMA)**
  - De um indivíduo ligado a uma entidade de nível Intermédio
  - De um indivíduo ligado a uma entidade de alto nível
- **De uma pessoa física ligada a uma entidade (AUTENTICAÇÃO)**
  - De um indivíduo ligado a uma entidade de alto nível

- **De un individuo ligado a una entidade com pseudónimo (FIRMA)**
    - De um indivíduo ligado a uma entidade de nível Intermédio
    - De um indivíduo ligado a uma entidade de alto nível
- **De uma pessoa física ligada a uma entidade com pseudónimo (AUTENTICAÇÃO)**
    - De um indivíduo ligado a uma entidade de alto nível
- **Selo do Órgão**
    - Selo de Órgão Nível Médio
- **Selo Eletrónico para TSA/TSU**
    - Selo eletrónico para TSU no HSM
- **Selo Eletrónico**
    - Selo eletrónico no software
    - Selo eletrónico com gestão centralizada

1.2 Nome e identificação do documento

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

1.2.1 Identificadores de Certificados

Número OID	Políticas de certificados
	Funcionário Público (FIRMA)
1.3.6.1.4.1.47281.1.1.1	*Funcionário Público – Nível elevado no cartão*
1.3.6.1.4.1.47281.1.1.4	*Funcionário Público – Nível Intermédio em HSM*
	Funcionário Público (AUTENTICAÇÃO)
1.3.6.1.4.1.47281.1.1.5	*Funcionário Público – Nível elevado no cartão*
	De Funcionário Público com Pseudónimo (ASSINATURA)
1.3.6.1.4.1.47281.1.3.1	*Do EP com pseudónimo – High Level on Card*
1.3.6.1.4.1.47281.1.3.4	*PE com pseudónimo – Nível Intermédio em HSM*
	Funcionário Público Pseudónimo (AUTENTICAÇÃO)
1.3.6.1.4.1.47281.1.3.5	*Do EP com pseudónimo – High Level on Card*
	De Indivíduo ligado à entidade (FIRMA)

1.3.6.1.4.1.47281.1.6.1	*Do PF ligado à entidade – Assinatura eletrónica qualificada, no cartão*
1.3.6.1.4.1.47281.1.6.4	*PF ligada a entidades – Assinatura Eletrónica Centralizada*
	De uma pessoa física ligada a uma entidade (AUTENTICAÇÃO)
1.3.6.1.4.1.47281.1.6.5	*PF ligado à entidade – no cartão*
	De uma pessoa física com pseudónimo ligado a uma entidade (FIRMA)
1.3.6.1.4.1.47281.1.7.1	*Do PF com pseudónimo associado a uma entidade – Assinatura eletrónica qualificada, no cartão*
1.3.6.1.4.1.47281.1.7.4	*De PF com pseudónimo ligado a uma entidade – Firma-e Centralizado*
	De uma Pessoa com pseudónimo, ligada a uma entidade (AUTENTICAÇÃO)
1.3.6.1.4.1.47281.1.7.5	*Do PF com pseudónimo, ligado à entidade – em Card*
	Selo do Órgão
1.3.6.1.4.1.47281.1.2.2	*Selo de Órgão – Nível Intermédio em Software*
1.3.6.1.4.1.47281.1.2.4	*Selo de Órgão – Nível Intermédio em HSM*
	Selo Eletrónico para TSA/TSU
1.3.6.1.4.1.47281.1.5.1	*E-Seal para TSA/TSU no HSM*
1.3.6.1.4.1.47281.1.5.2	*E-Seal Qualificado pela TSA/TSU em HSM*
	Selo Eletrónico
1.3.6.1.4.1.47281.1.8.2	*Selo Eletrónico em Software*
1.3.6.1.4.1.47281.1.8.4	*Selo Eletrónico Centralizado*

Em caso de contradição entre esta Declaração de Práticas de Certificação e outros documentos de práticas e procedimentos do esFIRMA, prevalecerão as disposições desta 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 prestador de serviços de certificação é a pessoa, física ou jurídica, que emite e gere certificados para entidades finais, utilizando um Organismo de Certificação ou prestando outros serviços relacionados com assinaturas eletrónicas.

ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN SA (ANTERIORMENTE AULOCE SA), doravante ESPUBLICO, com morada na Calle Bari 39 (Edifício Binário Dif.), C.P. 50.197, Saragoça, CIF A-50.878.842, registada no Registo Mercantil de Saragoça no volume 2.649, Fólio 215, página Z-28722, e operando sob a marca comercial esFIRMA, nome comercial que será utilizado em todo este documento para a designar, é um prestador de serviços de certificação que atua de acordo com as disposições do regime de obrigações e responsabilidades do Regulamento (UE) 910/2014, da Lei 6/2020, de 11 de novembro, que regula certos aspetos dos serviços eletrónicos fiduciários, da Lei Orgânica 3/2018, de 5 de dezembro, sobre a Proteção de Dados Pessoais e garantia dos direitos digitais, e as normas técnicas ETSI aplicáveis à emissão e gestão da de certificados qualificados, principalmente ETSI EN 319 411-1 e ETSI EN 319 411-2, para facilitar o cumprimento dos requisitos legais e o reconhecimento internacional dos seus serviços.

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

Raiz enFIRMA AC 2

Esta é a CA raiz na hierarquia que emite certificados a outras CAs, e cujo certificado de chave pública foi auto-assinado.

Dados de identificação:

CN:	ESFIRMA AC RAIZ 2
Impressão digital SHA-256:	C6:09:F9:4F:9C:CE:20:CB:2B:A0:2E:8B:5B:33:55:20:06:C1:5D :17:78:32:26:11:07:0F:A1:4F:FF:9D:C9:16
Válido de:	2017-11-02T12:52:43Z
Válido até:	2042-11-02T12:52:43Z

Comprimento da Chave RSA:	4.096 bits

SIGNATURE AC AAPP 2

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

Dados de identificação:

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

Plataforma de Administração Eletrónica

É a plataforma exclusiva de gestão do ciclo de vida dos certificados para candidatura, aprovação, emissão e revogação.

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

1.3.2 Autoridades de Registo

Uma autoridade de registo realiza a verificação e identificação dos candidatos ao certificado.

Em geral, o próprio fornecedor de serviços de certificação atua como autoridade de registo para a identidade dos subscritores do certificado.

As autoridades de registo dos certificados sujeitas a esta Declaração de Práticas de Certificação, devido ao seu estatuto de certificados corporativos, são também as unidades designadas para esta função pelos subscritores dos certificados, como o Secretário da sociedade, o departamento de pessoal ou o Representante Legal da Administração, uma vez que possuem registos autênticos sobre a relação dos signatários com o assinante.

As funções de registo dos subscritores são desempenhadas por delegação e de acordo com as instruções do prestador do serviço de certificação, nos termos definidos pelo Regulamento (UE) 910/2014 e pela Lei 6/2020, de 11 de novembro, que regula certos aspetos dos serviços fiduciários eletrónicos, e sob total responsabilidade do prestador de serviços de certificação face a terceiros.

1.3.3 Entidades Finais

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

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

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

1.3.4 Partidos Utilizadores

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

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

1.3.5 Outros participantes

Assinantes do Serviço de Certificação

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

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

O assinante do serviço de certificação é, portanto, o cliente do prestador do serviço de certificação, de acordo com o direito comercial, e detém os direitos e obrigações definidos pelo prestador do serviço de certificação, que são adicionais e prejudicam os direitos e obrigações dos signatários, conforme autorizados e regulados nas normas técnicas europeias aplicáveis à emissão de certificados eletrónicos qualificados, em particular ETSI EN 319 411-2, secções 5.4.2 e 6.3.4.e)

Signatários

Os signatários são as pessoas singulares que possuem exclusivamente ou têm sob o seu controlo exclusivo, 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 certos aspetos dos serviços eletrónicos fiduciários, as chaves de assinatura digital para identificação e assinatura eletrónica avançada ou qualificada; tipicamente os titulares ou membros dos órgãos administrativos, nos certificados de assinatura eletrónica do órgão, as pessoas ao serviço das Administrações Públicas, nos certificados dos funcionários públicos ou das pessoas que pertencem a uma entidade, nos certificados das pessoas singulares vinculadas.

Os signatários são devidamente autorizados pelo subscritor e devidamente identificados no certificado pelo seu nome e apelidos, e pelo número de identificação fiscal válido na jurisdição da emissão do certificado, ou com o pseudónimo correspondente nos certificados deste tipo.

Dada a existência de certificados para usos que não sejam assinaturas eletrónicas, como a identificação, também é utilizado o termo mais genérico "pessoa física identificada no certificado", sempre com total respeito pelo cumprimento da legislação sobre assinaturas eletrónicas relativamente aos direitos e obrigações do signatário.

1.4 Utilização de certificados

Esta secção lista as aplicações para as quais cada tipo de certificado pode ser utilizado, estabelece limitações a certas aplicações e proíbe certas aplicações de certificados.

1.4.1 Utilizações Permitidas para Certificados

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

Certificado de Funcionário Público de Alto Nível no Cartão

Este certificado possui os seguintes OIDs:

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

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

Estes certificados são emitidos a funcionários públicos para os identificar como pessoas ao serviço da Administração, órgão, entidade de direito público ou outra entidade, ligando-os a esta, cumprindo os requisitos estabelecidos no Artigo 43 da Lei 40/2015, de

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

Os certificados de pessoas físicas de alto nível de funcionário público funcionam com um dispositivo seguro de criação de assinaturas, 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 pessoas físicas de alto nível de funcionário público são emitidos de acordo com os elevados níveis de garantia dos perfis de certificados estabelecidos no ponto 10 do documento "Perfis de Certificados Eletrónicos" do Secretário de Estado para a Digitalização e Inteligência Artificial do Ministério dos Assuntos Económicos e Transformação Digital.

Estes certificados garantem a identidade do subscritor e do signatário, e permitem a geração da "assinatura eletrónica qualificada"; isto é, a assinatura eletrónica avançada baseada num certificado qualificado e gerada através de um dispositivo qualificado, de acordo com as disposições do artigo 25.2 do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, terá efeito legal equivalente ao de uma assinatura manuscrita.

Podem também ser usados em aplicações que não requerem a assinatura eletrónica equivalente à assinatura escrita, como as aplicações listadas abaixo:

a) Assinatura de email segura.
b) Outras aplicações de assinatura digital.

A esFIRMA não oferece serviços de backup nem de recuperação de chaves. Portanto, a esFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

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

a) O campo "utilização da chave" ativou, permitindo assim executar, as seguintes funções:

   a. Compromisso de conteúdo (para desempenhar a função de assinatura eletrónica)

b) No campo "Declarações de Certificado Qualificadas", 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 utilizado exclusivamente em conjunto com um dispositivo seguro de criação de assinaturas.
c) O campo "Aviso ao Utilizador" descreve a utilização deste certificado.

Certificado de Funcionário Público ao nível intermédio na HSM

Este certificado possui os seguintes OIDs:

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

Os certificados de pessoas físicas no cargo público 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 dos regulamentos técnicos identificados com a referência ETSI EN 319 411-2.

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

Os certificados de pessoas físicas no cargo público de nível intermédio são geridos de forma centralizada.

Os certificados de pessoas físicas de funcionários públicos de nível médio são emitidos de acordo com os níveis médios de garantia dos perfis de certificados estabelecidos no ponto 10 do documento "Perfis de Certificados Eletrónicos" do Secretário de Estado para a Digitalização e Inteligência Artificial do Ministério dos Assuntos Económicos e Transformação Digital.

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

Podem também ser usados em aplicações que não requerem a assinatura eletrónica equivalente à assinatura escrita, como as aplicações listadas abaixo:

a) Assinatura de email segura.
b) Outras aplicações de assinatura digital.

A esFIRMA não oferece serviços de backup nem de recuperação de chaves. Portanto, a esFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

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

a) O campo "uso de chaves" ativou, e por isso permite-nos executar, as seguintes funções:
    a. Compromisso de conteúdo (para desempenhar a função de assinatura eletrónica)

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

Certificado de Funcionário Público de Alto Nível no cartão para autenticação

Este certificado possui os seguintes OIDs:

1.3.6.1.4.1.47281.1.1.5	Na hierarquia da CA 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 emitidos de acordo com a política padronizada de certificados (NCP+) e cumprem as disposições da norma técnica identificada com a referência ETSI EN 319 411-1.

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

Estes certificados de pessoas de alto nível de funcionários públicos trabalham 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 das pessoas de alto nível dos funcionários públicos são emitidos de acordo com os elevados níveis de garantia dos perfis de certificados estabelecidos no ponto 10 do documento "Perfis de Certificados Eletrónicos" do Secretário de Estado para a Digitalização e Inteligência Artificial do Ministério dos Assuntos Económicos e Transformação Digital.

Estes certificados garantem a identidade do assinante e da pessoa indicada no certificado, permitindo a autenticação destes últimos em aplicações e websites.

A esFIRMA não oferece serviços de backup nem de recuperação de chaves. Portanto, a esFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

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

d) O campo "uso de chaves" ativou, e por isso permite-nos executar, as seguintes funções:
    a. Assinatura digital (para realizar a função de autenticação)

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

Certificado de Selo de Órgão de nível médio em software

Este certificado possui os seguintes OIDs:

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

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

Estes certificados são emitidos para a identificação e autenticação do exercício da competência em ação administrativa automatizada, de acordo com o Artigo 42 da Lei 40/2015, de 1 de outubro, sobre o Regime Jurídico do Setor Público.

Os certificados de selos eletrónicos de órgãos de nível médio são emitidos de acordo com os níveis de garantia média dos perfis de certificados estabelecidos no ponto 9 do documento "Perfis de Certificados Eletrónicos" do Secretário de Estado para a Digitalização e Inteligência Artificial do Ministério dos Assuntos Económicos e Transformação Digital.

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

A esFIRMA não oferece serviços de backup nem de recuperação de chaves. Portanto, a esFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

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

a) O campo "uso de chaves" ativou, e por isso permite-nos executar, as seguintes funções:
    a. Compromisso de conteúdo (para desempenhar a função de assinatura eletrónica)

b) No campo "Declarações de Certificado Qualificadas", 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 Utilizador" descreve a utilização deste certificado.

Certificado de Selo de Órgão ao nível intermédio em HSM

Este certificado possui os seguintes OIDs:

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

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

Estes certificados são emitidos para a identificação e autenticação do exercício da competência em ação administrativa automatizada, de acordo com o Artigo 42 da Lei 40/2015, de 1 de outubro, sobre o Regime Jurídico do Setor Público.

Os certificados eletrónicos de selos do organismo intermédio são geridos centralmente.

Os certificados de selos eletrónicos de órgãos de nível médio são emitidos de acordo com os níveis de garantia média dos perfis de certificados estabelecidos no ponto 9 do documento "Perfis de Certificados Eletrónicos" do Secretário de Estado para a Digitalização e Inteligência Artificial do Ministério dos Assuntos Económicos e Transformação Digital.

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

A esFIRMA não oferece serviços de backup nem de recuperação de chaves. Portanto, a esFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

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

a) O campo "uso de chaves" ativou, e por isso permite-nos executar, as seguintes funções:
    a. Compromisso de conteúdo (para desempenhar a função de assinatura eletrónica)

b) No campo "Declarações de Certificado Qualificadas", 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 Utilizador" descreve a utilização deste certificado.

Certificado de Funcionário Público com Pseudónimo de Alto Nível no Cartão

Este certificado possui os seguintes OIDs:

1.3.6.1.4.1.47281.1.3.1	Na hierarquia da CA esFIRMA

0.4.0.194112.1.2	De acordo com a política QCP-n-qscd
2.16.724.1.3.5.4.1	Funcionário público espanhol com pseudónimo de alto nível

Os certificados de pessoas físicas de funcionários públicos com pseudónimo de alto nível são certificados qualificados de acordo com o Artigo 28.º e o Anexo I do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, e cumprem as disposições dos regulamentos técnicos identificados com a referência ETSI EN 319 411-2.

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

Os certificados de pessoas físicas de funcionários públicos com pseudónimo de alto nível funcionam com um dispositivo seguro de criação de assinaturas, 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, são emitidos certificados de funcionários públicos de pessoas físicas com pseudónimo de alto nível de acordo com os elevados níveis de garantia dos perfis de certificados estabelecidos no ponto 11 do documento "Perfis de Certificados Eletrónicos" do Secretário de Estado para a Digitalização e Inteligência Artificial do Ministério dos Assuntos Económicos e Transformação Digital.

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

Podem também ser usados em aplicações que não requerem a assinatura eletrónica equivalente à assinatura escrita, como as aplicações listadas abaixo:

a) Assinatura de email segura.
b) Outras aplicações de assinatura digital.

A esFIRMA não oferece serviços de backup nem de recuperação de chaves. Portanto, a esFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

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

a) O campo "utilização da chave" ativou, permitindo assim executar, as seguintes funções:
    a. Compromisso de conteúdo (para desempenhar a função de assinatura eletrónica)

b) No campo "Declarações de Certificado Qualificadas", 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 utilizado exclusivamente em conjunto com um dispositivo seguro de criação de assinaturas.
c) O campo "Aviso ao Utilizador" descreve a utilização deste certificado.

Certificado de Funcionário Público com pseudónimo de nível intermédio, na HSM

Este certificado possui os seguintes OIDs:

1.3.6.1.4.1.47281.1.3.4	Na hierarquia da CA esFIRMA
0.4.0.194112.1.0	De acordo com a política QCP-n
2.16.724.1.3.5.4.2	Funcionário público espanhol com pseudónimo de nível médio

Os certificados de pessoas físicas de funcionários públicos com pseudónimo 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 dos regulamentos técnicos identificados com a referência ETSI EN 319 411-2.

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

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

Os certificados de pessoas singulares de funcionários públicos com pseudónimo 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 Eletrónicos" do Secretário de Estado para a Digitalização e Inteligência Artificial do Ministério dos Assuntos Económicos e Transformação Digital.

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

Podem também ser usados em aplicações que não requerem a assinatura eletrónica equivalente à assinatura escrita, como as aplicações listadas abaixo:

c) Assinatura de email segura.
d) Outras aplicações de assinatura digital.

A esFIRMA não oferece serviços de backup nem de recuperação de chaves. Portanto, a esFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

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

a) O campo "uso de chaves" ativou, e por isso permite-nos executar, as seguintes funções:
    a. Compromisso de conteúdo (para desempenhar a função de assinatura eletrónica)

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

Certificado de Funcionário Público com pseudónimo, nível superior no cartão para autenticação

Este certificado possui os seguintes OIDs:

1.3.6.1.4.1.47281.1.3.5	Na hierarquia da CA 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 pseudónimo de alto nível

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

Estes certificados são emitidos a funcionários públicos para os identificar (por pseudónimo) como pessoas ao serviço da Administração, órgão, entidade de direito público ou outra entidade, ligando-os a esta, cumprindo os requisitos estabelecidos na Lei 40/2015, de 1 de outubro, sobre o Regime Jurídico do Setor Público.

Estes certificados de pessoas físicas que são funcionários públicos com pseudónimo de alto nível funcionam com um dispositivo seguro de criação de assinaturas, 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 pessoas físicas de funcionários públicos com pseudónimo de alto nível são emitidos de acordo com os elevados níveis de garantia dos perfis de certificados estabelecidos no ponto 11 do documento "Perfis de Certificados Eletrónicos" do Secretário de Estado para a Digitalização e Inteligência Artificial do Ministério dos Assuntos Económicos e Transformação Digital.

Estes certificados garantem a identidade do assinante e da pessoa indicada no certificado, permitindo a autenticação destes últimos em aplicações e websites.

A esFIRMA não oferece serviços de backup nem de recuperação de chaves. Portanto, a esFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

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

f) O campo "uso de chaves" ativou, e por isso permite-nos executar, as seguintes funções:
    a. Assinatura digital (para realizar a função de autenticação)

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

Certificado de Selo Eletrónico Qualificado pela TSA/TSU

Este certificado possui os seguintes OIDs:

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

Os certificados de selo eletrónico da 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 dos regulamentos técnicos identificados com as referências ETSI EN 319 421 e ETSI EN 319 422.

