Declaración de Prácticas de Certificación

esFIRMA

Información general

Control documental

Clasificación de seguridad:	Público
Autor:	ESFIRMA
Versión:	1.21

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Oficina de seguridad Fecha: 08/07/2026	Responsable de seguridad Fecha: 08/07/2026	Comité de seguridad Fecha: 08/07/2026

Control de versiones

Ver	Descripción del cambio	Fecha
1.0	Creación del documento	29/04/2016
1.1	Subsanaciones	02/06/2016
1.2	Revisión ETSI	19/05/2017
1.3	Revisión tipos de certificados	
1.4	Revisión tipos de certificados, Acrónimos y Definiciones	02/06/2017
1.5	Ajustes referencias normativas, cambio de denominación, cambio 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 Duración TSA	20/06/2018
1.7	Corrección referente a la firma en la emisión de certificados software	08/08/2018
1.8	Adaptación por cambio normativo (Reglamento (UE) 910/2014 y Reglamento (UE) 2016/679) y revisión sobre los apartados de renovación.	13/11/2018
1.9	3.1.1.1 Aclaración sobre el segundo apellido opcional. 3.1.1.2 OrganizationIdentifier condicionado a CA/Browser Forum Guidelines 3.1.1.4 Ajuste de errores tipográficos las descripciones de los OID 3.1.1.7 CN del certificado EV de sede opcional	14/06/2019
1.10	Clarificaciones varias en 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 Alineación con RFC 3647 1.5.3. movido a 1.5.2 Datos de contacto de la organización 1.5.2 movido a 1.5.3 Organización que aprueba el documento “DEFINITIONS ACRONYMS” movido a 1.6 Acrónimos y definiciones 4.4.2 movido a 4.4.1 Conducta que constituye aceptación del certificado 4.4.3 movido a 4.4.2 Publicación del certificado 4.4.4 movido a 4.4.3 Notificación de la emisión a terceros Añadido 4.6.1 Circunstancias para la renovación del certificado Añadido 4.6.2 Quién puede pedir una renovación Añadido 4.6.3 Procesamiento de la solicitud de renovación de certificados Añadido 4.6.4 Notificación de nueva emisión de certificado al suscriptor Añadido 4.6.5 Conducta que constituya la aceptación de un certificado de renovación Añadido 4.6.6 Publicación del certificado de renovación por la CA Añadido 4.6.7 Notificación de la emisión del certificado por la CA a otras entidades Añadido 4.7.2 Procedimiento con nueva identificación 4.7. movido a 4.7.3 Procesamiento de solicitudes de nueva clave de certificado 4.7.3 movido a 4.7.4 Notificación de la emisión del certificado renovado 4.7.4 movido a 4.7.5 Conducta que constituye aceptación del certificado 4.7.5 movido a 4.7.6 Publicación del certificado 4.7.6 movido a 4.7.7 Notificación de la emisión a terceros 4.11 movido a 4.10 Servicios de comprobación de estado de certificados 4.11.1 movido a 4.10.1 Características operativas de los servicios 4.11.2 movido a 4.10.2 Disponibilidad de los servicios Añadido 4.10.3 Características opcionales 4.10 movido a 4.11 Finalización de la suscripción 6.1.9 movido a 6.1.7 Propósitos de uso de claves 6.2.9 movido a 6.2.9 Método de desactivación de la clave privada 6.2.10 movido a 6.2.10 Método de destrucción de la clave privada Añadido 6.2.11 Clasificación del módulo criptográfico Añadido 6.4.3 Otros aspectos de los datos de activación	08/06/2020

	6.6.2.5 movido a 6.6.3 Evaluación de la seguridad del ciclo de vida 6.9 movido a 6.8 Fuentes de Tiempo Añadido 7.1.7 Uso de la extensión de restricciones de política Añadido 7.1.8 Calificadores de política sintaxis y semántica Añadido 7.1.9 Semántica de procesamiento para la extensión crítica de Políticas de certificado Añadido 7.2.2 CRL y extensiones CRL Añadido 7.3.1 Número de versión Añadido 7.3.2 Extensiones OCSP Añadido 9.4.1 Plan de privacidad Añadido 9.4.2 Información tratada como privada Añadido 9.4.3 Información no considerada privada Añadido 9.4.4 Responsabilidad de proteger la información privada Añadido 9.4.5 Aviso y consentimiento para usar información privada Añadido 9.4.6 Divulgación de conformidad con un proceso judicial o administrativo Añadido 9.4.7 Otras circunstancias de divulgación de información Añadido 9.6.2 RA representations and warranties 9.6.2 movido a 9.6.3 Garantías ofrecidas a suscriptores y terceros que confían en certificados Añadido 9.6.4 Obligación y responsabilidad de terceras partes 9.6.2 movido a 9.6.5 Obligación y responsabilidad de otras participantes 9.6.3 movido a 9.7 Exoneración de responsabilidad 9.6.4 movido a 9.8 Limitación de responsabilidad en caso de pérdidas por transacciones 9.6.5 movido a 9.9 Indemnizaciones Añadido 9.10. Plazo y Finalización Añadido 9.10.1 Plazo Añadido 9.10.2 Terminación Añadido 9.10.3 Efecto de la terminación y la supervivencia Añadido 9.11 Notificaciones individuales y comunicación con los participantes Añadido 9.12 Modificaciones Añadido 9.12.1 Procedimiento de modificación Añadido 9.12.2 Mecanismo de notificación y plazos Añadido 9.12.3 Circunstancias en las que se debe cambiar el OID 9.6.10 movido a 9.13 Procedimiento de resolución de conflictos 9.6.7 movido a 9.14 Legislación aplicable Añadido 9.15 Conformidad con la Ley Aplicable Añadido 9.16 Otras disposiciones Añadido 9.16.1 Acuerdo completo Añadido 9.16.2 Asignación 9.6. movido a 9.16.3 Separabilidad Añadido 9.16.4 Cumplimiento (honorarios de abogados y exención de derechos) 9.6.6 movido a 9.16.5 Fuerza mayor Añadido 9.17 Otras provisiones Se incluyen nuevos certificados: certificado de empleado público (Autenticación), certificado de empleado público con seudónimo (Autenticación), certificado de persona física vinculada a entidad (Autenticación), certificado de persona física vinculada a entidad (FIRMA), certificado de persona física con seudónimo vinculada a entidad(Autenticación), certificado de persona física con seudónimo vinculada a entidad (FIRMA)	
1.11	Se incluye nuevos certificados cualificados de sellos electrónicos Se elimina el perfil de certificado de sede electrónica. Adaptación por cambio normativo (Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza).	03/05/2021

	Se añade en el apartado 5.8 Terminación del Servicio de la DPC el detalle de cómo se provee la información de estado de los certificados más allá del tiempo de vida de estos. Se actualizan las referencias al Ministerio de Industria, Energía y Turismo por el Ministerio de Asuntos Económicos y Transformación Digital.	
1.12	Se modifica el punto 5.2.1 cambiando la denominación de "Administrador de Registro" a "Operador de Registro". Se eliminan referencias a CA/B Forum.	10/05/2021
1.13	Modificación punto 5.8 Terminación del Servicio, acorde al Plan de Cese Se modifica el punto 4.9.1 incluyendo el fin de la certificación del QSCD Modificación punto 6.5.1, incluyendo el fin de la certificación DCCF. Eliminación de referencia al documento de seguridad de esFIRMA del apartado 6.6.2 (Operaciones de gestión) Sustitución de "política de seguridad" por "sistema de gestión de seguridad de la información" en el apartado 6.6.2 (Clasificación y gestión de información y bienes) Se añade el apartado 6.9 conforme a ETSI TS 119 431-1: OVR-5.1-02 Se modifica el punto 9.6.4, incluyendo la Cadena de Certificación como punto de verificación. Se añade el sistema de integración con DIR3 como medio para la verificación de la identidad de la entidad (3.2.2) Se añade la verificación del estado de los certificados de la cadena de certificación en el apartado 4.9.6.	18/07/2022
1.14	Información del nuevo certificado de TSA	16/03/2023
1.15	Ajustes información sobre TSA e incorporación sello de tiempo no cualificado	31/03/2023
1.16	Nuevas restricciones de longitud de los elementos de los perfiles de certificados Nuevos subperfiles europeos de Persona física y Sello electrónico Simplificación de los apartados 3.2.2 y 3.2.3 Se añade apartado 4.5.3 para separar la información y obligaciones de los terceros que confían en los certificados. Diferencias y consideraciones entre las consultas de estado de revocación de un certificado mediante OCSP y CRL 4.10.1	21/04/2023
1.17	Se elimina del apartado 5.8 la posibilidad de transferir la gestión de los certificados emitidos a otro prestador en el caso de terminación del servicio.	10/02/2024
1.18	Se incluye tiempo máximo entre la validación de la identidad y la emisión del certificado (apartado 3.2.3.2) Se incluye proceso excepcional en caso de no poder confirmar la solicitud de revocación en menos de 24 hs (apartado 4.9.5) Nuevo apartado 1.4.3. Emisión de certificados de prueba	26/07/2024
1.19	Revisión del apartado 9.11	17/03/2025

1.20	Modificación apartado 5.8 y 9.11. Se añade FIPS 140-3 Level 3 por la TSA. Modificación punto 5.8 Terminación del Servicio, acorde al Plan de Cese	02/05/2026
1.21	Se eliminan referencias al RSA2048 Se elimina referencia a apartados y versiones concretas de normas ETSI. Se añade referencia al Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital. Se modifica el apartado 9.13 Procedimiento de resolución de conflictos	08/07/2026

Índice

1. Introducción....18
1.1 Presentación....18
1.2 Nombre del documento e identificación....19
1.2.1 Identificadores de certificados....19
1.3 Participantes en los servicios de certificación....20
1.3.1. Prestador de servicios de certificación....20
esFIRMA AC raíz 2....21
esFIRMA AC AAPP 2....22
Plataforma de Administración Electrónica....22
1.3.2 Autoridades de Registro....22
1.3.3 Entidades finales....23
1.3.4 Partes usuarias....23
1.3.5 Otros participantes....24
Firmantes....24
1.4 Uso de los certificados....25
1.4.1 Usos permitidos para los certificados....25
Certificado de Empleado Público nivel alto en Tarjeta....25
Certificado de Empleado Público nivel medio en HSM....27
Certificado de Empleado Público nivel alto en tarjeta para autenticación....29
Certificado de Sello de Órgano nivel medio en software....30
Certificado de Sello de Órgano nivel medio en HSM....31
Certificado de Empleado Público con Seudónimo nivel alto en Tarjeta....33
Certificado de Empleado Público con seudónimo nivel medio, en HSM....34
Certificado de Empleado Público con seudónimo, nivel alto en tarjeta para autenticación....36
Certificado de Sello electrónico cualificado de TSA/TSU....37
Certificado de Sello electrónico de TSA/TSU....39
Certificado de persona física vinculada, en Tarjeta para firma....40

Certificado de persona física vinculada, centralizado, para firma 41
Certificado de persona física vinculada, en tarjeta para autenticación 43
Certificado de persona física vinculada, con seudónimo, en Tarjeta para firma ..44
Certificado de persona física vinculada, con seudónimo, centralizado, para firma 45
Certificado de persona física vinculada, con seudónimo, en tarjeta para autenticación 46
Certificado de Sello electrónico en software 47
Certificado de Sello electrónico con gestión centralizada 48
1.4.2 Límites y prohibiciones de uso de los certificados.....49
1.4.3 Emisión de certificados de prueba.....50
1.5 Administración de la política.....50
1.5.1 Organización que administra el documento.....51
1.5.2 Datos de contacto de la organización.....51
1.5.3 Organización que aprueba el documento.....51
1.5.4 Procedimientos de gestión del documento.....51
1.6 Acrónimos y definiciones.....53
1.6.1. Acrónimos.....53
1.6.2 Definiciones.....56
2. Publicación de información y depósito de certificados.....58
2.1 Depósito de certificados.....58
2.2 Publicación de información de certificación.....58
2.3 Frecuencia de publicación.....58
2.4 Control de acceso.....59
3. Identificación y autenticación.....60
3.1 Registro inicial.....60
3.1.1 Tipos de nombres.....60
3.1.1.1 Certificado de firma de empleado público, nivel alto, en tarjeta 60
3.1.1.2 Certificado de firma de empleado público, nivel medio, en HSM 61
3.1.1.3 Certificado de autenticación de empleado público, nivel alto, en tarjeta 62
3.1.1.4 Certificado de sello de órgano, nivel medio, en software 63

3.1.1.5 Certificado de sello de órgano, nivel medio, en HSM 63

3.1.1.6 Certificado de firma de empleado público con seudónimo, nivel alto, en tarjeta 64

3.1.1.7 Certificado de firma de empleado público con seudónimo, nivel medio, en HSM 64

3.1.1.8 Certificado de autenticación de empleado público, con seudónimo, nivel alto, en tarjeta 65

3.1.1.9 Certificado de sello electrónico de TSA/TSU 66

3.1.1.10 Certificado de firma de persona física vinculada, en tarjeta 66

3.1.1.11 Certificado de firma de persona física vinculada, en HSM 67

3.1.1.12 Certificado de autenticación de persona física vinculada, en tarjeta 69

3.1.1.13 Certificado de firma de persona física vinculada, en tarjeta, con seudónimo 70

3.1.1.14 Certificado de firma de persona física vinculada, en HSM 71

3.1.1.15 Certificado de autenticación de persona física vinculada, en tarjeta, con seudónimo 71

3.1.1.16 Certificado de sello electrónico, en software 72

3.1.1.17 Certificado de sello electrónico con gestión centralizada 73

3.1.2. Significado de los nombres 73

3.1.3 Empleo de anónimos y seudónimos 73

3.1.4 Interpretación de formatos de nombres 74

3.1.5 Unicidad de los nombres 74

3.1.6 Resolución de conflictos relativos a nombres 75

3.2 Validación inicial de la identidad 75

3.2.1 Prueba de posesión de clave privada 76

3.2.2 Identificación de la entidad 76

3.2.3 Autenticación de la identidad de una persona física 78

3.2.3.1 En los certificados 79

3.2.3.2 Necesidad de presencia personal 79

3.2.3.3 Vinculación de la persona física 80

3.2.4 Información de suscriptor no verificada 80

3.2.5 Criterios de interoperabilidad 80
3.3 Identificación y autenticación de solicitudes de renovación 80
3.3.1 Validación para la renovación rutinaria de certificados 80
3.3.2 Identificación y autenticación de renovación tras revocación 81
3.4 Identificación y autenticación de la solicitud de revocación 81
4. Requisitos de operación del ciclo de vida de los certificados 81
4.1 Solicitud de certificado 81
4.1.1 Legitimación para solicitar la emisión 81
4.1.2 Procedimiento de alta y responsabilidades 82
4.2 Procesamiento de la solicitud de certificación 82
4.2.1 Ejecución de las funciones de identificación y autenticación 82
4.2.2 Aprobación o rechazo de la solicitud 83
4.2.3 Plazo para resolver la solicitud 84
4.3 Emisión del certificado 84
4.3.1 Acciones de la CA durante el proceso de emisión 84
4.3.2 Notificación de la emisión al suscriptor 85
4.4 Entrega y aceptación del certificado 85
4.4.1 Conducta que constituye aceptación del certificado 86
4.4.2 Publicación del certificado 86
4.4.3 Notificación de la emisión a terceros 86
4.5 Uso del par de claves y del certificado 87
4.5.1 Uso por el suscriptor o firmante 87
4.5.2 Uso por el suscriptor 88
4.5.3 Uso por el tercero que confía en certificados 89
4.6. Renovación de certificados 90
4.6.1 Circunstancias para la renovación del certificado 90
4.6.2 Quién puede pedir una renovación 90
4.6.3 Procesamiento de la solicitud de renovación de certificados 90
4.6.4 Notificación de nueva emisión de certificado al suscriptor 90
4.6.5 Conducta que constituya la aceptación de un certificado de renovación 91
4.6.6 Publicación del certificado de renovación por la CA 91
4.6.7 Notificación de la emisión del certificado por la CA a otras entidades 91
4.7 Renovación de claves y certificados 91
4.7.1 Quién puede solicitar el certificado de una nueva clave pública 91
4.7.2 Procedimiento con nueva identificación 91

4.7.3 Procesamiento de solicitudes de nueva clave de certificado 91
4.7.4 Notificación de la emisión del certificado renovado 92
4.7.5 Conducta que constituye aceptación del certificado 92
4.7.6 Publicación del certificado 92
4.7.7 Notificación de la emisión a terceros 92
4.8 Modificación de certificados 92
4.9 Revocación y suspensión de certificados 92
4.9.1 Causas de revocación de certificados 92
4.9.2 Legitimación para solicitar la revocación 94
4.9.3 Procedimientos de solicitud de revocación 94
4.9.4 Plazo temporal de solicitud de revocación 95
4.9.5 Plazo temporal de procesamiento de la solicitud 95
4.9.6 Obligación de consulta de información de revocación de certificados por terceros 96
4.9.7 Frecuencia de emisión de listas de revocación de certificados (CRLs) 96
4.9.8 Plazo máximo de publicación de CRLs 97
4.9.9 Disponibilidad de servicios de comprobación en línea de estado de certificados 97
4.9.10 Obligación de consulta de servicios de comprobación de estado de certificados 97
4.9.11 Otras formas de información de revocación de certificados 98
4.9.12 Requisitos especiales en caso de compromiso de la clave privada 98
4.9.13 Causas de suspensión de certificados 98
4.9.14 Solicitud de suspensión 99
4.9.15 Procedimientos para la petición de suspensión 99
4.9.16 Período máximo de suspensión 99
4.10 Servicios de comprobación de estado de certificados 99
4.10.1 Características operativas de los servicios 99
4.10.2 Disponibilidad de los servicios 100
4.10.3 Características opcionales 100
4.11 Finalización de la suscripción 100
4.12 Depósito y recuperación de claves 100
4.12.1 Política y prácticas de depósito y recuperación de claves 100
4.12.2 Política y prácticas de encapsulado y recuperación de claves de sesión 101
5. Controles de seguridad física, de gestión y de operaciones 102
5.1 Controles de seguridad física 102
5.1.1 Localización y construcción de las instalaciones 103

5.1.2 Acceso físico 103
5.1.3 Electricidad y aire acondicionado 104
5.1.4 Exposición al agua 104
5.1.5 Prevención y protección de incendios 104
5.1.6 Almacenamiento de soportes 104
5.1.7 Tratamiento de residuos 104
5.1.8 Copia de respaldo fuera de las instalaciones 105
5.2 Controles de procedimientos 105
5.2.1 Funciones fiables 105
5.2.2 Número de personas por tarea 106
5.2.3 Identificación y autenticación para cada función 107
5.2.4 Roles que requieren separación de tareas 107
5.2.5 Sistema de gestión PKI 107
5.3 Controles de personal 108
5.3.1 Requisitos de historial, calificaciones, experiencia y autorización 108
5.3.2 Procedimientos de investigación de historial 108
5.3.3 Requisitos de formación 109
5.3.4 Requisitos y frecuencia de actualización formativa 110
5.3.5 Secuencia y frecuencia de rotación laboral 110
5.3.6 Sanciones para acciones no autorizadas 110
5.3.7 Requisitos de contratación de profesionales 110
5.3.8 Suministro de documentación al personal 111
5.4 Procedimientos de auditoría de seguridad 111
5.4.1 Tipos de eventos registrados 111
5.4.2 Frecuencia de tratamiento de registros de auditoría 112
5.4.3 Período de conservación de registros de auditoría 113
5.4.4 Protección de los registros de auditoría 113
5.4.5 Procedimientos de copia de respaldo 113
5.4.6 Localización del sistema de acumulación de registros de auditoría 114
5.4.7 Notificación del evento de auditoría al causante del evento 114
5.4.8 Análisis de vulnerabilidades 114
5.5. Archivos de informaciones 114
5.5.1 Tipos de registros archivados 115

5.5.2 Período de conservación de registros 115
5.5.3 Protección del archivo 115
5.5.4 Procedimientos de copia de respaldo 116
5.5.5 Requisitos de sellado de fecha y hora 116
5.5.6 Localización del sistema de archivo 116
5.5.7 Procedimientos de obtención y verificación de información de archivo 117
5.6 Renovación de claves 117
5.7 Compromiso de claves y recuperación de desastre 117
5.7.1 Procedimientos de gestión de incidencias y compromisos 117
5.7.2 Corrupción de recursos, aplicaciones o datos 117
5.7.3 Compromiso de la clave privada de la entidad 118
5.7.4 Continuidad del negocio después de un desastre 118
5.8 Terminación del servicio 119
6. Controles de seguridad técnica 120
6.1 Generación e instalación del par de claves 120
6.1.1 Generación del par de claves 120
6.1.2 Envío de la clave privada al firmante 123
6.1.3 Envío de la clave pública al emisor del certificado 123
6.1.4 Distribución de la clave pública del prestador de servicios de certificación 124
6.1.5 Tamaños de claves 124
6.1.6 Generación de parámetros de clave pública y comprobación de calidad 124
6.1.7 Propósitos de uso de claves 125
6.2 Protección de la clave privada y controles de los módulos criptográficos 125
6.2.1 Estándares de módulos criptográficos 125
6.2.2 Control por más de una persona (n de m) sobre la clave privada 125
6.2.3 Depósito de la clave privada 126
6.2.4 Copia de respaldo de la clave privada 126
6.2.5 Archivo de la clave privada 126
6.2.6 Introducción de la clave privada en el módulo criptográfico 126
6.2.7 Almacenamiento de las claves privada en los módulos criptográficos 126
6.2.8 Método de activación de la clave privada 127
6.2.9 Método de desactivación de la clave privada 127
6.2.10 Método de destrucción de la clave privada 127
6.2.11 Clasificación del módulo criptográfico 128
6.3 Otros aspectos de gestión del par de claves 128