Este certificado permite que as Unidades de Carimbo Temporal, ou TSU, emitam carimbos temporais quando recebem um pedido segundo as especificações do RFC3161.

As chaves são geradas para suportar um dispositivo HSM.

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

a) O campo "uso de chaves" ativou, e por isso permite-nos executar, as seguintes funções:
    a. Compromisso de Conteúdo
b) O campo "estender uso de chave" tem a seguinte funcionalidade ativada:
    a. Carimbo temporal
c) No campo "Declarações de Certificado Qualificadas", aparece a seguinte declaração:
    a. QcCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.
d) O campo "Aviso ao Utilizador" descreve a utilização deste certificado. Opcional
e) Inclui a extensão "privateKeyUsage", que limita o uso da chave privada, seguindo as recomendações das normas ETSI EN 319 421 e ETSI EN 319 422.

Outras considerações:

- São estabelecidos controlos para garantir a cessação do uso da chave privada antes do seu término da sua validade.
- Em caso de alteração de certificado, as chaves associadas serão destruídas conforme descrito no ciclo de vida.
- As chaves privadas são destruídas após o seu tempo definido de uso, substituição, revogação ou outras causas terem expirado.
- A destruição é feita de forma a que a chave privada não possa ser recuperada, seguindo o procedimento estabelecido pelo fabricante do módulo criptográfico que as armazena.

- Para a validação a longo prazo dos carimbos temporais, o Último CRL emitido pela esFIRMA pode ser utilizado seguindo as orientações fornecidas. No momento da verificação, pode ser considerada válida se, na data do carimbo temporal, a chave privada não foi comprometida, o algoritmo de impressão digital não colidiu e os algoritmos usados estiveram fora do alcance dos ataques criptográficos da época.

Certificado de Selo Eletrónico TSA/TSU

Este certificado possui os seguintes OIDs:

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

Este certificado permite que as Unidades de Carimbo Temporal, ou TSU, emitam carimbos temporais quando recebem um pedido segundo as especificações do RFC3161.

As chaves são geradas para suportar um dispositivo HSM.

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

f) O campo "uso de chaves" ativou, e por isso permite-nos executar, as seguintes funções:
   a. Compromisso de Conteúdo
g) O campo "estender uso de chave" tem a seguinte funcionalidade ativada:
   a. Carimbo temporal
h) O campo "Aviso ao Utilizador" descreve a utilização deste certificado. Opcional
i) Inclui a extensão "privateKeyUsage", que limita o uso da chave privada, seguindo as recomendações das normas ETSI EN 319 421 e ETSI EN 319 422.

Outras considerações:

- São estabelecidos controlos para garantir a cessação do uso da chave privada antes do seu término da sua validade.
- Em caso de alteração de certificado, as chaves associadas serão destruídas conforme descrito no ciclo de vida.

- As chaves privadas são destruídas após o seu tempo definido de uso, substituição, revogação ou outras causas terem expirado.
- A destruição é feita de forma a que a chave privada não possa ser recuperada, seguindo o procedimento estabelecido pelo fabricante do módulo criptográfico que as armazena.
- Para a validação a longo prazo dos carimbos temporais, o Último CRL emitido pela esFIRMA pode ser utilizado seguindo as orientações fornecidas. No momento da verificação, pode ser considerada válida se, na data do carimbo temporal, a chave privada não foi comprometida, o algoritmo de impressão digital não colidiu e os algoritmos usados estiveram fora do alcance dos ataques criptográficos da época.

Certificado de pessoa física ligada, no cartão para assinatura

Este certificado possui os seguintes OIDs:

1.3.6.1.4.1.47281.1.6.1	Na hierarquia da CA 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 dos regulamentos técnicos identificados com a referência ETSI EN 319 411-2.

Estes certificados funcionam com um dispositivo seguro de criação de assinaturas, 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 subscritor e do signatário, e permitem a geração da "assinatura eletrónica qualificada"; isto é, a assinatura eletrónica avançada baseada num certificado qualificado e gerada através de um dispositivo qualificado, de acordo com as disposições do artigo 25.2 do Regulamento (UE) 910/2014 do Parlamento

Europeu e do Conselho, de 23 de julho de 2014, terá efeito legal equivalente ao de uma assinatura manuscrita.

Podem também ser usados em aplicações que não requerem a assinatura eletrónica equivalente à assinatura escrita, como as aplicações listadas abaixo:

c) Assinatura de email segura.
d) Outras aplicações de assinatura digital.

A esFIRMA não oferece serviços de backup nem de recuperação de chaves. Portanto, a esFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

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

d) O campo "utilização da chave" ativou, permitindo assim executar, as seguintes funções:
    a. Compromisso de conteúdo (para desempenhar a função de assinatura eletrónica)

e) No campo "Declarações de Certificado Qualificadas", 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 utilizado exclusivamente em conjunto com um dispositivo seguro de criação de assinaturas.
f) O campo "Aviso ao Utilizador" descreve a utilização deste certificado. Opcional

Certificado de uma pessoa física ligada, centralizado, para assinatura

Este certificado possui os seguintes OIDs:

1.3.6.1.4.1.47281.1.6.4	Na hierarquia da CA 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 dos regulamentos técnicos identificados com a referência ETSI EN 319 411-2.

Estes certificados são geridos centralmente.

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

Podem também ser usados em aplicações que não requerem a assinatura eletrónica equivalente à assinatura escrita, como as aplicações listadas abaixo:

e) Assinatura de email segura.
f) Outras aplicações de assinatura digital.

A esFIRMA não oferece serviços de backup nem de recuperação de chaves. Portanto, a esFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

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

h) O campo "uso de chaves" ativou, e por isso permite-nos executar, as seguintes funções:
    a. Compromisso de conteúdo (para desempenhar a função de assinatura eletrónica)

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

Certificado de pessoa física ligada, no cartão para autenticação

Este certificado possui os seguintes OIDs:

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

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

Estes certificados funcionam com um dispositivo seguro de criação de assinaturas, 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, permitindo a autenticação destes últimos em aplicações e websites.

A esFIRMA não oferece serviços de backup nem de recuperação de chaves. Portanto, a esFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

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

k) O campo "uso de chaves" ativou, e por isso permite-nos executar, as seguintes funções:
    a. Assinatura digital (para realizar a função de autenticação)

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

Certificado de uma pessoa física ligada, com pseudónimo, num cartão para assinatura

Este certificado possui os seguintes OIDs:

1.3.6.1.4.1.47281.1.7.1	Na hierarquia da CA 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 dos regulamentos técnicos identificados com a referência ETSI EN 319 411-2.

Estes certificados funcionam com um dispositivo seguro de criação de assinaturas, 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 através de um pseudónimo.
Estes certificados permitem a geração da "assinatura eletrónica qualificada"; isto é, a assinatura eletrónica avançada baseada num certificado qualificado e gerada utilizando um dispositivo qualificado, pelo que, em conformidade com as disposições do Artigo 25.2 do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, terá um efeito legal equivalente ao de uma assinatura manuscrita.

Podem também ser usados em aplicações que não requerem a assinatura eletrónica equivalente à assinatura escrita, como as aplicações listadas abaixo:

e) Assinatura de email segura.
f) Outras aplicações de assinatura digital.

A esFIRMA não oferece serviços de backup nem de recuperação de chaves. Portanto, a esFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

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

g) O campo "utilização da chave" ativou, permitindo assim executar, as seguintes funções:
    a. Compromisso de conteúdo (para desempenhar a função de assinatura eletrónica)

h) No campo "Declarações de Certificado Qualificadas", 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 utilizado exclusivamente em conjunto com um dispositivo seguro de criação de assinaturas.
i) O campo "Aviso ao Utilizador" descreve a utilização deste certificado. Opcional

Certificado de uma pessoa física ligada, com pseudónimo, centralizado, para assinatura

Este certificado possui os seguintes OIDs:

1.3.6.1.4.1.47281.1.6.4	Na hierarquia da CA 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 dos regulamentos técnicos identificados com a referência ETSI EN 319 411-2.

Estes certificados são geridos centralmente.
Estes certificados garantem a identidade do assinante.
Estes certificados garantem a identidade do signatário através de um pseudónimo.
Estes certificados permitem a geração da "assinatura eletrónica avançada baseada num certificado eletrónico qualificado".

Podem também ser usados em aplicações que não requerem a assinatura eletrónica equivalente à assinatura escrita, como as aplicações listadas abaixo:

g) Assinatura de email segura.

h) Outras aplicações de assinatura digital.

A esFIRMA não oferece serviços de backup nem de recuperação de chaves. Portanto, a esFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

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

m) O campo "uso de chaves" ativou, e por isso permite-nos executar, as seguintes funções:
    a. Compromisso de conteúdo (para desempenhar a função de assinatura eletrónica)

n) No campo "Declarações de Certificado Qualificadas", aparece a seguinte declaração:
    a. qCCcumprimento (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.

o) O campo "Aviso ao Utilizador" descreve a utilização deste certificado. Opcional

Certificado de uma pessoa física ligada, com pseudónimo, num cartão para autenticação

Este certificado possui os seguintes OIDs:

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

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

Estes certificados funcionam com um dispositivo seguro de criação de assinaturas, 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 através de um pseudónimo.
Estes certificados permitem a autenticação destes últimos em aplicações e websites.

A esFIRMA não oferece serviços de backup nem de recuperação de chaves. Portanto, a esFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

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

p) O campo "uso de chaves" ativou, e por isso permite-nos executar, as seguintes funções:
    a. Assinatura digital (para realizar a função de autenticação)

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

Certificado de Selo Eletrónico em software

Este certificado possui os seguintes OIDs:

1.3.6.1.4.1.47281.1.8.2	Na hierarquia da CA 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 as disposições dos regulamentos técnicos identificados com a referência ETSI EN 319 411-2.

A esFIRMA não oferece serviços de backup nem de recuperação de chaves. Portanto, a esFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

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

a) O campo "uso de chaves" ativou, e por isso permite-nos executar, as seguintes funções:

a. Assinatura digital (para função de autenticação)
b. Compromisso de conteúdo (para desempenhar a função de assinatura eletrónica)
c. Encriptação de chaves

b) No campo "Declarações de Certificado Qualificadas", 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 Utilizador" descreve a utilização deste certificado. Opcional

Certificado de Selo Eletrónico com gestão centralizada

Este certificado possui os seguintes OIDs:

1.3.6.1.4.1.47281.1.8.4	Na hierarquia da CA 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 as disposições dos regulamentos técnicos identificados com a referência ETSI EN 319 411-2.

Estes certificados são geridos centralmente.

A esFIRMA não oferece serviços de backup nem de recuperação de chaves. Portanto, a esFIRMA não será responsabilizada em circunstância alguma por qualquer perda de informação encriptada que não possa ser recuperada.

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

d) O campo "uso de chaves" ativou, e por isso permite-nos executar, as seguintes funções:
   a. Compromisso de conteúdo (para desempenhar a função de assinatura eletrónica)

e) No campo "Declarações de Certificado Qualificadas", 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 Utilizador" descreve a utilização deste certificado. Opcional

1.4.2 Limites e proibições ao uso de certificados

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

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

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

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

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

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

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

Da mesma forma, o subscritor, o signatário ou a pessoa responsável pela custódia será responsável por qualquer responsabilidade que possa surgir do seu uso fora dos limites e condições de uso estabelecidos neste DPC, dos documentos legais vinculativos de cada certificado, ou dos contratos ou acordos com as entidades de registo ou seus subscritores. bem como qualquer outro uso impróprio derivado desta secção ou que possa ser interpretado como tal de acordo com a legislação em vigor.

Os certificados são utilizados exclusivamente e exclusivamente a partir da Plataforma de Administração Eletrónica ou de extensões e complementos da mesma que a empresa ESPUBLICO disponibiliza ao assinante.

1.4.3 Emissão de certificados de teste

O esFIRMA emite certificados de teste sob a hierarquia de produção, para realizar testes técnicos de interoperabilidade e permitir a sua avaliação pelo órgão supervisor.

Os dados contidos nos certificados de teste são fictícios e cumprem as diretrizes emitidas pelo órgão supervisor.

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

1.5 Gestão de Políticas

1.5.1 Organização que administra o documento

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

Identificação de Registo	Registo Mercantil de Saragoça
Tome	2649
Folio	215
Folha	Z-28722
CIF	A-50.878.842

1.5.2 Contactos da organização

SERVIÇOS PÚBLICOS PARA A ADMINISTRAÇÃO SA (esFIRMA)
CALLE BARI 39 (Edifício Binário)
50197 - ZARAGOZA
(+34) 976300110

1.5.3 Organização aprovando o documento

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

O Comité de Segurança da esFIRMA, composto pelo seu Presidente, pelo Gestor de Informação e Serviços e pelo Gestor de Segurança da esFirma, é responsável por aprovar esta Declaração de Práticas.

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

1.5.4 Procedimentos de gestão documental

O sistema de documentos e organização da esFIRMA garante, através da existência e aplicação dos respetivos procedimentos, a correta manutenção deste documento e das especificações de serviço relacionadas.

A esFIRMA realiza revisões deste documento pelo menos anualmente ou quando exigidas devido a alterações nas diretrizes e documentos com os quais deve cumprir.

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

O Gabinete de Segurança é responsável pela redação, manutenção e administração do DPC, dos textos de divulgação (PDS), das folhas de entrega e aceitação, bem como do restante da documentação legal (acordos, contratos, etc.) do esFirma.

Sempre que existem alterações de importância suficiente na gestão dos certificados definidos neste DPC, é criada uma nova revisão deste documento, que aparece na caixa inicial de "controlo de versões" na secção de "informação geral".

A ação do Gabinete de Segurança é realizada a pedido do seu chefe, de acordo com as necessidades que surgem.

A esFirma pode fazer alterações que não exijam notificação quando não afetam 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 dos selos, deve notificá-la publicamente para que possam apresentar os seus comentários ao Gabinete de Segurança no prazo de 15 dias após a publicação das futuras alterações.

Para notificar publicamente as alterações produzidas, esta será publicada na secção de "documentação" no site https://www.esfirma.com

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

1.6 Siglas e definições

1.6.1. Siglas

AC (*ou também CA)*	*Autoridade* Certificadora
AR (ou também AR)	*Autoridade de Registo* Autoridade de Registo
CPD	Centro de Processamento de Dados
CPS (ou também DPC)	*Declaração de Prática de* Certificação. Declaração de Práticas de Certificação
CRL (ou também LRC)	*Lista de Revogação de Certificados.* Lista de certificados revogados
DN	*Nome distinto.* Nome distintivo dentro do certificado digital
DNI	Documento Nacional de Identidade
ETSI EN	*Instituto Europeu de Normas de Telecomunicações – Norma Europeia.*
EV (para SSL)	*Validação Alargada* Validação alargada, em certificados SSL.
FIPS	*Publicação da Norma Federal de Processamento de Informação*
HSM	*Módulo de* Segurança de Hardware
IETF	*Força-Tarefa de Engenharia de Internet*
NIF	Número de Identificação Fiscal
NTP	*Protocolo* de Tempo de Rede
OCSP	*Protocolo de Estado de Certificado Online.* Protocolo de Acesso ao Estado do Certificado
OID	*Identificador de* objeto. Identificador de Objeto
PDS	*Declarações de Divulgação da PKI* .
PIN	*Número de identificação pessoal*. Número de Identificação Pessoal

PKI	*Infraestrutura de Chave Pública*. Infraestrutura de Chave Pública
QSCD (ou também DCCF)	*Dispositivo Qualificado de Criação de Assinatura/Selos Eletrónicos.* Dispositivo qualificado para criação de assinaturas/carimbos
QCP	*Política de Certificados Qualificados Política* de Certificados Qualificados
QCP-n	*Política de Certificado Qualificado - Pessoa Física Política de Certificado Qualificado* para pessoas físicas.
QCP-l	*Política de Certificado Qualificado - Pessoa Jurídica Política de Certificado Qualificado* para Entidades Jurídicas.
QCP-n-qscd	*Política de Certificado Qualificado - Pessoa Física - QSCD Política de Certificado Qualificado* para Pessoas Físicas em Dispositivo de Assinatura/Selo Qualificado
QCP-l-qscd	*Política de Certificado Qualificado - Pessoa Jurídica - QSCD Política de Certificado Qualificado* para Pessoas Jurídicas com Dispositivo de Assinatura/Selo Qualificado
RFC	*Pedido de Comentários* Documento RFC
RSA	Rivest-Shamir-Adleman. Tipo de algoritmo de encriptação
SHA	*Algoritmo de Hash Seguro.* Algoritmo de Hashing Seguro
SSL	*Camada de Soquetes Seguros.* Um protocolo concebido pela Netscape e transformado num padrão de rede, permite a transmissão de informação encriptada entre um navegador de Internet e um servidor.
TCP/IP	*Controlo de Transmissão. Protocolo/Protocolo de Internet*. Sistema de protocolos, definidos no âmbito

	do IEFT.
TSA	*Autoridade de Carimbo Temporal* Autoridade Eletrónica de Carimbo de Hora
TSU	*Unidade de Marcação Temporal* Unidade de carimbo temporal.
UTC	*Tempo* Universal Coordenado
VPN	*Rede Privada Virtual.* Rede Privada Virtual

1.6.2 Definições

Autoridade Certificadora	*É a entidade responsável pela emissão e gestão de certificados digitais.*
Autoridade de Registo	*Entidade responsável pela gestão das candidaturas, identificação e registo dos candidatos a certificados. Podes fazer parte da Autoridade de Certificação ou ser um outsider.*
Certificado	*Ficheiro que associa a chave pública a alguns dados identificativos do Sujeito/Signatário e é assinado pela CA.*
Chave Pública	*Um valor matemático publicamente conhecido e utilizado para a verificação de uma assinatura digital ou para a encriptação de dados.*
Chave Privada	*Valor matemático conhecido apenas pelo Sujeito/Signatário e usado para a criação de uma assinatura digital ou para a desencriptação de dados.* *A chave privada da CA será usada para assinatura de certificados e CRL.* *A chave privada do serviço TSA será usada para assinar os carimbos temporais.*
CPS	*Um conjunto de práticas adotadas por uma Autoridade de Certificação para a emissão de certificados de acordo com uma política específica de certificação.*
CRL	*Um ficheiro que contém uma lista de certificados que foram revogados num determinado período de tempo e que é assinado pela CA.*
Dados de Ativação	*Dados privados, como PINs ou palavras-passe usados para ativar a chave privada*
DCCF	*Dispositivo qualificado para criação de assinaturas. Elemento de software ou hardware, devidamente certificado, utilizado pelo Sujeito/Signatário para a geração de assinaturas eletrónicas, de modo a que operações criptográficas sejam realizadas dentro do dispositivo e o seu controlo seja garantido apenas pelo Sujeito/Signatário.*
Assinatura digital	*O resultado da transformação de uma mensagem, ou de qualquer tipo de dado, pela aplicação da chave privada em*

	conjunto com algoritmos conhecidos, garantindo assim: *a) que os dados não foram modificados (completude)* *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 repudiação na origem)*
OID	*Identificador numérico único registado sob a normalização ISO e referindo-se a um objeto ou classe específica de objetos.*
Par de chaves	*Um conjunto formado pela chave pública e privada, ambas matematicamente relacionadas entre si.*
PKI	*Um conjunto de hardware, software, recursos humanos, procedimentos, etc., que compõem um sistema baseado na criação e gestão de certificados de chave pública.*
Requerente	*No contexto deste documento, o requerente será uma pessoa física autorizada com uma procuração especial para realizar determinados procedimentos em nome e representação da entidade.*
Assinante	*No contexto deste documento, a entidade legal que detém o certificado (ao nível da empresa)*
Sujeito/Signatário	*No contexto deste documento, a pessoa física cuja chave pública é certificada pela CA e tem, ou tem acesso exclusivo a, uma chave privada válida para gerar assinaturas digitais.*
Partido do Utilizador	*No contexto deste documento, uma pessoa que confia voluntariamente no certificado digital e utiliza-o como meio de acreditar a autenticidade e integridade do documento assinado*

2. Publicação de informações e depósito de certificados

2.1 Depósito do certificado

A esFIRMA possui um Depósito de Certificados, no qual são publicadas informações relativas a serviços de certificação:

https://www.esfirma.com

Este serviço está disponível 24 horas por dia, 7 dias por semana, e, no caso de uma falha do sistema fora do controlo da esFIRMA, a esFIRMA fará os seus melhores esforços para tornar o serviço novamente disponível dentro do prazo estabelecido na secção 5.7.4 desta Declaração de Práticas de Certificação.

2.2 Publicação de informações de certificação

A esFIRMA publica as seguintes informações no seu Depósito:

- Listas de certificados revogados e outras informações sobre o estado da revogação de certificados.
- As políticas de certificados aplicáveis.
- A Declaração de Práticas de Certificação.
- Declarações de Divulgação da PKI (PDS), pelo menos em espanhol e inglês.

2.3 Frequência de publicação

A informação sobre os fornecedores de serviços de certificação, incluindo políticas e a Declaração de Práticas de Certificação, é publicada assim que estiver disponível.

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

A informação sobre o estado de revogação de certificados é publicada de acordo com as secções 4.9.7 e 4.9.8 desta Declaração de Práticas de Certificação.

2.4 Controlo de Acesso

O esFIRMA não limita o acesso de leitura à informação referida na secção 2.2, mas estabelece controlos para impedir que pessoas não autorizadas adicionem, modifiquem ou eliminem registos do Depósito, para proteger a integridade e autenticidade da informação, especialmente do estado de revogação.

A esFIRMA utiliza sistemas fiáveis para o Depósito, de modo que:

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

3. Identificação e autenticação

3.1 Registo inicial

3.1.1 Tipos de nomes

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

Os nomes contidos nos certificados são os seguintes.

3.1.1.1 Certificado de assinatura do funcionário público, de alto nível, no cartão

País (C)	"É"
Organização (O)	Nome ("nome oficial") da Administração, entidade, entidade de direito público ou outra entidade que subscreve o certificado ao qual o trabalhador está ligado
NomeUnidadeOrganizacional (OU)	CERTIFICADO ELETRÓNICO DE FUNCIONÁRIO PÚBLICO
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Apelido	Primeiro e segundo apelido (opcional), de acordo com o documento de identidade (DNI/Passaporte)
Nome próprio	Primeiro nome, de acordo com o documento de identidade (DNI/Passaporte)
Número de Série	DNI/NIE do funcionário
Nome Comum (CN)	Nome Apelido1 Apelido2 – NIF do Funcionário
Tipo de certificadoOID: 2.16.724.1.3.5.7.1.1	CERTIFICADO QUALIFICADO DE ASSINATURA DE ALTO FUNCIONÁRIO PÚBLICO
Nome da entidade subscritorOID: 2.16.724.1.3.5.7.1.2	Nome da entidade subscritora
NIF de subscritor OID: 2.16.724.1.3.5.7.1.3	Subscrição da entidade NIF
DNI/NIE da pessoa responsável OID: 2.16.724.1.3.5.7.1.4	DNI ou NIE da pessoa responsável

Nome da Bateria OID: 2.16.724.1.3.5.7.1.6	Primeiro nome do mantenedor do certificado
Primeiro apelido OID: 2.16.724.1.3.5.7.1.7	Primeiro apelido da pessoa responsável pelo certificado
Segundo apelido OID: 2.16.724.1.3.5.7.1.8	Segundo apelido da pessoa responsável pelo certificado. Opcional.
Email OID: 2.16.724.1.3.5.7.1.9	Email da pessoa responsável pelo certificado. Opcional.

3.1.1.2 Certificado de assinatura do funcionário público, nível intermédio, no HSM

País (C)	"É"
Organização (O)	Nome ("nome oficial") da Administração, órgão ou entidade de direito público que subscreve o certificado ao qual o trabalhador está ligado
NomeUnidadeOrganizacional (OU)	CERTIFICADO ELETRÓNICO DE FUNCIONÁRIO PÚBLICO
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Apelido	Primeiro e segundo apelido (opcional), de acordo com o documento de identidade (DNI/Passaporte)
Nome próprio	Primeiro nome, de acordo com o documento de identidade (DNI/Passaporte)
Número de Série	DNI/NIE do funcionário
Nome Comum (CN)	Nome Apelido1 Apelido2 – NIF do Funcionário
Tipo de certificadoOID: 2.16.724.1.3.5.7.2.1	CERTIFICADO ELETRÓNICO DE FUNCIONÁRIO PÚBLICO DE NÍVEL INTERMÉDIO
Nome da entidade subscritorOID: 2.16.724.1.3.5.7.2.2	Nome da entidade subscritora
Entidade assinante NIFOID: 2.16.724.1.3.5.7.2.3	Entidade subscritora da NIF
DNI/NIE da pessoa responsável OID: 2.16.724.1.3.5.7.2.4	DNI ou NIE da pessoa responsável
Número de Autenticação Pessoal do OID: 2.16.724.1.3.5.7.2.5	NRP ou PIN do Mantenedor do Assinante do Certificado
Nome da Bateria OID: 2.16.724.1.3.5.7.2.6	Primeiro nome do mantenedor do certificado

Primeiro apelido OID: 2.16.724.1.3.5.7.2.7	Primeiro apelido da pessoa responsável pelo certificado
Segundo apelido OID: 2.16.724.1.3.5.7.2.8	Segundo apelido da pessoa responsável pelo certificado. Opcional.
Email OID: 2.16.724.1.3.5.7.2.9	Email da pessoa responsável pelo certificado. Opcional.

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

País (C)	"É"
Organização (O)	Nome ("nome oficial") da Administração, entidade, entidade de direito público ou outra entidade que subscreve o certificado ao qual o trabalhador está ligado
NomeUnidadeOrganizacional (OU)	CERTIFICADO ELETRÓNICO DE FUNCIONÁRIO PÚBLICO
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Apelido	Primeiro e segundo apelido (opcional), de acordo com o documento de identidade (DNI/Passaporte)
Nome próprio	Primeiro nome, de acordo com o documento de identidade (DNI/Passaporte)
Número de Série	DNI/NIE do funcionário
Nome Comum (CN)	Nome Apelido1 Apelido2 – NIF do Funcionário
Tipo de certificadoOID: 2.16.724.1.3.5.7.1.1	CERTIFICADO ELETRÓNICO DE FUNCIONÁRIO PÚBLICO COM UM ELEVADO NÍVEL DE AUTENTICAÇÃO
Nome da entidade subscritorOID: 2.16.724.1.3.5.7.1.2	Nome da entidade subscritora
NIF de subscritor OID: 2.16.724.1.3.5.7.1.3	Subscrição da entidade NIF
DNI/NIE da pessoa responsável OID: 2.16.724.1.3.5.7.1.4	DNI ou NIE da pessoa responsável
Nome da Bateria OID: 2.16.724.1.3.5.7.1.6	Primeiro nome do mantenedor do certificado
Primeiro apelido OID: 2.16.724.1.3.5.7.1.7	Primeiro apelido da pessoa responsável pelo certificado
Segundo apelido OID: 2.16.724.1.3.5.7.1.8	Segundo apelido da pessoa responsável pelo certificado. Opcional.
Email OID: 2.16.724.1.3.5.7.1.9	Email da pessoa responsável pelo certificado. Opcional.

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

País (C)	"É"
Organização (O)	Nome do assinante (nome "oficial")
NomeUnidadeOrganizacional (OU)	SELO ELETRÓNICO
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Número de Série	DNI/NIE da organização subscritora
Nome Comum (CN)	Nomeação do sistema ou aplicação de um processo automático.
Tipo de certificadoOID: 2.16.724.1.3.5.6.2.1	SELO ELETRÓNICO DE NÍVEL INTERMÉDIO
Nome da entidade subscritora OID: 2.16.724.1.3.5.6.2.2	Nome da entidade subscritora
Entidade assinante NIF, OID: 2.16.724.1.3.5.6.2.3	Entidade subscritora da NIF
Nome do sistemaOID: 2.16.724.1.3.5.6.2.5	Nome do sistema
Email OID: 2.16.724.1.3.5.6.2.9	Email da pessoa responsável pelo selo

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

País (C)	"É"
Organização (O)	Nome do assinante (nome "oficial")
NomeUnidadeOrganizacional (OU)	SELO ELETRÓNICO
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Número de Série	DNI/NIE da organização subscritora
Nome Comum (CN)	Nomeação do sistema ou aplicação de um processo automático.
Tipo de certificadoOID: 2.16.724.1.3.5.6.2.1	SELO ELETRÓNICO DE NÍVEL INTERMÉDIO
Nome da entidade subscritora OID: 2.16.724.1.3.5.6.2.2	Nome da entidade subscritora
Entidade assinante NIF, OID: 2.16.724.1.3.5.6.2.3	Entidade subscritora da NIF
Nome do sistemaOID: 2.16.724.1.3.5.6.2.5	Nome do sistema

3.1.1.6 Certificado de assinatura de funcionário público com pseudónimo, de alto nível, num cartão

País (C)	"É"
Organização (O)	Nome ("nome oficial") da Administração, órgão ou entidade de direito público que subscreve o certificado ao qual o trabalhador está ligado
NomeUnidadeOrganizacional (OU)	CERTIFICADO ELETRÓNICO DE FUNCIONÁRIO PÚBLICO COM PSEUDÓNIMO
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Pseudónimo	Pseudónimo obrigatório segundo ETSI EN 319 412-2 para este tipo de certificado
Nome Comum (CN)	Pseudónimo e a Agência
Tipo de certificadoOID: 2.16.724.1.3.5.4.1.1	CERTIFICADO ELETRÓNICO DE FUNCIONÁRIO PÚBLICO COM PSEUDÓNIMO DE ALTO NÍVEL
Nome da entidade subscritorOID: 2.16.724.1.3.5.4.1.2	Nome da entidade subscritora
Entidade subscritora do NIF, OID: 2.16.724.1.3.5.4.1.3	Entidade subscritora da NIF
Pseudónimo OID: 2.16.724.1.3.5.4.1.12	Pseudónimo usado pelo signatário e autorizado pelo assinante

3.1.1.7 Certificado de assinatura do funcionário público com pseudónimo, nível intermédio, no HSM

País (C)	"É"
Organização (O)	Nome ("nome oficial") da Administração, órgão ou entidade de direito público que subscreve o certificado ao qual o trabalhador está ligado
NomeUnidadeOrganizacional (OU)	CERTIFICADO ELETRÓNICO DE FUNCIONÁRIO PÚBLICO COM PSEUDÓNIMO
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Pseudónimo	Pseudónimo obrigatório segundo ETSI EN 319 412-2 para este tipo de certificado
Nome Comum (CN)	Pseudónimo e a Agência

Tipo de certificadoOID: 2.16.724.1.3.5.4.2.1	CERTIFICADO ELETRÓNICO DE FUNCIONÁRIO PÚBLICO COM PSEUDÓNIMO INTERMÉDIO
Nome da entidade subscritora OID: 2.16.724.1.3.5.4.2.2	Nome da entidade subscritora
Entidade subscritora NIF OID: 2.16.724.1.3.5.4.2.3	Entidade subscritora da NIF
Pseudónimo OID: 2.16.724.1.3.5.4.2.12	Pseudónimo usado pelo signatário e autorizado pelo assinante

3.1.1.8 Certificado de autenticação de funcionário público, com pseudónimo, de alto nível, no cartão

País (C)	"É"
Organização (O)	Nome ("nome oficial") da Administração, entidade, entidade de direito público ou outra entidade que subscreve o certificado ao qual o trabalhador está ligado
NomeUnidadeOrganizacional (OU)	CERTIFICADO ELETRÓNICO DE FUNCIONÁRIO PÚBLICO
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Pseudónimo	Pseudónimo obrigatório segundo ETSI EN 319 412-2
Nome Comum (CN)	Cargo ou posição ou "PSEUDÓNIMO" – NÚMERO DE IDENTIFICAÇÃO – NOME OFICIAL DA ORGANIZAÇÃO
Tipo de certificadoOID: 2.16.724.1.3.5.4.1.1	CERTIFICADO DE AUTENTICAÇÃO DE FUNCIONÁRIO PÚBLICO COM PSEUDÓNIMO
Nome da entidade subscritorOID: 2.16.724.1.3.5.4.1.2	Nome da entidade subscritora
Entidade subscritora do NIF, OID: 2.16.724.1.3.5.4.1.3	Entidade subscritora da NIF

3.1.1.9 Certificado de Selo Eletrónico TSA/TSU

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

3.1.1.10 Certificado de assinatura de pessoa física relacionada, num cartão

Subperfil de Espanha:

País (C)	"É"
Organização (O)	Nome ("nome oficial") da entidade que subscreve o certificado ao qual o trabalhador está ligado
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Apelido	Primeiro e segundo apelido (opcional), de acordo com o documento de identidade (DNI/Passaporte)
Nome próprio	Primeiro nome, de acordo com o documento de identidade (DNI/Passaporte)
Número de Série	DNI/NIE do indivíduo
Nome Comum (CN)	Apelido1 Apelido2 Nome – NIF pessoa natural (ASSINATURA)
Tipo de Certificado OID : 1.3.6.1.4.1.47281.0.7.1	CERTIFICADO DE PESSOA FÍSICA LIGADA À ENTIDADE
Nome da entidade subscritora OID: 1.3.6.1.4.1.47281.0.7.2	Nome da entidade subscritora
Assinante NIF OID: 1.3.6.1.4.1.47281.0.7.3	Subscrição da entidade NIF
DNI/NIE da pessoa responsável OID : 1.3.6.1.4.1.47281.0.7.4	DNI ou NIE da pessoa responsável
Nome da Bateria OID: 1.3.6.1.4.1.47281.0.7.6	Primeiro nome do mantenedor do certificado
Primeiro apelido OID: 1.3.6.1.4.1.47281.0.7.7	Primeiro apelido da pessoa responsável pelo certificado
Segundo apelido OID: 1.3.6.1.4.1.47281.0.7.8	Segundo apelido da pessoa responsável pelo certificado. Opcional.
Email OID: 1.3.6.1.4.1.47281.0.7.9	Email da pessoa responsável pelo certificado. Opcional.

Subperfil da Europa:

País (C)	País
Organização (O)	Nome ("nome oficial") da entidade que subscreve o certificado ao qual o trabalhador está ligado
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1

Apelido	Primeiro e segundo apelido (opcional), de acordo com o documento de identidade
Nome próprio	Primeiro nome, segundo o documento de identidade
Número de Série	Número do documento de identidade da pessoa física
Nome Comum (CN)	Apelido1 Apelido2 Primeiro Nome – número do documento (ASSINATURA)
Tipo de Certificado OID : 1.3.6.1.4.1.47281.0.19.1	PV
Nome da entidade subscritora OID: 1.3.6.1.4.1.47281.0.19.2	Corresponde à organização do sujeito
Identificador da Entidade de Subscrição OID : 1.3.6.1.4.1.47281.0.19.3	Corresponde ao identificador organizacional do sujeito
ID do Controlador OID : 1.3.6.1.4.1.47281.0.19.4	DNI ou NIE da pessoa responsável
Nome da Bateria OID: 1.3.6.1.4.1.47281.0.19.6	Primeiro nome do mantenedor do certificado
Primeiro apelido OID: 1.3.6.1.4.1.47281.0.19.7	Primeiro apelido da pessoa responsável pelo certificado
Apelido do Meio OID: 1.3.6.1.4.1.47281.0.19.8	Segundo apelido da pessoa responsável pelo certificado. Opcional.
Unidade da entidade subscritora OID: 1.3.6.1.4.1.47281.0.19.10	Corresponde à Unidade de Organização do sujeito. Opcional

3.1.1.11 Certificado de assinatura de pessoa física relacionada, no HSM

Subperfil de Espanha:

País (C)	"É"
Organização (O)	Nome ("nome oficial") da entidade subscritora, à qual o colaborador está ligado
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Apelido	Primeiro e segundo apelido (opcional), de acordo com o documento de identidade (DNI/Passaporte)

Nome próprio	Primeiro nome, de acordo com o documento de identidade (DNI/Passaporte)
Número de Série	DNI/NIE do funcionário
Nome Comum (CN)	Apelido1 Apelido2 Primeiro Nome – NIF pessoa natural
Tipo de Certificado OID : 1.3.6.1.4.1.47281.0.7.1	CERTIFICADO DE PESSOA FÍSICA LIGADA À ENTIDADE
Nome da entidade subscritora OID: 1.3.6.1.4.1.47281.0.7.2	Nome da entidade subscritora
Assinante NIF OID: 1.3.6.1.4.1.47281.0.7.3	Subscrição da entidade NIF
DNI/NIE da pessoa responsável OID : 1.3.6.1.4.1.47281.0.7.4	DNI ou NIE da pessoa responsável
Nome da Bateria OID: 1.3.6.1.4.1.47281.0.7.6	Primeiro nome do mantenedor do certificado
Primeiro apelido OID: 1.3.6.1.4.1.47281.0.7.7	Primeiro apelido da pessoa responsável pelo certificado
Segundo apelido OID: 1.3.6.1.4.1.47281.0.7.8	Segundo apelido da pessoa responsável pelo certificado. Opcional.
Email OID: 1.3.6.1.4.1.47281.0.7.9	Email da pessoa responsável pelo certificado. Opcional.

Subperfil da Europa:

País (C)	País
Organização (O)	Nome ("nome oficial") da entidade que subscreve o certificado ao qual o trabalhador está ligado
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Apelido	Primeiro e segundo apelido (opcional), de acordo com o documento de identidade
Nome próprio	Primeiro nome, segundo o documento de identidade
Número de Série	Número do documento de identidade da pessoa física
Nome Comum (CN)	Apelido1 Apelido2 Primeiro Nome – número do documento
Nome da Bateria OID: 1.3.6.1.4.1.47281.0.19.6	O Primeiro Nome do Mantenedor do Certificado corresponde ao Nome Próprio
Primeiro apelido OID: 1.3.6.1.4.1.47281.0.19.7	Primeiro apelido da pessoa responsável pelo certificado

Apelido do Meio OID: 1.3.6.1.4.1.47281.0.19.8	Segundo apelido da pessoa responsável pelo certificado. Opcional.

3.1.1.12 Certificado de autenticação da pessoa física ligada, no cartão

Subperfil de Espanha:

País (C)	"É"
Organização (O)	Nome ("nome oficial") da entidade que subscreve o certificado ao qual o trabalhador está ligado
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Apelido	Primeiro e segundo apelido (opcional), de acordo com o documento de identidade (DNI/Passaporte)
Nome próprio	Primeiro nome, de acordo com o documento de identidade (DNI/Passaporte)
Número de Série	DNI/NIE do funcionário
Nome Comum (CN)	Apelido1 Apelido2 Nome – NIF pessoa física (AUTENTICAÇÃO)
Tipo de Certificado OID : 1.3.6.1.4.1.47281.0.7.1	CERTIFICADO DE PESSOA FÍSICA LIGADA À ENTIDADE
Nome da entidade subscritora OID: 1.3.6.1.4.1.47281.0.7.2	Nome da entidade subscritora
Assinante NIF OID: 1.3.6.1.4.1.47281.0.7.3	Subscrição da entidade NIF
DNI/NIE da pessoa responsável OID : 1.3.6.1.4.1.47281.0.7.4	Corresponde ao Número de Série do sujeito
Nome da Bateria OID: 1.3.6.1.4.1.47281.0.7.6	Primeiro nome do mantenedor do certificado
Primeiro apelido OID: 1.3.6.1.4.1.47281.0.7.7	Primeiro apelido da pessoa responsável pelo certificado
Segundo apelido OID: 1.3.6.1.4.1.47281.0.7.8	Segundo apelido da pessoa responsável pelo certificado. Opcional.
Email OID: 1.3.6.1.4.1.47281.0.7.9	Email da pessoa responsável pelo certificado. Opcional.