6.3.1 Archivo de la clave pública 128
6.3.2 Períodos de utilización de las claves pública y privada 128
6.4 Datos de activación 128
6.4.1 Generación e instalación de datos de activación 128
6.4.2 Protección de datos de activación 129
6.4.3 Otros aspectos de los datos de activación 129
6.5. Controles de seguridad informática 129
6.5.1 Requisitos técnicos específicos de seguridad informática 129
6.5.2 Evaluación del nivel de seguridad informática 130
6.6 Controles técnicos del ciclo de vida 130
6.6.1 Controles de desarrollo de sistemas 130
6.6.2 Controles de gestión de seguridad 131
Clasificación y gestión de información y bienes 131
Operaciones de gestión 131
Tratamiento de los soportes y seguridad 132
Gestión del sistema de acceso 132
6.6.3 Evaluación de la seguridad del ciclo de vida 133
6.7 Controles de seguridad de red 134
6.8 Fuentes de Tiempo 134
6.9 Algoritmos de firma y parámetros del sistema de firma centralizada 134
7. Perfiles de certificados, CRL y OCSP 136
7.1 Perfil de certificado 136
7.1.1 Número de versión 136
7.1.2 Extensiones del certificado 136
7.1.3 Identificadores de objeto (OID) de los algoritmos 136
7.1.4 Formato de Nombres 137
7.1.5 Restricción de los nombres 137
7.1.6 Identificador de objeto (OID) de los tipos de certificados 137
7.1.7 Uso de la extensión de restricciones de política 137
7.1.8 Calificadores de política sintaxis y semántica 137
7.1.9 Semántica de procesamiento para la extensión crítica de Políticas de certificado 137
7.1.10 Restricciones de longitud de los elementos 138
7.2 Perfil de la lista de revocación de certificados 138

7.2.1 Número de versión 138
7.2.2 CRL y extensiones CRL 138
7.3 Perfil OCSP 139
7.3.1 Número de versión 139
7.3.2 Extensiones OCSP 139
8. Auditoría de conformidad 140
8.1 Frecuencia de la auditoría de conformidad 140
8.2 Identificación y calificación del auditor 140
8.3 Relación del auditor con la entidad auditada 140
8.4 Listado de elementos objeto de auditoría 141
8.5 Acciones a emprender como resultado de una falta de conformidad 141
8.6 Tratamiento de los informes de auditoría 141
9. Requisitos comerciales y legales 143
9.1 Tarifas 143
9.1.1 Tarifa de emisión o renovación de certificados 143
9.1.2 Tarifa de acceso a certificados 143
9.1.3 Tarifa de acceso a información de estado de certificado 143
9.1.4 Tarifas de otros servicios 143
9.1.5 Política de reintegro 143
9.2 Responsabilidad financiera 143
9.2.1 Cobertura de seguro 144
9.2.2 Otros activos 144
9.3 Confidencialidad de la información 144
9.3.1 Informaciones confidenciales 144
9.3.2 Informaciones no confidenciales 145
9.3.3 Divulgación de información de suspensión y revocación 145
9.3.4 Divulgación legal de información 146
9.3.5 Divulgación de información por petición de su titular 146
9.3.6 Otras circunstancias de divulgación de información 146
9.4 Privacidad de la información personal 146
9.4.1 Plan de privacidad 147
9.4.2 Información tratada como privada 147
9.4.3 Información no considerada privada 147
9.4.4 Responsabilidad de proteger la información privada 148
9.4.5 Aviso y consentimiento para usar información privada 148

9.4.6 Divulgación de conformidad con un proceso judicial o administrativo 148
9.4.7 Otras circunstancias de divulgación de información 148
9.5 Derechos de propiedad intelectual 148
9.5.1 Propiedad de los certificados e información de revocación 149
9.5.2 Propiedad de la Declaración de Prácticas de Certificación 149
9.5.3 Propiedad de la información relativa a nombres 149
9.5.4 Propiedad de claves 149
9.6 Obligaciones y responsabilidad civil 150
9.6.1 Obligaciones de la Entidad de Certificación "esFIRMA" 150
9.6.2. Obligación y responsabilidad de la RA 151
9.6.3 Garantías ofrecidas a suscriptores y terceros que confían en certificados 154
9.6.4 Obligación y responsabilidad de terceras partes 155
9.6.5 Obligación y responsabilidad de otras participantes 155
9.7. Exención de garantía 156
9.8. Limitación de responsabilidad en caso de pérdidas por transacciones 157
9.9. Indemnizaciones 157
9.10. Plazo y Finalización 157
9.10.1 Plazo 157
9.10.2 Terminación 157
9.10.3 Efecto de la terminación y la supervivencia 157
9.11. Comunicaciones a las partes interesadas y al órgano de supervisión 157
9.12. Enmiendas 158
9.12.1 Procedimiento de modificación 158
9.12.2 Mecanismo de notificación y plazos 158
9.12.3 Circunstancias en las que se debe cambiar el OID 159
9.13 Procedimiento de resolución de conflictos 159
9.14. Legislación aplicable 159
9.15. Conformidad con la Ley Aplicable 159
9.16. Otras disposiciones 159
9.16.1 Acuerdo completo 160
9.16.2 Asignación 160
9.16.3 Separabilidad 160
9.16.4 Cumplimiento (honorarios de abogados y exención de derechos) 160
9.16.5 Fuerza mayor 161
9.17 Otras provisiones 161

9.17.1 Cláusula de indemnidad de suscriptor 161
9.17.2 Cláusula de indemnidad de tercero que confía en el certificado 161

1. Introducción

1.1 Presentación

Este documento declara las prácticas de certificación de firma electrónica de esFIRMA.

Los certificados que se emiten son los siguientes:

- **De Empleado Público (FIRMA)**
  - De Empleado Público nivel Medio
  - De Empleado Público nivel Alto
- **De Empleado Público (AUTENTICACIÓN)**
  - De Empleado Público nivel Alto
- **De Empleado Público con seudónimo (FIRMA)**
  - De Empleado Público nivel Medio
  - De Empleado Público nivel Alto
- **De Empleado Público con seudónimo (AUTENTICACIÓN)**
  - De Empleado Público nivel Alto
- **De persona física vinculada a entidad (FIRMA)**
  - De persona física vinculada a entidad nivel Medio
  - De persona física vinculada a entidad nivel Alto
- **De persona física vinculada a entidad (AUTENTICACIÓN)**
  - De persona física vinculada a entidad nivel Alto
- **De persona física vinculada a entidad con seudónimo (FIRMA)**
  - De persona física vinculada a entidad nivel Medio
  - De persona física vinculada a entidad nivel Alto
- **De persona física vinculada a entidad con seudónimo (AUTENTICACIÓN)**
  - De persona física vinculada a entidad nivel Alto
- **De Sello de Órgano**
  - De Sello de Órgano nivel Medio
- **De Sello electrónico para TSA/TSU**
  - De sello electrónico para TSU en HSM
- **De Sello electrónico**
  - De sello electrónico en software
  - De sello electrónico con gestión centralizada

1.2 Nombre del documento e identificación

Este documento es la "Declaración de Prácticas de Certificación" de esFIRMA.

1.2.1 Identificadores de certificados

Número OID	Políticas de certificados
	De Empleado Público (FIRMA)
1.3.6.1.4.1.47281.1.1.1	*De Empleado Público – Nivel Alto en tarjeta*
1.3.6.1.4.1.47281.1.1.4	*De Empleado Público – Nivel Medio en HSM*
	De Empleado Público (AUTENTICACIÓN)
1.3.6.1.4.1.47281.1.1.5	*De Empleado Público – Nivel Alto en tarjeta*
	De Empleado Público con Seudónimo (FIRMA)
1.3.6.1.4.1.47281.1.3.1	*De EP con Seudónimo – Nivel Alto en Tarjeta*
1.3.6.1.4.1.47281.1.3.4	*De EP con Seudónimo – Nivel Medio en HSM*
	De Empleado Público con Seudónimo (AUTENTICACIÓN)
1.3.6.1.4.1.47281.1.3.5	*De EP con Seudónimo – Nivel Alto en Tarjeta*
	De Persona Física vinculada a entidad (FIRMA)
1.3.6.1.4.1.47281.1.6.1	*De PF vinculada a entidad – Firma-e Cualificada, en Tarjeta*
1.3.6.1.4.1.47281.1.6.4	*De PF vinculada a entidad – Firma-e Centralizada*
	De Persona Física vinculada a entidad (AUTENTICACIÓN)
1.3.6.1.4.1.47281.1.6.5	*De PF vinculada a entidad – en Tarjeta*
	De Persona Física con seudónimo vinculada a entidad (FIRMA)
1.3.6.1.4.1.47281.1.7.1	*De PF con seudónimo vinculada a entidad – Firma-e Cualificada, en Tarjeta*
1.3.6.1.4.1.47281.1.7.4	*De PF con seudónimo vinculada a entidad – Firma-e Centralizada*

	De Persona Física con seudónimo, vinculada a entidad (AUTENTICACIÓN)
1.3.6.1.4.1.47281.1.7.5	*De PF con seudónimo, vinculada a entidad – en Tarjeta*
	De Sello de Órgano
1.3.6.1.4.1.47281.1.2.2	*De Sello de Órgano – Nivel Medio en software*
1.3.6.1.4.1.47281.1.2.4	*De Sello de Órgano – Nivel Medio en HSM*
	De Sello electrónico para TSA/TSU
1.3.6.1.4.1.47281.1.5.1	*De Sello-e para TSA/TSU en HSM*
1.3.6.1.4.1.47281.1.5.2	*De Sello-e cualificado para TSA/TSU en HSM*
	De Sello electrónico
1.3.6.1.4.1.47281.1.8.2	*De Sello electrónico en software*
1.3.6.1.4.1.47281.1.8.4	*De Sello electrónico centralizado*

En caso de contradicción entre esta Declaración de Prácticas de Certificación y otros documentos de prácticas y procedimientos de esFIRMA, prevalecerá lo establecido en esta Declaración de Prácticas.

Este documento está estructurado de acuerdo a IETF RFC 3647.

1.3 Participantes en los servicios de certificación

1.3.1. Prestador de servicios de certificación

El prestador de servicios de certificación es la persona, física o jurídica, que expide y gestiona certificados para entidades finales, empleando una Entidad de Certificación, o prestando otros servicios relacionados con la firma electrónica.

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION, S.A. (anteriormente, AULOCE, S.A.), en adelante "**ESPUBLICO**", con domicilio en la Calle Bari 39 (Edif. Binary Building), C.P. 50.197, de Zaragoza, CIF A-50.878.842, inscrita en el Registro Mercantil de Zaragoza al tomo 2.649, Folio 215, hoja Z-28722, y que opera bajo el nombre comercial "**esFIRMA**" (el cual se utilizará a lo largo de este documento para designarla) es un prestador de servicios de certificación que actúa de acuerdo con lo dispuesto en el régimen de obligaciones y responsabilidades de:

- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, modificado por Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Normas técnicas del ETSI aplicables a la expedición y gestión de certificados cualificados, principalmente ETSI EN 319 411-1 y ETSI EN 319 411-2, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

Para la prestación de los servicios de certificación, esFIRMA ha establecido una jerarquía de entidades de certificación:

esFIRMA AC raíz 2

Se trata de la entidad de certificación raíz de la jerarquía que emite certificados a otras entidades de certificación, y cuyo certificado de clave pública ha sido autofirmado.

Datos de identificación:

CN:	ESFIRMA AC RAIZ 2

Huella digital SHA-256:	c6:09:f9:4f:9c:ce:20:cb:2b:a0:2e:8b:5b:33:55:20:06:c1:5d:17:78:32:26:11:07:0f:a1:4f:ff:9d:c9:16
Válido desde:	2017-11-02T12:52:43Z
Válido hasta:	2042-11-02T12:52:43Z
Longitud de clave RSA:	4.096 bits

esFIRMA AC AAPP 2

Se trata de la entidad de certificación dentro de la jerarquía que emite los certificados a las entidades finales, y cuyo certificado de clave pública ha sido firmado digitalmente por "esFIRMA AC RAIZ 2".

Datos de identificación:

CN:	ESFIRMA AC AAPP 2
Huella digital SHA-256:	2c:18:23:61:9d:80:73:11:6c:8f:14:8b:d3:85:79:de:9c:05:39:16:02:db:ce:b9:65:73:e4:a1:88:e1:32:6e
Válido desde:	2017-11-02T13:12:47Z
Válido hasta:	2030-11-02T13:12:47Z
Longitud de clave RSA:	4.096 bits

Plataforma de Administración Electrónica

Se trata de la plataforma de gestión del ciclo de vida del certificado en exclusiva, para su solicitud, aprobación, emisión y revocación.

Para completar la información sobre las funcionalidades de la Plataforma de Administración Electrónica en los servicios de certificación consultar su documentación.

1.3.2 Autoridades de Registro

Una autoridad de registro realiza labores de comprobación e identificación de los solicitantes de los certificados.

En general, el propio prestador del servicio de certificación actúa como autoridad de registro de la identidad de los suscriptores de certificados.

También son autoridades de registro de los certificados sujetos a esta Declaración de Prácticas de Certificación, debido a su condición de certificados corporativos, las unidades designadas para esta función por los suscriptores de los certificados, como la Secretaría de la corporación, el departamento de personal o el Representante legal de la Administración, dado que disponen de los registros auténticos acerca de la vinculación de los firmantes con el suscriptor.

Las funciones de registro de los suscriptores se realizan por delegación y de acuerdo con las instrucciones del prestador de servicios de certificación, en los términos que define el Reglamento (UE) 910/2014, y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, y bajo la plena responsabilidad del prestador de servicios de certificación frente a terceros.

1.3.3 Entidades finales

Las entidades finales son las personas y organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para los usos de identificación y firma electrónica.

Serán entidades finales de los servicios de certificación de esFIRMA las siguientes:

1. Suscriptores del servicio de certificación.
2. Firmantes.
3. Partes usuarias.

1.3.4 Partes usuarias

Las partes usuarias son las personas y las organizaciones que reciben firmas digitales y certificados digitales.

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en esta declaración de prácticas de certificación y en las correspondientes instrucciones disponibles en la página web de la Entidad de Certificación.

1.3.5 Otros participantes

Suscriptores del servicio de certificación

Los suscriptores del servicio de certificación son las administraciones públicas o entidades que los adquieren a esFIRMA para su uso en su ámbito corporativo u organizativo, y se encuentran identificados en los certificados.

El suscriptor del servicio de certificación adquiere una licencia de uso del certificado, para su uso propio – certificados de sello electrónico–, o al objeto de facilitar la certificación de la identidad de una persona concreta debidamente autorizada para diversas actuaciones en el ámbito organizativo del suscriptor – certificados de firma electrónica. En este último caso, esta persona figura identificada en el certificado, según se dispone en el epígrafe siguiente.

El suscriptor del servicio de certificación es, por tanto, el cliente del prestador de servicios de certificación, de acuerdo con la legislación mercantil, y tiene los derechos y obligaciones que se definen por el prestador del servicio de certificación, que son adicionales y se entienden sin perjuicio de los derechos y obligaciones de los firmantes, como se autoriza y regula en las normas técnicas europeas aplicables a la expedición de certificados electrónicos cualificados.

Firmantes

Los firmantes son las personas físicas que poseen de forma exclusiva o tienen bajo su exclusivo control, de acuerdo al régimen de obligaciones y responsabilidades del Reglamento (UE) 910/2014, y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, las claves de firma digital para identificación y firma electrónica avanzada o cualificada; siendo típicamente las personas titulares o miembros de los órganos administrativos, en los certificados de firma electrónica de órgano, las personas al servicio de las Administraciones Públicas, en

los certificados de empleado público o las personas que pertenecen a una entidad, en los certificados de persona física vinculada.

Los firmantes se encuentran debidamente autorizados por el suscriptor y debidamente identificados en el certificado mediante su nombre y apellidos, y número de identificación fiscal válido en la jurisdicción de expedición del certificado, o bien con el correspondiente seudónimo en los certificados de este tipo.

Dada la existencia de certificados para usos diferentes de la firma electrónica, como la identificación, también se emplea el término más genérico de "persona física identificada en el certificado", siempre con pleno respeto al cumplimiento de la legislación de firma electrónica en relación con los derechos y obligaciones del firmante.

1.4 Uso de los certificados

Esta sección lista las aplicaciones para las que puede emplearse cada tipo de certificado, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

1.4.1 Usos permitidos para los certificados

Se deben tener en cuenta los usos permitidos indicados en los diversos campos de los perfiles de certificados, visibles en la web https://www.esfirma.com

Certificado de Empleado Público nivel alto en Tarjeta

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.1.1	En la jerarquía de la AC esFIRMA
0.4.0.194112.1.2	De acuerdo con la política QCP-n-qscd
2.16.724.1.3.5.7.1	Empleado público español de nivel alto

Los certificados de persona física empleado público nivel alto son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten a empleados públicos para identificarlos como personas al servicio de la Administración, organismo, entidad de derecho público u otra entidad, vinculándolos con ésta, cumpliendo los requisitos establecidos en el artículo 43 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para la firma electrónica del personal al servicio de las Administraciones Públicas.

Los certificados de persona física empleado público nivel alto, funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Asimismo, los certificados de persona física empleado público nivel alto se emiten de acuerdo con los niveles de aseguramiento alto de los perfiles de certificados establecidos en el punto 10 del documento “Perfiles de Certificados electrónicos” de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

Estos certificados garantizan la identidad del suscriptor y del firmante, y permiten la generación de la “firma electrónica cualificada”; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
c) El campo "User Notice" describe el uso de este certificado.

Certificado de Empleado Público nivel medio en HSM

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.1.4	En la jerarquía de la AC esFIRMA
0.4.0.194112.1.0	De acuerdo con la política QCP-n
2.16.724.1.3.5.7.2	Empleado público español de nivel medio

Los certificados de persona física empleado público nivel medio son certificados cualificados de acuerdo con el artículo 28 y el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten a empleados públicos para identificarlos como personas al servicio de la Administración, organismo, entidad de derecho público u otra entidad, vinculándolos con ésta, cumpliendo los requisitos establecidos en el artículo 43 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para la firma electrónica del personal al servicio de las Administraciones Públicas.

Los certificados de persona física empleado público nivel medio son gestionados de forma centralizada.

Los certificados de persona física empleado público nivel medio se emiten de acuerdo con los niveles de aseguramiento medio de los perfiles de certificados establecidos en el punto 10 del documento "Perfiles de Certificados electrónicos" de Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la generación de la "firma electrónica avanzada basada en certificado electrónico cualificado".

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
c) El campo “User Notice” describe el uso de este certificado.

Certificado de Empleado Público nivel alto en tarjeta para autenticación

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.1.5	En la jerarquía de la AC esFIRMA
0.4.0.2042.1.2	De acuerdo con la política NCP+
2.16.724.1.3.5.7.1	Empleado público español de nivel alto

Estos certificados son certificados emitidos de acuerdo con la política de certificados normalizados (NCP+) y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-1.

Estos certificados se emiten a empleados públicos para identificarlos como personas al servicio de la Administración, organismo, entidad de derecho público u otra entidad, vinculándolos con ésta, cumpliendo los requisitos establecidos en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Estos certificados de persona física empleado público nivel alto, funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Los certificados de persona física empleado público nivel alto se emiten de acuerdo con los niveles de aseguramiento alto de los perfiles de certificados establecidos en el punto 10 del documento “Perfiles de Certificados electrónicos” de la Secretaría de Estado de

Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la autenticación de ésta última ante aplicaciones y sitios web.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

d) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Firma digital (para realizar la función de autenticación)

e) El campo "User Notice" describe el uso de este certificado.

Certificado de Sello de Órgano nivel medio en software

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.2.2	En la jerarquía de la AC esFIRMA
0.4.0.194112.1.1	De acuerdo con la política QCP-l
2.16.724.1.3.5.6.2	Empleado público español de nivel medio

Los certificados de sello electrónico de órgano nivel medio son certificados cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada de acuerdo con el artículo 42 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Los certificados de sello electrónico de órgano nivel medio se emiten de acuerdo con los niveles de aseguramiento medio de los perfiles de certificados establecidos en el punto 9 del documento "Perfiles de Certificados electrónicos" de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

Estos certificados garantizan la identidad del suscriptor y del organismo público incluidos en el certificado.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
c) El campo "User Notice" describe el uso de este certificado.

Certificado de Sello de Órgano nivel medio en HSM

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.2.4	En la jerarquía de la AC esFIRMA
0.4.0.194112.1.1	De acuerdo con la política QCP-l
2.16.724.1.3.5.6.2	Empleado público español de nivel medio

Los certificados de sello electrónico de órgano nivel medio son certificados cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada de acuerdo con el artículo 42 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Los certificados de sello electrónico de órgano nivel medio son gestionados de forma centralizada.

Los certificados de sello electrónico de órgano nivel medio se emiten de acuerdo con los niveles de aseguramiento medio de los perfiles de certificados establecidos en el punto 9 del documento "Perfiles de Certificados electrónicos" de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

Estos certificados garantizan la identidad del suscriptor y del organismo público incluidos en el certificado.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

c) El campo “User Notice” describe el uso de este certificado.

Certificado de Empleado Público con Seudónimo nivel alto en Tarjeta

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.3.1	En la jerarquía de la AC esFIRMA
0.4.0.194112.1.2	De acuerdo con la política QCP-n-qscd
2.16.724.1.3.5.4.1	Empleado público español con seudónimo nivel alto

Los certificados de persona física empleado público con seudónimo nivel alto son certificados cualificados de acuerdo con el artículo 28 y el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten a empleados públicos para identificarlos (por medio de un seudónimo) como personas al servicio de la Administración, organismo, entidad de derecho público u otra entidad, vinculándolos con ésta, cumpliendo los requisitos establecidos en el artículo 43 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para la firma electrónica del personal al servicio de las Administraciones Públicas.

Los certificados de persona física empleado público con seudónimo nivel alto, funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Asimismo, los certificados de persona física empleado público con seudónimo nivel alto se emiten de acuerdo con los niveles de aseguramiento alto de los perfiles de certificados establecidos en el punto 11 del documento “Perfiles de Certificados electrónicos” de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

Estos certificados permiten la generación de la "firma electrónica cualificada"; es decir, la firma electrónica avanzada que se basa en un certificado cualificada y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
c) El campo "User Notice" describe el uso de este certificado.