Subperfil da Europa:

País (C)	País
Organização (O)	Nome ("nome oficial") da entidade que subscreve o certificado ao qual o trabalhador está ligado
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Apelido	Primeiro e segundo apelido (opcional), de acordo com o documento de identidade
Nome próprio	Primeiro nome, segundo o documento de identidade
Número de Série	Número do documento de identidade da pessoa física
Nome Comum (CN)	Apelido1 Apelido2 Primeiro Nome – número do documento (AUTENTICAÇÃO)
Nome da Bateria OID: 1.3.6.1.4.1.47281.0.19.6	O Primeiro Nome do Mantenedor do Certificado corresponde ao Nome Próprio
Primeiro apelido OID: 1.3.6.1.4.1.47281.0.19.7	Primeiro apelido da pessoa responsável pelo certificado
Apelido do Meio OID: 1.3.6.1.4.1.47281.0.19.8	Segundo apelido da pessoa responsável pelo certificado. Opcional.

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

Subperfil de Espanha:

País (C)	"É"
Organização (O)	Nome ("nome oficial") da entidade que subscreve o certificado ao qual o trabalhador está ligado
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Pseudónimo	Pseudónimo obrigatório segundo ETSI EN 319 412-2
Nome Comum (CN)	Posição ou "PSEUDÓNIMO" – NÚMERO DE IDENTIFICAÇÃO – NOME DA ENTIDADE

Subperfil da Europa:

País (C)	País
Organização (O)	Nome ("nome oficial") da entidade que subscreve o certificado ao qual o trabalhador está ligado
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Pseudónimo	Pseudónimo obrigatório segundo ETSI EN 319 412-2

Nome Comum (CN)	PSEUDÓNIMO - NOME DA ENTIDADE

3.1.1.14 Certificado de assinatura de pessoa física relacionada, na HSM

Subperfil de Espanha:

País (C)	"É"
Organização (O)	Nome ("nome oficial") da entidade subscritora, à qual o colaborador está ligado
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Pseudónimo	Pseudónimo obrigatório segundo ETSI EN 319 412-2
Nome Comum (CN)	Posição ou "PSEUDÓNIMO" – NÚMERO DE IDENTIFICAÇÃO – NOME DA ENTIDADE

Subperfil da Europa:

País (C)	País
Organização (O)	Nome ("nome oficial") da entidade que subscreve o certificado ao qual o trabalhador está ligado
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Pseudónimo	Pseudónimo obrigatório segundo ETSI EN 319 412-2
Nome Comum (CN)	PSEUDÓNIMO - NOME DA ENTIDADE

3.1.1.15 Certificado de autenticação de uma pessoa física ligada, em cartão, com pseudónimo

Subperfil de Espanha:

País (C)	"É"
Organização (O)	Nome ("nome oficial") da entidade que subscreve o certificado ao qual o trabalhador está ligado
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Nome Comum (CN)	Posição ou "PSEUDÓNIMO" – NÚMERO DE IDENTIFICAÇÃO – NOME DA ENTIDADE

Subperfil da Europa:

País (C)	País
Organização (O)	Nome ("nome oficial") da entidade que subscreve o certificado ao qual o trabalhador está ligado

IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Pseudónimo	Pseudónimo obrigatório segundo ETSI EN 319 412-2
Nome Comum (CN)	PSEUDÓNIMO - NOME DA ENTIDADE

3.1.1.16 Certificado de selo eletrónico, em software

Subperfil de Espanha:

País (C)	"É"
Organização (O)	Nome do assinante (nome "oficial")
NomeUnidadeOrganizacional (OU)	SELO ELETRÓNICO
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Número de Série	DNI/NIE da organização subscritora
Nome Comum (CN)	Nomeação do sistema ou aplicação de um processo automático.

Subperfil da Europa:

País (C)	País
Organização (O)	Nome do assinante (nome "oficial")
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Número de Série	Subscrever a Identificação da Organização (legalPersonSemanticsIdentifier)

3.1.1.17 Certificado eletrónico de selo com gestão centralizada

Subperfil de Espanha:

País (C)	"É"
Organização (O)	Nome do assinante (nome "oficial")
NomeUnidadeOrganizacional (OU)	SELO ELETRÓNICO
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Número de Série	DNI/NIE da organização subscritora
Nome Comum (CN)	Nomeação do sistema ou aplicação de um processo automático.

Subperfil da Europa:

País (C)	País
Organização (O)	Nome do assinante (nome "oficial")
IdentificadorOrganizacional	Identificador da organização de acordo com a norma técnica ETSI EN 319 412-1
Número de Série	Subscrever a Identificação da Organização (legalPersonSemanticsIdentifier)

3.1.2. Significado dos nomes

Os nomes contidos nos campos *StemName* e *SubjectAlternativeName* dos certificados são compreensíveis em linguagem natural, conforme referido na secção anterior.

3.1.3 Uso de anónimos e pseudónimos

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

3.1.4 Interpretação dos Formatos dos Nomes

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

O campo "país" será sempre Espanha porque os certificados são emitidos exclusivamente às Administrações Públicas Espanholas.

O certificado demonstra a relação entre uma pessoa física e a Administração, entidade, entidade de direito público ou outra entidade com a qual está ligada, independentemente da nacionalidade da pessoa física. Isto deriva da natureza corporativa do certificado, do qual a sociedade é assinante, e da pessoa física vinculada à pessoa autorizada a utilizá-lo.

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

3.1.5 Unicidade dos nomes

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

Um nome de assinante que já foi utilizado não pode ser atribuído a outro assinante, uma situação que, em princípio, não tem de ocorrer, graças à presença do Número de Identificação Fiscal, ou equivalente, no esquema de nomenclatura.

Um assinante pode solicitar mais do que um certificado desde que a combinação dos seguintes valores no pedido 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 assinante.
- Tipo de Certificado (Campo de Descrição do Certificado).

3.1.6 Resolução de disputas de nomeação

Os requerentes de certificados não incluirão nomes em candidaturas que possam infringir os direitos de terceiros por parte do futuro subscritor.

A esFIRMA não será obrigada a determinar antecipadamente que um requerente de certificado tem direitos de propriedade industrial sobre o nome que consta numa candidatura de certificação, mas em princípio procederá à sua certificação.

E não atuará como árbitro ou mediador, nem resolverá qualquer litígio relativo à propriedade de nomes de pessoas ou organizações, nomes de domínio, marcas registadas ou nomes comerciais.

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

Em todo o caso, o prestador do serviço de certificação reserva-se o direito de rejeitar uma candidatura de certificado devido a um conflito de nome.

Qualquer controvérsia ou conflito decorrente deste documento será definitivamente resolvido por arbitragem por lei de um árbitro, no âmbito do Tribunal de Arbitragem de Espanha, de acordo com as suas Regras e Estatutos, que é incumbido da administração da arbitragem e da nomeação do árbitro ou tribunal arbitral. As partes declaram o seu compromisso em cumprir a decisão emitida no documento contratual que formaliza o serviço.

3.2 Validação inicial de identidade

A identidade dos subscritores do certificado é estabelecida no momento da assinatura do contrato entre a esFIRMA e o assinante ou antes da ativação do serviço esFIRMA, altura em que a existência do assinante é verificada e a documentação fornecida justificando a sua identidade, a posição e/ou condição em que assina e a sua morada, de acordo com as disposições do regulamento administrativo aplicável.

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

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

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

3.2.1 Prova de Posse de Chave Privada

A posse da chave privada é demonstrada através do procedimento fiável de entrega e aceitação do certificado pelo signatário da Plataforma de Administração Eletrónica, ao assinar a folha de aceitação, e da sua utilização nessa plataforma.

3.2.2 Identificação da entidade

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

A EsFIRMA verifica a existência de cada Administração Pública, órgão ou entidade ao abrigo do direito público, quando necessário, antes do inventário das entidades do setor público do Ministério das Finanças e Funções Públicas em https://www.hacienda.gob.es/es-ES/CDI/Paginas/Inventario/Inventario.aspx, perante um Diário Oficial do seu âmbito ou através da integração com o Sistema Comum de Diretórios (DIR3).

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

Indivíduos com capacidade para agir em nome de uma Administração, órgão, entidade de direito público ou outra entidade subscritora dos certificados podem atuar como representantes da mesma em relação às disposições deste DPC, desde que exista uma situação prévia de representação legal ou voluntária entre a pessoa física e a Administração. entidade, entidade de direito público ou outra entidade subscritora dos certificados, que requer o seu reconhecimento pela esFIRMA, o que será realizado através de um dos seguintes procedimentos:

1. No caso de a pessoa que ocupa o cargo de Secretário ter poder de fé pública, serão recolhidos e verificados os seguintes documentos:
    a. Certificado do Secretário nomeando o representante legal, com as seguintes informações:
        i. Nome e apelido do representante legal
        ii. Documento: NIF do representante
        iii. CIF da entidade que representa
        iv. Nome da entidade que representa
        v. Endereço postal da entidade que representa

2. No caso de a pessoa que ocupa o cargo de Secretário não ter poder de fé pública, serão recolhidos e verificados os seguintes documentos:
    a. Um certificado do Secretário da nomeação do representante legal contendo as seguintes informações:
        i. Detalhes representativos:
            1. Nome e apelido do representante legal
            2. Documento: NIF do representante
        ii. Detalhes da entidade que representa:
            1. CIF
            2. Nome
            3. Endereço postal
        iii. Informação sobre a validade da representação
    b. Documentação oficial que permita acreditar os dados relativos à representação ou capacidade de atuação detida pelo representante legal.
    c. Todos os documentos necessários para provar os pontos acima referidos de forma fiável, de acordo com as disposições dos regulamentos administrativos aplicáveis, e o seu registo no respetivo registo público, se necessário.

Após a verificação da documentação recolhida, o Representante Legal prosseguirá à assinatura do contrato de prestação de serviços de certificação entre a esFIRMA (ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA) e a entidade através da qual são reguladas as condições sob as quais a ESFIRMA prestará os serviços de certificação à entidade, constituída como Autoridade de Registo. nomeando os Operadores autorizados a exercer as funções correspondentes à RA.

Uma vez que os documentos tenham sido assinados eletronicamente, as funções de RA serão ativadas para os utilizadores da entidade que estejam listados no contrato como operadores autorizados a desempenhar esta função.

3.2.3 Autenticação da identidade de uma pessoa natural

Esta secção descreve os métodos para verificar a identidade de uma pessoa física identificada num certificado.

O procedimento de solicitação e geração de certificados é realizado através de um procedimento eletrónico na Plataforma de Administração Eletrónica disponível para o assinante e os signatários.

O procedimento eletrónico para a emissão de um certificado a uma pessoa física seguirá os seguintes passos e serão gerados os seguintes documentos:

1. Candidatura pelo indivíduo através da Plataforma Eletrónica de Administração (com o respetivo registo de entrada e abertura do ficheiro).
2. Um certificado em que o Operador de Verificação certifica a ligação entre o requerente e a entidade.
3. Ordem de emissão assinada pelo Operador de Verificação e Autorização da entidade, registada na saída e notificada à ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (anexando uma cópia do certificado e o pedido do utilizador).

O procedimento eletrónico para a emissão de um certificado de selo eletrónico seguirá os seguintes passos e serão gerados os seguintes documentos:

1. Ordem de emissão do Representante Legal através da Plataforma Eletrónica de Administração (com o respetivo registo de entrada e abertura do processo). Para apresentar tal pedido, o Representante Legal deve identificar-se na plataforma utilizando meios eletrónicos de identificação, para os quais a presença da pessoa física está garantida de acordo com o Artigo 8.º do Regulamento eIDAS relativamente aos níveis de segurança "substanciais" ou "elevados".

3.2.3.1 Em certificados

A informação de identificação das pessoas físicas identificadas nos certificados é validada comparando a informação da candidatura da Administração, entidade, entidade de direito público ou outra entidade subscritora dos certificados, com os registos da Administração, entidade, entidade de direito público ou outra entidade a que está ligada, gerados conforme indicado no ponto 3.2 deste DPC, garantir a correção da informação a certificar.

3.2.3.2 Necessidade de presença pessoal

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

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

O certificado deve ser emitido no prazo máximo de 15 dias civis a contar da validação da identidade da pessoa física pelo operador de verificação e autorização. Assim, se decorrerem 15 dias corridos desde que o operador de verificação e autorização validou a identidade do requerente e ordenou a emissão, o requerente não aceitar o certificado, o processo expirará e o indivíduo terá de apresentar um novo pedido.

3.2.3.3 Relação da pessoa física

A justificação documental da ligação de uma pessoa física identificada num certificado com a Administração, entidade, entidade de direito público ou outra entidade é dada pelo seu registo nos Registos de Pessoal da Administração, entidade, entidade de direito público ou outra entidade à qual a pessoa física está ligada.

3.2.4 Informação não verificada do assinante

A esFIRMA não inclui qualquer informação não verificada dos assinantes nos certificados.

3.2.5 Critérios de interoperabilidade

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

A esFIRMA não emite certificados de CA subordinados a terceiros e a sua CA emissora não é tecnicamente limitada.

3.3 Identificação e autenticação de pedidos de renovação

3.3.1 Validação para renovação rotineira de certificados

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

3.3.2 Identificação e Autenticação da Renovação após a Revogação

A esFIRMA não renova certificados.

3.4 Identificação e autenticação do pedido de revogação

Os pedidos e relatórios relativos à revogação de um certificado são autênticos, verificando que provêm de uma pessoa autorizada.
Os métodos aceitáveis para tais testes são os seguintes:

- O envio de um pedido de revogação pelo assinante ou pela pessoa física identificada no certificado, assinado eletronicamente.
- A utilização da "frase de verificação de identidade", ou outros métodos pessoais de autenticação, que consistem em informações conhecidas apenas pela pessoa física identificada no certificado, e que permitem revogar automaticamente o seu certificado.

- Aparência física num escritório da entidade subscritora.
- Outros meios de comunicação, como o telefone, quando existem garantias razoáveis da identidade do requerente à revogação, na opinião da esFIRMA.

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

4. Requisitos de Operação do Ciclo de Vida do Certificado

4.1 Candidatura ao Certificado

4.1.1 Legitimidade para solicitar a emissão

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

Da mesma forma, antes da emissão e entrega de um certificado, existe um pedido de certificados num formulário de pedido de certificado através da Plataforma de Administração Eletrónica.

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

4.1.2 Procedimento de registo e responsabilidades

A esFIRMA recebe pedidos de certificados feitos por Administrações, órgãos, entidades de direito público ou outras entidades públicas.

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

O pedido deve ser acompanhado por documentação que justifique a identidade e outras circunstâncias da pessoa física identificada no certificado, de acordo com as disposições da secção 3.2.3. Deve também ser anexada uma morada física, ou outra informação, que permita o contacto da pessoa física identificada no certificado.

4.2 Processamento da candidatura à certificação

4.2.1 Execução das funções de identificação e autenticação

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

Se assim for, a esFIRMA verifica as informações fornecidas, verificando se os requisitos descritos na secção 3.2 foram corretamente cumpridos.

A documentação que justifica a aprovação do pedido deve ser mantida e devidamente registada e com garantias de segurança e integridade por um período de 15 anos a contar da expiração do certificado ou do fim do serviço prestado, mesmo em caso de perda antecipada de validade devido à revogação, uma vez que os certificados são qualificados.

A esFIRMA mantém procedimentos documentados que identificam e exigem atividade adicional de verificação para pedidos de certificados de alto risco, phishing ou outros usos fraudulentos, consultando diferentes listas de reputação de domínios e os próprios critérios de mitigação de risco da esFIRMA.

4.2.2 Aprovação ou rejeição da candidatura

A esFIRMA aprova o pedido do certificado e procede à sua emissão e entrega, seguindo o pedido realizado na Plataforma de Administração Eletrónica.

Em caso de suspeita de que a informação não é correta ou que possa afetar a reputação do Organismo Certificador ou dos subscritores, a esFIRMA negará o pedido ou suspenderá a sua aprovação até ter realizado as verificações complementares que considerar adequadas.

Caso as verificações adicionais não indiquem a correção da informação a verificar, a esFIRMA negará definitivamente o pedido.

A esFIRMA notifica o requerente sobre a aprovação ou recusa do pedido.

A esFIRMA pode automatizar os procedimentos para verificar a correção da informação contida nos certificados e para aprovar as candidaturas.

4.2.3 Prazo para resolver a candidatura

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

As candidaturas mantêm-se ativas até serem aprovadas ou rejeitadas.

4.3 Emissão do certificado

4.3.1 Ações da AC 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, enviando um link para o dispositivo móvel e/ou endereço de email designado pelo assinante no pedido do certificado, de acordo com o procedimento indicado na secção 4.4.2 ou através do sistema de mensagens da Plataforma de Administração Eletrónica.

Durante o processo, é a ASSINATURA:

- Protege a confidencialidade e integridade dos dados de registo disponíveis para si.
- Utiliza sistemas e produtos fiáveis, protegidos contra qualquer alteração e que garantem a segurança técnica e, quando apropriado, criptográfica dos processos de certificação que suportam.

- Gera o par de chaves, utilizando um procedimento de geração de certificados ligado de forma segura ao procedimento de geração de chaves.
- Emprega um procedimento de geração de certificados que liga de forma segura o certificado à informação de registo, incluindo a chave pública certificada.
- Assegura que o certificado é emitido por sistemas que utilizam proteção contra falsificação e que garantem a confidencialidade das chaves durante o processo de geração.
- Inclui no certificado a informação estabelecida no Anexo 1 do Regulamento (UE) 910/2014, em conformidade com as disposições dos artigos 3.1.1 e 7.1.
- Indica a data e hora em que o certificado foi emitido.

4.3.2 Notificação do problema ao assinante

A esFIRMA notifica a Administração, órgão, entidade de direito público ou outra entidade subscritora do certificado, e à pessoa física identificada no certificado, através dos seus endereços de email, já incluídos na informação na Plataforma de Administração Eletrónica, sobre a emissão do certificado.

4.4 Entrega e aceitação do certificado

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

- Provar de forma definitiva a identidade da pessoa física identificada no certificado, com a colaboração da Administração, órgão, entidade de direito público ou outra entidade, de acordo com as disposições dos artigos 3.2.2, 3.2.3 e 4.3.1.
- Entregar a folha de entrega e aceitação do certificado à pessoa física identificada nele, que contém o seguinte conteúdo mínimo:
    - Informações básicas sobre a utilização do certificado, incluindo, em particular, informações sobre o prestador de serviços de certificação e a Declaração de Práticas de Certificação aplicável, tais como as suas obrigações, poderes e responsabilidades
    - Informação sobre o certificado.

  - Reconhecimento, pelo signatário, da receção do certificado e aceitação dos elementos referidos.
  - Regime de obrigações do signatário.
  - Responsabilidade do signatário.
  - Método de atribuição exclusiva ao signatário dos seus dados de ativação da chave privada e do certificado, em conformidade com as disposições das secções 6.2 e 6.4.
  - A data do ato de entrega e aceitação.
- Obtenha a assinatura, escrita ou eletrónica, da pessoa identificada no certificado.

Quando necessário, a Administração, órgão, entidade de direito público ou outra entidade colabora nestes processos, tendo de registar os atos anteriores e conservar os documentos originais referidos (folhas de entrega e aceitação), enviando uma cópia eletrónica para a esFIRMA, bem como os originais quando a esFIRMA necessita de acesso a eles.

4.4.1 Conduta que constitui aceitação do certificado

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

Nos certificados emitidos por software, o certificado e as chaves são geridos num HSM, com o signatário a ter controlo exclusivo sobre a sua utilização.

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

Além disso, a aceitação do certificado pela pessoa física identificada no certificado ocorre através da assinatura da folha de entrega e aceitação, através da Plataforma Eletrónica de Administração.

4.4.2 Publicação do certificado

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

4.4.3 Notificação da questão a terceiros

A esFIRMA não notifica terceiros sobre o problema.

4.5 Utilização do Par de Chaves e do Certificado

4.5.1 Utilização pelo subscritor ou signatário

A esFIRMA compromete-se com o seguinte:

- Fornecer à esFIRMA informações completas e adequadas, de acordo com os requisitos desta Declaração de Práticas de Certificação, especialmente no que diz respeito ao procedimento de aceitação.
- Expressar o seu consentimento antes da emissão e entrega do certificado.
- Utilize o certificado de acordo com as disposições da secção 1.4.
- Quando o certificado funciona em conjunto com um DCCF, reconhece a sua capacidade para produzir assinaturas eletrónicas qualificadas; ou seja, equivalente a assinaturas manuscritas, bem como a outros tipos de assinaturas eletrónicas e mecanismos de encriptação de informação.
- Seja especialmente diligente na custódia da sua chave privada, para evitar o uso não autorizado, de acordo com as disposições das secções 6.1, 6.2 e 6.4.
- Comunique à esFIRMA e a qualquer pessoa que se acredite poder confiar no certificado, sem atrasos injustificáveis:
    - A perda, roubo ou possível comprometimento da sua chave privada.
    - Perda de controlo sobre a sua chave privada, devido ao comprometimento dos dados de ativação (por exemplo, código PIN) ou por qualquer outro motivo.
    - Imprecisões ou alterações no conteúdo do certificado que o assinante conhece ou pode saber.
- Deixe de usar a chave privada após o período indicado na secção 6.3.2.
- Que toda a informação fornecida pelo signatário contida no certificado está correta.

- Que o certificado é utilizado exclusivamente para fins legais e autorizados, de acordo com a Declaração de Prática de Certificação.
- Que nenhuma pessoa não autorizada alguma vez teve acesso à chave privada do certificado, e que ele 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 prestador de serviços de certificação, e que não utilizará a chave privada correspondente à chave pública listada no certificado para assinar qualquer certificado (ou qualquer outro formato de chave pública certificada), ou Lista de Revogação de Certificados, título de prestador de serviços de certificação, ou de outra forma.

4.5.2 Utilização pelo Assinante

A esFIRMA obriga contratualmente o subscritor a:

- Fornecer ao Organismo de Certificação informação completa e adequada, de acordo com os requisitos desta Declaração de Práticas de Certificação, especialmente no que diz respeito ao procedimento de aceitação.
- Expressar o seu consentimento antes da emissão e entrega do certificado.
- Utilize o certificado de acordo com as disposições da secção 1.4.
- Comunique com a esFIRMA e com qualquer pessoa que o assinante acredite poder confiar no certificado, sem atrasos injustificáveis:
    - A perda, roubo ou possível comprometimento da sua chave privada.
    - Perda de controlo sobre a sua chave privada, devido ao comprometimento dos dados de ativação (por exemplo, código PIN) ou por qualquer outro motivo.
    - Imprecisões ou alterações no conteúdo do certificado que o assinante conhece ou pode saber.
    - A perda, alteração, uso não autorizado, roubo ou compromisso, quando possível, do cartão.
- Transferir às pessoas físicas identificadas no certificado o cumprimento das suas obrigações específicas e estabelecer mecanismos para garantir o seu cumprimento eficaz.

- Não monitorizar, manipular ou realizar atos de engenharia reversa na implementação técnica dos serviços de certificação do esFIRMA, sem autorização prévia por escrito.
- Não comprometer a segurança dos serviços de certificação do fornecedor de serviços de certificação da esFIRMA, sem autorização prévia por escrito.
- Que todas as afirmações feitas na candidatura estão corretas.
- Que toda a informação fornecida pelo assinante contida no certificado está correta.
- Que o certificado é utilizado exclusivamente para fins legais e autorizados, de acordo com a Declaração de Prática de Certificação.
- Que nenhuma pessoa não autorizada alguma vez teve acesso à chave privada do certificado, e que ele 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 prestador de serviços de certificação, e que não utilizará a chave privada correspondente à chave pública listada no certificado para assinar qualquer certificado (ou qualquer outro formato de chave pública certificada), ou Lista de Revogação de Certificados, título de fornecedor de serviços de certificação, ou em qualquer outro caso.

4.5.3 Utilização pelo certificado com base em terceiros

A esFIRMA informa o terceiro que depende dos certificados que deve assumir as seguintes obrigações:

- Seja informado de forma independente sobre o facto de o certificado ser adequado para o uso pretendido.
- Verificar a validade, suspensão ou revogação dos certificados emitidos, para os quais utilizará informações sobre o estado dos certificados.
- Verifique todos os certificados na hierarquia de certificados, antes de confiar na assinatura digital ou em qualquer um dos certificados da hierarquia.
- Reconheça que, para ser considerado um certificado qualificado, deve estar incluído na Lista Nacional de Confiança.
- Reconhecer que as assinaturas eletrónicas verificadas, produzidas num Dispositivo de Criação de Assinaturas Qualificadas (DCCF), são legalmente consideradas assinaturas eletrónicas qualificadas; ou seja, equivalente a

assinaturas manuscritas, bem como o certificado permite a criação de outros tipos de assinaturas eletrónicas e mecanismos de encriptação.

- Esteja ciente de quaisquer limitações no uso do certificado, independentemente de estarem presentes no próprio certificado ou no contrato do terceiro que se baseia no certificado.
- Tenha em conta quaisquer precauções estabelecidas num contrato ou outro instrumento, independentemente da sua natureza legal.
- Não monitorizar, manipular ou realizar atos de engenharia reversa na implementação técnica dos serviços de certificação do esFIRMA, sem autorização prévia por escrito.
- Não comprometer a segurança dos serviços de certificação da esFIRMA sem autorização prévia por escrito.

A esFIRMA informa o terceiro que confia nos certificados que deve assumir as seguintes responsabilidades:

- Que tem informação suficiente para tomar uma decisão informada sobre se confiar ou não no certificado.
- Que é o único responsável por confiar ou não nas informações contidas no certificado.
- Que será a única responsável caso não cumpra as suas obrigações como terceiro que se baseie no certificado.

4.6. Renovação de certificados

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

4.6.1 Circunstâncias para a Renovação do Certificado

Não aplicável.

4.6.2 Quem pode pedir a renovação

Não aplicável.

4.6.3 Processamento do Pedido de Renovação de Certificado

Não aplicável.

4.6.4 Notificação da emissão de novo certificado ao assinante

Não aplicável.

4.6.5 Conduta que constitui aceitação de um certificado de renovação

Não aplicável.

4.6.6 Publicação do certificado de renovação pela CA

Não aplicável.

4.6.7 Notificação da emissão do certificado pela CA a outras entidades

Não aplicável.

4.7 Renovação de Chaves e Certificados

4.7.1 Quem pode solicitar o certificado de uma nova chave pública

Não aplicável.

4.7.2 Procedimento com nova identificação

Não aplicável.

4.7.3 Processamento de Novos Pedidos de Chave de Certificado

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

Tal comparência e identificação devem ser realizadas de acordo com as disposições da secção 3.2.

A assinatura da folha de aceitação será realizada de acordo com as disposições da secção 4.4.2.

4.7.4 Notificação da emissão do certificado renovado

Não se aplica porque não há renovações.

4.7.5 Conduta que constitui aceitação do certificado

Não aplicável.

4.7.6 Publicação do certificado

Não aplicável.

4.7.7 Notificação da emissão a terceiros

A esFIRMA não notifica terceiros sobre o problema.

4.8 Modificação de certificados

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

4.9 Revogação e suspensão de certificados

4.9.1 Causas para revogação de certificados

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

1) Circunstâncias que afetam a informação contida no certificado:
   a) Modificação de qualquer um 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 de chaves ou certificados:
   a) Comprometimento da chave privada, infraestrutura ou sistemas do fornecedor de serviços de certificação que emitiu o certificado, desde que afete a fiabilidade dos certificados emitidos a partir desse incidente.
   b) Violação, por esFIRMA, dos requisitos estabelecidos nos procedimentos de gestão de certificados, estabelecidos nesta Declaração de Práticas de Certificação.
   c) Comprometimento ou suspeita de comprometimento da segurança da chave ou certificado emitido.
   d) Acesso ou utilização não autorizada, 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 custódia da chave privada.

3) Circunstâncias que afetam o assinante ou a pessoa física identificada no certificado:
   a) Rescisão da relação jurídica para a prestação de serviços entre a esFIRMA e o assinante.
   b) Modificação ou cessação da relação ou causa jurídica subjacente que levou à emissão do certificado à pessoa física identificada no certificado.
   c) Violação, por parte do requerente, do certificado dos requisitos pré-estabelecidos para a sua aplicação.
   d) Violação, por parte do subscritor ou da pessoa identificada no certificado, das suas obrigações, responsabilidade e garantias, estabelecidas no documento legal correspondente.
   e) A incapacidade ou morte supervenente do portador da chave.
   f) A cessação da entidade legal que subscrive o certificado, bem como o fim da autorização do assinante ao titular da chave ou a terminação da relação entre o assinante e a pessoa identificada no certificado.

g) Pedido do assinante para revogação do certificado, em conformidade com as disposições da secção 3.4.

4) Outras circunstâncias:
   a) A cessação do serviço de certificação esFIRMA, de acordo com as disposições da secção 5.8.
   b) O uso do certificado é prejudicial e contínuo para a esFIRMA. Neste caso, um uso é considerado prejudicial com base nos seguintes critérios:
      - A natureza e o número de queixas 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 queixas recebidas.
   c) Perda da certificação de qualquer um dos dispositivos qualificados de criação de assinaturas que a esFIRMA utilizava como Prestador de Serviços de Confiança Qualificado,

4.9.2 Legitimidade para solicitar revogação

Os seguintes podem solicitar a revogação de um certificado:

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

4.9.3 Procedimentos de Pedido de Revogação

O pedido de revogação deverá incluir as seguintes informações:

- Data do pedido de revogação.
- Identidade do assinante ou signatário.
- Motivo detalhado para o pedido de revogação.

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

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

O serviço de revogação está localizado na Plataforma de Administração Eletrónica, onde o signatário e o assinante gerem os seus certificados.

No caso de o destinatário de um pedido de revogação por parte de uma pessoa física identificada no certificado ser a entidade subscritora, uma vez autenticado o pedido, esta última deve enviar um pedido a este respeito ao esFIRMA.

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

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

Está disponível um serviço 24/7 no número de telefone +34 976 579 516, para solicitar a revogação de certificados. A comunicação é gravada e gravada, para que seja usado como apoio e garantia de aceitação da revogação solicitada.

4.9.4 Prazo para pedido de revogação

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

4.9.5 Prazo para o Processamento de Candidaturas

Os pedidos de revogação terão efeito num prazo máximo de 24 horas[4].

[2] Parágrafo 6.2.4.a) iii) da ETSI EN 319 411-1

[3] Parágrafo 6.2.4(a)(vi) da ETSI EN 319 411-1

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

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

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

Terceiros devem verificar o estado dos certificados em que desejam confiar.

Um método para verificar o estado dos certificados é consultar a Lista de Revogação de Certificados mais recente emitida pela Autoridade de Certificação esFIRMA.

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

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

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

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

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

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

A CRL indica o prazo previsto para a emissão de uma nova CRL, embora uma CRL possa ser emitida antes do prazo indicado na CRL anterior, para refletir revogações.

O CRL deve manter o certificado revogado ou suspenso até expirar.

4.9.8 Prazo Máximo de Publicação para CRLs

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

4.9.9 Disponibilidade de Serviços de Verificação de Saúde com Certificado Online

A esFIRMA informa sobre o estado da revogação dos certificados, utilizando o protocolo OCSP, que lhe permite conhecer o estado de validade dos certificados online a partir dos endereços:

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

No caso de falha dos sistemas de verificação de estado do certificado por razões fora do controlo do esFIRMA, este último deve fazer o seu melhor esforço para garantir que este serviço permaneça inativo pelo tempo mínimo possível, que não pode exceder um dia.

A esFIRMA fornece informações a terceiros, baseando-se em certificados, sobre o funcionamento do serviço de informação sobre o estado dos certificados.

Os serviços de verificação de saúde com certificado são gratuitos[5].

A esFIRMA mantém as informações sobre o estado de revogação disponíveis após o período de validade do certificado[6].

4.9.10 Obrigação de consultar os serviços de verificação de saúde certificado

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

---

5 ETSI EN 319 411-2 AP 6.3.10

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

O esFIRMA suporta o método GET para OCSP.

A esFIRMA atualiza o OCSP pelo menos de quatro em quatro dias e imediatamente em condições normais.

As respostas OCSP têm um prazo máximo de validade de 48 horas.

Para conhecer o estado dos Certificados CA subordinados, a informação fornecida através do OCSP é atualizada pelo menos a cada seis meses e no prazo de 24 horas após a revogação de um Certificado CA subordinado.

Se o respondente OCSP receber um pedido de estado para um certificado que não foi emitido, então devolverá *"revogado, certificateHold a 1 de janeiro de 1970",* registando tais pedidos como parte dos procedimentos de resposta de segurança do esFIRMA.

4.9.11 Outras formas de informação sobre revogação de certificados

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

A esFIRMA não delega as suas respostas OCSP usando o grampo OCSP.

4.9.12 Requisitos especiais em caso de comprometimento de chave privada

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

4.9.13 Causas para suspensão de certificados

A esFIRMA não suspende certificados.

4.9.14 Pedido de suspensão

A esFIRMA não suspende certificados

4.9.15 Procedimentos para o pedido de suspensão

A esFIRMA não suspende certificados.

4.9.16 Período Máximo de Suspensão

A esFIRMA não suspende certificados.

4.10 Certificados de Serviços de Verificação de Saúde

4.10.1 Características operacionais dos serviços

Os serviços de verificação de certificado de saúde são fornecidos através de uma interface de consulta web, na web, https://www.esfirma.com

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

As entradas de revogação numa resposta CRL ou OCSP nunca são apagadas.

Diferenças e considerações entre consultas de estado de revogação de certificados usando OCSP e CRL:

- Tanto o OCSP como o CRL apresentam 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 os dois métodos. Eventualmente, o estado de revogação de um certificado não expirado é o mesmo em consulta via OCSP e CRL.
- As CRLs não incluem certificados revogados que já expiraram, enquanto o OCSP inclui essa informação. Adicionar certificados expirados a um CRL aumenta o tempo necessário para verificar a validade dos certificados porque a lista é maior e demora mais a descarregar e processar. Além disso, existe um crescimento indefinido dos CRLs até ao fim da validade do emissor.

- A EsFIRMA emite um Último CRL, que se refere ao último CRL emitido antes de o certificado emitidor de CRL deixar de ser válido devido a expiração, revogação ou outros casos. Este CRL, juntamente com um ficheiro de assinatura LTA, é usado para verificar se um certificado era válido num determinado momento. Se o Último CRL não puder ser validado, o certificado deve ser assumido como inválido. Uma vez verificado o Último CRL, o estado do certificado deve ser verificado no CRL.
- O OCSP requer ligação em tempo real à autoridade certificadora para obter o estatuto de revogação, enquanto os CRLs podem ser descarregados e armazenados localmente para uso offline.
- O OCSP pode ser menos privado do que os CRLs, pois os pedidos OCSP podem revelar à autoridade certificadora os sites que o cliente está a visitar.

4.10.2 Disponibilidade de Serviços

Os serviços de verificação de certificado de saúde e o serviço de carimbo temporal estão disponíveis 24 horas por dia, 7 dias por semana, durante todo o ano, com exceção de encerramentos programados.

Os serviços de verificação de saúde com certificado são gratuitos.

4.10.3 Funcionalidades Opcionais

Não aplicável.

4.11 Cessação da Subscrição

Após o período de validade do certificado, a subscrição do serviço termina.

4.12 Depósito de Chave e Recuperação

4.12.1 Política e Práticas de Depósito e Recuperação de Chaves

A esFIRMA não fornece serviços de depósito e recuperação de chaves.

4.12.2 Política e Práticas de Envolvimento e Recuperação de Chaves de Sessão

Sem estipulação.

5. Controlos de segurança física, de gestão e operacionais

5.1 Controlos de Segurança Física

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

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

- Controlos físicos de acesso.
- Proteção contra desastres naturais.
- Medidas de proteção contra incêndios.
- Falha dos sistemas de suporte (e-power, telecomunicações, etc.)
- Colapso da estrutura.
- Cheias.
- Proteção contra roubo.
- Saída não autorizada de equipamentos, informações, suportes e aplicações relativos a componentes utilizados para os serviços do prestador de serviços de certificação.

Estas medidas aplicam-se às instalações onde os certificados são produzidos sob total responsabilidade da esFIRMA, que os fornece a partir das suas instalações de alta segurança, tanto as principais como, quando apropriado, operações de contingência, que são devidamente auditadas periodicamente.

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

5.1.1 Localização e construção das instalações

A proteção física é alcançada através da criação de perímetros de segurança claramente definidos em torno dos serviços. A qualidade e robustez dos materiais de construção da instalação garantem níveis adequados de proteção contra intrusões de força bruta, estando localizada numa área de baixo risco de desastre e permitindo um acesso rápido.

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

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

A esFIRMA dispõe de funcionalidades que protegem fisicamente a prestação de aprovação de pedidos de certificados e serviços de gestão de revogação contra comprometimento causado por acesso não autorizado a sistemas ou dados, bem como contra a sua divulgação

5.1.2 Acesso Físico

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

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

- Está limitada a pessoal expressamente autorizado, com identificação no momento do acesso e registo, incluindo filmagens e arquivo por CCTV.

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

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

5.1.3 Eletricidade e ar condicionado

As instalações da esFIRMA dispõem de equipamento de estabilização de corrente e de um sistema de fornecimento elétrico duplicado com um conjunto gerador.

As divisões que albergam equipamento informático têm sistemas de controlo de temperatura com ar condicionado.

5.1.4 Exposição à água

As instalações situam-se numa zona de baixo risco de inundação.

As salas onde se guarda o equipamento informático têm um sistema de deteção de humidade.

5.1.5 Prevenção e proteção contra incêndios

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

5.1.6 Armazenamento de Media

Apenas pessoal autorizado tem acesso ao suporte de armazenamento.

O nível mais elevado de informação de classificação é guardado numa caixa de segurança fora das instalações do Centro de Processamento de Dados.

5.1.7 Tratamento de resíduos

A eliminação dos suportes, tanto de papel como magnéticos, é feita através de mecanismos que garantem a impossibilidade de recuperar a informação.

No caso dos suportes magnéticos, a formatação, eliminação permanente ou destruição física do suporte é realizada através de software especializado que realiza no mínimo 3 passagens de apagamento e com padrões de apagamento variáveis.

No caso da documentação em papel, por trituradores ou em contentores fornecidos para este fim, para serem posteriormente destruídos, sob controlo.

5.1.8 Backup fora do local

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

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

5.2 Controlos Procedurais

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

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

5.2.1 Funcionalidades Fiáveis

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

- **Auditor Interno:** Responsável pelo cumprimento dos procedimentos operacionais. Esta é uma pessoa externa ao departamento de Sistemas de Informação. As tarefas do Auditor Interno são incompatíveis no tempo com as tarefas de Certificação e incompatíveis com os Sistemas. Estas funções estarão subordinadas ao chefe de operações, reportando-se tanto a este como à gestão técnica.

- **Administrador de** Sistemas: Responsável pelo correto funcionamento do suporte de hardware e software da plataforma de certificação
- **Administrador da CA**: Responsável pelas ações a realizar com o material criptográfico, ou pelo desempenho de qualquer função que envolva a ativação das chaves privadas das autoridades certificadoras aqui descritas, ou de qualquer um dos seus elementos.
- **Operador de CA:** Responsável conjuntamente com o Administrador da CA pela custódia do material de ativação de chaves criptográficas, também responsável pelas operações de backup e manutenção da CA.
- **Operador de Registo:** Pessoa responsável por aprovar pedidos de certificação feitos pelo assinante.
- **Gestor de Segurança**: Responsável por coordenar, controlar e aplicar as medidas de segurança definidas pelas políticas de segurança do esFIRMA. Deve ser responsável por aspetos relacionados com a segurança da informação: lógico, físico, de redes, organizacional, etc.
- **Gestor de Informação e Serviço**: Define os requisitos de informação e serviços em termos de segurança. Este papel tem a responsabilidade última pela utilização da informação e dos serviços e, consequentemente, pelo seu nível de proteção.
- **Especialista em** Validação: Responsável pela validação dos pedidos de certificados.
- **Oficial de Revogação:** Responsável pela alteração do estado dos certificados.