Certificado de Empleado Público con seudónimo nivel medio, en HSM

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.3.4	En la jerarquía de la AC esFIRMA
0.4.0.194112.1.0	De acuerdo con la política QCP-n
2.16.724.1.3.5.4.2	Empleado público español con seudónimo nivel medio

Los certificados de persona física empleado público con seudónimo nivel medio son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten a empleados públicos para identificarlos (por medio de un seudónimo) como personas al servicio de la Administración, organismo, entidad de derecho público u otra entidad, vinculándolos con ésta, cumpliendo los requisitos establecidos en el artículo 43 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para la firma electrónica del personal al servicio de las Administraciones Públicas.

Los certificados de persona física empleado público con seudónimo nivel medio son gestionados de forma centralizada.

Los certificados de persona física empleado público con seudónimo nivel medio se emiten de acuerdo con los niveles de aseguramiento medio de los perfiles de certificados establecidos en el punto 11 del documento “Perfiles de Certificados electrónicos” de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

Estos certificados permiten la generación de la “firma electrónica avanzada basada en certificado electrónico cualificado”.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

c) Firma de correo electrónico seguro.

d) Otras aplicaciones de firma digital.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
c) El campo "User Notice" describe el uso de este certificado.

Certificado de Empleado Público con seudónimo, nivel alto en tarjeta para autenticación

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.3.5	En la jerarquía de la AC esFIRMA
0.4.0.2042.1.2	De acuerdo con la política NCP+
2.16.724.1.3.5.4.1	Empleado público español con seudónimo de nivel alto

Estos certificados son certificados emitidos de acuerdo con la política de certificados normalizados (NCP+) y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-1.

Estos certificados se emiten a empleados públicos para identificarlos (por medio de un seudónimo) como personas al servicio de la Administración, organismo, entidad de derecho público u otra entidad, vinculándolos con ésta, cumpliendo los requisitos establecidos en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Estos certificados de persona física empleado público con seudónimo nivel alto, funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Los certificados de persona física empleado público con seudónimo nivel alto se emiten de acuerdo con los niveles de aseguramiento alto de los perfiles de certificados establecidos en el punto 11 del documento "Perfiles de Certificados electrónicos" de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la autenticación de ésta última ante aplicaciones y sitios web.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

f) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Firma digital (para realizar la función de autenticación)

g) El campo "User Notice" describe el uso de este certificado.

Certificado de Sello electrónico cualificado de TSA/TSU

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.5.2	En la jerarquía de la AC esFIRMA
0.4.0.194112.1.1	De acuerdo con la política QCP-l

Los certificados de sello electrónico de TSA/TSU son certificados cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 421 y ETSI EN 319 422.

Este certificado permite a Unidades de Sellado de Tiempo o TSU emitir los sellos de tiempo cuando reciben una solicitud bajo las especificaciones de la RFC3161.

Las claves se generan en soporte de un dispositivo HSM.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Content Commitment
b) El campo “extend key usage” tiene activada la función:
    a. TimeStamping
c) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
d) El campo “User Notice” describe el uso de este certificado. Opcional
e) Incluye la extensión “privateKeyUsage”, que limita el uso de la clave privada, siguiendo las recomendaciones de las normas ETSI EN 319 421 y ETSI EN 319 422.

Otras consideraciones:

- Se establecen controles para garantizar el cese de uso de la clave privada antes de la extinción de su vigencia.
- En caso de cambio de certificado, las claves asociadas serán destruidas según se describe en el ciclo de vida.
- Las claves privadas se destruyen una vez expirado su tiempo de uso definido, su reemplazo, revocación u otras causas.

- La destrucción se realiza de una manera tal que la clave privada no se pueda recuperar, siguiendo el procedimiento establecido por el fabricante del módulo criptográfico que las almacena.
- Para validación a largo plazo de los sellos de tiempos se podrá utilizar la Última CRL emitida por esFIRMA siguiendo las guías proporcionadas. En el momento de la verificación se puede considerar como válido si, en el momento de la fecha de sello de tiempo, la clave privada no fue comprometida, el algoritmo de huella digital no presentaba colisiones y los algoritmos usados estaban fuera del alcance de los ataques criptográficos del momento.

Certificado de Sello electrónico de TSA/TSU

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.5.1	En la jerarquía de la AC esFIRMA
0.4.0.194112.1.1	De acuerdo con la política QCP-l

Este certificado permite a Unidades de Sellado de Tiempo o TSU emitir los sellos de tiempo cuando reciben una solicitud bajo las especificaciones de la RFC3161.

Las claves se generan en soporte de un dispositivo HSM.

La información de usos en el perfil de certificado indica lo siguiente:

f) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
   a. Content Commitment

g) El campo “extend key usage” tiene activada la función:
   a. TimeStamping

h) El campo “User Notice” describe el uso de este certificado. Opcional

i) Incluye la extensión “privateKeyUsage”, que limita el uso de la clave privada, siguiendo las recomendaciones de las normas ETSI EN 319 421 y ETSI EN 319 422.

Otras consideraciones:

- Se establecen controles para garantizar el cese de uso de la clave privada antes de la extinción de su vigencia.
- En caso de cambio de certificado, las claves asociadas serán destruidas según se describe en el ciclo de vida.
- Las claves privadas se destruyen una vez expirado su tiempo de uso definido, su reemplazo, revocación u otras causas.
- La destrucción se realiza de una manera tal que la clave privada no se pueda recuperar, siguiendo el procedimiento establecido por el fabricante del módulo criptográfico que las almacena.
- Para validación a largo plazo de los sellos de tiempos se podrá utilizar la Última CRL emitida por esFIRMA siguiendo las guías proporcionadas. En el momento de la verificación se puede considerar como válido si, en el momento de la fecha de sello de tiempo, la clave privada no fue comprometida, el algoritmo de huella digital no presentaba colisiones y los algoritmos usados estaban fuera del alcance de los ataques criptográficos del momento.

Certificado de persona física vinculada, en Tarjeta para firma

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.6.1	En la jerarquía de la AC esFIRMA
0.4.0.194112.1.2	De acuerdo con la política QCP-n-qscd

Estos certificados son cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados garantizan la identidad del suscriptor y del firmante, y permiten la generación de la "firma electrónica cualificada"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

c) Firma de correo electrónico seguro.
d) Otras aplicaciones de firma digital.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

d) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

e) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
f) El campo "User Notice" describe el uso de este certificado. Opcional

Certificado de persona física vinculada, centralizado, para firma

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.6.4	En la jerarquía de la AC esFIRMA
0.4.0.194112.1.0	De acuerdo con la política QCP-n

Estos certificados son cualificados de acuerdo con el artículo 28 y el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados son gestionados de forma centralizada.

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la generación de la "firma electrónica avanzada basada en certificado electrónico cualificado".

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

e) Firma de correo electrónico seguro.
f) Otras aplicaciones de firma digital.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

h) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

i) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

j) El campo “User Notice” describe el uso de este certificado. Opcional

Certificado de persona física vinculada, en tarjeta para autenticación

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.6.5	En la jerarquía de la AC esFIRMA
0.4.0.2042.1.2	De acuerdo con la política NCP+

Estos certificados son certificados emitidos de acuerdo con la política de certificados normalizados (NCP+) y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-1.

Estos certificados funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la autenticación de ésta última ante aplicaciones y sitios web.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

k) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Firma digital (para realizar la función de autenticación)

l) El campo “User Notice” describe el uso de este certificado. Opcional

Certificado de persona física vinculada, con seudónimo, en Tarjeta para firma

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.7.1	En la jerarquía de la AC esFIRMA
0.4.0.194112.1.2	De acuerdo con la política QCP-n-qscd

Estos certificados son cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados garantizan la identidad del suscriptor.
Estos certificados garantizan la identidad del firmante por medio de un seudónimo.
Estos certificados permiten la generación de la "firma electrónica cualificada"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

e) Firma de correo electrónico seguro.
f) Otras aplicaciones de firma digital.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

g) El campo “key usage” tiene activadas, y por tanto permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

h) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.

i) El campo “User Notice” describe el uso de este certificado. Opcional

Certificado de persona física vinculada, con seudónimo, centralizado, para firma

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.6.4	En la jerarquía de la AC esFIRMA
0.4.0.194112.1.0	De acuerdo con la política QCP-n

Estos certificados son cualificados de acuerdo con el artículo 28 y el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados son gestionados de forma centralizada.
Estos certificados garantizan la identidad del suscriptor.
Estos certificados garantizan la identidad del firmante por medio de un seudónimo.
Estos certificados permiten la generación de la “firma electrónica avanzada basada en certificado electrónico cualificado”.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

g) Firma de correo electrónico seguro.
h) Otras aplicaciones de firma digital.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

m) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

n) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
o) El campo "User Notice" describe el uso de este certificado. Opcional

Certificado de persona física vinculada, con seudónimo, en tarjeta para autenticación

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.7.5	En la jerarquía de la AC esFIRMA
0.4.0.2042.1.2	De acuerdo con la política NCP+

Estos certificados son certificados emitidos de acuerdo con la política de certificados normalizados (NCP+) y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-1.

Estos certificados funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados garantizan la identidad del suscriptor.
Estos certificados garantizan la identidad del firmante por medio de un seudónimo.
Estos certificados permiten la autenticación de esta última ante aplicaciones y sitios web.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

p) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Firma digital (para realizar la función de autenticación)

q) El campo "User Notice" describe el uso de este certificado. Opcional

Certificado de Sello electrónico en software

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.8.2	En la jerarquía de la AC esFIRMA
0.4.0.194112.1.1	De acuerdo con la política QCP-l

Estos certificados son cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (para la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Cifrado de claves

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
   a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
c) El campo "User Notice" describe el uso de este certificado. Opcional

Certificado de Sello electrónico con gestión centralizada

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.8.4	En la jerarquía de la AC esFIRMA
0.4.0.194112.1.1	De acuerdo con la política QCP-l

Estos certificados son cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados son gestionados de forma centralizada.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

d) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
   a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

e) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
f) El campo “User Notice” describe el uso de este certificado. Opcional

1.4.2 Límites y prohibiciones de uso de los certificados

Los certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados no pueden emplearse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (CRL).

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, visibles en el web de esFIRMA https://www.esfirma.com

El uso de los certificados digitales de forma que se incumpla esta DPC y el resto de documentación aplicable, especialmente el contrato firmado con el suscriptor y los textos de divulgación o PDS tiene la consideración de uso indebido a los efectos legales oportunos, y exime a esFIRMA de cualquier responsabilidad por este uso indebido, ya sea del firmante o de tercero alguno.

esFIRMA no tiene autorización de acceso ni obligación legal de supervisar los datos sobre los que se puede aplicar el uso de una clave certificada. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de esFIRMA emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en esta DPC, los documentos jurídicos vinculantes con cada certificado, o los contratos o convenios con las entidades de registro o con sus suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

Los certificados se usan de forma exclusiva y únicamente desde la Plataforma de Administración Electrónica o extensiones y complementos de la misma que la empresa ESPUBLICO pone a disposición del suscriptor.

1.4.3 Emisión de certificados de prueba

esFIRMA emite certificados de prueba bajo la jerarquía de producción, con la finalidad de realizar pruebas técnicas de interoperabilidad y permitir su evaluación al órgano de supervisión.

Los datos contenidos en los certificados de prueba son ficticios y se ajustan a las directrices emitidas por el órgano de supervisión.

Estos certificados de pruebas carecen de validez legal, por lo que esFIRMA queda exenta de cualquier responsabilidad como consecuencia de su utilización por terceros.

1.5 Administración de la política

1.5.1 Organización que administra el documento

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

Identificación Registro	Registro Mercantil de Zaragoza
Tomo	2649
Folio	215
Hoja	Z-28722
CIF	A-50.878.842

1.5.2 Datos de contacto de la organización

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

1.5.3 Organización que aprueba el documento

Comité de Seguridad de ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)

El comité de seguridad de esFIRMA, formado por el Presidente del mismo, el Responsable de Información y servicio y el Responsable de Seguridad de esFirma, tiene la responsabilidad de la aprobación de esta Declaración de Prácticas.

Tanto las funciones como los miembros de dicho Comité se encuentran definidos en la Política de Seguridad de esFirma.

1.5.4 Procedimientos de gestión del documento

El sistema documental y de organización de esFIRMA garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones de servicio relacionados con el mismo.

esFIRMA realiza revisiones como mínimo anuales de este documento o cuando es requerido por cambios en las guías y documentos con los cuales debe cumplir.

Tal y como se define en la Política de Seguridad de esFIRMA, la Oficina de Seguridad será la entidad responsable del mantenimiento de este documento.

La Oficina de Seguridad se responsabiliza de la redacción, mantenimiento y administración de la DPC, los textos de divulgación (PDS), hojas de entrega y aceptación, y el resto de documentación jurídica (convenios, contratos, etc.) de esFirma.

Siempre que existan cambios de importancia suficiente en la gestión de los certificados definidos en esta DPC, se crea una nueva revisión de este documento, que consta en el cuadro inicial de "control de versiones" dentro del apartado de "información general".

La actuación de la Oficina de Seguridad se produce a instancia de su responsable en función de las necesidades que se produzcan.

esFirma puede realizar cambios que no requieran notificación cuando éstos no afecten directamente a los derechos de los firmantes y suscriptores de los certificados o de los suscriptores de los sellos.
Cuando esFirma vaya a introducir cambios que modifiquen los derechos de los firmantes y suscriptores de los certificados y de los suscriptores de sellos deberá notificarlo públicamente con el objeto que presenten sus comentarios a la Oficina de Seguridad durante 15 días siguientes a la publicación de los futuros cambios.

Para notificar públicamente los cambios producidos se publicará en el apartado de "documentación" en la página web https://www.esfirma.com

Las revisiones de esta DPC serán publicadas en la web de esFirma tras ser aprobadas por el Comité de Seguridad de Esfirma.

1.6 Acrónimos y definiciones

1.6.1. Acrónimos

AC (*o también CA*)	*Certificate Authority* Autoridad de Certificación
AR (o también RA)	*Registration Authority* Autoridad de Registro
CPD	Centro de Proceso de Datos
CPS (o también DPC)	*Certification Practice Statement*. Declaración de Prácticas de Certificación
CRL (o tambien LRC)	*Certificate Revocation List.* Lista de certificados revocados
DN	*Distinguished Name.* Nombre distintivo dentro del certificado digital
DNI	Documento Nacional de Identidad
ECC	*Elliptic Curve Cryptography*
ETSI EN	*European Telecommunications Standards Institute – European Standard.*
EV (para SSL)	*Extended Validation* Validación extendida, en certificados SSL.
FIPS	*Federal Information Processing Standard Publication*
HSM	*Hardware Security Module* Módulo de seguridad en Hardware
IETF	*Internet Engineering Task Force*
NIF	Número de Identificación Fiscal
NTP	*Network Time Protocol* Protocolo de tiempo en red.
OCSP	*Online Certificate Status Protocol.* Protocolo de acceso al estado de los certificados
OID	*Object Identifier*. Identificador de objeto
PDS	*PKI Disclosure Statements* Texto de Divulgación de PKI.
PIN	*Personal Identification Number*.

	Número de identificación personal
PKI	*Public Key Infrastructure*. Infraestructura de clave pública
QSCD (o también DCCF)	*Qualified Electronic Signature/Seal Creation Device.* Dispositivo cualificado de creación de firma/sellos
QCP	*Qualified Certificate Policy* Política de certificados cualificados
QCP-n	*Qualified Certificate Policy-natural person* Política de certificados cualificados para personas físicas.
QCP-l	*Qualified Certificate Policy-legal person* Política de certificados cualificados para personas jurídicas.
QCP-n-qscd	*Qualified Certificate Policy-natural person-qscd* Política de certificados cualificados para personas físicas en dispositivo cualificado de firma/sello
QCP-l-qscd	*Qualified Certificate Policy-legal person-qscd* Política de certificados cualificados para personas jurídicas con dispositivo cualificado de firma/sello
RFC	*Request for Comments* Documento RFC
RSA	Rivest-Shamir-Adleman. Tipo de algoritmo de cifrado
SHA	*Secure Hash Algorithm.* Algoritmo seguro de Hash
SSL	*Secure Sockets Layer.* Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.
TCP/IP	*Transmission Control. Protocol/Internet Protocol*. Sistema de protocolos, definidos en el marco de la IEFT.
TSA	*Time Stamping Authority* Autoridad de Sellado de Tiempo Electrónico
TSU	*Time Stamping Unit* Unidad de Sellado de Tiempo.

UTC	*Coordinated Universal Time* Tiempo universal coordinado
VPN	*Virtual Private Network.* Red privada virtual

1.6.2 Definiciones

Autoridad de Certificación	*Es la entidad responsable de la emisión y gestión de los certificados digitales.*
Autoridad de Registro	*Entidad responsable de la gestión de las solicitudes, identificación y registro de los solicitantes de un certificado. Puede formar parte de la Autoridad de Certificación o ser ajena.*
Certificado	*Archivo que asocia la clave pública con algunos datos identificativos del Sujeto/Firmante y es firmada por la AC.*
Clave pública	*Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos.*
Clave privada	*Valor matemático conocido únicamente por el Sujeto/Firmante y usado para la creación de una firma digital o el descifrado de datos.* *La clave privada de la AC será usada para firma de certificados y firma de CRL's.* *La clave privada del servicio TSA será usada para firma de los sellos de tiempo.*
CPS	*Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta.*
CRL	*Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la AC.*
Datos de Activación	*Datos privados, como PIN's o contraseñas empleados para la activación de la clave privada*
DCCF	*Dispositivo Cualificado de creación de firma. Elemento software o hardware, convenientemente certificado, empleado por el Sujeto/Firmante para la generación de firmas electrónicas, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el Sujeto/Firmante.*
Firma digital	*El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera:*

	a) que los datos no han sido modificados (integridad) *b) que la persona que firma los datos es quien dice ser (identificación)* *c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)*
OID	*Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.*
Par de claves	*Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.*
PKI	*Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública.*
Solicitante	*En el contexto de este documento, el solicitante será una persona física apoderada con un poder especial para realizar determinados trámites en nombre y representación de la entidad.*
Suscriptor	*En el contexto de este documento la persona jurídica propietaria del certificado (a nivel corporativo)*
Sujeto/Firmante	*En el contexto de este documento, la persona física cuya clave pública es certificada por la AC y dispone de, o tiene acceso de forma exclusiva a, una clave privada válida para generar firmas digitales.*
Parte Usuaria	*En el contexto de este documento, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado*

2. Publicación de información y depósito de certificados

2.1 Depósito de certificados

esFIRMA dispone de un Depósito de certificados, en el que se publican las informaciones relativas a los servicios de certificación:

https://www.esfirma.com

Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de esFIRMA, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.7.4 de esta Declaración de Prácticas de Certificación.

2.2 Publicación de información de certificación

esFIRMA publica las siguientes informaciones, en su Depósito:

- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- Las políticas de certificados aplicables.
- La Declaración de Prácticas de Certificación.
- Los textos de divulgación (PKI Disclosure Statements - PDS), como mínimo en lengua española y en lengua inglesa.

2.3 Frecuencia de publicación

La información del prestador de servicios de certificación, incluyendo las políticas y la Declaración de Prácticas de Certificación, se publica en cuanto se encuentra disponible.

Los cambios en la Declaración de Prácticas de Certificación se rigen por lo establecido en la sección 1.5 de este documento.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones 4.9.7 y 4.9.8 de esta Declaración de Prácticas de Certificación.

2.4 Control de acceso

esFIRMA no limita el acceso de lectura a las informaciones establecidas en la sección 2.2, pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Depósito, para proteger la integridad y autenticidad de la información, especialmente la información de estado de revocación.

esFIRMA emplea sistemas fiables para el Depósito, de modo tal que:

- Únicamente las personas autorizadas puedan hacer anotaciones y modificaciones.
- Se pueda comprobar la autenticidad de la información.
- Se pueda detectar cualquier cambio técnico que afecte a los requisitos de seguridad.

3. Identificación y autenticación

3.1 Registro inicial

3.1.1 Tipos de nombres

Todos los certificados contienen un nombre diferenciado X.501 en el campo *Subject*, incluyendo un componente *Common Name* (CN), relativo a la identidad del suscriptor y de la persona física identificada en el certificado, así como diversas informaciones de identidad adicionales en el campo *SubjectAlternativeName*.

Los nombres contenidos en los certificados son los siguientes.

3.1.1.1 Certificado de firma de empleado público, nivel alto, en tarjeta

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la Administración, organismo, entidad de derecho público u otra entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationalUnitName (OU)	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Surname	Primer y segundo(opcional) apellido, de acuerdo con documento de identidad (DNI/Pasaporte)
Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)
Serial Number	DNI/NIE del empleado
Common Name (CN)	Nombre Apellido1 Apellido2 – NIF del empleado
Tipo de certificado OID: 2.16.724.1.3.5.7.1.1	CERTIFICADO CUALIFICADO DE FIRMA DE EMPLEADO PUBLICO DE NIVEL ALTO
Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.7.1.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 2.16.724.1.3.5.7.1.3	NIF entidad subscription
DNI/NIE del responsable OID: 2.16.724.1.3.5.7.1.4	DNI o NIE del responsable

Nombre de pila OID: 2.16.724.1.3.5.7.1.6	Nombre de pila del responsable del certificado
Primer apellido OID: 2.16.724.1.3.5.7.1.7	Primer apellido del responsable del certificado
Segundo apellido OID: 2.16.724.1.3.5.7.1.8	Segundo apellido del responsable del certificado. Opcional.
Correo electrónico OID: 2.16.724.1.3.5.7.1.9	Correo electrónico del responsable del certificado. Opcional.

3.1.1.2 Certificado de firma de empleado público, nivel medio, en HSM

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationalUnitName (OU)	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Surname	Primer y segundo(opcional) apellido, de acuerdo con documento de identidad (DNI/Pasaporte)
Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)
Serial Number	DNI/NIE del empleado
Common Name (CN)	Nombre Apellido1 Apellido2 – NIF del empleado
Tipo de certificado OID: 2.16.724.1.3.5.7.2.1	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO DE NIVEL MEDIO
Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.7.2.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 2.16.724.1.3.5.7.2.3	NIF entidad subscriptora
DNI/NIE del responsable OID: 2.16.724.1.3.5.7.2.4	DNI o NIE del responsable
Número de autenticación personal OID: 2.16.724.1.3.5.7.2.5	NRP o NIP del responsable del suscriptor del certificado
Nombre de pila OID: 2.16.724.1.3.5.7.2.6	Nombre de pila del responsable del certificado

Primer apellido OID: 2.16.724.1.3.5.7.2.7	Primer apellido del responsable del certificado
Segundo apellido OID: 2.16.724.1.3.5.7.2.8	Segundo apellido del responsable del certificado. Opcional.
Correo electrónico OID: 2.16.724.1.3.5.7.2.9	Correo electrónico del responsable del certificad. Opcional.