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

5.2.2 Número de pessoas por tarefa

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

5.2.3 Identificação e autenticação para cada função

As pessoas atribuídas a cada função são identificadas pelo auditor interno, que garantirá que cada pessoa executa as operações para as quais está designada.

Cada pessoa controla apenas os recursos necessários para o seu papel, garantindo assim que ninguém tem acesso a recursos não alocados.

O acesso aos recursos é feito consoante o ativo, utilizando cartões criptográficos e códigos de ativação.

5.2.4 Papéis que Exigem Separação de Funções

As seguintes tarefas são realizadas por pelo menos duas pessoas:

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

5.2.5 Sistema de Gestão de PKI

O sistema PKI é composto pelos seguintes módulos:

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

5.3 Verificações de pessoal

5.3.1 Histórico, qualificações, experiência e requisitos de autorização

Todo o pessoal que desempenha tarefas qualificadas como fiáveis trabalha no local de produção há pelo menos um ano e tem contratos de trabalho permanente.

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

O pessoal em posições de confiança não tem interesses pessoais que entrem em conflito com o desempenho da função que lhes foi confiada.

A esFIRMA assegura que o pessoal de registo é fiável para realizar tarefas de registo.

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

De um modo geral, a esFIRMA remove um trabalhador das suas funções de confiança quando toma conhecimento da existência da prática de um ato criminal que possa afetar o desempenho das suas funções.
A esFIRMA não atribuirá a um local fiável ou de gestão uma pessoa que não seja adequada para o cargo, especialmente porque foi condenada por um crime ou contravenção que afete a sua aptidão para o cargo.

5.3.2 Procedimentos de Investigação do Histórico

A esFIRMA realiza verificações de antecedentes a potenciais colaboradores antes de serem contratados ou de entrarem no emprego.

A esFIRMA obtém o consentimento inequívoco do sujeito para tal 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, sobre a Proteção de Dados Pessoais e garantia dos direitos digitais.

A investigação será repetida com periodicidade suficiente.

Todas as verificações são realizadas na medida permitida pela legislação aplicável. As razões que podem levar à rejeição do candidato para uma posição fiável são as seguintes:

- Falsidades na candidatura, feitas pelo candidato.
- Referências profissionais muito negativas ou pouco fiáveis em relação ao candidato.

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

5.3.3 Requisitos de Formação

A esFIRMA forma os colaboradores em posições fiáveis e de gestão nos termos estabelecidos nas Políticas de Certificação. Para tal, as ações correspondentes são definidas no Plano de Formação ESFIRMA.

A formação inclui, pelo menos, os seguintes conteúdos:

- Princípios e mecanismos de segurança da hierarquia de certificação, bem como do ambiente de utilizador da pessoa a ser treinada.
- Tarefas que a pessoa tem de desempenhar.
- Políticas e procedimentos de segurança da esFIRMA. Utilização e operação das máquinas e aplicações instaladas.
- Gestão e processamento de incidentes e compromissos de segurança.
- Continuidade do negócio e procedimentos de emergência.
- Procedimentos de gestão e segurança relativos ao tratamento de dados pessoais.

5.3.4 Requisitos e frequência das atualizações de formação

A esFIRMA atualiza a formação do pessoal conforme necessário e com frequência suficiente para desempenhar as suas funções de forma competente e satisfatória, especialmente quando são feitas modificações substanciais nas tarefas de certificação

5.3.5 Sequência e frequência de rotatividade de trabalho

Não aplicável.

5.3.6 Penalizações por Ações Não Autorizadas

A esFIRMA possui um sistema de sancionamento para clarificar as responsabilidades decorrentes de ações não autorizadas, adaptado à legislação laboral aplicável e, em particular, coordenado com o sistema sancionador do acordo coletivo aplicável ao pessoal.

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

5.3.7 Requisitos para a contratação de profissionais

Os colaboradores contratados para realizar tarefas fiáveis assinam previamente as cláusulas de confidencialidade e os requisitos operacionais utilizados pela esFIRMA. Qualquer ação que comprometa a segurança dos processos aceites pode, uma vez avaliada, levar à rescisão do contrato de trabalho.

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

5.3.8 Fornecimento de documentação ao pessoal

O prestador de serviços de certificação fornecerá a documentação de que a sua equipa necessita estritamente em todos os momentos, para que o seu trabalho seja realizado de forma competente e satisfatória.

5.4 Procedimentos de auditoria de segurança

5.4.1 Tipos de Eventos Registados

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

- Ligar e desligar o sistema.
- Tentativas de criar, eliminar, definir palavras-passe ou alterar privilégios.
- Tentativas de iniciar sessão e sair de sessão.
- Tentativas de obter acesso não autorizado ao sistema de AC através da rede.
- Tentativas de acesso não autorizado ao sistema de ficheiros.
- Acesso físico aos registos.
- Alterações na configuração e manutenção do sistema.
- Registos de candidaturas à Califórnia.
- Ligar e desligar a aplicação AC.
- Alterações aos detalhes e/ou chaves da CA.
- Alterações na criação de políticas de certificados.
- Geração das próprias chaves.
- Criação e revogação de certificados.
- Registos da destruição do suporte que continha as chaves, dados de ativação.
- Eventos relacionados com o ciclo de vida do módulo criptográfico, como receber, usar e desinstalar o módulo.
- As atividades dos firewalls e routers[7]
- A cerimónia de geração de chaves e as bases de dados de gestão de chaves.
- Registos físicos de acesso.
- Manutenção e alterações na configuração do sistema.
- Mudanças no pessoal.
- Relatórios de compromissos e discrepâncias.
- Registos da destruição de material contendo informações-chave, 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 Autoridade de Certificação.
- Relatórios abrangentes de tentativas de intrusão física em infraestruturas que suportam a emissão e gestão de certificados.

As entradas do registo incluem os seguintes itens:

- Data e hora de entrada.

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

- Número de série ou sequência da entrada, em registos automáticos.
- Identidade da entidade que entra no registo.
- Tipo de multa.

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

5.4.2 Frequência do Processamento dos Registos de Auditoria

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

O processamento dos registos de auditoria consiste numa revisão dos registos que inclui a verificação de que não foram adulterados, uma breve inspeção de todas as entradas dos registos e uma investigação mais aprofundada de quaisquer alertas ou irregularidades nos registos. As ações tomadas na revisão da auditoria estão documentadas.

A esFIRMA mantém um sistema que lhe permite garantir:

- Espaço suficiente para armazenamento de registos
- Os ficheiros de registo não são reescritos.
- Que a informação guardada inclua pelo menos: tipo de evento, data e hora, utilizador que executa o evento e resultado da operação.
- Os ficheiros de registo serão armazenados em ficheiros estruturados que poderão ser incorporados numa base de dados para exploração posterior.

5.4.3 Período de Retenção dos Registos de Auditoria

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

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

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

5.4.4 Proteção dos Registos de Auditoria

Os registos dos sistemas:

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

O acesso aos ficheiros de registo é reservado apenas para pessoas autorizadas. Da mesma forma, os dispositivos são operados em todos os momentos por pessoal autorizado.
Existe um procedimento interno onde os processos de gestão dos dispositivos que contêm dados de registo de auditoria são detalhados.

5.4.5 Procedimentos de Backup

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

A esFIRMA implementou um procedimento de backup seguro para registos de auditoria, fazendo uma cópia semanal de todos os registos num meio externo. Além disso, uma cópia é guardada num centro de custódia externo.

5.4.6 Localização do Sistema de Acumulação de Registos de Auditoria

A informação de auditoria de eventos é recolhida internamente e de forma automatizada pelo sistema operativo, comunicações de rede e software de gestão de certificados, bem como dados gerados manualmente, que serão armazenados por pessoal devidamente autorizado. Tudo isto compõe o sistema de acumulação de registos de auditoria.

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

5.4.7 Notificação do evento de auditoria à pessoa que o causou

Quando o sistema de auditoria regista 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 abrangida pelos processos de auditoria do esFIRMA.

As varreduras de vulnerabilidades devem ser executadas, revistas e revistas através da análise destes eventos monitorizados. Estas análises devem ser realizadas diariamente, mensalmente e anualmente.

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

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

5.5. Ficheiros de informação

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

5.5.1 Tipos de Registos Arquivados

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

- Todos os dados de auditoria do sistema (PKI, TSA e OCSP).
- Todos os dados relativos aos certificados, incluindo contratos com os signatários e dados relativos à sua identificação e localização

- Pedidos de emissão e revogação de certificados, incluindo todos os relatórios relativos ao processo de revogação[10].
- Quaisquer escolhas específicas que o signatário ou subscritor tenha durante o acordo de subscrição[11].
- Tipo de documento submetido na candidatura do certificado.
- Identidade da Autoridade de Registo que aceita o pedido de certificado.
- Número de identificação único fornecido pelo documento acima.
- Todos os certificados emitidos ou publicados.
- CRLs emitidos ou registos do estado dos certificados gerados.
- A história das chaves geradas.
- Comunicações entre elementos da PKI.
- Políticas e Práticas de Certificação
- Todos os dados de auditoria identificados na secção 5.4
- Informação sobre Pedidos de Certificação.
- Documentação fornecida para justificar pedidos de certificação.
- Informação sobre o ciclo de vida do certificado.

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

5.5.2 Período de retenção de recordes

A esFIRMA arquiva os registos acima especificados por pelo menos 15 anos.

5.5.3 Proteção de ficheiros

A esFIRMA protege o ficheiro para que apenas pessoas devidamente autorizadas possam aceder a ele. O ficheiro está protegido contra visualização, modificação, eliminação ou qualquer outra manipulação ao ser armazenado num sistema fiável.

A esFIRMA assegura a proteção correta dos ficheiros ao atribuir pessoal qualificado para o seu processamento e armazená-los em caixas de segurança à prova de fogo e em instalações externas.

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

11 Parágrafo 6.4.5(c)(iv) da ETSI EN 319 411-1

5.5.4 Procedimentos de Backup

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

A esFIRMA realiza, no mínimo, backups incrementais diários de todos os seus documentos eletrónicos e faz cópias de segurança completas semanalmente para casos de recuperação de dados.

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

5.5.5 Requisitos de Marcação de Data e Hora

Os registos são datados com uma fonte fiável via NTP.

O esFIRMA tem um procedimento que descreve a configuração dos horários do equipamento utilizado na emissão de certificados.
O tempo utilizado para registar os eventos no registo de auditoria deve ser sincronizado com o UTC pelo menos uma vez por dia[12].

Esta informação não precisa de ser assinada digitalmente.

5.5.6 Localização do Sistema de Ficheiros

A esFIRMA possui um sistema centralizado para recolher informações sobre a atividade das equipas envolvidas no serviço de gestão de certificados.

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

5.5.7 Procedimentos para Obtenção e Verificação de Informação de Arquivo

A esFIRMA tem um procedimento que descreve o processo para verificar se a informação registada está correta e acessível.

5.6 Renovação de chaves

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

A alteração das palavras-passe dos assinantes é feita através de um novo processo de emissão.

5.7 Compromisso Chave e Recuperação em Desastres

5.7.1 Procedimentos para a gestão de incidentes e compromissos

Cópias de segurança das seguintes informações são armazenadas em instalações de armazenamento externas ao esFIRMA, que são disponibilizadas em caso de comprometimento ou desastre: dados técnicos de pedidos de certificados, dados de auditoria e registos de bases de dados de todos os certificados emitidos.

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

5.7.2 Corrupção de Recursos, Aplicações ou Dados

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

5.7.3 Compromisso da chave privada da entidade

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

Em caso de comprometimento da chave privada esFIRMA, pode acontecer que os estados dos certificados e dos processos de revogação que utilizam esta chave possam não ser [13]válidos. Em qualquer caso, todos os certificados ativos serão revogados, gerando posteriormente uma CRL final que incluirá todos os certificados revogados, estejam ou não expirados. As instruções para a validação de um certificado ou carimbo temporal serão publicadas no site da esFIRMA.

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

O caso de compromisso da chave raiz deve ser tratado como um caso separado no processo de contingência e continuidade do negócio. Este incidente afeta, no caso de substituição das palavras-passe, os reconhecimentos por diferentes aplicações e serviços privados e públicos. A recuperação da eficácia das chaves em termos empresariais dependerá principalmente da duração destes processos. O documento de contingência e continuidade do negócio tratará dos termos puramente operacionais para que as novas chaves estejam disponíveis, e não do seu reconhecimento por terceiros.

Qualquer falha em atingir os objetivos definidos por este Plano de Contingência será considerada razoavelmente inevitável, salvo se tal falha se deve a um incumprimento das obrigações da CA de implementar tais processos.

5.7.4 Continuidade dos Negócios Após um Desastre

A esFIRMA irá restaurar serviços críticos (suspensão e revogação, e publicação de informações sobre o estado dos certificados) de acordo com o Plano de Continuidade de Negócio existente.

---

[13] Parágrafo 6.4.8(g)(ii) da ETSI EN 319 411-1

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

Tanto o serviço de gestão de revogações como o serviço de consultoria são considerados serviços críticos e estão assim referidos no Plano de Continuidade de Negócios do esFIRMA.

5.8 Término do Serviço

A esFIRMA assegura que as possíveis interrupções para subscritores e terceiros sejam mínimas devido à cessação dos serviços do prestador de serviços de certificação e, em particular, assegura a manutenção contínua dos registos necessários para fornecer provas de certificação no caso de uma investigação civil ou criminal.

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

- Fornecer os fundos necessários para continuar a conclusão das atividades de revogação.
- Deve notificar o órgão fiscal, pelo menos três meses antes da data prevista de término, a cessação da sua atividade e o destino dos certificados, especificando se a gestão é transferida e a quem, ou se a sua validade será extinta.
- Também notificará o Ministério dos Assuntos Económicos e Transformação Digital sobre a abertura de quaisquer processos de falência contra a esFIRMA, bem como quaisquer outras circunstâncias relevantes que possam impedir a continuação da atividade.
- Informará todos os Signatários/Assinantes, Terceiros de confiança e outras CAs com quem tenha acordos ou outros tipos de relação sobre a rescisão, com um aviso mínimo de três meses.
- Revogará qualquer autorização para que entidades subcontratadas atuem em nome da CA no procedimento de emissão de certificados.
- Destruir ou desativar as chaves privadas da CA para uso.
- Os certificados de Unidade com carimbo temporal (TSU) serão revogados.
- Todos os certificados ativos e o sistema de verificação e revogação serão mantidos até à extinção de todos os certificados emitidos durante 15 anos.

Para tal, será emitida uma CRL final que incluirá todos os certificados revogados, estejam ou não expirados, estabelecendo os meios necessários para garantir a sua conservação a longo prazo.

6. Verificações técnicas de segurança

6.1 Geração e Instalação de Pares de Chaves

6.1.1 Geração de Pares de Chaves

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

As atividades realizadas durante a cerimónia de geração de chaves foram registadas, datadas e assinadas por todos os participantes nela, com a presença de um Auditor CISA. Estes registos são mantidos para fins de auditoria e monitorização durante um período apropriado determinado pela esFIRMA.

Para a geração da chave dos organismos de certificação raiz, intermédia e TSA, utilizar dispositivos com certificações Common Criteria EAL 4+, FIPS 140-2 Nível 3 e FIPS 140-3 Nível 3.

ROOT	4.096 bits	25 anos
INTERMÉDIO	4.096 bits	13 anos
- Certificados da Entidade Final	2.048 bits	2 anos
- Certificado TSA	4.096 bits	5 anos (2 anos de chave privada)

Mais informações nas seguintes localizações do PDS:

CERTIFICADO	PDS
Funcionário Público (FIRMA)	Espanhol:

CERTIFICADO	PDS
	https://esfirma.com/doc-pki/PDS-V2.0/PDS-AAPP-ES.pdf Inglês: https://esfirma.com/doc-pki/PDS-V2.0/PDS-AAPP-EN.pdf
Funcionário Público – Alto Nível 1.3.6.1.4.1.47281.1.1.1	
Funcionário Público – Nível Médio 1.3.6.1.4.1.47281.1.1.4	
Funcionário Público (AUTENTICAÇÃO)	
Funcionário Público – Alto Nível 1.3.6.1.4.1.47281.1.1.5	
De Funcionário Público com Pseudónimo (ASSINATURA)	
Do EP com pseudónimo – Alto Nível 1.3.6.1.4.1.47281.1.3.1	
Do EP com pseudónimo – Nível Intermédio 1.3.6.1.4.1.47281.1.3.4	
Funcionário Público Pseudónimo (AUTENTICAÇÃO)	
Do Funcionário Público com Pseudónimo – 1.3.6.1.4.1.47281.1.3.5	
Selo do Órgão	
Selo de Órgão – Nível Intermédio 1.3.6.1.4.1.47281.1.2.2	
Selo do Órgão – Nível Intermédio Centralizado *1.3.6.1.4.1.47281.1.2.4*	
De Indivíduo ligado à entidade (FIRMA)	Espanhol: 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

CERTIFICADO	PDS
PF ligado à entidade – Qualificado F. 1.3.6.1.4.1.47281.1.6.1	
PF ligado a entidades – F. Centralizado 1.3.6.1.4.1.47281.1.6.4	
De uma pessoa física ligada a uma entidade (AUTENTICAÇÃO)	
De PF ligada a uma entidade 1.3.6.1.4.1.47281.1.6.5	
De uma pessoa física com pseudónimo ligado a uma entidade (FIRMA)	
De PF com pseudónimo ligado à entidade – Assinatura Qualificada 1.3.6.1.4.1.47281.1.7.1	
De PF com pseudónimo associado à entidade – Firma Centralizado 1.3.6.1.4.1.47281.1.7.4	
De uma Pessoa com pseudónimo, ligada a uma entidade (AUTENTICAÇÃO)	
Do PF com pseudónimo, ligado a uma entidade 1.3.6.1.4.1.47281.1.7.5	
Selo Eletrónico	
Selo Eletrónico em Software 1.3.6.1.4.1.47281.1.8.2	
Selo Eletrónico Centralizado 1.3.6.1.4.1.47281.1.8.4	
Selo Eletrónico para TSA/TSU	Espanhol: https://esfirma.com/doc-pki/PDS-V1.5/TSADS-ES.pdf Inglês: https://esfirma.com/doc-pki/PDS-V1.5/TSADS-EN.pdf
E-Seal para TSA/TSU no HSM 1.3.6.1.4.1.47281.1.5.2	

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

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

O esFIRMA nunca gera chaves em software para serem enviadas através de 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 curva elíptica de 256 bits 1.2.840.10045.3.1.7 (NIST-P256/secp256r1).

6.1.2 Envio da Chave Privada ao Signatário

Em certificados num dispositivo de assinatura segura, a chave privada está devidamente protegida dentro do dispositivo seguro.

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

6.1.3 Envio da chave pública ao emissor do certificado

O método de encaminhar a chave pública para o fornecedor do serviço de certificação é o PKCS#10, outra prova criptográfica equivalente, ou qualquer outro método aprovado pelo esFIRMA.

Quando as chaves são geradas num DCCF, o esFIRMA assegura que a chave pública enviada ao fornecedor do serviço de certificação provém de um par de chaves geradas por esse DCCF.[14]

6.1.4 Distribuição da chave pública do fornecedor de serviços de certificação

As chaves do esFIRMA são comunicadas a terceiros que dependem de certificados, garantindo a integridade da chave e autenticando a sua origem, através da sua publicação no Depositário.

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

Os utilizadores podem aceder ao Cofre para obter as chaves públicas e, adicionalmente, em aplicações S/MIME, a mensagem de dados pode conter uma cadeia de certificados, que são assim distribuídos aos utilizadores.

O certificado das ACs raiz e subordinadas estará disponível para os utilizadores no site da esFIRMA.

6.1.5 Tamanhos das teclas

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

6.1.6 Geração de parâmetros de chave pública e verificação de qualidade

A chave pública da Root CA, das CAs subordinadas e dos certificados de assinante está codificada de acordo com o RFC 5280.

Qualidade dos parâmetros de chave pública

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

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

6.1.7 Finalidades do Uso de Teclas

As principais utilizações dos certificados de AC são exclusivamente para assinar certificados e CRLs.

As utilizações de chaves para certificados de entidades finais são exclusivamente para assinatura digital e não repudiação.

6.2 Proteção de Chave Privada e Controlos de Módulos Criptográficos

6.2.1 Normas para Módulos Criptográficos

No que diz respeito aos módulos que gerem as chaves esFIRMA e aos subscritores de certificados de assinatura eletrónica, é assegurado o nível exigido pelas normas indicadas nas secções anteriores.

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

É necessário um controlo multi-pessoa para a ativação da chave privada da CA. No caso deste DPC, existe uma política de **3 em cada 5** pessoas para a ativação das palavras-passe.

Os dispositivos criptográficos estão fisicamente protegidos conforme determinado aqui.

6.2.3 Depósito de Chave Privada

A esFIRMA não armazena cópias das chaves privadas dos signatários.

6.2.4 Backup de Chave Privada

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

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

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

6.2.5 Arquivamento de Chave Privada

As chaves privadas da Califórnia são arquivadas por um período de **10 anos** após a emissão do último certificado. Serão guardados em ficheiros seguros e à prova de fogo e

no centro de custódia externo. Pelo menos duas pessoas serão obrigadas a recuperar a chave privada das CAs 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 de Chaves Privadas em Módulos Criptográficos

As chaves privadas da Autoridade Certificadora são armazenadas encriptadas nos módulos criptográficos de produção do esFIRMA.

6.2.8 Método de Ativação de Chave Privada

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

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

A ativação das chaves privadas Intermédias CA é tratada com o mesmo m de n processo que as chaves CA.

6.2.9 Método de Desativação de 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 deve introduzir o PIN para a nova ativação.

6.2.10 Método de Destruição de Chave Privada

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

Dispositivos que tenham qualquer parte das chaves privadas esFIRMA armazenadas serão fisicamente destruídos ou reiniciados a um nível baixo. Para a remoção, serão seguidos os passos descritos no manual do administrador do computador criptográfico.

Finalmente, os backups serão destruídos de forma segura.

As chaves do signatário no software podem ser destruídas ao eliminá-las, seguindo as instruções da aplicação que as aloja.

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

6.2.11 Classificação do Módulo Criptográfico

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

Os algoritmos de geração de chaves usados são geralmente aceites para a utilização da chave para a qual se destinam.

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

6.3 Outros aspetos da gestão de pares de chaves

6.3.1 Ficheiro de Chave Pública

A esFIRMA arquiva rotineiramente as suas chaves públicas de acordo com a secção 5.5 deste documento.

6.3.2 Períodos de utilização de chaves públicas e privadas

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

6.4 Dados de Ativação

6.4.1 Geração e instalação de dados de ativação

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

A criação e distribuição desses dispositivos é registada.

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

6.4.2 Proteção dos dados de ativação

Os dados de ativação dos dispositivos que protegem as chaves privadas das Autoridades Certificadoras raiz e subordinadas são protegidos pelos detentores dos cartões de administrador dos módulos criptográficos, conforme indicado no documento da cerimónia de chaves.

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

6.4.3 Outros aspetos dos dados de ativação

Não aplicável.

6.5. Controlos de segurança informática

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

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

- Definições de segurança do sistema operativo.
- Definições de segurança da aplicação.
- Dimensionamento correto do sistema.
- Definições de Utilizador e Permissões.
- Definir as Definições do Evento.
- Plano de backup e recuperação.
- Definições antivírus.
- Requisitos de tráfego de rede.

6.5.1 Requisitos técnicos específicos para segurança informática

Cada servidor esFIRMA inclui as seguintes funcionalidades:

- Controlo de acesso aos serviços SubCA e gestão de privilégios.
- Fazer cumprir a separação de deveres para a gestão de privilégios.
- Identificação e autenticação de papéis associados a identidades.
- Arquivamento do histórico dos assinantes e dos dados de auditoria SubCA.
- Auditoria de eventos relacionados com segurança.
- Auto-diagnóstico de segurança relacionado com serviços SubCA.
- Chave SubCA e mecanismos de recuperação do sistema.

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

No caso de a esFIRMA distribuir dispositivos qualificados para criação de assinaturas, irá verificar em todos os momentos que estes dispositivos continuam certificados como DCCF.[15]

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

---

15 ETSI 319 411-2 Ap 6.5.1.a)

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

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

6.5.2 Avaliação do nível de segurança informática

A autoridade certificadora e as aplicações de registo utilizadas pela esFIRMA são fiáveis.

6.6 Controlos técnicos do ciclo de vida

6.6.1 Controlos de Desenvolvimento do Sistema

As aplicações são desenvolvidas e implementadas pela esFIRMA de acordo com os padrões de desenvolvimento e controlo de alterações.

As aplicações têm métodos para verificar a integridade e autenticidade, bem como a correção da versão a utilizar.

6.6.2 Controlos de Gestão de Segurança

A esFIRMA desenvolve as atividades necessárias para a formação e sensibilização dos colaboradores em termos de segurança. Os materiais utilizados para a formação e os documentos que descrevem os processos são atualizados após aprovação por um grupo de gestão de segurança. Para desempenhar esta função, tem um plano anual de treino.

A esFIRMA exige, por contrato, as medidas de segurança equivalentes a qualquer fornecedor externo envolvido no trabalho de certificação.

Classificação e gestão de informação e ativos

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

O sistema de gestão de segurança da informação da esFIRMA detalha os procedimentos de gestão de informação onde é classificado, de acordo com o 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 para gerir e responder a incidentes, através da implementação de um sistema de alertas e da geração de relatórios periódicos.

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

Tratamento e segurança dos media

Todos os meios de comunicação 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 voltarem a ser necessários.

Planeamento do sistema

O departamento de Sistemas da esFIRMA mantém um registo das capacidades do equipamento. Juntamente com a aplicação do controlo de recursos de cada sistema, pode-se prever uma possível redimensionação.

Relatórios de incidentes e respostas

A esFIRMA tem um procedimento para monitorizar incidentes e a sua resolução.

Procedimentos e responsabilidades operacionais

A esFIRMA define atividades, atribuídas a pessoas com um papel de confiança, para além das pessoas responsáveis pela realização das operações diárias que não são confidenciais.

Gestão do sistema de acesso

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

Em particular:

AC General

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

Geração de Certificados

A autenticação do processo de emissão é realizada através de um sistema de n operadores para a ativação da chave privada esFIRMA.

Gestão de Revogações

A revogação será realizada por autenticação forte às candidaturas de um administrador autorizado. Os sistemas de registo irão gerar a prova que garante a não repudiação da ação realizada pelo administrador da esFIRMA.

Estado de revogação

A aplicação de estado de revogação tem controlo de acesso baseado em certificado ou autenticação de dois fatores para evitar tentativas de modificar a informação sobre o estado da revogação.

6.6.3 Avaliação da Segurança ao Longo do Ciclo de Vida

O esFIRMA assegura que o hardware criptográfico utilizado para a assinatura de certificados não é adulterado durante o transporte, inspecionando o material entregue.

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

O esFIRMA regista toda a informação relevante do dispositivo para adicionar ao catálogo de ativos.

A utilização de hardware de assinatura de certificados criptográficos requer o uso de pelo menos dois colaboradores de confiança.

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

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

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

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

6.7 Controlo de Segurança de Rede

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

A informação confidencial que é transferida por redes não seguras é encriptada usando protocolos SSL ou o sistema VPN com autenticação de dois fatores.

6.8 Fontes Temporais

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

6.9 Algoritmos de assinatura e parâmetros do sistema centralizado de assinaturas

O serviço centralizado de assinatura gera chaves para 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 (Gerador Determinístico de Bits Aleatórios) em Modo Real Aleatório (ruído de hardware) segundo o NIST SP 800-90A e testes contínuos segundo o FIPS 140-2. Fora do módulo HSM, as chaves são armazenadas encriptadas com o algoritmo AES-GCM e com um comprimento de chave de 256 bits. A chave de encriptação é derivada do PIN de utilizador e da chave mestra do HSM. A chave mestra HSM utiliza o algoritmo ECDSA NIST-P256/secp256r1 (OID 1.2.840.10045.3.1.7) e requer 3 dos 5 cartões para ativação, tendo sido gerada numa cerimónia de inicialização de alta segurança. O PIN do utilizador é derivado de um servidor salt com o algoritmo PBKDF2-SHA1. O transporte do SAD (Dados de Ativação de Assinatura) do SIC (Componente de Interação de Assinatura) para o SAM (Módulo de Ativação de Assinatura) é protegido por AES-GCM com uma chave de 256 bits derivada de uma troca de chaves usando o algoritmo ECDH, de acordo com o NIST SP 800-56A. A chave do servidor é publicada no repositório web esFirma, secção "Informação de Segurança de Assinatura Remota". O sistema permite a geração de assinaturas eletrónicas com o algoritmo RSA PKCS#1 v1.5, DSA com chave de curva elíptica e algoritmos de resumo SHA-256 e SHA-512.

7. Perfis de Certificados, CRL e OCSP

7.1 Perfil de Certificado

Todos os certificados qualificados emitidos ao abrigo desta política cumprem a seguinte norma X.509 versão 3, RFC 5280, RFC 3739 e normas ETSI:

- 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 de QCStatements de certificados qualificados em conformidade com a RD (UE) 910/2014.

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

7.1.1 Número de Versão

A esFIRMA emite certificados X.509 Versão 3

7.1.2 Prorrogações de Certificados

As extensões dos certificados estão detalhadas nos documentos de perfil acessíveis no site da esFIRMA https://www.esfirma.com

7.1.3 Identificadores de Objeto (OIDs) de Algoritmos

O ID do objeto do algoritmo de assinatura é:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption
- 1.2.840.10045.4.3.2 sha256WithECDSA

O identificador de 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 Formatação do Nome

Os certificados devem conter a informação necessária para o seu uso, conforme determinado pela política correspondente.

A codificação de certificados segue a recomendação RFC 5280 "Lista de Certificados e Revogação de Certificados de Infraestruturas de Chave Pública de Internet (CRL) X.509
Ver perfis no https://www.esfirma.com

7.1.5 Restrição de nomes

Os nomes contidos nos certificados estão restritos a X.500 "Nomes Distintos", que são únicos e inequívocos.

7.1.6 Identificador de Objeto (OID) dos Tipos de Certificados

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

7.1.7 Utilização da Extensão de Restrições de Política

Não aplicável

7.1.8 Qualificadores de Política, Sintaxe e Semântica

Não aplicável

7.1.9 Processamento Semântico para Extensão Crítica de Políticas de Certificados

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

7.1.10 Restrições de Comprimento dos Elementos

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

Elemento	**Comprimento Máximo esFIRMA**	**Duração Base**	**Standard**
2.5.4.42 *(nomeDado, GN)*	**127**	32000***	RFC5280
2.5.4.10 (NomeOrganização)	**256**	64	RFC5280
2.5.4.11 (NomeUnidadeOrganizacional)	**256**	32	RFC5280
2.5.4.4 (apelidos)	**256**	40	RFC5280
2.5.4.3 (NomeComum, CN)	**400**	64	RFC5280
2.5.4.5 (Número de série, SN)	32*	32	RFC5280
2.5.4.97 (identificadorOrganização)	**32**	MAX**	X520
2.5.4.65 (pseudónimo)	**64***	128	RFC5280
2.5.4.12 (título)	64*	64	RFC5280
*As normas ETSI EN 319 412-2 4.2.4 e ETSI EN 319 412-3 4.2.1 permitem exceder os limites estabelecidos no RFC 5280 (desde que estejam indicados no DPC) para os campos de assunto indicados de acordo com o tipo de certificado (NomeDado, apelido, pseudónimo, NomeComum, NomeOrganização e NomeUnidadeOrganizacional), mas não para os restantes campos. O comprimento destes campos está de acordo com o RFC 5280. ** MAX indica que o limite superior não está especificado (RFC5280 Apêndice B. ASN1 Notas) 32000 nome ub usado em vez de nome dado ub (16)			

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

7.2 Perfil da Lista de Revogação de Certificados

De acordo com a norma IETF RFC 3280

7.2.1 Número de Versão

Os CRLs emitidos pela esFIRMA são a versão 2.

7.2.2 CRL e extensões CRL

crlExtensões:

2.5.29.35 (Identificador de chave de autoridade)

2.5.29.20 (Número CRL)

crlEntryExtensions

2.5.29.21 (ReasonCode)

7.3 Perfil OCSP

De acordo com a norma IETF RFC 6960

7.3.1 Número de Versão

Os OCSPs emitidos pela esFIRMA são a versão 3.

7.3.2 Extensões OCSP

responseExtensões

Id: 1.3.6.1.5.5.7.48.1.2 (Extensão OCSP Nãoce)

Crítico: verdade

8. Auditoria de conformidade

A esFIRMA anunciou o início da sua atividade como prestador de serviços de certificação pelo Ministério dos Assuntos Económicos e a Transformação Digital está sujeita às revisões de controlo que este organismo considerar necessárias.

8.1 Frequência da Auditoria de Conformidade

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

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

8.2 Identificação e qualificação do auditor

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

8.3 Relação do auditor com a entidade auditada

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

8.4 Lista de itens sujeitos a auditoria

A auditoria verifica relativamente a esta ASSINATURA:

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

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

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

8.5 Ações a serem tomadas devido à falta de conformidade

Depois de a gestão receber o relatório da auditoria de conformidade realizada, as deficiências encontradas são analisadas com a empresa que executou a auditoria e é desenvolvido e executado um plano corretivo para resolver essas deficiências.

Se a esFIRMA não conseguir desenvolver e/ou executar tal plano ou se as deficiências encontradas representarem uma ameaça imediata à segurança ou integridade do sistema, deve notificar imediatamente a gestão sénior da esFIRMA, que poderá realizar as seguintes ações:

- Cessar temporariamente as operações.
- Revogue a chave da CA e regenere a infraestrutura.
- Termina o serviço de ar condicionado.
- Outras ações complementares que podem ser necessárias.

8.6 Tratamento dos relatórios de auditoria

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

9. Requisitos Empresariais e Jurídicos

9.1 Taxas

9.1.1 Taxa de Emissão ou Renovação de Certificados

A esFIRMA pode estabelecer uma taxa pela emissão de certificados, da qual, quando apropriado, os subscritores serão informados oportunamente.

9.1.2 Taxa de Acesso ao Certificado

A esFIRMA não estabeleceu qualquer taxa de acesso aos certificados.

9.1.3 Taxa de Acesso à Informação sobre o Estado do Certificado

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

9.1.4 Taxas por Outros Serviços

Sem estipulação.

9.1.5 Política de Retirada

Sem estipulação.

9.2 Responsabilidade Financeira

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

9.2.1 Cobertura de Seguro

A esFIRMA tem garantia de cobertura suficiente da sua responsabilidade civil, através de seguro de responsabilidade civil profissional que cumpra as disposições do 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, que regula certos aspetos dos serviços fiduciários eletrónicos, com um seguro mínimo de 3.000.000 de euros.

9.2.2 Outros ativos

Sem estipulação.

9.2.3 Cobertura de Seguro para Assinantes e Terceiros Com Base em Certificados

A esFIRMA tem garantia de cobertura suficiente da sua responsabilidade civil, através de seguro de responsabilidade civil profissional que cumpra as disposições do regime de obrigações e responsabilidades do Regulamento (UE) 910/2014, e o artigo 9.3.b) da Lei 6/2020, de 11 de novembro, que regula certos aspetos dos serviços eletrónicos de trust com um seguro mínimo de 3.000.000 de euros.

9.3 Confidencialidade da Informação

9.3.1 Informação confidencial

As seguintes informações são mantidas confidenciais pela esFIRMA:

- Pedidos de certificados, aprovados ou recusados, bem como qualquer outra informação pessoal obtida para a emissão e manutenção de certificados, exceto a informação indicada na secção seguinte.
- Chaves privadas geradas e/ou armazenadas pelo fornecedor do serviço de certificação.
- Registos de transações, incluindo registos completos e registos de auditoria das transações.
- Registos de auditoria interna e externa, criados e/ou mantidos pelo Organismo de Certificação e pelos seus auditores.
- Continuidade do negócio e planos de emergência.
- Política e planos de segurança.

- Documentação de operações e outros planos operacionais, como arquivamento, monitorização e outros documentos semelhantes.
- Todas as outras informações identificadas como "Confidenciais."

9.3.2 Informação não confidencial

As seguintes informações são consideradas não confidenciais:

- Certificados emitidos ou em processo de emissão.
- A ligação do assinante a um certificado emitido pela Autoridade de Certificação.
- O nome e os apelidos da pessoa física identificada no certificado, bem como quaisquer outras circunstâncias ou dados pessoais do titular, caso sejam significativos para o propósito do certificado.
- O endereço de email da pessoa física identificada no certificado, ou o endereço de email atribuído pelo assinante, se significativo em relação ao propósito do certificado.
- Os usos e os limites económicos delineados no certificado.
- O período de validade do certificado, bem como a data de emissão do certificado e a data de validade.
- O número de série do certificado.
- Os diferentes estados ou situações do certificado e a data de início de cada um deles, especificamente: geração pendente e/ou entrega, válido, revogado, suspenso ou expirado e a razão que causou a alteração de estatuto.
- Listas de revogação de certificados (CRLs), bem como outras informações sobre o estado da revogação.
- Qualquer outra informação que não esteja listada na secção anterior.

9.3.3 Divulgação de Informações de Suspensão e Revogação

Ver a secção anterior.

9.3.4 Divulgação Legal de Informação

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

Especificamente, os registos que garantem a fiabilidade dos dados contidos no certificado, bem como os registos relacionados com a fiabilidade dos dados e os relacionados com a operação[17], serão divulgados se for necessário para apresentar prova da certificação num processo judicial, mesmo sem o consentimento do subscritor do certificado.

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

9.3.5 Divulgação de informações a pedido do proprietário

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

9.3.6 Outras Circunstâncias de Divulgação de Informação

Sem estipulação.

9.4 Privacidade das Informações Pessoais

A esFIRMA compromete-se a cumprir os regulamentos sobre a proteção de dados pessoais, com as respetivas medidas de segurança, conforme previsto 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 revogando a Diretiva 95/46/CE. e na Lei Orgânica 3/2018, de 5 de dezembro, sobre a Proteção dos Dados Pessoais e garantia dos direitos digitais.

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

[17] Secção 7.10.c) do ETSI EN 319 401

A esFIRMA tem o estatuto de responsável pelo tratamento de dados pessoais e, como tal, processa os dados de forma exclusiva e exclusiva para os fins contidos nesta Declaração de Práticas de Certificação, de acordo com as instruções do responsável pelo tratamento de dados, que é o ASSINANTE, e que estão incluídas no Anexo "*Anexo 1: Para o tratamento de dados pessoais pela ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A., na sua qualidade de RESPONSÁVEL*", que rege o contrato para a prestação do serviço "Gestiona" entre o SUBSCRITOR e ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.

9.4.1 Plano de Privacidade

A esFIRMA desenvolveu uma política de privacidade em conformidade com o REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 sobre a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, revogando a Diretiva 95/46/CE, e com a Lei Orgânica 3/2018, de 5 de dezembro, sobre a Proteção dos Dados Pessoais e garantia dos direitos digitais, e documentou nesta Declaração de Práticas de Certificação, bem como no Anexo "Anexo 1: *Para o tratamento de dados pessoais pela ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. na sua qualidade de RESPONSÁVEL PELO TRATAMENTO DE DADOS*" que regula o contrato para a prestação do serviço "Gerir" entre o SUBSCRITOR e a ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A., os aspetos, procedimentos e medidas de segurança e organizacionais em conformidade com o regime de obrigações e responsabilidades contido nos regulamentos anteriores.