3.1.1.3 Certificado de autenticación de empleado público, nivel alto, en tarjeta

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la Administración, organismo, entidad de derecho público u otra entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationalUnitName (OU)	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Surname	Primer y segundo(opcional) apellido, de acuerdo con documento de identidad (DNI/Pasaporte)
Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)
Serial Number	DNI/NIE del empleado
Common Name (CN)	Nombre Apellido1 Apellido2 – NIF del empleado
Tipo de certificado OID: 2.16.724.1.3.5.7.1.1	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO DE NIVEL ALTO DE AUTENTICACION
Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.7.1.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 2.16.724.1.3.5.7.1.3	NIF entidad subscription
DNI/NIE del responsable OID: 2.16.724.1.3.5.7.1.4	DNI o NIE del responsable
Nombre de pila OID: 2.16.724.1.3.5.7.1.6	Nombre de pila del responsable del certificado
Primer apellido OID: 2.16.724.1.3.5.7.1.7	Primer apellido del responsable del certificado
Segundo apellido OID: 2.16.724.1.3.5.7.1.8	Segundo apellido del responsable del certificado. Opcional.

Correo electrónico OID: 2.16.724.1.3.5.7.1.9	Correo electrónico del responsable del certificado. Opcional.

3.1.1.4 Certificado de sello de órgano, nivel medio, en software

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial" de la organización) del suscriptor
organizationalUnitName (OU)	SELLO ELECTRONICO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Serial Number	DNI/NIE de la organización suscriptora
Common Name (CN)	Denominación de sistema o aplicación de proceso automático.
Tipo de certificado OID: 2.16.724.1.3.5.6.2.1	SELLO ELECTRONICO DE NIVEL MEDIO
Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.6.2.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 2.16.724.1.3.5.6.2.3	NIF entidad suscriptora
Denominación del sistema OID: 2.16.724.1.3.5.6.2.5	Denominación del sistema
Correo electrónico OID: 2.16.724.1.3.5.6.2.9	Correo electrónico del responsable del sello

3.1.1.5 Certificado de sello de órgano, nivel medio, en HSM

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial" de la organización) del suscriptor
organizationalUnitName (OU)	SELLO ELECTRONICO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Serial Number	DNI/NIE de la organización suscriptora
Common Name (CN)	Denominación de sistema o aplicación de proceso automático.

Tipo de certificado OID: 2.16.724.1.3.5.6.2.1	SELLO ELECTRONICO DE NIVEL MEDIO
Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.6.2.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 2.16.724.1.3.5.6.2.3	NIF entidad suscriptora
Denominación del sistema OID: 2.16.724.1.3.5.6.2.5	Denominación del sistema

3.1.1.6 Certificado de firma de empleado público con seudónimo, nivel alto, en tarjeta

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationalUnitName (OU)	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Pseudonym	Seudónimo obligatorio según ETSI EN 319 412-2 para este tipo de certificados
Common Name (CN)	Seudónimo y el Organismo
Tipo de certificado OID: 2.16.724.1.3.5.4.1.1	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO DE NIVEL ALTO
Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.4.1.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 2.16.724.1.3.5.4.1.3	NIF entidad suscriptora
Seudónimo OID: 2.16.724.1.3.5.4.1.12	Seudónimo usado por el firmante y autorizado por el suscriptor

3.1.1.7 Certificado de firma de empleado público con seudónimo, nivel medio, en HSM

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado

organizationalUnitName (OU)	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Pseudonym	Seudónimo obligatorio según ETSI EN 319 412-2 para este tipo de certificados
Common Name (CN)	Seudónimo y el Organismo
Tipo de certificado OID: 2.16.724.1.3.5.4.2.1	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO DE NIVEL MEDIO
Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.4.2.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 2.16.724.1.3.5.4.2.3	NIF entidad suscriptora
Seudónimo OID: 2.16.724.1.3.5.4.2.12	Seudónimo usado por el firmante y autorizado por el suscriptor

3.1.1.8 Certificado de autenticación de empleado público, con seudónimo, nivel alto, en tarjeta

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la Administración, organismo, entidad de derecho público u otra entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationalUnitName (OU)	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
pseudonym	Seudónimo Obligatorio según ETSI EN 319 412-2
Common Name (CN)	Puesto o cargo o "SEUDONIMO" – NUMERO IDENTIFICATIVO - NOMBRE OFICIAL DEL ORGANISMO
Tipo de certificado OID: 2.16.724.1.3.5.4.1.1	CERTIFICADO DE AUTENTICACIÓN DE EMPLEADO PUBLICO CON SEUDONIMO
Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.4.1.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 2.16.724.1.3.5.4.1.3	NIF entidad suscriptora

3.1.1.9 Certificado de sello electrónico de TSA/TSU

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial" de la organización) del suscriptor
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Common Name (CN)	Denominación de la TSU

3.1.1.10 Certificado de firma de persona física vinculada, en tarjeta

Subperfil España:

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Surname	Primer y segundo(opcional) apellido, de acuerdo con documento de identidad (DNI/Pasaporte)
Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)
Serial Number	DNI/NIE de la persona física
Common Name (CN)	Apellido1 Apellido2 Nombre – NIF persona física (FIRMA)
Tipo de certificado OID: 1.3.6.1.4.1.47281.0.7.1	CERTIFICADO DE PERSONA FÍSICA VINCULADA A ENTIDAD
Nombre de la entidad suscriptora OID: 1.3.6.1.4.1.47281.0.7.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 1.3.6.1.4.1.47281.0.7.3	NIF entidad subscription
DNI/NIE del responsable OID: 1.3.6.1.4.1.47281.0.7.4	DNI o NIE del responsable
Nombre de pila OID: 1.3.6.1.4.1.47281.0.7.6	Nombre de pila del responsable del certificado
Primer apellido OID: 1.3.6.1.4.1.47281.0.7.7	Primer apellido del responsable del certificado
Segundo apellido OID: 1.3.6.1.4.1.47281.0.7.8	Segundo apellido del responsable del certificado. Opcional.

Correo electrónico OID: 1.3.6.1.4.1.47281.0.7.9	Correo electrónico del responsable del certificado. Opcional.

Subperfil Europa:

Country (C)	País
Organization (O)	Denominación (nombre "oficial") de la entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Surname	Primer y segundo(opcional) apellido, de acuerdo con documento de identidad
Given Name	Nombre de pila, de acuerdo con documento de identidad
Serial Number	Número del documento de identidad de la persona física
Common Name (CN)	Apellido1 Apellido2 Nombre – num documento (FIRMA)
Tipo de certificado OID: 1.3.6.1.4.1.47281.0.19.1	PV
Nombre de la entidad suscriptora OID: 1.3.6.1.4.1.47281.0.19.2	Corresponde con el organization del sujeto
Identificador entidad suscriptora OID: 1.3.6.1.4.1.47281.0.19.3	Corresponde con el organizationIdentifier del sujeto
Identificador del responsable OID: 1.3.6.1.4.1.47281.0.19.4	DNI o NIE del responsable
Nombre de pila OID: 1.3.6.1.4.1.47281.0.19.6	Nombre de pila del responsable del certificado
Primer apellido OID: 1.3.6.1.4.1.47281.0.19.7	Primer apellido del responsable del certificado
Segundo apellido OID: 1.3.6.1.4.1.47281.0.19.8	Segundo apellido del responsable del certificado. Opcional.
Unidad de la entidad suscriptora OID: 1.3.6.1.4.1.47281.0.19.10	Corresponde con OrganizationUnit del sujeto. Opcional

3.1.1.11 Certificado de firma de persona física vinculada, en HSM

Subperfil España:

Country (C)	"ES"

Organization (O)	Denominación (nombre "oficial") de la entidad subscriptora, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Surname	Primer y segundo(opcional) apellido, de acuerdo con documento de identidad (DNI/Pasaporte)
Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)
Serial Number	DNI/NIE del empleado
Common Name (CN)	Apellido1 Apellido2 Nombre – NIF persona física
Tipo de certificado OID: 1.3.6.1.4.1.47281.0.7.1	CERTIFICADO DE PERSONA FÍSICA VINCULADA A ENTIDAD
Nombre de la entidad suscriptora OID: 1.3.6.1.4.1.47281.0.7.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 1.3.6.1.4.1.47281.0.7.3	NIF entidad subscription
DNI/NIE del responsable OID: 1.3.6.1.4.1.47281.0.7.4	DNI o NIE del responsable
Nombre de pila OID: 1.3.6.1.4.1.47281.0.7.6	Nombre de pila del responsable del certificado
Primer apellido OID: 1.3.6.1.4.1.47281.0.7.7	Primer apellido del responsable del certificado
Segundo apellido OID: 1.3.6.1.4.1.47281.0.7.8	Segundo apellido del responsable del certificado. Opcional.
Correo electrónico OID: 1.3.6.1.4.1.47281.0.7.9	Correo electrónico del responsable del certificado. Opcional.

Subperfil Europa:

Country (C)	País
Organization (O)	Denominación (nombre "oficial") de la entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Surname	Primer y segundo(opcional) apellido, de acuerdo con documento de identidad
Given Name	Nombre de pila, de acuerdo con documento de identidad
Serial Number	Número del documento de identidad de la persona física

Common Name (CN)	Apellido1 Apellido2 Nombre – num documento
Nombre de pila OID: 1.3.6.1.4.1.47281.0.19.6	Nombre de pila del responsable del certificado , corresponde con Given Name
Primer apellido OID: 1.3.6.1.4.1.47281.0.19.7	Primer apellido del responsable del certificado
Segundo apellido OID: 1.3.6.1.4.1.47281.0.19.8	Segundo apellido del responsable del certificado. Opcional.

3.1.1.12 Certificado de autenticación de persona física vinculada, en tarjeta

Subperfil España:

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Surname	Primer y segundo(opcional) apellido, de acuerdo con documento de identidad (DNI/Pasaporte)
Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)
Serial Number	DNI/NIE del empleado
Common Name (CN)	Apellido1 Apellido2 Nombre – NIF persona física (AUTENTICACION)
Tipo de certificado OID: 1.3.6.1.4.1.47281.0.7.1	CERTIFICADO DE PERSONA FÍSICA VINCULADA A ENTIDAD
Nombre de la entidad suscriptora OID: 1.3.6.1.4.1.47281.0.7.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 1.3.6.1.4.1.47281.0.7.3	NIF entidad subscription
DNI/NIE del responsable OID: 1.3.6.1.4.1.47281.0.7.4	Corresponde con SerialNumber del sujeto
Nombre de pila OID: 1.3.6.1.4.1.47281.0.7.6	Nombre de pila del responsable del certificado
Primer apellido OID: 1.3.6.1.4.1.47281.0.7.7	Primer apellido del responsable del certificado

Segundo apellido OID: 1.3.6.1.4.1.47281.0.7.8	Segundo apellido del responsable del certificado. Opcional.
Correo electrónico OID: 1.3.6.1.4.1.47281.0.7.9	Correo electrónico del responsable del certificado. Opcional.

Subperfil Europa:

Country (C)	País
Organization (O)	Denominación (nombre "oficial") de la entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Surname	Primer y segundo(opcional) apellido, de acuerdo con documento de identidad
Given Name	Nombre de pila, de acuerdo con documento de identidad
Serial Number	Número del documento de identidad de la persona física
Common Name (CN)	Apellido1 Apellido2 Nombre – num documento (AUTENTICACION)
Nombre de pila OID: 1.3.6.1.4.1.47281.0.19.6	Nombre de pila del responsable del certificado , corresponde con Given Name
Primer apellido OID: 1.3.6.1.4.1.47281.0.19.7	Primer apellido del responsable del certificado
Segundo apellido OID: 1.3.6.1.4.1.47281.0.19.8	Segundo apellido del responsable del certificado. Opcional.

3.1.1.13 Certificado de firma de persona física vinculada, en tarjeta, con seudónimo

Subperfil España:

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
pseudonym	Seudónimo Obligatorio según ETSI EN 319 412-2
Common Name (CN)	Puesto o "SEUDONIMO" – NUMERO IDENTIFICATIVO - NOMBRE ENTIDAD

Subperfil Europa:

Country (C)	País
Organization (O)	Denominación (nombre "oficial") de la entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
pseudonym	Seudónimo Obligatorio según ETSI EN 319 412-2
Common Name (CN)	SEUDONIMO - NOMBRE ENTIDAD

3.1.1.14 Certificado de firma de persona física vinculada, en HSM

Subperfil España:

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la entidad subscriptora, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
pseudonym	Seudónimo Obligatorio según ETSI EN 319 412-2
Common Name (CN)	Puesto o "SEUDONIMO" – NUMERO IDENTIFICATIVO - NOMBRE ENTIDAD

Subperfil Europa:

Country (C)	País
Organization (O)	Denominación (nombre "oficial") de la entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
pseudonym	Seudónimo Obligatorio según ETSI EN 319 412-2
Common Name (CN)	SEUDONIMO - NOMBRE ENTIDAD

3.1.1.15 Certificado de autenticación de persona física vinculada, en tarjeta, con seudónimo

Subperfil España:

Country (C)	"ES"

Organization (O)	Denominación (nombre "oficial") de la entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Common Name (CN)	Puesto o "SEUDONIMO" – NUMERO IDENTIFICATIVO - NOMBRE ENTIDAD

Subperfil Europa:

Country (C)	País
Organization (O)	Denominación (nombre "oficial") de la entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
pseudonym	Seudónimo Obligatorio según ETSI EN 319 412-2
Common Name (CN)	SEUDONIMO - NOMBRE ENTIDAD

3.1.1.16 Certificado de sello electrónico, en software

Subperfil España:

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial" de la organización) del suscriptor
organizationalUnitName (OU)	SELLO ELECTRONICO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Serial Number	DNI/NIE de la organización suscriptora
Common Name (CN)	Denominación de sistema o aplicación de proceso automático.

Subperfil Europa:

Country (C)	País
Organization (O)	Denominación (nombre "oficial" de la organización) del suscriptor
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1

Serial Number	Identificación de la organización suscriptora (legalPersonSemanticsIdentifier)

3.1.1.17 Certificado de sello electrónico con gestión centralizada

Subperfil España:

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial" de la organización) del suscriptor
organizationalUnitName (OU)	SELLO ELECTRONICO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Serial Number	DNI/NIE de la organización suscriptora
Common Name (CN)	Denominación de sistema o aplicación de proceso automático.

Subperfil Europa:

Country (C)	País
Organization (O)	Denominación (nombre "oficial" de la organización) del suscriptor
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Serial Number	Identificación de la organización suscriptora (legalPersonSemanticsIdentifier)

3.1.2. Significado de los nombres

Los nombres contenidos en los campos *SubjectName* y *SubjectAlternativeName* de los certificados son comprensibles en lenguaje natural, de acuerdo con lo establecido en la sección anterior.

3.1.3 Empleo de anónimos y seudónimos

En ningún caso se pueden utilizar seudónimos para identificar una entidad/empresa/organización, y en ningún caso se emiten certificados anónimos, a excepción hecha de que, por razones de seguridad pública, los sistemas de firma electrónica puedan referirse sólo al número de identificación profesional del empleado público.

3.1.4 Interpretación de formatos de nombres

Los formatos de nombres se interpretarán de acuerdo con la ley del país de establecimiento del suscriptor, en sus propios términos.

El certificado muestra la relación entre una persona física y la Administración, organismo, entidad de derecho público u otra entidad con la que está vinculada, con independencia de la nacionalidad de la persona física. Ello deriva de la naturaleza corporativa del certificado, del cual es suscriptor la corporación, y la persona física vinculada la persona autorizada a su uso.

En los certificados emitidos, el campo “número de serie” debe incluir el número de documento de la identidad de la persona firmante , al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

3.1.5 Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos, para cada política de certificado de esFIRMA.

No se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente, situación que, en principio no se ha de dar, gracias a la presencia del Número de Identificación Fiscal, o equivalente, en el esquema de nombres.

Un suscriptor puede pedir más de un certificado siempre que la combinación de los siguientes valores existentes en la solicitud fuera diferente de un certificado válido:

- Número de Identificación Fiscal (NIF) u otro identificador legalmente válido de la persona física.
- Número de Identificación Fiscal (NIF) u otro identificador legalmente válido del suscriptor.
- Tipo de Certificado (Campo descripción del certificado).

3.1.6 Resolución de conflictos relativos a nombres

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

esFIRMA no estará obligada a determinar previamente que un solicitante de certificados tiene derechos de propiedad industrial sobre el nombre que aparece en una solicitud de certificado, sino que en principio procederá a certificarlo.

Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

Sin embargo, en caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación del país del suscriptor, podrá emprender las acciones pertinentes orientadas a bloquear o retirar el certificado emitido.

En todo caso, el prestador de servicios de certificación se reserva el derecho de rechazar una solicitud de certificado debido a un conflicto de nombres.

Toda controversia o conflicto que se derive del presente documento, se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte en el documento contractual que formaliza el servicio.

3.2 Validación inicial de la identidad

La identidad de los suscriptores de certificados resulta fijada en el momento de la firma del contrato entre esFIRMA y el suscriptor o previamente a la activación del servicio de esFIRMA, momento en el que se verifica la existencia del suscriptor, y de la documentación aportada justificativa de su identidad, del cargo y/o condición en el cual firma y de su dirección, de conformidad con lo indicado en la normativa de derecho administrativo que sea de aplicación.

La identidad de las personas físicas identificadas en los certificados se valida mediante los registros corporativos de la Administración, organismo, entidad de derecho público u otra entidad suscriptora de los certificados. El suscriptor producirá una certificación de los datos necesarios, y la remitirá a esFIRMA, por los medios que ésta habilite, para el registro de la identidad de los firmantes. Cuando el suscriptor no disponga de Secretaría, esta certificación será emitida por el Responsable del servicio de certificación designado.

El responsable del tratamiento de los datos personales de cada Administración, organismo, entidad de derecho público u otra entidad, es cada una de ellas, siendo esFIRMA encargado del tratamiento de dichos datos.

Para evitar cualquier conflicto de intereses las Administraciones Públicas u otras entidades suscriptoras son entidades independientes del Prestador de servicios de confianza "esFIRMA" y de la empresa ESPUBLICO.

3.2.1 Prueba de posesión de clave privada

La posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del certificado por el firmante desde la Plataforma de Administración Electrónica, al firmar la hoja de aceptación, y su uso en dicha plataforma.

3.2.2 Identificación de la entidad

En Administraciones públicas no se exige la documentación acreditativa de la existencia de la administración pública, organismo o entidad de derecho público, dado que dicha identidad forma parte del ámbito corporativo de la Administración General del Estado o de otras AAPP del Estado.

EsFIRMA verifica la existencia de cada Administración Pública, organismo o entidad de derecho público, cuando sea necesario, ante el inventario de entes del sector público del Ministerio de Hacienda y Función Pública en https://www.hacienda.gob.es/es-ES/CDI/Paginas/Inventario/Inventario.aspx, ante un Boletín Oficial de su ámbito ó mediante la integración con el Sistema de Directorio Común (DIR3).

En caso de que la entidad no forme parte del ámbito corporativo de la Administración General del Estado o de otras AAPP del Estado, ESFIRMA verificará la existencia de la entidad mediante los documentos o consulta de registros públicos pertinentes según lo indicado en la normativa de derecho administrativo que sea de aplicación.

Las personas físicas con capacidad de actuar en nombre de una Administración, organismo, entidad de derecho público u otra entidad suscriptora de los certificados, podrán actuar como representantes de las mismas en relación a lo previsto en esta DPC, siempre y cuando exista una situación previa de representación legal o voluntaria entre la persona física y la Administración, organismo, entidad de derecho público u otra entidad suscriptora de los certificados, que exige su reconocimiento por esFIRMA, el cual se realizará mediante uno de los procedimientos siguientes:

1. En caso de que la persona que ostente el cargo de Secretario tenga la facultad de fe pública, se recabarán y verificarán los siguientes documentos:
    a. Certificado del Secretario en el que se nombra al representante legal, con los siguientes datos:
        i. Nombre y apellidos del representante legal
        ii. Documento: NIF del representante
        iii. CIF de la entidad a la que representa
        iv. Nombre de la entidad a la que representa
        v. Dirección postal de la entidad a la que representa

2. En caso de que la persona que ostente el cargo de Secretario no tenga la facultad de fe pública, se recabarán y verificarán los siguientes documentos:
    a. Un certificado del Secretario del nombramiento del representante legal en el que figuran los siguientes datos:
        i. Datos del representante:
            1. Nombre y apellidos del representante legal
            2. Documento: NIF del representante
        ii. Datos de la entidad a la que representa:
            1. CIF
            2. Nombre
            3. Dirección postal

iii. Información sobre la vigencia de la representación

b. Documentación oficial que permita acreditar los datos relativos a la representación o la capacidad de actuación que ostenta el representante legal.
c. Todos los documentos necesarios para acreditar los extremos citados de manera fehaciente de conformidad con lo indicado en la normativa de derecho administrativo que sea de aplicación, y su inscripción en el correspondiente registro público si así resulta exigible.

Tras la verificación de la documentación recabada, el Representante legal procederá a la firma del contrato de prestación de servicios de certificación entre esFIRMA (ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA) y la entidad por medio del cual se regulan las condiciones bajo las cuales ESFIRMA prestará los servicios de certificación a la entidad, que se constituye como Autoridad de Registro, nombrando a los Operadores autorizados para ejercer las funciones correspondientes a la RA.

Una vez firmados los documentos electrónicamente, se activarán las funciones de RA a los usuarios de la entidad que figuren en el contrato como operadores autorizados para desempeñar esta función.

3.2.3 Autenticación de la identidad de una persona física

Esta sección describe los métodos de comprobación de la identidad de una persona física identificada en un certificado.

El procedimiento para solicitar y generar certificados se realiza a través de un procedimiento electrónico en la Plataforma de Administración Electrónica a disposición del suscriptor y de los firmantes.

El procedimiento electrónico para emitir un certificado a una persona física seguirá los siguientes pasos y se generarán los siguientes documentos:

1. Solicitud de la persona física a través de la Plataforma de Administración Electrónica (con su correspondiente registro de entrada y apertura de expediente).
2. Un certificado en el que el Operador de verificación acredita la vinculación entre el solicitante y la entidad.

3. Orden de emisión firmada por el Operador de verificación y autorización de la entidad, que se registra de salida y se notifica a ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (adjuntando copia del certificado y de la solicitud del usuario).

El procedimiento electrónico para emitir un certificado de sello electrónico seguirá los siguientes pasos y se generarán los siguientes documentos:

1. Orden de emisión del Representante legal a través de la Plataforma de Administración Electrónica (con su correspondiente registro de entrada y apertura de expediente). Para presentar dicha solicitud, el Representante legal deberá identificarse en la plataforma utilizando medios de identificación electrónica, para los cuales se haya garantizado la presencia de la persona física conforme al artículo 8 del Reglamento eIDAS en relación a los niveles de seguridad "sustancial" o "alto".

3.2.3.1 En los certificados

La información de identificación de las personas físicas identificadas en los certificados se valida comparando la información de la solicitud de la Administración, organismo, entidad de derecho público u otra entidad suscriptora de los certificados, con los registros de la Administración, organismo, entidad de derecho público u otra entidad a la que está vinculado, generados según lo indicado en el punto 3.2 de esta DPC, asegurando la corrección de la información a certificar.

3.2.3.2 Necesidad de presencia personal

Para realizar la solicitud de los certificados no se requiere la presencia física directa debido a la relación ya acreditada entre la persona física y la Administración, organismo, entidad de derecho público u otra entidad a la que está vinculada. Esta acreditación se refleja en la validación de la solicitud por parte del Operador de verificación autorizado por el suscriptor, que hace constar la identificación presencial y unívoca del firmante.

Para aceptar el certificado no es necesaria la presencia física directa del firmante puesto que ésta se puede realizar mediante firma electrónica avanzada. Durante este trámite se confirma la identidad de la persona física identificada en el certificado.

El certificado deberá emitirse en el plazo máximo de 15 días naturales desde que se produzca la validación de la identidad de la persona física por parte del operador de verificación y autorización. Por tanto, si transcurridos 15 días naturales desde que el operador de verificación y autorización valida la identidad del solicitante y ordena la emisión, éste no acepta su certificado el proceso caducará, debiendo realizar la persona física una nueva solicitud.

3.2.3.3 Vinculación de la persona física

La justificación documental de la vinculación de una persona física identificada en un certificado con la Administración, organismo, entidad de derecho público u otra entidad viene dada por su constancia en los Registros de Personal de la Administración, organismo, entidad de derecho público u otra entidad a las que está vinculada la persona física.

3.2.4 Información de suscriptor no verificada

esFIRMA no incluye ninguna información de suscriptor no verificada en los certificados.

3.2.5 Criterios de interoperabilidad

esFIRMA no tiene relaciones de interoperabilidad con otras autoridades de certificación externas.

esFIRMA no emite certificados de CA subordinados a terceros y su CA emisora no está técnicamente limitada.

3.3 Identificación y autenticación de solicitudes de renovación

3.3.1 Validación para la renovación rutinaria de certificados

esFirma no realiza renovaciones de certificados. esFirma emitirá un certificado nuevo, siguiendo el procedimiento de solicitud registrado en la Plataforma de Administración Electrónica.

3.3.2 Identificación y autenticación de renovación tras revocación

esFIRMA no realiza renovaciones de certificados.

3.4 Identificación y autenticación de la solicitud de revocación

esFIRMA auténtica las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada.
Los métodos aceptables para dicha comprobación son los siguientes:

- El envío de una solicitud de revocación por parte del suscriptor o de la persona física identificada en el certificado, firmada electrónicamente.
- El uso de la "frase de comprobación de identidad", o de otros métodos de autenticación personal, que consiste en información que sólo conoce la persona física identificada en el certificado, y que le permite revocar de forma automática su certificado.
- La personación física en una oficina de la entidad suscriptora.
- Otros medios de comunicación, como el teléfono, cuando existan garantías razonables de la identidad del solicitante de la revocación, a juicio de esFIRMA.

esFIRMA no realiza suspensiones de certificados. Las peticiones de suspensión son tratadas como peticiones de revocación.

4. Requisitos de operación del ciclo de vida de los certificados

4.1 Solicitud de certificado

4.1.1 Legitimación para solicitar la emisión

La Administración, organismo, entidad de derecho público u otra entidad debe firmar un contrato de prestación de servicios de certificación con esFIRMA.

Asimismo, con anterioridad a la emisión y entrega de un certificado, existe una solicitud de certificados en una hoja de solicitud de certificados por medio de la Plataforma de Administración Electrónica.

Existe una autorización del suscriptor para que el solicitante pueda realizar la solicitud, que se instrumenta jurídicamente mediante una hoja de solicitud de certificados suscrita por dicho solicitante en nombre de la Administración, organismo, entidad de derecho público u otra entidad.

4.1.2 Procedimiento de alta y responsabilidades

esFIRMA recibe solicitudes de certificados, realizadas por las Administraciones, organismos, entidades de derecho público públicas u otras entidades.

Las solicitudes se instrumentan mediante un documento en formato electrónico, cumplimentado por la Administración, organismo, entidad de derecho público u otra entidad, cuyo destinatario es esFIRMA, el cual incluirá los datos de las personas a las que se expedirán certificados. La solicitud será realizada por el operador autorizado por el suscriptor (responsable de certificación) y que ha sido identificado en el contrato entre este suscriptor y esFIRMA.

A la solicitud se deberá acompañar documentación justificativa de la identidad y otras circunstancias de la persona física identificada en el certificado, de acuerdo con lo establecido en la sección 3.2.3. También se deberá acompañar una dirección física, u otros datos, que permitan contactar a la persona física identificada en el certificado.

4.2 Procesamiento de la solicitud de certificación

4.2.1 Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de certificado, esFIRMA se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

En caso afirmativo, esFIRMA verifica la información proporcionada, comprobando que se han cumplido correctamente los requisitos descritos en la sección 3.2.

La documentación justificativa de la aprobación de la solicitud debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante el plazo de 15 años desde la extinción del certificado o la finalización del servicio prestado, incluso en caso de pérdida anticipada de vigencia por revocación, al ser los certificados, cualificados.

esFIRMA mantiene procedimientos documentados que identifican y requieren actividad de verificación adicional para Solicitudes de certificados de alto riesgo, phishing u otros usos fraudulentos, consultando distintas listas de reputación de dominios y los criterios de mitigación de riesgos propios de esFIRMA.

4.2.2 Aprobación o rechazo de la solicitud

esFIRMA aprueba la solicitud del certificado y procede a su emisión y entrega, tras la petición que se produce en la Plataforma de Administración Electrónica.

En caso de sospecha que la información no es correcta o que puede afectar a la reputación de la Entidad de Certificación o de los suscriptores, esFIRMA denegará la petición, o detendrá su aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

En caso de que de las comprobaciones adicionales no se desprenda la corrección de las informaciones a verificar, esFIRMA denegará la solicitud definitivamente.

esFIRMA notifica al solicitante la aprobación o denegación de la solicitud.

esFIRMA podrá automatizar los procedimientos de verificación de la corrección de la información que será contenida en los certificados, y de aprobación de las solicitudes.

4.2.3 Plazo para resolver la solicitud

esFIRMA atiende las solicitudes de certificados por orden de llegada, en un plazo razonable, pudiendo especificarse una garantía de plazo máximo en el contrato de emisión de certificados.

Las solicitudes se mantienen activas hasta su aprobación o rechazo.

4.3 Emisión del certificado

4.3.1 Acciones de la CA durante el proceso de emisión

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone a disposición del firmante para su aceptación mediante el envío de un enlace al dispositivo móvil y/o dirección de correo electrónico que se haya designado por el suscriptor en la petición de certificados, según el procedimiento indicado en el apartado 4.4.2 o mediante el sistema de mensajería de la Plataforma de Administración Electrónica.

Durante el proceso, esFIRMA:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.

- Incluye en el certificado las informaciones establecidas en el anexo 1 del Reglamento (UE) 910/2014, de acuerdo con lo establecido en las secciones 3.1.1 y 7.1.
- Indica la fecha y la hora en que se expidió un certificado.

4.3.2 Notificación de la emisión al suscriptor

esFIRMA notifica la emisión del certificado a la Administración, organismo, entidad de derecho público u otra entidad suscriptora del certificado, y a la persona física identificada en el certificado, a través de sus direcciones de correo electrónico, ya incluidas en la información de la Plataforma de Administración Electrónica.

4.4 Entrega y aceptación del certificado

Durante este proceso, esFIRMA debe realizar las siguientes actuaciones:

- Acreditar definitivamente la identidad de la persona física identificada en el certificado, con la colaboración de la Administración, organismo, entidad de derecho público u otra entidad de acuerdo con lo establecido en las secciones 3.2.2, 3.2.3, y 4.3.1.
- Entregar la hoja de entrega y aceptación del certificado a la persona física identificada en él, la cual dispone de los siguientes contenidos mínimos:
    - Información básica acerca del uso del certificado, incluyendo especialmente información acerca del prestador de servicios de certificación y de la Declaración de Prácticas de Certificación aplicable, como sus obligaciones, facultades y responsabilidades
    - Información acerca del certificado.
    - Reconocimiento, por parte del firmante, de recibir el certificado y la aceptación de los citados elementos.
    - Régimen de obligaciones del firmante.
    - Responsabilidad del firmante.
    - Método de imputación exclusiva al firmante, de su clave privada y de sus datos de activación del certificado, de acuerdo con lo establecido en las secciones 6.2 y 6.4.
    - La fecha del acto de entrega y aceptación.

- Obtener la firma, escrita o electrónica, de la persona identificada en el certificado.

Cuando sea necesario, la Administración, organismo, entidad de derecho público u otra entidad colabora en estos procesos, debiendo registrar documentalmente los anteriores actos y conservando los citados documentos originales (hojas de entrega y aceptación), remitiendo copia electrónica a esFIRMA, así como los originales cuando esFIRMA precise de acceso a los mismos.

4.4.1 Conducta que constituye aceptación del certificado

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se avisa al firmante para su aceptación mediante el envío de un enlace al dispositivo móvil y/o dirección de correo electrónico que se haya designado por el suscriptor en la petición de certificados o mediante el sistema de mensajería de la Plataforma de Administración Electrónica.

En los certificados emitidos en software, el certificado y las claves son gestionadas en un HSM, disponiendo el firmante de control exclusivo de su uso.

En los certificados emitidos en tarjeta, estas son enviadas al responsable de certificación del suscriptor, y los correspondientes PIN es directamente a la dirección postal del firmante.

Además, la aceptación del certificado por la persona física identificada en el certificado se produce mediante la firma de la hoja de entrega y aceptación, por medio de la Plataforma de Administración Electrónica.

4.4.2 Publicación del certificado

En el caso del certificado de TSA/TSU, esFIRMA lo publica en su página web.

4.4.3 Notificación de la emisión a terceros

esFIRMA no realiza ninguna notificación de la emisión a terceras entidades.

4.5 Uso del par de claves y del certificado

4.5.1 Uso por el suscriptor o firmante

esFIRMA obliga a lo siguiente:

- Facilitar a esFIRMA información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de aceptación.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4.
- Cuando el certificado funcione conjuntamente con un DCCF, reconocer su capacidad de producción de firmas electrónicas cualificadas; esto es, equivalentes a firmas manuscritas, así como otros tipos de firmas electrónicas y mecanismos de cifrado de información.
- Ser especialmente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.1, 6.2 y 6.4.
- Comunicar a esFIRMA y a cualquier persona que se crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2.
- Que todas las informaciones suministradas por el firmante que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.

- Que el firmante es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

4.5.2 Uso por el suscriptor

esFIRMA obliga contractualmente al suscriptor a:

- Facilitar a la Entidad de Certificación información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de aceptación.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4.
- Comunicar a esFIRMA y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
    - La pérdida, la alteración, el uso no autorizado, el robo o el compromiso, cuando exista, de la tarjeta.
- Trasladar a las personas físicas identificadas en el certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de las mismas.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de esFIRMA, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación del prestador de servicios de certificación de esFIRMA, sin permiso previo por escrito.
- Que todas las manifestaciones realizadas en la solicitud son correctas.

- Que todas las informaciones suministradas por el suscriptor que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el suscriptor es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

4.5.3 Uso por el tercero que confía en certificados

esFIRMA informa al tercero que confía en certificados de que el mismo debe asumir las siguientes obligaciones:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía.
- Reconocer que para considerarse certificado cualificado debe estar incluido en la Lista de Confianza nacional (Trusted List).
- Reconocer que las firmas electrónicas verificadas, producidas en un dispositivo cualificado de creación de firma (DCCF) tienen la consideración legal de firmas electrónicas cualificadas; esto es, equivalentes a firmas manuscritas, así como que el certificado permite la creación de otros tipos de firmas electrónicas y mecanismos de cifrado.
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.

- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de esFIRMA, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de esFIRMA, sin permiso previo por escrito.

esFIRMA informa al tercero que confía en certificados de que el mismo debe asumir las siguientes responsabilidades:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

4.6. Renovación de certificados

esFIRMA no realiza renovación de certificados. esFirma emitirá un certificado nuevo, siguiendo el procedimiento de solicitud registrado en la Plataforma de Administración Electrónica.

4.6.1 Circunstancias para la renovación del certificado

No aplica.

4.6.2 Quién puede pedir una renovación

No aplica.

4.6.3 Procesamiento de la solicitud de renovación de certificados

No aplica.

4.6.4 Notificación de nueva emisión de certificado al suscriptor

No aplica.

4.6.5 Conducta que constituya la aceptación de un certificado de renovación

No aplica.

4.6.6 Publicación del certificado de renovación por la CA

No aplica.

4.6.7 Notificación de la emisión del certificado por la CA a otras entidades

No aplica.

4.7 Renovación de claves y certificados

4.7.1 Quién puede solicitar el certificado de una nueva clave pública

No aplica.

4.7.2 Procedimiento con nueva identificación

No aplica.

4.7.3 Procesamiento de solicitudes de nueva clave de certificado

esFIRMA advertirá al suscriptor de la necesidad de proceder a una nueva personación del firmante y firma de la hoja de aceptación, en aquellos casos en los que así sea necesario por transcurso del plazo legal de identificación de 5 años.

Dicha personación e identificación se realizará de conformidad con lo indicado en el apartado 3.2.

La firma de la hoja de aceptación se realizará de conformidad con lo indicado en el apartado 4.4.2.

4.7.4 Notificación de la emisión del certificado renovado

No aplica por no existir renovaciones.

4.7.5 Conducta que constituye aceptación del certificado

No aplica.

4.7.6 Publicación del certificado

No aplica.

4.7.7 Notificación de la emisión a terceros

esFIRMA no realiza notificación alguna de la emisión a terceras entidades.

4.8 Modificación de certificados

La modificación de certificados será tratada como una nueva emisión de certificado, aplicándose lo descrito en las secciones 4.1, 4.2, 4.3 y 4.4.

4.9 Revocación y suspensión de certificados

4.9.1 Causas de revocación de certificados

esFIRMA extinguirá la vigencia de los certificados electrónicos mediante revocación cuando concurra alguna de las siguientes causas:

1) Circunstancias que afectan a la información contenida en el certificado:
   a) Modificación de alguno de los datos contenidos en el certificado, después de la correspondiente emisión del certificado que incluye las modificaciones.

b) Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.

c) Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.

2) Circunstancias que afectan a la seguridad de la clave o del certificado:

a) Compromiso de la clave privada, de la infraestructura o de los sistemas del prestador de servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.

b) Infracción, por esFIRMA, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas de Certificación.

c) Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.

d) Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.

e) El uso irregular del certificado por la persona física identificada en el certificado, o la falta de diligencia en la custodia de la clave privada.

3) Circunstancias que afectan al suscriptor o a la persona física identificada en el certificado:

a) Finalización de la relación jurídica de prestación de servicios entre esFIRMA y el suscriptor.

b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado a la persona física identificada en el certificado.

c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.

d) Infracción por el suscriptor o por la persona identificada en el certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente.

e) La incapacidad sobrevenida o el fallecimiento del poseedor de claves.

f) La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor al poseedor de claves o la finalización de la relación entre suscriptor y persona identificada en el certificado.

g) Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.4.

4) Otras circunstancias:
   a) La terminación del servicio de certificación de esFIRMA, de acuerdo con lo establecido en la sección 5.8.
   b) El uso del certificado que sea dañino y continuado para esFIRMA. En este caso, se considera que un uso es dañino en función de los siguientes criterios:
      - La naturaleza y el número de quejas recibidas.
      - La identidad de las entidades que presentan las quejas.
      - La legislación relevante vigente en cada momento.
      - La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.
   c) Pérdida de certificación de alguno de los dispositivos cualificados de creación de firma de los que estuviera utilizando esFIRMA en calidad de Prestador Cualificado de Servicios de Confianza,

4.9.2 Legitimación para solicitar la revocación

Pueden solicitar la revocación de un certificado:

- La persona identificada en el certificado, mediante petición dirigida a esFIRMA o al suscriptor.
- El suscriptor del certificado, mediante petición dirigida a esFIRMA.

4.9.3 Procedimientos de solicitud de revocación

La solicitud de revocación comprenderá la siguiente información:

- Fecha de solicitud de la revocación.
- Identidad del suscriptor o del firmante.
- Razón detallada para la petición de revocación.

La solicitud debe ser autenticada, por esFIRMA, de acuerdo con los requisitos establecidos en la sección 3.4 de esta política, antes de proceder a la revocación.

esFIRMA podrá incluir cualquier otro requisito para la confirmación de las solicitudes de revocación.

El servicio de revocación se encuentra en la Plataforma de Administración Electrónica, en la que el firmante y el suscriptor gestionan sus certificados.

En caso de que el destinatario de una solicitud de revocación por parte de una persona física identificada en el certificado fuera la entidad suscriptora una vez autenticada la solicitud ésta debe remitir una solicitud en este sentido a esFIRMA.

La solicitud de revocación será procesada a su recepción, y se informará al suscriptor y, a la persona física identificada en el certificado, acerca del cambio de estado del certificado revocado.

esFIRMA no reactiva el certificado una vez ha sido revocado.

Hay un servicio 24/7 disponible en el número de teléfono +34 976 579 516, para solicitar la revocación de los certificados. La comunicación es grabada y registrada, para ser utilizado como soporte y garantía de aceptación de la revocación solicitada.

4.9.4 Plazo temporal de solicitud de revocación

Las solicitudes de revocación se remitirán de forma inmediata en cuanto se tenga conocimiento de la causa de revocación, y no será superior a las 24 horas.

4.9.5 Plazo temporal de procesamiento de la solicitud

Las solicitudes de revocación se harán efectivas en un plazo máximo de 24 horas.

En caso de que, por circunstancias excepcionales, no fuera posible confirmar la solicitud de revocación en dicho plazo de 24 horas, la revocación se realizará a la mayor brevedad posible; debiendo elaborar un informe de las circunstancias que han impedido la

revocación en el plazo establecido y las acciones a tomar para que no se repita dicha situación.

4.9.6 Obligación de consulta de información de revocación de certificados por terceros

Los terceros deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Certificados más reciente emitida por la Entidad de Certificación de esFIRMA.

Las Listas de Revocación de Certificados se publican en el Depósito de la Entidad de Certificación, así como en las siguientes direcciones web, indicadas dentro de los certificados:

- *CA RAÍZ 2:*
  - https://crls2.esfirma.com/acraiz/acraiz2.crl
- https://crls1.esfirma.com/acraiz/acraiz2.crl

- *CA INTERMEDIA AAPP 2:*
  - https://crls1.esfirma.com/acaapp/acaapp2.crl
  - https://crls2.esfirma.com/acaapp/acaapp2.crl

Además, los terceros deberán verificar el estado de los certificados incluidos en la cadena de certificación.

4.9.7 Frecuencia de emisión de listas de revocación de certificados (CRLs)

esFIRMA emite una CRL al menos cada 24 horas y siempre que se produzca una revocación.

En la jerarquía AAPP, la CRL indica el momento programado de emisión de una nueva CRL, si bien se puede emitir una CRL antes del plazo indicado en la CRL anterior, para reflejar revocaciones.

En la jerarquía ECC-1 las CRL mantienen obligatoriamente el certificado revocado o suspendido hasta que expira y después de que expire.

4.9.8 Plazo máximo de publicación de CRLs

Las CRLs se publican en el Depósito en un periodo inmediato razonable tras su generación, que en ningún caso supera unos pocos minutos.

4.9.9 Disponibilidad de servicios de comprobación en línea de estado de certificados

esFIRMA informa acerca del estado de revocación de los certificados, mediante el protocolo OCSP, que permite conocer el estado de vigencia de los certificados en línea desde las direcciones:

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

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de esFIRMA, ésta deberá realizar sus mejores esfuerzos por asegurar que este servicio se mantenga inactivo el mínimo tiempo posible, que no podrá superar un día.

esFIRMA suministra información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

Los servicios de comprobación de estado de los certificados son de uso gratuito.

esFIRMA mantiene disponible la información del estado de revocación pasado el período de validez del certificado.

4.9.10 Obligación de consulta de servicios de comprobación de estado de certificados

Resulta obligatorio consultar el estado de los certificados antes de confiar en los mismos, de forma prioritaria, mediante acceso al servicio OCSP.

esFIRMA admite el método GET para OCSP.

esFIRMA actualiza el OCSP al menos cada cuatro días e inmediatamente en condiciones normales.

Las respuestas de OCSP tienen un tiempo de vencimiento máximo de 48 horas.

Para conocer el estado de los Certificados de CA subordinados, la información que se proporciona a través de OCSP es actualizada al menos cada seis meses y dentro de las 24 horas posteriores a la revocación de un Certificado de CA subordinada.

Si el respondedor OCSP recibe una solicitud de estado de un certificado que no se ha emitido, entonces devolverá *"revoked, certificateHold 1 enero 1970"*, registrando dichas solicitudes como parte de los procedimientos de respuesta de seguridad de esFIRMA.