9.4.2 Informação tratada como privada

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

9.4.3 Informação não considerada privada

As informações pessoais sobre um indivíduo disponíveis no conteúdo de um certificado ou CRL são consideradas não privadas, pois são necessárias para a prestação do serviço contratado, sem prejuízo dos direitos correspondentes ao titular dos dados pessoais ao abrigo da legislação LOPD/RGPD.

9.4.4 Responsabilidade de Proteger a Informação Privada

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

9.4.5 Aviso e Consentimento para o Uso de Informação Privada

Antes de celebrar uma relação contratual, as partes interessadas deverão ser oferecidas as

informações prévias sobre o tratamento dos seus dados pessoais e exercício dos seus direitos, e, quando apropriado, obterão o consentimento obrigatório para o tratamento diferenciado do tratamento principal para a prestação dos serviços contratados.

9.4.6 Divulgação ao abrigo de processos judiciais ou administrativos

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

9.4.7 Outras Circunstâncias de Divulgação de Informação

Os dados pessoais não são transferidos para terceiros, salvo obrigação legal.

9.5 Direitos de Propriedade Intelectual

9.5.1 Propriedade de Certificados e Informações de Revogação

Apenas a esFIRMA detém direitos de propriedade intelectual sobre os certificados que emite, sem prejuízo dos direitos dos assinantes, detentores de chaves e terceiros, a quem concede uma licença não exclusiva para reproduzir e distribuir certificados, gratuitamente, desde que a reprodução seja completa e não altere qualquer elemento do

certificado, sendo necessária em relação a assinaturas digitais e/ou sistemas de encriptação no âmbito de utilização do certificado. e de acordo com a documentação que os liga.

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

As mesmas regras aplicam-se à utilização de informações de revogação de certificados.

9.5.2 Propriedade da Declaração de Práticas de Certificação

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

9.5.3 Propriedade da Informação do Nome

O assinante e, quando aplicável, a pessoa física identificada no certificado, detém todos os direitos, se existirem, sobre a marca, produto ou nome comercial contido no certificado.

O assinante é o proprietário do nome distinto do certificado, que consiste nas informações especificadas na secção 3.1.1

9.5.4 Propriedade de Chaves

Os pares de chaves são propriedade dos signatários do certificado.

Quando uma chave é partida em partes, todas as partes da chave pertencem ao proprietário da chave.

9.6 Obrigações e responsabilidade civil

9.6.1 Obrigações do Organismo de Certificação "esFIRMA"

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

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

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

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

A esFIRMA vincula subscritores, detentores de chaves e terceiros que dependem de certificados através do referido texto de divulgação ou PDS, em linguagem escrita e compreensível, com o seguinte conteúdo mínimo:

- Requisitos para cumprir as Secções 4.5.3, 9.2, 9.6.7, 9.6.8, 9.6.9 e 9.6.10.
- Indicação da política aplicável, indicando que os certificados não são emitidos ao público.
- Declaração de que a informação contida no certificado está correta, salvo notificação em contrário pelo assinante.
- Consentimento para o armazenamento da informação utilizada para o registo do subscritor e para a transferência dessa informação a terceiros, no caso de

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

cessação das operações do Organismo Certificador sem revogação de certificados válidos.

- Limites de utilização de certificados, incluindo os estabelecidos na secção 1.4.2
- Informação sobre como validar um certificado, incluindo a exigência de verificar o estado do certificado, e as condições sob as quais o certificado pode ser razoavelmente confiável, o que se aplica quando o assinante atua como um terceiro confiante no certificado.
- A forma como a responsabilidade financeira do Organismo de Certificação é garantida.
- Limitações de responsabilidade aplicáveis, incluindo os usos para os quais o Organismo de Certificação aceita ou exclui a sua responsabilidade.
- Período de arquivamento das informações do pedido de certificado.
- Período de arquivamento dos registos de auditoria.
- Procedimentos Aplicáveis de Resolução de Litígios.
- Lei aplicável e jurisdição competente.
- Se o Organismo de Certificação foi declarado em conformidade com a política de certificação e, se aplicável, de acordo com qual sistema.

9.6.2. Obrigação e Responsabilidade da RA

Os ARs são as entidades designadas pela CA para realizar as tarefas de registo e aprovação dos pedidos de certificação, pelo que a RA também está obrigada, nos termos definidos nas Práticas de Certificação, para a emissão de certificados, principalmente:

• Respeitar as disposições deste CPS e do respetivo PDS.

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

• Verificar a identidade dos Sujeitos/Signatários e Requerentes dos certificados quando necessário, acreditando de forma definitiva a identidade do Signatário, no caso de certificados individuais, ou do titular da chave, no caso de certificados de organização, de acordo com as disposições das respetivas secções deste documento.

• Verificar a precisão e autenticidade das informações fornecidas pelo Requerente.

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

• Entregar, quando apropriado, o dispositivo criptográfico correspondente.

• Arquivo, para o período previsto na legislação vigente, os documentos fornecidos pelo requerente ou Signatário.

• Respeitar as disposições dos contratos assinados com a esFIRMA e com o Sujeito/Signatário.
• Informar a esFIRMA das causas da revogação, desde que tenham conhecimento.
• Fornecer informações básicas sobre a política e a utilização do certificado, incluindo especialmente informações sobre o esFIRMA e a Declaração de Práticas de Certificação aplicável, bem como as suas obrigações, poderes e responsabilidades.
• Fornecer informações sobre o certificado e o dispositivo criptográfico.
• Recolher informações e provas do titular da receção do certificado e, quando apropriado, do dispositivo criptográfico, e da aceitação desses elementos.
• Informar o titular da chave privada e dos seus dados de ativação do certificado e, quando apropriado, do dispositivo criptográfico do método exclusivo de imputação, de acordo com as disposições das secções correspondentes deste documento.
Estas obrigações aplicam-se mesmo nos casos de entidades por elas delegadas, como os pontos de verificação presencial (PVP).
Informações sobre a utilização e responsabilidades dos assinantes são fornecidas através do
Aceitação das cláusulas de utilização antes da confirmação do pedido do certificado e por email.

Os RAs assinam um contrato de prestação de serviços com a esFIRMA através do qual a esFIRMA delega as funções de registo aos RAs, consistindo principalmente em:
1.- Obrigações anteriores à emissão de um certificado.
a) Informar adequadamente os candidatos sobre a assinatura das suas obrigações e responsabilidades.
b) A identificação adequada dos candidatos, que devem ser pessoas qualificadas ou qualificadas.
autorizado a solicitar um certificado digital.
c) A verificação correta da validade e validade destes dados dos requerentes, e
da Entidade, caso exista uma relação de relação de relação de relação ou representação.
d) Aceder à candidatura da Autoridade de Registo para gerir candidaturas e
Certificados emitidos.
2.- Obrigações após a emissão do certificado.
a) Assinar os contratos para a Prestação de Serviços de Certificação Digital com os candidatos. Na maioria dos processos de emissão, este contrato é formalizado pela aceitação de condições nos sites que fazem parte do processo

da emissão do certificado, e a emissão não pode ser realizada sem antes ter aceite as condições de utilização.

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

c) Apresentar cópias da documentação submetida e dos contratos devidamente assinados pelos requerentes, de acordo com as Políticas de Certificação publicadas pela esFIRMA e a legislação em vigor.

Assim, os RAs são responsáveis pelas consequências em caso de incumprimento das suas tarefas de registo, e também se comprometem a respeitar as regras regulatórias internas do organismo certificador esFIRMA (Políticas e CPS), que devem ser perfeitamente controladas pelos RAs e que devem servir como manual de referência.

No caso de uma reclamação por parte de um Sujeito, uma Entidade ou um utilizador, a AC deve fornecer o

prova de ação diligente e, se se verificar que a origem da queixa reside num erro na validação ou verificação dos dados, a CA pode, em virtude dos acordos assinados com os RAs, fazer com que a RA responsável assuma as consequências.

Porque, embora a CA seja legalmente responsável perante o Sujeito, uma Entidade ou Parte Utilizadora, e que para tal dispõe de seguro de responsabilidade civil, de acordo com o acordo atual, a RA tem a obrigação contratual de "identificar e autenticar corretamente o Requerente e, quando apropriado, a Entidade correspondente", e, em virtude disso, deve responder a esta ASSINATURA pelas suas violações.

Claro que não é intenção da esFIRMA descarregar todo o peso da assunção de responsabilidade aos RAs em termos de possíveis danos cuja origem resultaria de uma violação das tarefas delegadas aos RAs. Por esta razão, conforme previsto para a AC, a RA está sujeita a um regime de controlo que será exercido pela esFIRMA, não apenas através dos controlos dos arquivos e dos procedimentos de conservação dos arquivos assumidos pela RA através da realização de auditorias para avaliar, entre outros, os recursos utilizados e o conhecimento e controlo dos procedimentos operacionais para prestar serviços à RA.

As mesmas responsabilidades devem ser assumidas pelo RA em virtude de violações do entidades delegadas, como os Pontos de Verificação no Local (PVPs), sem

prejuízo ao seu direito de ter repercussões contra si.

9.6.3 Garantias Oferecidas a Assinantes e Terceiros Com Base em Certificados

o esFIRMA, na documentação que o liga a assinantes e terceiros que dependem de certificados, estabelece e renuncia a garantias, bem como às limitações de responsabilidade aplicáveis.

A esFIRMA, pelo menos, garante ao assinante:

- Que não existem erros factuais na informação contida nos certificados, conhecidos ou emitidos pelo Organismo Certificador.
- Que não existem erros factuais na informação contida nos certificados, devido à falta de diligência devida na gestão da candidatura do certificado ou na criação do mesmo.
- Que os certificados cumpram todos os requisitos materiais estabelecidos na Declaração de Práticas de Certificação.
- Que os serviços de revogação e a utilização do Depósito cumpram todos os requisitos materiais estabelecidos na Declaração de Práticas de Certificação.

O esFIRMA, no mínimo, garantirá que o terceiro confie no certificado:

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

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

- Que o certificado contém a informação que um certificado qualificado deve conter, de acordo com o Anexo 1 do Regulamento (UE) 910/2014.
- Que, no caso de gerar as chaves privadas do assinante ou, quando apropriado, da pessoa física identificada no certificado, a sua confidencialidade é mantida durante o processo.
- Responsabilidade do Organismo de Certificação, dentro dos limites estabelecidos. Em nenhum caso a ESFIRMA será responsável por acontecimentos fortuitos e em caso de força maior.

- A chave privada da CA usada para emitir certificados não foi comprometida, a menos que a esFIRMA não tenha comunicado o contrário.
- Não originou nem introduziu declarações falsas ou erradas na informação de qualquer certificado, nem deixou de incluir as informações necessárias fornecidas pelo assinante e validadas pelo esFIRMA no momento da emissão do certificado.
- Todos os certificados cumprem os requisitos formais e de conteúdo desta Declaração de Prática, incluindo todos os requisitos legais aplicáveis e aplicáveis.
- Está vinculado pelos procedimentos de segurança e operacionais descritos nesta Declaração de Prática.

9.6.4 Responsabilidade e responsabilidade de terceiros

Será obrigação da Parte Utilizadora cumprir as disposições dos regulamentos em vigor e, adicionalmente:

- Verifique a validade dos certificados e de toda a cadeia de certificação antes de realizar qualquer operação baseada neles. A esFIRMA dispõe de vários mecanismos para realizar esta verificação, como o acesso a listas de certificados revogados ou os serviços de consulta online da OCSP.
- Conheça, esteja vinculado e concorde em estar vinculado pelas garantias, limites e responsabilidades aplicáveis à aceitação e utilização dos certificados em que confia.
- Verifique a validade da qualificação de uma assinatura associada a um certificado emitido pela esFIRMA, verificando que a autoridade certificadora que emitiu o certificado está publicada na lista de confiança do supervisor nacional correspondente.

9.6.5 Responsabilidade e obrigação dos outros participantes

Não estipulado

9.7. Renúncia da Garantia

De acordo com a legislação atual, a responsabilidade da esFIRMA e dos seus RAs não se estende aos casos em que o uso indevido do certificado tem origem em

conduta atribuível ao Sujeito, e à Parte Utilizadora por:

- Falha em fornecer informação adequada, inicialmente ou posteriormente, tais como
- Como resultado de alterações nas circunstâncias refletidas no certificado eletrónico, quando a sua imprecisão não pôde ser detetada pelo prestador do serviço de certificação
- Negligência relativamente à retenção de dados de criação de assinaturas e à sua confidencialidade.
- Não ter solicitado a revogação dos dados do certificado eletrónico em caso de dúvida sobre a manutenção da confidencialidade
- Utilizar a assinatura após o período de validade do certificado eletrónico ter expirado
- Exceda os limites que constam no certificado eletrónico.
- Em conduta atribuível à Parte do Utilizador, se o Utilizador agir de forma negligente, ou seja, quando não verifica ou não tem em conta as restrições contidas no certificado quanto aos seus possíveis usos e limite ao montante das transações; ou quando não tem em conta o estatuto de validade do certificado
- Danos causados ao Sujeito ou a terceiros a eles confiados devido à imprecisão dos dados contidos no certificado eletrónico, se estes tiverem sido acreditados através de um documento público, registado num registo público se necessário.
- Uma utilização inadequada ou fraudulenta do certificado no caso de o Sujeito/Titular o ter cedido ou autorizado a sua utilização a favor de um terceiro em virtude de uma transação legal, como o mandato ou procuração, sendo responsabilidade exclusiva do Sujeito/Titular controlar as chaves associadas ao seu certificado.

A esFIRMA e os seus RAs não serão responsabilizados em qualquer caso quando se depararem com qualquer uma destas circunstâncias:

- Estado de guerra, desastres naturais ou qualquer outro caso de Força Maior.
- Para o uso dos certificados, desde que ultrapasse as disposições dos regulamentos e Políticas de Certificação vigentes
- Devido à utilização indevida ou fraudulenta de certificados ou CRLs emitidos pela CA
- Para a utilização da informação contida no Certificado ou no CRL.
- Pelos danos causados no período de verificação das causas de revogação.

- Pelo conteúdo das mensagens ou documentos assinados ou encriptados digitalmente.
- Para a não recuperação de documentos encriptados com a chave pública do Sujeito.

9.8. Limitação de Responsabilidade por Perdas de Transação

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

9.9. Compensação

Ver secção 9.2

9.10. Período e Conclusão

9.10.1 Mandato

Ver secção 5.8

9.10.2 Rescisão

Ver secção 5.8

9.10.3 Efeito da terminação e sobrevivência

Ver secção 5.8

9.11. Comunicação com as partes interessadas e o órgão supervisor

A esFIRMA estabelece no contrato com o subscritor os meios para notificações entre ambas as partes.

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

No caso de um incidente que possa afetar a segurança, os dados pessoais ou a integridade de uma pessoa física ou jurídica, aplicar-se-ão as disposições do procedimento de gestão de incidentes da esFIRMA.

A esFIRMA tem procedimentos para comunicar alterações relevantes na prestação de serviços fiduciários ao órgão supervisor. Tais alterações devem ser notificadas ao órgão supervisor pelo menos um mês antes da sua implementação. No caso da cessação de um serviço fiduciário, a esFIRMA deve notificar o órgão supervisor pelo menos três meses antes da data de fim prevista.

9.12. Alterações

9.12.1 Procedimento de modificação

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

9.12.2 Mecanismo de notificação e prazos

Todas as alterações propostas a esta política serão imediatamente publicadas no site da esFIRMA. Neste mesmo documento existe uma secção de alterações e versões onde pode

saber sobre as alterações que ocorreram desde a sua criação e a data dessas modificações.
As alterações a este documento são comunicadas às entidades e empresas terceirizadas que emitem certificados ao abrigo deste CPS, bem como aos respetivos auditores. Em particular, alterações neste CPS serão notificadas aos Órgãos Nacionais de Supervisão.

Os Signatários/Assinantes e os Terceiros afetados de confiança podem submeter os seus comentários à organização de administração da política no prazo de 15 dias após a receção da notificação.

9.12.3 Circunstâncias em que o OID deve ser alterado

Não estipulado

9.13 Procedimento de resolução de litígios

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

9.14. Legislação aplicável

A esFIRMA estabelece, no contrato de subscrição e no texto de divulgação ou PDS, que a lei aplicável à prestação de serviços, incluindo a política e práticas de certificação, é 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 dependem dos Certificados assumem plenamente o conteúdo desta Declaração de Práticas e Políticas de Certificação

9.16.2 Atribuição

As partes deste DPC não podem ceder quaisquer dos seus direitos ou obrigações ao abrigo deste DPC ou acordos aplicáveis sem o consentimento escrito da esFIRMA.

9.16.3 Separabilidade

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

- Ao abrigo da cláusula de separabilidade, a invalidade de uma cláusula não afeta o restante do contrato.
- Ao abrigo da cláusula de sobrevivência, certas regras continuarão em vigor após a cessação da relação jurídica que regula a notificação entre as partes. Para tal, o Organismo de Certificação assegura que, pelo menos, os requisitos contidos nas secções 9.6.1 (Obrigações e responsabilidade), 8.6.1 (Auditoria de conformidade) e 9.3 (Confidencialidade) continuem após a cessação do serviço e as condições gerais de emissão/utilização.
- Em virtude da cláusula de todo o acordo, entende-se que o documento legal que regula a notificação contém o testamento completo e todos os acordos entre as partes.
- A cláusula de notificação estabelecerá o procedimento pelo qual as partes se notificam mutuamente dos factos.

9.16.4 Conformidade (Honorários de Advogados e Renúncia)

A esFIRMA pode pedir compensação e honorários advocatícios a uma das partes para danos, perdas e despesas relacionadas com a conduta dessa parte. O facto de que A esFIRMA não faz cumprir uma disposição deste CPS não elimina o direito da esFIRMA para fazer cumprir as mesmas disposições posteriormente ou o direito de fazer cumprir qualquer outra disposição deste SPC. Para ser eficaz, qualquer renúncia deve ser por escrito e assinada pela esFIRMA

9.16.5 Força Maior

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

9.17 Outras disposições

9.17.1 Cláusula de indemnização do assinante

A esFIRMA inclui no contrato com o subscritor uma cláusula pela qual este se compromete a isentar a Entidade Certificadora de qualquer dano resultante de qualquer ação ou omissão que resulte em responsabilidade, prejuízo ou prejuízo, despesas de qualquer tipo, incluindo despesas legais e de representação jurídica que possam ser incorridas, para a publicação e utilização do certificado, quando ocorrer qualquer uma das seguintes causas:

- Falsidade ou declaração errada feita pelo utilizador do certificado.
- Erro do utilizador do certificado ao fornecer os dados da aplicação, se a ação ou omissão envolveu intenção ou negligência relativamente ao Organismo de Certificação ou a qualquer pessoa que confie no certificado.
- Negligência na proteção da chave privada, na utilização de um sistema de confiança ou na manutenção das precauções necessárias para evitar comprometimento não autorizado, perda, divulgação, modificação ou utilização da chave privada.
- Utilização, pelo assinante, de um nome (incluindo nomes comuns, endereços de e-mail e nomes de domínio), ou outra informação no certificado, que infrinja os direitos de propriedade intelectual ou industrial de terceiros.

9.17.2 Cláusula de indemnização de terceiros que se baseiam no certificado

A esFIRMA inclui no texto de divulgação ou PDS uma cláusula pela qual o terceiro que se baseia no certificado concorda em isentar o Organismo de Certificação de quaisquer danos resultantes de qualquer ação ou omissão resultando em responsabilidade, dano ou perda, despesas de qualquer tipo, incluindo despesas legais e de representação legal que possam ser incorridas, para a publicação e utilização do certificado, quando ocorrer qualquer uma das seguintes causas:

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

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

- Incumprimento das obrigações do terceiro com base no certificado.
- Confiança imprudente num certificado, dependendo das circunstâncias.
- Falha em verificar o estado de um certificado, para determinar que não é
é suspenso ou revogado.
- Falha em verificar todas as medidas de segurança prescritas no
DCP ou outras regras aplicáveis.

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