4.9.11 Otras formas de información de revocación de certificados

De forma alternativa, los terceros que confían en certificados podrán verificar el estado de revocación de los certificados consultando las CRLs más reciente emitida por esFIRMA. Éstas se encuentran publicadas en el sitio web de esFIRMA, así como en las direcciones web indicadas en los certificados.

esFIRMA no delega sus respuestas OCSP mediante OCSP stapling.

4.9.12 Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de esFIRMA es notificado a todos los participantes en los servicios de certificación, en la medida de lo posible, mediante la publicación de este hecho en la página web de esFIRMA, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

4.9.13 Causas de suspensión de certificados

esFIRMA no realiza suspensión de certificados.

4.9.14 Solicitud de suspensión

esFIRMA no realiza suspensión de certificados

4.9.15 Procedimientos para la petición de suspensión

esFIRMA no realiza suspensión de certificados.

4.9.16 Período máximo de suspensión

esFIRMA no realiza suspensión de certificados.

4.10 Servicios de comprobación de estado de certificados

4.10.1 Características operativas de los servicios

Los servicios de comprobación de estado de certificados se prestan mediante una interfaz de consulta web, en la web https://www.esfirma.com

También se pueden comprobar mediante acceso al servicio OCSP en las direcciones web indicadas en el apartado 4.9.9

Las entradas de revocación en una respuesta CRL u OCSP no son nunca eliminadas.

Diferencias y consideraciones entre las consultas de estado de revocación de un certificado mediante OCSP y CRL:

- Tanto OCSP como CRL muestran la información más reciente sobre el estado de revocación de un certificado no expirado. Sin embargo, la CRL requiere de un proceso de publicación de unos pocos minutos que puede resultar en discrepancias temporales entre ambos métodos. Eventualmente el estado de revocación de un certificado no expirado es el mismo en consulta via OCSP y CRL.
- En la jerarquía AAPP las CRL no incluyen certificados revocados que ya han expirado, mientras que OCSP sí incluyen dicha información. Al agregar certificados expirados a una CRL, se aumenta el tiempo necesario para verificar la validez de los certificados, ya que la lista es más grande y lleva más tiempo descargarla y

procesarla. Además, se produce un crecimiento indefinido en las CRL hasta el fin de la validez del emisor.

- En la jerarquía ECC-1 las CRL incluyen certificados revocados que ya han expirado.
- EsFIRMA emite una Última CRL, que se refiere a la última CRL emitida antes de que el certificado emisor de las CRL deje de tener vigencia por expiración, revocación u otros casos. Esta CRL junto con un archivo de firma LTA se utiliza para verificar si un certificado era válido o no en un momento determinado. Si no se puede validar la Última CRL se debe asumir que el certificado es inválido. Una vez verificada la Última CRL se deberá comprobar el estado del certificado en la CRL.
- OCSP requiere conexión en tiempo real con la autoridad de certificación para obtener el estado de revocación, mientras que las CRL se pueden descargar y almacenar localmente para su uso sin conexión.
- OCSP puede ser menos privado que las CRL, ya que las solicitudes OCSP pueden revelar a la autoridad de certificación los sitios que un cliente está visitando.

4.10.2 Disponibilidad de los servicios

Los servicios de comprobación de estado de certificados y el servicio de sellado de tiempo se encuentran disponibles las 24 horas del día, los 7 días de la semana, durante todo el año, con excepción de las paradas programadas.

Los servicios de comprobación de estado de los certificados son de uso gratuito.

4.10.3 Características opcionales

No aplica.

4.11 Finalización de la suscripción

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción al servicio.

4.12 Depósito y recuperación de claves

4.12.1 Política y prácticas de depósito y recuperación de claves

esFIRMA no presta servicios de depósito y recuperación de claves.

4.12.2 Política y prácticas de encapsulado y recuperación de claves de sesión

Sin estipulación.

5. Controles de seguridad física, de gestión y de operaciones

5.1 Controles de seguridad física

esFIRMA ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones de registro y aprobación de las solicitudes, generación técnica de los certificados y la gestión del hardware criptográfico.

En concreto, la política de seguridad física y ambiental aplicable a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación ha establecido prescripciones para las siguientes contingencias:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobos.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones donde se producen los certificados bajo la plena responsabilidad de esFIRMA, que la presta desde sus instalaciones de alta seguridad, tanto principales como, en su caso, de operación en contingencia, que son debidamente auditadas de forma periódica.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso.

5.1.1 Localización y construcción de las instalaciones

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

La sala donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos:

- Cuenta con redundancia en sus infraestructuras.
- Cuenta con varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.
- Las operaciones de mantenimiento no requieren que el Centro esté offline en ningún momento.
- Fiabilidad del 99,995% mensual

esFIRMA dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de los mismos

5.1.2 Acceso físico

El CPD donde se ubica la CA de esFIRMA dispone de los controles de seguridad y medidas acordes con el reglamento vigente.

El acceso físico a las dependencias de esFIRMA donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales. Así:

- Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

- El acceso a las salas se realiza con lectores de tarjeta de identificación.

- Para el acceso al rac donde se ubican los procesos criptográficos es necesario la autorización previa de esFIRMA a los administradores del servicio de hospedaje que disponen de la llave para abrir la jaula.

5.1.3 Electricidad y aire acondicionado

Las instalaciones de esFIRMA disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado.

5.1.4 Exposición al agua

Las instalaciones están ubicadas en una zona de bajo riesgo de inundación.

Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

5.1.5 Prevención y protección de incendios

Las instalaciones y activos de esFIRMA cuentan con sistemas automáticos de detección y extinción de incendios.

5.1.6 Almacenamiento de soportes

Únicamente personal autorizado tiene acceso a los medios de almacenamiento.

La información de más alto nivel de clasificación se guarda en una caja de seguridad fuera de las instalaciones del Centro de Proceso de Datos.

5.1.7 Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se realizan mediante mecanismos que garanticen la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se procede al formateo, borrado permanente, o destrucción física del soporte, mediante software especializado que realice un mínimo de 3 pasadas de borrado y con patrones de borrado variable.

En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

5.1.8 Copia de respaldo fuera de las instalaciones

esFIRMA utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del centro de operaciones.

Se requieren al menos dos personas autorizadas expresamente para el acceso, depósito o retirada de dispositivos.

5.2 Controles de procedimientos

esFIRMA garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal al servicio de esFIRMA ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

5.2.1 Funciones fiables

esFIRMA ha identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- **Auditor Interno:** Responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de Sistemas de Información. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.

- **Administrador de Sistemas**: Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación
- **Administrador de CA**: Responsable de las acciones a ejecutar con el material criptográfico, o con la realización de alguna función que implique la activación de las claves privadas de las autoridades de certificación descritas en este documento, o de cualquiera de sus elementos.
- **Operador de CA:** Responsable necesario conjuntamente con el Administrador de CA de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de copia de respaldo y mantenimiento de la AC.
- **Operador de Registro:** Persona responsable de aprobar las peticiones de certificación realizadas por el suscriptor.
- **Responsable de Seguridad**: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de esFIRMA. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.
- **Responsable de Información y servicio**: Define los requisitos de la información y de los servicios en materia de seguridad. Este rol tiene la responsabilidad última del uso que se haga de la información y los servicios y por tanto de su nivel de protección.
- **Especialista en Validación**: Responsable de la validación de las solicitudes de certificados.
- **Oficial de Revocación:** Responsable de la operación de cambio de estado de los certificados.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos.

5.2.2 Número de personas por tarea

esFIRMA garantiza al menos dos personas para realizar las tareas que se detallen en las Políticas de Certificación correspondientes. Especialmente en la manipulación del dispositivo de custodia de las claves de la Autoridad de Certificación raíz.

5.2.3 Identificación y autenticación para cada función

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante tarjetas criptográficas y códigos de activación.

5.2.4 Roles que requieren separación de tareas

Las siguientes tareas son realizadas, al menos, por dos personas:

- Emisión y revocación de certificados, y el acceso al depósito.
- Generación, emisión y destrucción de certificados de la Entidad de Certificación.
- Puesta en producción de la Entidad de Certificación.

5.2.5 Sistema de gestión PKI

El sistema de PKI se compone de los siguientes módulos:

- Componente/módulo de gestión de la Autoridad de Certificación Subordinada.
- Componente/módulo de gestión de la Autoridad de Registro.
- Componente/módulo de gestión de solicitudes.
- Componente/módulo de gestión de claves (HSM).
- Componente/módulo de bases de datos.
- Componente/módulo de gestión de CRL.
- Componente/módulo de gestión del servicio de OCSP.
- Componente/módulo de gestión de la Autoridad de Sellado de Tiempo (TSA)
- Componente/módulo de gestión de las unidades de Sellado de Tiempo (TSU)

5.3 Controles de personal

5.3.1 Requisitos de historial, calificaciones, experiencia y autorización

Todo el personal que realiza tareas calificadas como confiables, lleva al menos un año trabajando en el centro de producción y tiene contratos laborales fijos.

Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

El personal en puestos de confianza no tiene intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

esFIRMA se asegura de que el personal de registro es confiable para realizar las tareas de registro.

El Operador de Registro ha realizado un curso de preparación para la realización de las tareas de validación de las peticiones.

En general, esFIRMA retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.
esFIRMA no asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por haber sido condenada por delito o falta que afecte su idoneidad para el puesto.

5.3.2 Procedimientos de investigación de historial

esFIRMA realiza comprobaciones sobre los antecedentes de los posibles empleados antes de su contratación o de su acceso al puesto de trabajo.

esFIRMA obtiene el consentimiento inequívoco del afectado para dicha investigación previa, y procesa y protege todos sus datos personales de acuerdo con el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos

personales y a la libre circulación de estos datos, y con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

La investigación se repetirá con una periodicidad suficiente.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

En la solicitud para el puesto de trabajo se informa acerca de la necesidad de someterse a una investigación previa, advirtiéndose de que la negativa a someterse a la investigación implicará el rechazo de la solicitud.

5.3.3 Requisitos de formación

esFIRMA forma al personal en puestos fiables y de gestión en los términos establecidos en las Políticas de Certificación. Para ello, se definen las acciones correspondientes en el Plan de Formación de ESFIRMA.

La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad de esFIRMA. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

5.3.4 Requisitos y frecuencia de actualización formativa

esFIRMA actualiza la formación del personal de acuerdo con las necesidades, y con la frecuencia suficientes para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación

5.3.5 Secuencia y frecuencia de rotación laboral

No aplicable.

5.3.6 Sanciones para acciones no autorizadas

esFIRMA dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable y, en especial, coordinado con el sistema sancionador del convenio colectivo que resulte de aplicación al personal.

Las acciones disciplinarias incluyen la suspensión y el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

5.3.7 Requisitos de contratación de profesionales

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por esFIRMA. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la DPC, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante, lo cual, la entidad de certificación será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto a esFIRMA.

5.3.8 Suministro de documentación al personal

El prestador de servicios de certificación suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

5.4 Procedimientos de auditoría de seguridad

5.4.1 Tipos de eventos registrados

esFIRMA produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de éste.
- Las actividades de los cortafuegos y enrutadores
- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.

- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de certificados individuales, o de la persona física identificada en el certificado, en caso de certificados de organización.
- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

Quedan registrados todos los sucesos relacionados con la preparación de los dispositivos cualificados de creación de firmas que son usados por los firmantes o custodios.

5.4.2 Frecuencia de tratamiento de registros de auditoría

esFIRMA revisa sus logs cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

esFIRMA mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.

- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

5.4.3 Período de conservación de registros de auditoría

esFIRMA almacena la información de los logs durante un periodo de entre 1 y 15 años, en función del tipo de información registrada.

esFIRMA pone estos registros de auditoría a disposición de su Auditor Cualificado, previa solicitud.

5.4.4 Protección de los registros de auditoría

Los logs de los sistemas:

- Están protegidos de manipulación, borrado o eliminación mediante la firma de los ficheros que los contienen.
- Son almacenados en dispositivos ignífugos.
- Se protege su disponibilidad mediante su almacenamiento en instalaciones externas al centro donde se ubica la AC.

El acceso a los ficheros de logs está reservado sólo a las personas autorizadas. Asimismo, los dispositivos son manejados en todo momento por personal autorizado.
Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

5.4.5 Procedimientos de copia de respaldo

esFIRMA dispone de un procedimiento adecuado de backup de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

esFIRMA tiene implementado un procedimiento de backup seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. Adicionalmente se mantiene copia en centro de custodia externo.

5.4.6 Localización del sistema de acumulación de registros de auditoría

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo, las comunicaciones de red y por el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

5.4.7 Notificación del evento de auditoría al causante del evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

5.4.8 Análisis de vulnerabilidades

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de esFIRMA.

Los análisis de vulnerabilidad deben ser ejecutados, repasadas y revisadas por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados diariamente, mensualmente y anualmente.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

El programa de seguridad de esFIRMA incluye una evaluación anual de riesgos.

5.5. Archivos de informaciones

esFIRMA, garantiza que toda la información relativa a los certificados se conserva durante un período de tiempo apropiado, según lo establecido en la sección 5.5.2 de esta política.

5.5.1 Tipos de registros archivados

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por esFIRMA (o por las entidades de registro):

- Todos los datos de auditoría de sistema (PKI, TSA y OCSP).
- Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y los datos relativos a su identificación y su ubicación
- Solicitudes de emisión y revocación de certificados, incluidos todos los informes relativos al proceso de revocación.
- Todas aquellas elecciones específicas que el firmante o el suscriptor disponga durante el acuerdo de suscripción.
- Tipo de documento presentado en la solicitud del certificado.
- Identidad de la Entidad de Registro que acepta la solicitud de certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación
- Todos los datos de auditoría identificados en la sección 5.4
- Información de solicitudes de certificación.
- Documentación aportada para justificar las solicitudes de certificación.
- Información del ciclo de vida del certificado.

esFIRMA es responsable del correcto archivo de todo este material.

5.5.2 Período de conservación de registros

esFIRMA archiva los registros especificados anteriormente durante al menos 15 años.

5.5.3 Protección del archivo

esFIRMA protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo es protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.

esFIRMA asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas.

5.5.4 Procedimientos de copia de respaldo

esFIRMA dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido sólo a personal autorizado.

esFIRMA como mínimo realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos y realizar copias de respaldo completas semanalmente para casos de recuperación de datos.

Además, esFIRMA (o las organizaciones que realizan la función de registro) guarda copia de los documentos en papel en un lugar seguro diferente de las instalaciones de la propia Entidad de certificación.

5.5.5 Requisitos de sellado de fecha y hora

Los registros están fechados con una fuente fiable vía NTP.

esFIRMA dispone de un procedimiento donde describe la configuración de tiempos de los equipos utilizados en la emisión de certificados.
La hora empleada para registrar los sucesos del registro de auditoría deberá ser sincronizada con la UTC, como mínimo, una vez al día.

No es necesario que esta información se encuentre firmada digitalmente.

5.5.6 Localización del sistema de archivo

esFIRMA dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

5.5.7 Procedimientos de obtención y verificación de información de archivo

esFIRMA dispone de un procedimiento donde se describe el proceso para verificar que la información archivada es correcta y accesible.

5.6 Renovación de claves

Con anterioridad a que el uso de la clave privada de la AC/SUBCA/TSA caduque, será realizado un cambio de claves. La antigua AC/SUBCA y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por dicha AC/SUBCA. Se generará una nueva AC /SUBCA/TSA con una clave privada nueva y un nuevo DN. La clave privada de la TSA será destruida.

El cambio de claves del suscriptor es realizado mediante la realización de un nuevo proceso de emisión.

5.7 Compromiso de claves y recuperación de desastre

5.7.1 Procedimientos de gestión de incidencias y compromisos

Son almacenadas copias de seguridad de la siguiente información en instalaciones de almacenamiento externo a esFIRMA, que se ponen a disposición en caso de compromiso o desastre: datos técnicos de solicitud de certificados, datos de auditoría y registros de base de datos de todos los certificados emitidos.

Las copias de seguridad de las claves privadas de esFIRMA son generadas y mantenidas de acuerdo con lo establecido en la sección 6.2.4

5.7.2 Corrupción de recursos, aplicaciones o datos

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se comunicará la incidencia a seguridad, y se iniciarán los procedimientos de gestión oportunos, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres de esFIRMA.

5.7.3 Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso de esFIRMA, se activarán los procedimientos de compromiso de claves, dirigidos por un equipo de respuesta que evaluará la situación, desarrollará un plan de acción, que será ejecutado bajo la aprobación de la dirección de la Entidad de Certificación.

En caso de compromiso de la clave privada de esFIRMA puede darse el caso que los estados de los certificados y de los procesos de revocación usando esta clave, podrían no ser válidos. En cualquier caso, se revocarán todos los certificados activos, generando posteriormente una última CRL en la que se incluirán todos los certificados revocados, estén expirados o no. Las instrucciones para la validación de un certificado o sello de tiempo se se publicarán en la web de esFIRMA.

esFIRMA ha desarrollado un Plan de contingencias para recuperar los sistemas críticos, si fuera necesario en un centro de datos alternativo.

El caso de compromiso de la clave raíz debe tomarse como un caso separado en el proceso de contingencia y continuidad de negocio. Esta incidencia afecta, en caso de sustitución de las claves, a los reconocimientos por diferentes aplicativos y servicios privados y públicos. Una recuperación de la efectividad de las claves en términos de negocio dependerá principalmente de la duración de estos procesos. El documento de contingencia y continuidad de negocio tratará los términos puramente operativos para que las nuevas claves estén disponibles, no así su reconocimiento por terceros.

Cualquier fallo en la consecución de las metas marcadas por este Plan de contingencias, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la AC para implementar dichos procesos.

5.7.4 Continuidad del negocio después de un desastre

esFIRMA restablecerá los servicios críticos (suspensión y revocación, y publicación de información de estado de certificados) de acuerdo con el Plan de continuidad de negocio existente.

esFIRMA dispone de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación descritos en el plan de continuidad de negocio.

Tanto el servicio de gestión de las revocaciones como el servicio de consulta son considerados servicios críticos y así constan en el Plan de continuidad de negocio de esFIRMA.

5.8 Terminación del servicio

esFIRMA asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios del prestador de servicios de certificación y, en particular, aseguran un mantenimiento continuo de los registros requeridos para proporcionar evidencia de certificación en caso de investigación civil o criminal.

Antes de terminar sus servicios, esFIRMA desarrolla un Plan de terminación, con las siguientes provisiones:

- Proveerá de los fondos necesarios para continuar la finalización de las actividades de revocación.
- Notificará al órgano supervisor, al menos, tres meses antes de la fecha de finalización prevista, el cese de su actividad y el destino de los certificados especificando si se transfiere la gestión y a quién, o si se extinguirá su vigencia.
- Comunicará, también al Ministerio de Asuntos Económicos y Transformación Digital, la apertura de cualquier proceso concursal que se siga contra esFIRMA así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.
- Informará a todos Firmantes/Suscriptores, Terceros que confían y otras AC's con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de tres meses.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.
- Destruirá o deshabilitará para su uso las claves privadas de la AC.
- Se revocarán los certificados de las Unidades de Sellado de Tiempo (TSU).

- Se mantendrán todos los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos durante 15 años. Para ello, se emitirá una última CRL que incluirá todos los certificados revocados, estén o no expirados, estableciendo los medios necesarios que garanticen su conservación a largo plazo.

6. Controles de seguridad técnica

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

El par de claves de la entidad de certificación intermedia es creado por la entidad de certificación raíz de acuerdo con los procedimientos de ceremonia de esFIRMA, dentro del perímetro de alta seguridad destinado a esta tarea.

Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma, con la presencia de un Auditor CISA. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por esFIRMA.

Para la generación de la clave de las entidades de certificación raíz, intermedia y TSA se utilizan dispositivos con las certificaciones Common Criteria EAL 4+, FIPS 140-2 Nivel 3 y FIPS 140-3 Nivel 3.

Jerarquía RSA

ROOT	4.096 bits	25 años
INTERMEDIA	4.096 bits	13 años
- Certificados de entidad final	ECC256 bits	2 años
- Certificado de TSA/TSU	4.096 bits	5 años (2 años clave privada)

Jerarquía ECC

ROOT	ECC 521 bits	23 años

INTERMEDIA	ECC 521 bits	11 años
- Certificados de entidad final	ECC 256 bits	2 años
- Certificado de TSA	ECC 521 bits	11 años
- Certificado de TSU	EC 256 bits	7 años (1 año clave privada)

Más información en las siguientes ubicaciones de las PDS:

CERTIFICADO	PDS
De Empleado Público (FIRMA)	Español: https://www.esfirma.com/doc-pki/index-ES.html Inglés: https://www.esfirma.com/doc-pki/index-EN.html
De Empleado Público – Nivel Alto 1.3.6.1.4.1.47281.1.1.1	
De Empleado Público – Nivel Medio 1.3.6.1.4.1.47281.1.1.4	
De Empleado Público (AUTENTICACIÓN)	
De Empleado Público – Nivel Alto 1.3.6.1.4.1.47281.1.1.5	
De Empleado Público con Seudónimo (FIRMA)	
De EP con Seudónimo – Nivel Alto 1.3.6.1.4.1.47281.1.3.1	
De EP con Seudónimo – Nivel Medio 1.3.6.1.4.1.47281.1.3.4	
De Empleado Público con Seudónimo (AUTENTICACIÓN)	
De Empleado Público con Seudónimo – 1.3.6.1.4.1.47281.1.3.5	
De Sello de Órgano	
De Sello de Órgano – Nivel Medio 1.3.6.1.4.1.47281.1.2.2	
De Sello de Órgano – Nivel Medio centralizado *1.3.6.1.4.1.47281.1.2.4*	
De Persona Física vinculada a entidad (FIRMA)	

CERTIFICADO	PDS
	Español: https://www.esfirma.com/doc-pki/index-ES.html Inglés: https://www.esfirma.com/doc-pki/index-EN.html
De PF vinculada a entidad – F. Cualificada 1.3.6.1.4.1.47281.1.6.1	
De PF vinculada a entidad – F. Centralizada 1.3.6.1.4.1.47281.1.6.4	
De Persona Física vinculada a entidad (AUTENTICACIÓN)	
De PF vinculada a entidad 1.3.6.1.4.1.47281.1.6.5	
De Persona Física con seudónimo vinculada a entidad (FIRMA)	
De PF con seudónimo vinculada a entidad – Firma Cualificada 1.3.6.1.4.1.47281.1.7.1	
De PF con seudónimo vinculada a entidad – Firma Centralizada 1.3.6.1.4.1.47281.1.7.4	
De Persona Física con seudónimo, vinculada a entidad (AUTENTICACIÓN)	
De PF con seudónimo, vinculada a entidad 1.3.6.1.4.1.47281.1.7.5	
De Sello electrónico	
De Sello electrónico en software 1.3.6.1.4.1.47281.1.8.2	
De Sello electrónico centralizado 1.3.6.1.4.1.47281.1.8.4	
De Sello electrónico para TSA/TSU	Español: https://www.esfirma.com/doc-pki/index-ES.html Inglés: https://www.esfirma.com/doc-pki/index-EN.html
De Sello-e para TSA/TSU en HSM 1.3.6.1.4.1.47281.1.5.2	

En los certificados en tarjeta, el suscriptor autoriza al firmante a generar sus claves privada y pública dentro de un dispositivo cualificado de creación de firma electrónica, y solicita, en nombre del firmante, la emisión del certificado a esFIRMA.

En los certificados generados en HSM o software, el suscriptor autoriza al firmante o creador de sellos a generar sus claves privada y pública, y solicita, en nombre del firmante o creador de sellos, la emisión del certificado a esFIRMA.

esFIRMA nunca genera claves en software para ser enviadas por canales inseguros al firmante.

Las claves son generadas usando el algoritmo de clave pública de curva elíptica 1.2.840.10045.3.1.7 (NIST-P256/secp256r1) de 256 bits.

6.1.2 Envío de la clave privada al firmante

En certificados en dispositivo seguro de creación de firma la clave privada se encuentra debidamente protegida en el interior de dicho dispositivo seguro.

En certificados en software la clave privada del firmante se crea en el sistema informático que utiliza este firmante cuando realiza la solicitud del certificado, por lo que la clave privada se encuentra debidamente protegida en el interior del sistema informático del firmante.

6.1.3 Envío de la clave pública al emisor del certificado

El método de remisión de la clave pública al prestador de servicios de certificación es PKCS#10, otra prueba criptográfica equivalente o cualquier otro método aprobado por esFIRMA.

Cuando las claves se generan en un DCCF, esFIRMA se asegura que la clave pública que se remite al prestador de servicios de certificación proviene de un par de claves generadas por dicho DCCF.

6.1.4 Distribución de la clave pública del prestador de servicios de certificación

Las claves de esFIRMA son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el Depósito.

Los usuarios pueden acceder al Depósito para obtener las claves públicas, y adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

El certificado de las CA root y subordinadas estarán a disposición de los usuarios en la página Web de esFIRMA.

6.1.5 Tamaños de claves

La longitud de las claves de la Entidad de Certificación raíz es de RSA 4096 bits para la jerarquía RSA
La longitud de las claves de la Entidad de Certificación raíz es de ECC 521 bits para la jerarquía ECC.
La longitud de las claves de la Entidad de Certificación subordinada es de RSA 4096 bits para la jerarquía RSA.
La longitud de las claves de la Entidad de Certificación subordinada es de ECC 521 bits para la jerarquía ECC.

La longitud de las claves de la TSA es de RSA 4096 bits para la jerarquía RSA.
La longitud de las claves de la TSA es de ECC 521 bits para la jerarquía ECC.
Las claves de los certificados de entidad final son de clave pública de curva elíptica 1.2.840.10045.3.1.7 (NIST-P256/secp256r1) de 256 bits.

6.1.6 Generación de parámetros de clave pública y comprobación de calidad

La clave pública de la CA Root, de la CA subordinadas y de los certificados de los suscriptores está codificada de acuerdo con RFC 5280

Calidad de parámetros de clave pública (Jerarquía RSA)

- Longitud del Módulo = 4096

- Algoritmo de generación de claves: rsagen1
- Funciones criptográficas de Resumen: SHA256.

Calidad de los parámetros de clave pública (Jerarquía ECC)

- Longitud del Módulo = 521 bits
- Algoritmo de generación de claves: ECDSA_P521
- Funciones criptográficas de Resumen: SHA512

Todas las claves se generan en bienes de equipo, de acuerdo con lo indicado en la sección 6.1.1.

6.1.7 Propósitos de uso de claves

Los usos de las claves para los certificados de las CA son exclusivamente para la firma de certificados y de CRLs.

Los usos de las claves para los certificados de entidad final son exclusivamente para la firma digital y el no repudio.

6.2 Protección de la clave privada y controles de los módulos criptográficos

6.2.1 Estándares de módulos criptográficos

En relación a los módulos que gestionan claves de esFIRMA y de los suscriptores de certificados de firma electrónica, se asegura el nivel exigido por los estándares indicados en las secciones anteriores.

6.2.2 Control por más de una persona (n de m) sobre la clave privada

Se requiere un control multi-persona para la activación de la clave privada de la AC.

Los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

6.2.3 Depósito de la clave privada

esFIRMA no almacena copias de las claves privadas de los firmantes.

6.2.4 Copia de respaldo de la clave privada

esFIRMA realiza copia de backup de las claves privadas de las CA que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de las mismas. Tanto la generación de la copia como la recuperación de ésta necesitan al menos de la participación de dos personas.

Estos ficheros de recuperación se almacenan en armarios ignífugos y en el centro de custodia externo.

Las claves del firmante en hardware no se pueden copiar ya que no pueden salir del dispositivo criptográfico.

6.2.5 Archivo de la clave privada

Las claves privadas de las AC son archivadas por un periodo de **15 años** después de la emisión del último certificado. Se almacenarán de forma segura centro de custodia externo. Al menos será necesaria la colaboración de tres personas para recuperar la clave privada de las AC en el dispositivo criptográfico inicial.

6.2.6 Introducción de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos de producción de esFIRMA.

6.2.7 Almacenamiento de las claves privada en los módulos criptográficos

Las claves privadas de la Entidad de Certificación se almacenan cifradas en los módulos criptográficos de producción de esFIRMA.

6.2.8 Método de activación de la clave privada

La clave privada de esFIRMA se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.2.2.

Las claves de la AC se activan por un proceso de m de n.

La activación de las claves privadas de la AC Intermedia es gestionada con el mismo proceso de m de n que las claves de la AC.

6.2.9 Método de desactivación de la clave privada

Para la desactivación de la clave privada de esFIRMA se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

Por su parte el firmante deberá introducir el PIN para la nueva activación.

6.2.10 Método de destrucción de la clave privada

Con anterioridad a la destrucción de las claves, se revocará el certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de esFIRMA. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

Finalmente se destruirán de forma segura las copias de seguridad.

Las claves del firmante en software se podrán destruir mediante el borrado de las mismas, siguiendo las instrucciones de la aplicación que las alberga.

Las claves del firmante en hardware podrán ser destruidas mediante una aplicación informática especial en las dependencias de las RA o de esFIRMA.

6.2.11 Clasificación del módulo criptográfico

Los módulos criptográficos se someten a los controles de ingeniería previstos en las normas indicadas a lo largo de esta sección.

Los algoritmos de generación de claves empleados se aceptan comúnmente para el uso de la clave a que están destinados.

Todas las operaciones criptográficas de esFIRMA son realizadas en módulos con las certificaciones FIPS 140-2 nivel 3 y FIPS 140-3 nivel 3.

6.3 Otros aspectos de gestión del par de claves

6.3.1 Archivo de la clave pública

esFIRMA archiva sus claves públicas de forma rutinaria, de acuerdo con lo establecido en la sección 5.5 de este documento.

6.3.2 Períodos de utilización de las claves pública y privada

Los periodos de utilización de las claves son los determinados por la duración del certificado, transcurrido el cual no pueden continuar utilizándose.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de esFIRMA son generados de acuerdo con lo establecido en la sección 6.2.2 y los procedimientos de ceremonia de claves.

La creación y distribución de dichos dispositivos es registrada.

Asimismo, esFIRMA genera de forma segura los datos de activación.

6.4.2 Protección de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de las Autoridades de certificación raíz y subordinadas, son protegidos por los poseedores de las tarjetas de administradores de los módulos criptográficos, según consta en el documento de ceremonia de claves.

El firmante del certificado es el responsable de la protección de su clave privada, con una contraseña lo más completa posible. El firmante debe recordar dicha contraseña.

6.4.3 Otros aspectos de los datos de activación

No aplica.

6.5. Controles de seguridad informática

esFIRMA emplea sistemas fiables para ofrecer sus servicios de certificación. esFIRMA ha realizado controles y auditorías informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de esFIRMA, en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de backup y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red.

6.5.1 Requisitos técnicos específicos de seguridad informática

Cada servidor de esFIRMA incluye las siguientes funcionalidades:

- Control de acceso a los servicios de la SubCA y gestión de privilegios.

- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del suscriptor y la SubCA y datos de auditoría.
- Auditoría de eventos relativos a la seguridad.
- Auto-diagnóstico de seguridad relacionado con los servicios de la SubCA.
- Mecanismos de recuperación de claves y del sistema de la SubCA.

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

En el caso que esFIRMA distribuyese dispositivos cualificados de creación de firma, verificará en todo momento que dichos dispositivos continúan certificados como DCCF.

La verificación de la certificación del DCCF se realiza durante todo el período de validez del certificado. Si el DCCF perdiera su certificación como tal, esFIRMA procederá a la revocación de los certificados emitidos en dichos DCCF, informando a los titulares de los mismos.

esFIRMA exige autenticación con múltiples factores para todas las cuentas capaces de causar directamente la emisión de certificados.

6.5.2 Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas por esFIRMA son fiables.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por esFIRMA de acuerdo con estándares de desarrollo y control de cambios.

Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

6.6.2 Controles de gestión de seguridad

esFIRMA desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos, son actualizados después de su aprobación por un grupo para la gestión de la seguridad. En la realización de esta función dispone de un plan de formación anual.

esFIRMA exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

Clasificación y gestión de información y bienes

esFIRMA mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

El sistema de gestión de seguridad de la información de esFIRMA detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en cuatro niveles: PÚBLICO, RESTRINGIDO, USO INTERNO y CONFIDENCIAL.

Operaciones de gestión

esFIRMA dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.

esFIRMA tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

Tratamiento de los soportes y seguridad

Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

Planificación del sistema

El departamento de Sistemas de esFIRMA mantiene un registro de las capacidades de los equipos. Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

Reportes de incidencias y respuesta

esFIRMA dispone de un procedimiento para el seguimiento de incidencias y su resolución.

Procedimientos operacionales y responsabilidades

esFIRMA define actividades, asignadas a personas con un rol de confianza, distintas de las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

Gestión del sistema de acceso

esFIRMA realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.

En particular:

AC General

- Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
- esFIRMA dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- esFIRMA dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones de certificación.

- El personal de esFIRMA es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

Generación del certificado
La autenticación para el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de esFIRMA.

Gestión de la revocación
La revocación se realizará mediante autenticación fuerte a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador de esFIRMA.

Estado de la revocación
La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación con certificados o con doble factor de identificación para evitar el intento de modificación de la información del estado de la revocación.

6.6.3 Evaluación de la seguridad del ciclo de vida

esFIRMA se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.

esFIRMA registra toda la información pertinente del dispositivo para añadir al catálogo de activos.

El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

esFIRMA realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

La clave privada de firma de esFIRMA almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema de esFIRMA, así como sus modificaciones y actualizaciones son documentadas y controladas.

esFIRMA posee un contrato de mantenimiento del dispositivo. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.7 Controles de seguridad de red

esFIRMA protege el acceso físico a los dispositivos de gestión de red, y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se transfiere por redes no seguras, se realiza de forma cifrada mediante uso de protocolos SSL o del sistema VPN con autenticación por doble factor.

6.8 Fuentes de Tiempo

esFIRMA tiene un procedimiento de sincronización de tiempo coordinado vía NTP. El valor de tiempo en la TSU es trazable hasta un valor de tiempo distribuido por una laboratorio UTC(k), el ROA (Real Observatorio de la Armada) y mantiene la precisión de reloj con por lo menos cuatro fuentes de tiempo STRATUM-1.

6.9 Algoritmos de firma y parámetros del sistema de firma centralizada

El servicio de firma centralizada genera claves para los firmantes con el algoritmo de curva elíptica 1.2.840.10045.3.1.7 (NIST-P256/secp256r1)[1] de 256 bits con primos probables usando el algoritmo FIPS 186-4 B.3.6 y DRBG (Deterministic Random Bit Generator) en Real Random Mode (hardware noise) según NIST SP 800-90A y test continuo acorde a FIPS 140-2. Fuera del módulo HSM las claves se almacenan cifradas con el algoritmo AES-GCM y una longitud de clave de 256 bits. La clave de cifrado se deriva del PIN de usuario y la clave maestra del HSM.

La clave maestra del HSM utiliza el algoritmo ECDSA NIST-P256/secp256r1 (OID 1.2.840.10045.3.1.7) y requiere 3 de 5 tarjetas para su activación y que fue generada en una ceremonia de inicialización de alta seguridad. El PIN de usuario se deriva de un salt del servidor con el algoritmo PBKDF2-SHA1. El transporte del SAD (Signature Activation Data) del SIC (Signature Interaction Component) al SAM (Signature Activation Module) se protege mediante AES-GCM con clave de 256 bits derivada de un intercambio de claves mediante el algoritmo ECDH según NIST SP 800-56A. La clave del SAM se encuentra publicada en el repositorio web de esFirma, sección “Información de seguridad de la firma remota”. El sistema permite generar firmas electrónicas con el algoritmo ECDSA con clave de curva elíptica y algoritmo de resumen SHA-256 y SHA-512.

[1] Debido a requerimientos de interoperabilidad, se podrán generar claves con algoritmo de firma RSA2048 hasta el 31 de diciembre de 2026.

7. Perfiles de certificados, CRL y OCSP

7.1 Perfil de certificado

Todos los certificados cualificados emitidos bajo esta política cumplen el estándar X.509 versión 3, RFC 5280, RFC 3739 y las normas ETSI siguientes:

- ETSI EN 319 412-2 para certificados emitidos a personas físicas
- ETSI EN 319 412-3 para certificados emitidos a personas jurídicas
- ETSI EN 319 412-5 para la definición de los QCStatements de los certificados cualificados de acuerdo al RD (EU) 910/2014.

esFIRMA genera números de serie de certificados no secuenciales mayores que cero (0) que contienen al menos 128 bits de salida de un CSPRNG.

7.1.1 Número de versión

esFIRMA emite certificados X.509 Versión 3

7.1.2 Extensiones del certificado

Las extensiones de los certificados se encuentran detalladas en los documentos de perfiles que son accesibles desde la página web de esFIRMA https://www.esfirma.com

7.1.3 Identificadores de objeto (OID) de los algoritmos

RSA Public Key (1.2.840.113549.1.1.1)
SHA-256 With RSA Encryption (1.2.840.113549.1.1.11)
SHA-512 With RSA Encryption (1.2.840.113549.1.1.13)
EC PublicKey (1.2.840.10045.2.1):
- params: 1.3.132.0.35 (NIST-P521)
- params: 1.3.132.0.34 (NIST-P384)
- params: 1.2.840.10045.3.1.7 (NIST-P256)

ECDSA With SHA-512 (1.2.840.10045.4.3.4)

ECDSA With SHA-384 (1.2.840.10045.4.3.3)
ECDSA With SHA-256 (1.2.840.10045.4.3.2)

7.1.4 Formato de Nombres

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política.

La codificación del certificado sigue la recomendación RFC 5280 "Certificado de infraestructura de clave pública de Internet X.509 y Lista de revocación de certificados (CRL)
Ver perfiles en https://www.esfirma.com

7.1.5 Restricción de los nombres

Los nombres contenidos en los certificados están restringidos a “Distinguished Names” X.500, que son únicos y no ambiguos.

7.1.6 Identificador de objeto (OID) de los tipos de certificados

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos, de acuerdo con la estructura indicada en el punto 1.2.1

7.1.7 Uso de la extensión de restricciones de política

No aplica

7.1.8 Calificadores de política sintaxis y semántica

No aplica

7.1.9 Semántica de procesamiento para la extensión crítica de Políticas de certificado

La extensión “Certificate Policy” identifica la política que define las prácticas que esFIRMA asocia explícitamente con el certificado. La extensión puede contener un calificador de la política. Ver 7.1.6

7.1.10 Restricciones de longitud de los elementos

Para todos los perfiles se establecen las siguientes restricciones de longitud máxima en caracteres de los siguientes elementos:

Elemento	**Longitud Máxima esFIRMA**	**Longitud Base**	**Norma**
2.5.4.42 *(givenName,GN)*	**127**	32000***	RFC5280
2.5.4.10 (organizationName)	**256**	64	RFC5280
2.5.4.11 (organizationalUnitName)	**256**	32	RFC5280
2.5.4.4 (surnames)	**256**	40	RFC5280
2.5.4.3 (commonName,CN)	**400**	64	RFC5280
2.5.4.5 (serialNumber,SN)	32*	32	RFC5280
2.5.4.97 (organizationIdentifier)	**32**	MAX**	X520
2.5.4.65 (pseudonym)	**64***	128	RFC5280
2.5.4.12 (title)	64*	64	RFC5280
*Las normas ETSI EN 319 412-2 y ETSI EN 319 412-3 permiten exceder los límites fijados en la RFC 5280 (siempre que se indique en la DPC) para los campos del subject indicados acorde al tipo de certificado (givenName, surname, pseudonym, commonName, organizationName y organizationalUnitName), pero no el resto de campos. La longitud de estos campos es acorde a RFC 5280. ** MAX indica que el límite superior no está especificado (RFC5280 Appendix B. ASN1 Notes) *** 32000 ub-name usado en lugar de ub-givenname (16)			

Las longitudes máximas para el resto de elementos están especificadas en RFC-5280

7.2 Perfil de la lista de revocación de certificados

Según el estándar IETF RFC 3280

7.2.1 Número de versión

Las CRL emitidas por esFIRMA son de la versión 2.

7.2.2 CRL y extensiones CRL

crlExtensions:

2.5.29.35 (Authority key identifier)

2.5.29.20 (CRL Number)

crlEntryExtensions

2.5.29.21 (ReasonCode)

7.3 Perfil OCSP

Según el estándar IETF RFC 6960

7.3.1 Número de versión

Los OCSP emitidos por esFIRMA son de la versión 3.

7.3.2 Extensiones OCSP

responseExtensions

Id: 1.3.6.1.5.5.7.48.1.2 (OCSP Nonce Extension)

Critical: true

8. Auditoría de conformidad

esFIRMA ha comunicado el inicio de su actividad como prestador de servicios de certificación por el Ministerio de Asuntos Económicos y Transformación Digital se encuentra sometida a las revisiones de control que este organismo considere necesarias.

8.1 Frecuencia de la auditoría de conformidad

esFIRMA lleva a cabo una auditoría de conformidad anualmente, además de las auditorías internas que realiza bajo su propio criterio o en cualquier momento, debido a una sospecha de incumplimiento de alguna medida de seguridad.

esFIRMA supervisa el cumplimiento de este documento y controla estrictamente la calidad de su servicio realizando auto auditorías al menos trimestralmente contra una muestra seleccionada al azar del mayor de un certificado o al menos el tres por ciento de los Certificados emitidos por él durante el período que comienza inmediatamente después de la auto auditoría anterior.

8.2 Identificación y calificación del auditor

Las auditorías son realizadas por una firma de auditoría independiente externa que demuestra competencia técnica y experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública, y los elementos relacionados.

8.3 Relación del auditor con la entidad auditada

Las empresas de auditoría son de reconocido prestigio con departamentos especializados en la realización de auditorías informáticas, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con esFIRMA.

8.4 Listado de elementos objeto de auditoría

La auditoría verifica respecto a esFIRMA:

a) Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.
b) Que la entidad cumple con los requerimientos de la DPC y otra documentación vinculada con la emisión de los distintos certificados digitales.
c) Que la DPC y demás documentación jurídica vinculada, se ajusta a lo acordado por esFIRMA y con lo establecido en la normativa vigente.
d) Que la entidad gestiona de forma adecuada sus sistemas de información

En particular, los elementos objeto de auditoría serán los siguientes:

a) Procesos de la AC, ARs y elementos relacionados.
b) Sistemas de información.
c) Protección del centro de proceso de datos.
d) Documentos.

8.5 Acciones a emprender como resultado de una falta de conformidad

Una vez recibido por la dirección el informe de la auditoría de cumplimiento realizada, se analizan, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta un plan correctivo que solvente dichas deficiencias.

Si esFIRMA es incapaz de desarrollar y/o ejecutar dicho plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicarlo inmediatamente a la alta dirección de esFIRMA que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar la clave de la AC y regenerar la infraestructura.
- Terminar el servicio de la AC.
- Otras acciones complementarias que resulten necesarias.

8.6 Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se entregan a la alta dirección de esFIRMA en un plazo máximo de 15 días tras la ejecución de la auditoría.

9. Requisitos comerciales y legales

9.1 Tarifas

9.1.1 Tarifa de emisión o renovación de certificados

esFIRMA puede establecer una tarifa por la emisión de los certificados, de la que, en su caso, se informará oportunamente a los suscriptores.

9.1.2 Tarifa de acceso a certificados

esFIRMA no ha establecido ninguna tarifa por el acceso a los certificados.

9.1.3 Tarifa de acceso a información de estado de certificado

esFIRMA no ha establecido ninguna tarifa por el acceso a la información de estado de certificados.

9.1.4 Tarifas de otros servicios

Sin estipulación.

9.1.5 Política de reintegro

Sin estipulación.

9.2 Responsabilidad financiera

esFIRMA dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios, según lo establecido en la ETSI EN 319 401, en relación a la gestión de la finalización de los servicios y plan de cese.

9.2.1 Cobertura de seguro

esFIRMA dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional que cumple con lo indicado en el régimen de obligaciones y responsabilidades del Reglamento (UE) 910/2014, y con el artículo 9.3.b) de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, con un mínimo asegurado de 3.000.000 de euros.

9.2.2 Otros activos

Sin estipulación.

9.2.3 Cobertura de seguro para suscriptores y terceros que confían en certificados

esFIRMA dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional que cumple con lo indicado en el régimen de obligaciones y responsabilidades del Reglamento (UE) 910/2014, y con el artículo 9.3.b) de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza con un mínimo asegurado de 3.000.000 de euros.

9.3 Confidencialidad de la información

9.3.1 Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales por esFIRMA:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.
- Claves privadas generadas y/o almacenadas por el prestador de servicios de certificación.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por la Entidad de Certificación y sus auditores.

- Planes de continuidad de negocio y de emergencia.
- Política y planes de seguridad.
- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.
- Toda otra información identificada como "Confidencial".

9.3.2 Informaciones no confidenciales

La siguiente información se considera no confidencial:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por la Entidad de Certificación.
- El nombre y los apellidos de la persona física identificada en el certificado, así como cualquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico de la persona física identificada en el certificado, o la dirección de correo electrónico asignada por el suscriptor, en el supuesto de que sea significativa en función de la finalidad del certificado.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (CRLs), así como las restantes informaciones de estado de revocación.
- Cualquier otra información que no esté indicada en la sección anterior.

9.3.3 Divulgación de información de suspensión y revocación

Véase la sección anterior.

9.3.4 Divulgación legal de información

esFIRMA divulga la información confidencial únicamente en los casos legalmente previstos.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado, así como los registros relacionados con la fiabilidad de los datos y los relacionados con la operativa, serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

esFIRMA indicará estas circunstancias en la política de privacidad prevista en la sección 9.4.

9.3.5 Divulgación de información por petición de su titular

esFIRMA incluye, en la política de privacidad prevista en la sección 9.4, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, de la persona física identificada en el certificado, directamente a los mismos o a terceros.

9.3.6 Otras circunstancias de divulgación de información

Sin estipulación.

9.4 Privacidad de la información personal

esFIRMA se obliga a cumplir la normativa sobre protección de datos de carácter personal, con las medidas de seguridad correspondientes, según se relaciona en el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

esFIRMA obtiene los datos personales que figuran en los ficheros por captación de los datos por parte del SUSCRIPTOR, que debe haberlos obtenido legalmente de quien

corresponda, en las condiciones previstas en la normativa sobre firma electrónica y sobre protección de datos de carácter personal.

esFIRMA tiene la condición de encargado del tratamiento de datos personales y, como tal, trata los datos única y exclusivamente para los fines que figuran en esta Declaración de Prácticas de Certificación de acuerdo con las instrucciones del responsable del tratamiento, que es el SUSCRIPTOR y que se encuentran incluidas en el Anexo "*Anexo 1: Para el tratamiento de datos personales por ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. en calidad de ENCARGADO DEL TRATAMIENTO*", que rige el contrato de prestación del servicio "Gestiona" entre el SUSCRIPTOR y ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.

9.4.1 Plan de privacidad

esFIRMA ha desarrollado una política de privacidad de acuerdo con el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y ha documentado en esta Declaración de Prácticas de Certificación, así como en el Anexo "Anexo 1: *Para el tratamiento de datos personales por ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. en calidad de ENCARGADO DEL TRATAMIENTO"* que rige el contrato de prestación del servicio "Gestiona" entre el SUSCRIPTOR y ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A., los aspectos, procedimientos y medidas de seguridad y organizativas en cumplimiento del régimen de obligaciones y responsabilidades contenidas en las normas previas.

9.4.2 Información tratada como privada

La información personal sobre un individuo que no está públicamente disponible en los contenidos de un certificado o CRL se considera privada.

9.4.3 Información no considerada privada

La información personal sobre un individuo disponible en los contenidos de un certificado o CRL, se considera como no privada al ser necesaria a la prestación del servicio

contratado, sin perjuicio de los derechos correspondientes al titular de los datos personales en virtud de la legislación LOPD/RGPD.

9.4.4 Responsabilidad de proteger la información privada

La información confidencial de acuerdo con la normativa en protección de datos personales se protege de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de conformidad con las prescripciones establecidas en este documento, que se encuentran alineadas con las obligaciones previstas en el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

9.4.5 Aviso y consentimiento para usar información privada

Antes de entablar una relación contractual, se ofrecerá a los interesados la información previa acerca del tratamiento de sus datos personales y ejercicio de derechos, y en su caso, recabará el consentimiento preceptivo para el tratamiento diferenciado del tratamiento principal para la prestación de los servicios contratados.

9.4.6 Divulgación de conformidad con un proceso judicial o administrativo

esFIRMA no divulga ni cede datos personales, excepto en los casos previstos en las secciones 9.3.2 a 9.3.6, y en la sección 5.8, en caso de terminación del servicio de certificación.

9.4.7 Otras circunstancias de divulgación de información

No se ceden datos personales a terceros salvo obligación legal.

9.5 Derechos de propiedad intelectual

9.5.1 Propiedad de los certificados e información de revocación

Únicamente esFIRMA goza de derechos de propiedad intelectual sobre los certificados que emita, sin perjuicio de los derechos de los suscriptores, poseedores de claves y terceros, a los que conceda licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de uso del certificado, y de acuerdo con la documentación que los vincula.

Adicionalmente, los certificados emitidos por esFIRMA contienen un aviso legal relativo a la propiedad de los mismos.

Las mismas reglas resultan de aplicación al uso de la información de revocación de los certificados.

9.5.2 Propiedad de la Declaración de Prácticas de Certificación

Únicamente esFIRMA goza de derechos de propiedad intelectual sobre esta Declaración de Prácticas de Certificación.

9.5.3 Propiedad de la información relativa a nombres

El suscriptor y, en su caso, la persona física identificada en el certificado, conserva la totalidad de derechos, de existir los mismos, sobre la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3.1.1

9.5.4 Propiedad de claves

Los pares de claves son propiedad de los firmantes de los certificados.

Cuando una clave se encuentra fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.6 Obligaciones y responsabilidad civil

9.6.1 Obligaciones de la Entidad de Certificación "esFIRMA"

esFIRMA garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la DPC, siendo el único responsable del cumplimiento de los procedimientos descritos, incluso si una parte o la totalidad de las operaciones se subcontratan externamente.

esFIRMA presta los servicios de certificación conforme con esta Declaración de Prácticas de Certificación.

Con anterioridad a la emisión y entrega del certificado al suscriptor, esFIRMA informa al suscriptor de los términos y condiciones relativos al uso del certificado, de su precio y de sus limitaciones de uso, mediante un contrato de suscriptor que incorpora por referencia los textos de divulgación (PDS) de cada uno de los certificados adquiridos.

El documento de texto de divulgación, también denominado PDS, cumple el contenido del anexo A de la ETSI EN 319 411-1, documento el cual puede ser transmitido por medios electrónicos, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.
esFIRMA comunica de forma permanente los cambios que se produzcan en sus obligaciones publicando nuevas versiones de su documentación jurídica en su web https://www.esfirma.com

esFIRMA vincula a suscriptores, poseedores de claves y terceros que confían en certificados mediante dicho texto de divulgación o PDS, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en las secciones 4.5.3, 9.2, 9.6.7, 9.6.8, 9.6.9 y 9.6.10.
- Indicación de la política aplicable, con indicación de que los certificados no se expiden al público.

- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Entidad de Certificación sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 1.4.2
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial de la Entidad de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Entidad de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Si la Entidad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

9.6.2. Obligación y responsabilidad de la RA

Las AR son las entidades delegadas por la AC para realizar las tareas de registro y aprobación de las solicitudes de certificados, por lo tanto la AR también se obliga en los términos definidos en las Prácticas de Certificación para la emisión de certificados, principalmente:

• Respetar lo dispuesto en esta CPS y en las PDS correspondiente.

• Proteger sus claves privadas que les servirán para el ejercicio de sus funciones.

• Comprobar la identidad de los Sujetos/Firmantes y Solicitantes de los certificados cuando resulte necesario, acreditando definitivamente la identidad del Firmante, en caso de certificados individuales, o del poseedor de claves, en caso de certificados de organización, de acuerdo con lo establecido en las secciones correspondientes de este documento.

• Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
• Proporcionar al Firmante, en caso de certificados individuales, o al futuro poseedor de claves, en caso de certificados de organización, acceso al certificado.
• Entregar, en su caso, el dispositivo criptográfico correspondiente.
• Archivar, por el periodo dispuesto en la legislación vigente, los documentos suministrados por el solicitante o Firmante.
• Respetar lo dispuesto en los contratos firmados con esFIRMA y con el Sujeto/Firmante.
• Informar a esFIRMA de las causas de revocación, siempre y cuando tomen conocimiento.
• Ofrecer información básica sobre la política y uso del certificado, incluyendo especialmente información sobre esFIRMA y la Declaración de Prácticas de Certificación aplicable, así como de sus obligaciones, facultades y responsabilidades.
• Ofrecer Información sobre el certificado y el dispositivo criptográfico.
• Recopilar información y evidencias del poseedor de recibir el certificado y, en su caso, el dispositivo criptográfico, y aceptación de dichos elementos.
• Informar del método de imputación exclusiva al poseedor de la clave privada y de sus datos de activación del certificado y, en su caso, del dispositivo criptográfico, de acuerdo con lo establecido en las secciones correspondientes de este documento.
Estas obligaciones se aplican incluso en los casos de entidades delegadas por estas como son los puntos de verificación presencial (PVP).
La información sobre el uso y responsabilidades de suscriptor se suministra mediante la aceptación de las cláusulas de uso previamente a la confirmación de la solicitud del certificado y mediante correo electrónico.

Las RA suscriben un contrato de prestación de servicio con esFIRMA mediante el cual esFIRMA delega las funciones de registro en las RA, consistente fundamentalmente en:
1.- Obligaciones previas a la expedición de un certificado.
a) Informar adecuadamente a los solicitantes de la firma de sus obligaciones y responsabilidades.
b) La adecuada identificación de los solicitantes, que deben ser personas capacitadas o autorizadas para solicitar un certificado digital.
c) La correcta comprobación de la validez y vigencia de esos datos de los solicitantes y de la Entidad, en el caso de que exista una relación de vinculación o representación.
d) Acceder a la aplicación de Autoridad de Registro para gestionar las solicitudes y los certificados emitidos.

2.- Obligaciones una vez expedido el certificado.

a) Suscribir los contratos de Prestación de Servicios de Certificación Digital con los solicitantes. En la mayoría de los procesos de emisiones este contrato es formalizado mediante la aceptación de condiciones en las páginas web que forman parte del proceso de emisión del certificado, no pudiéndose realizar la emisión sin antes no haber aceptado las condiciones de uso.

b) El mantenimiento de los certificados durante su vigencia (extinción, suspensión, revocación).

c) Archivar las copias de la documentación presentada y los contratos debidamente firmados por los solicitantes en conformidad con Políticas de Certificación publicadas por esFIRMA y la legislación vigente.

Así pues, las RA se responsabilizan de las consecuencias en caso de incumplimiento de sus labores de registro, y a través del cual se comprometen a respetar además las normas reguladoras internas de la entidad certificadora esFIRMA (Políticas y CPS) las cuales deberán ser perfectamente controladas por parte de las RA y que deberán servirles de manual de referencia.

En caso de reclamación por un Sujeto, una Entidad, o un usuario, la AC deberá aportar la prueba de la actuación diligente y si se constata que el origen de la reclamación radica en un error en la validación o comprobación de los datos, la AC podrá en virtud de los acuerdos firmados con las RA, hacer soportar a la RA responsable la asunción de las consecuencias.

Porque, aunque legalmente sea la AC la persona jurídica responsable frente al Sujeto, una Entidad, o Parte Usuaria, y que para ello dispone de un seguro de responsabilidad civil, según el acuerdo vigente, la RA tiene como obligación contractual “identificar y autenticar correctamente al Solicitante y, en su caso, a la Entidad que corresponda”, y en su virtud deberá responder frente a esFIRMA de sus incumplimientos.

Por supuesto, no es intención de esFIRMA descargar todo el peso de la asunción de responsabilidad a las RA en cuanto a los posibles daños cuyo origen vendría de un incumplimiento de las tareas delegadas a las RA. Por esta razón, al igual que lo previsto para la AC, la RA se ve sometida a un régimen de control que será ejercido por esFIRMA, no solamente a través de los controles de archivos y procedimientos de conservación de los archivos asumidos por la RA mediante la realización de auditorías para evaluar entre otros, los recursos empleados y el conocimiento y control de los procedimientos operativos para ofrecer los servicios de RA.

Las mismas responsabilidades deberá asumir las RA en virtud de incumplimientos de las

entidades delegadas como por ejemplo los puntos de verificación presencial (PVP), sin perjuicio de su derecho a repercutir contra ellas.

9.6.3 Garantías ofrecidas a suscriptores y terceros que confían en certificados

esFIRMA, en la documentación que la vincula con suscriptores y terceros que confían en certificados, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

esFIRMA, como mínimo, garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Entidad de Certificación.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación del mismo.
- Que los certificados cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- Que los servicios de revocación y el empleo del Depósito cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

esFIRMA, como mínimo, garantizará al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación.

Adicionalmente, esFIRMA garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado cualificado, de acuerdo con el anexo 1 del Reglamento (UE) 910/2014.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, persona física identificada en el certificado, se mantiene su confidencialidad durante el proceso.

- La responsabilidad de la Entidad de Certificación, con los límites que se establezcan. En ningún caso ESFIRMA responderá por caso fortuito y en caso de fuerza mayor.
- La clave privada de la entidad de certificación utilizada para emitir certificados no ha sido comprometida, a menos que esFIRMA no haya comunicado lo contrario.
- No ha originado ni ha introducido declaraciones falsas o erróneas en la información de ningún certificado, ni ha dejado de incluir información necesaria aportada por el suscriptor y validada por esFIRMA, en el momento de la emisión del certificado.
- Todos los certificados cumplen los requisitos formales y de contenido de esta Declaración de prácticas, incluyendo todos los requisitos legales en vigor y aplicables.
- Queda vinculada por los procedimientos operativos y de seguridad descritos en esta Declaración de prácticas.

9.6.4 Obligación y responsabilidad de terceras partes

Será obligación de la Parte Usuaria cumplir con lo dispuesto por lo dispuesto en la normativa vigente y, además:

- Verificar la validez de los certificados y de toda la cadena de certificación, antes de realizar cualquier operación basada en los mismos. esFIRMA dispone de diversos mecanismos para realizar dicha comprobación, como el acceso a listas de certificados revocados o a servicios de consulta en línea OCSP.
- Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.
- Comprobar la validez de la cualificación de una firma asociada a un certificado emitido por esFIRMA comprobando que la autoridad de certificación que ha emitido el certificado se encuentra publicada en la lista de confianza del supervisor nacional correspondiente.

9.6.5 Obligación y responsabilidad de otras participantes

No estipulado

9.7. Exención de garantía

Según la legislación vigente, la responsabilidad de esFIRMA y sus RA no se extiende a aquellos supuestos en los que la utilización indebida del certificado tiene su origen en conductas imputables al Sujeto, y a la Parte Usuaria por:

- No haber proporcionado información adecuada, inicial o posteriormente como
- consecuencia de modificaciones de las circunstancias reflejadas en el certificado electrónico, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación
- Haber incurrido en negligencia con respecto a la conservación de los datos de creación de firma y a su confidencialidad.
- No haber solicitado revocación de los datos del certificado electrónico en caso de duda sobre el mantenimiento de la confidencialidad
- Haber utilizado la firma después de haber expirado el periodo de validez del certificado electrónico
- Superar los límites que figuren en el certificado electrónico.
- En conductas imputables a la Parte Usuaria si éste actúa de forma negligente, es decir cuando no compruebe o tenga en cuenta las restricciones que figuran en el certificado en cuanto a sus posibles usos y límite de importe de las transacciones; o cuando no tenga en cuenta el estado de vigencia del certificado
- De los daños ocasionados al Sujeto o terceros que confía por la inexactitud de los datos que consten en el certificado electrónico, si éstos le han sido acreditados mediante documento público, inscrito en un registro público si así resulta exigible.
- Un uso inadecuado o fraudulento del certificado en caso de que el Sujeto/Titular lo haya cedido o haya autorizado su uso a favor de una tercera persona en virtud de un negocio jurídico como el mandato o apoderamiento, siendo exclusiva responsabilidad del Sujeto/Titular el control de las claves asociadas a su certificado.

esFIRMA y sus RAs tampoco serán responsables en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.
- Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y en las Políticas de Certificación
- Por el uso indebido o fraudulento de los certificados o CRLs emitidos por la AC
- Por el uso de la información contenida en el Certificado o en la CRL.

- Por el perjuicio causado en el periodo de verificación de las causas de revocación.
- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Por la no recuperación de documentos cifrados con la clave pública del Sujeto.

9.8. Limitación de responsabilidad en caso de pérdidas por transacciones

El límite máximo que esFIRMA permite en las transacciones económicas realizadas es de 0 (cero) euros.

9.9. Indemnizaciones

Ver apartado 9.2

9.10. Plazo y Finalización

9.10.1 Plazo

Ver apartado 5.8

9.10.2 Terminación

Ver apartado 5.8

9.10.3 Efecto de la terminación y la supervivencia

Ver apartado 5.8

9.11. Comunicaciones a las partes interesadas y al órgano de supervisión

esFIRMA establece en el contrato con el suscriptor los medios para las notificaciones entre ambas partes.

Con carácter general, las comunicaciones comunes o colectivas se realizarán a través de www.esfirma.com o la Plataforma de Administración electrónica. En el caso de notificaciones de carácter individual, se utilizará el correo electrónico o correo postal.

En el caso de que se produzca una incidencia que pueda afectar a la seguridad, datos personales o integridad de una persona, física o jurídica, se estará a lo previsto en el procedimiento de gestión de incidencias de esFIRMA.

esFIRMA dispone de procedimientos para la comunicación al órgano supervisor de cambios relevantes en la prestación de los servicios de confianza. Dichos cambios se notificarán al órgano de supervisión, al menos, un mes antes de su implementación. Si se trata de la finalización de un servicio de confianza, esFIRMA notificará al órgano supervisor, al menos, tres meses antes de la fecha de finalización prevista.

9.12. Enmiendas

9.12.1 Procedimiento de modificación

La CA se reserva el derecho de modificar este documento por razones técnicas o para reflejar cualquier cambio en los procedimientos que se hayan producido debido a requisitos legales, reglamentarios (eIDAS, Organismos de Supervisión Nacional, etc.) o como resultado de la optimización del ciclo de trabajo. Cada nueva versión de esta CPS reemplaza a todas las versiones anteriores, que siguen siendo, sin embargo, aplicables a los certificados emitidos mientras esas versiones estaban vigentes y hasta la primera fecha de vencimiento de esos certificados. Se publicará al menos una actualización anual. Estas actualizaciones quedarán reflejadas en el cuadro de versiones al inicio del documento.
Los cambios que pueden realizarse a esta CPS no requieren notificación excepto que afecte de forma directa a los derechos de los Sujetos/Firmantes de los certificados, en cuyo caso podrán presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la publicación.

9.12.2 Mecanismo de notificación y plazos

Todos los cambios propuestos de esta política serán inmediatamente publicados en la Web de esFIRMA. En este mismo documento existe un apartado de cambios y versiones

donde se puede conocer los cambios producidos desde su creación y la fecha de dichas modificaciones.
Los cambios de este documento se comunican a aquellos organismos y empresas terceras que emiten certificados bajo esta CPS así como a los auditores correspondientes. Especialmente se notificarán los cambios en esta CPS a los organismos de Supervisión Nacional.

Los Firmantes/Suscriptores y Terceros que confían, afectados pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la recepción de la notificación.

9.12.3 Circunstancias en las que se debe cambiar el OID

No estipulado

9.13 Procedimiento de resolución de conflictos

esFIRMA atenderá cualquier queja, disputa o sugerencia por parte de sus clientes o terceros que confían en sus servicios de confianza, de conformidad con el procedimiento interno de "resolución de quejas, apelaciones y disputas". El cliente o tercero que presente la queja, reclamación o sugerencia, deberá rellenar la hoja disponible en la web de esFIRMA https://www.esfirma.com/.

9.14. Legislación aplicable

esFIRMA establece, en el contrato de suscriptor y en el texto de divulgación o PDS, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la Ley española.

9.15. Conformidad con la Ley Aplicable

Ver punto 9.14

9.16. Otras disposiciones

9.16.1 Acuerdo completo

Los Titulares y terceros que confían en los Certificados asumen en su totalidad el contenido de la presente Declaración de Prácticas y Políticas de Certificación

9.16.2 Asignación

Las partes de esta DPC no pueden ceder ninguno de sus derechos u obligaciones bajo ella misma o acuerdos aplicables sin el consentimiento por escrito de esFIRMA.

9.16.3 Separabilidad

esFIRMA establece, en el contrato de suscriptor, y en el texto de divulgación o PDS, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la Entidad de Certificación vela porque, al menos los requisitos contenidos en las secciones 9.6.1 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 9.3 (Confidencialidad), continúen vigentes tras la terminación del servicio y de las condiciones generales de emisión/uso.
- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

9.16.4 Cumplimiento (honorarios de abogados y exención de derechos)

esFIRMA puede solicitar una indemnización y honorarios de abogados de una parte por daños, pérdidas y gastos relacionados con la conducta de dicha parte. El hecho de que esFIRMA no haga cumplir una disposición de esta CPS no elimina el derecho de esFIRMA de hacer cumplir las mismas disposiciones más adelante o el derecho de hacer cumplir cualquier otra disposición de esta CPS. Para ser efectiva, cualquier renuncia debe estar por escrito y firmada por esFIRMA

9.16.5 Fuerza mayor

esFIRMA incluye en el texto de divulgación o PDS, cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

9.17 Otras provisiones

9.17.1 Cláusula de indemnidad de suscriptor

esFIRMA incluye en el contrato con el suscriptor, una cláusula por la cual el suscriptor se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.
- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión medió dolo o negligencia con respecto a la Entidad de Certificación o a cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de dominio), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

9.17.2 Cláusula de indemnidad de tercero que confía en el certificado

esFIRMA incluye en el texto de divulgación o PDS, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.

- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.

El tercero que confía en el certificado se compromete a mantener indemne a ESFIRMA de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.
- Falta de comprobación de la totalidad de medidas de aseguramiento prescritas en la DCP o resto de normas de aplicación.

ESFIRMA no será responsable de los daños y perjuicios ocasionados en los términos indicados en el artículo 11 de Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.