Declaración de Prácticas de Certificación



Información general

Control documental

Clasificación de seguridad:	Público
Entidad de destino:	UANATACA
Versión:	1.2
Fecha edición:	06/04/2017
Fichero:	UANATACA DPC v1r2.docx
Formato:	Open Office XML
Autores:	GA/AC

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: GA/AC Fecha: 15/03/2016	Nombre: FA/NA Fecha: 22/03/2016	Nombre: Fecha:

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	GA/AC	22/03/2016
1.1	5.8	Se añade comunicación al Ministerio en caso de cese de actividad.	AC	24/05/2016
	6.1.1.1	Se añade que UANATACA puede crear las claves únicamente por medio de un DCCF o en un HSM, y	AC	24/05/2016

		que UANATACA nunca genera claves en software para ser enviadas al firmante.		
	6.2.5	Se añade que UANATACA no genera ni archiva claves de certificados, emitidas en software. Se borra que el suscriptor pueda almacenar las claves entregadas en software.	AC	24/05/2016
	6.1.1	Se corrige el periodo de validez de los certificados de UANATACA CA1 2016 y UANATACA CA2 2016.	AC	24/05/2016
1.2	1.1 1.2.1 1.4.1.5 1.4.1.6 1.4.1.7 1.4.1.8 3.1.1.5 3.1.1.6 6.1.1	Se añaden perfiles de certificado de persona física representante ante las Administraciones de Persona Jurídica y Certificados de Persona Física Representante ante las Administraciones de Entidad sin Personalidad Jurídica con la información correspondiente a cada sección.	DMP	30/01/2017
	1.3.3.1 3.2 3.2.3 3.2.3.2 4.1.1 4.7.3.1	Se añade el supuesto de personas físicas como suscriptores del servicio de certificación.	DMP	30/01/2017
	3.2.5	Se añade la autenticación de Autoridades de Registro y sus operadores	DMP	30/01/2017
	6.1.1	Se realizó aclaratoria sobre el período de validez de los certificados de usuarios finales	DMP	07/01/2017

	General	Adecuación de términos, normas y referencias de acuerdo al Reglamento (UE) 910/2014 eIDAS. Se suprimieron los servicios de emisión de certificados de sellos electrónicos de órgano para AAPP nivel medio y nivel alto.	DMP	06/04/2017

Índice

INFORMACIÓN GENERAL 2

CONTROL DOCUMENTAL 2
ESTADO FORMAL 2
CONTROL DE VERSIONES 2

ÍNDICE 5

1. INTRODUCCIÓN 13

1.1. PRESENTACIÓN 13
1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN 14
1.2.1. Identificadores de certificados 14
1.3. PARTICIPANTES EN LOS SERVICIOS DE CERTIFICACIÓN 16
1.3.1. Prestador de servicios de certificación 16
1.3.1.1. UANATACA ROOT 2016 17
1.3.1.2. UANATACA CA1 2016 17
1.3.1.3. UANATACA CA2 2016 17
1.3.2. Registradores 18
1.3.3. Entidades finales 18
1.3.3.1. Suscriptores del servicio de certificación 19
1.3.3.2. Firmantes 19
1.3.3.3. Partes usuarias 20
1.4. USO DE LOS CERTIFICADOS 20
1.4.1. Usos permitidos para los certificados 20
1.4.1.1. Certificado de persona física, emitido en software 21
1.4.1.2. Certificado de persona física, emitido en DCCF 22
1.4.1.3. Certificado de representante, emitido en software 23
1.4.1.4. Certificado de representante, emitido en DCCF 25
1.4.1.5. Certificado de persona física representante ante las Administraciones de Persona Jurídica emitido en software 26
1.4.1.6. Certificado de persona física representante ante las Administraciones de Persona Jurídica emitido en DCCF 28
1.4.1.7. Certificado de persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica emitido en software 29
1.4.1.8. Certificado de persona física representante ante las Administraciones de Persona Jurídica emitido en DCCF 31
1.4.1.9. Certificado de empleado público, nivel medio 32
1.4.1.10. Certificado de empleado público, nivel alto 34
1.4.1.11. Certificado de la Unidad de Sellado de tiempo electrónico 36
1.4.2. Límites y prohibiciones de uso de los certificados 36
1.5. ADMINISTRACIÓN DE LA POLÍTICA 38
1.5.1. Organización que administra el documento 38
1.5.2. Datos de contacto de la organización 38

1.5.3. Procedimientos de gestión del documento 38

2. PUBLICACIÓN DE INFORMACIÓN Y DEPÓSITO DE CERTIFICADOS 39

2.1. DEPÓSITO(S) DE CERTIFICADOS 39
2.2. PUBLICACIÓN DE INFORMACIÓN DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN 39
2.3. FRECUENCIA DE PUBLICACIÓN 39
2.4. CONTROL DE ACCESO 40

3. IDENTIFICACIÓN Y AUTENTICACIÓN 41

3.1. REGISTRO INICIAL 41
3.1.1. Tipos de nombres 41
3.1.1.1. Certificado de persona física, emitido en software 41
3.1.1.2. Certificado de persona física, emitido en DCCF 41
3.1.1.3. Certificado de representante, emitido en software 42
3.1.1.4. Certificado de representante, emitido en DCCF 42
3.1.1.5. Certificado de persona física representante ante las Administraciones de Persona Jurídica emitido en software 43
3.1.1.6. Certificado de persona física representante ante las Administraciones de Persona Jurídica emitido en DCCF 43
3.1.1.7. Certificado de persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica emitido en software 44
3.1.1.8. Certificado de persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica emitido en DCCF 45
3.1.1.9. Sello de órgano, de nivel medio 46
3.1.1.10. Sello de órgano, de nivel alto 46
3.1.1.11. Certificado de empleado público, nivel medio 47
3.1.1.12. Certificado de empleado público, nivel alto 48
3.1.2. Significado de los nombres 49
3.1.3. Empleo de anónimos y seudónimos 49
3.1.4. Interpretación de formatos de nombres 49
3.1.5. Unicidad de los nombres 50
3.1.6. Resolución de conflictos relativos a nombres 50
3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD 51
3.2.1. Prueba de posesión de clave privada 52
3.2.2. Autenticación de la identidad de una organización, empresa o entidad mediante representante 52
3.2.3. Autenticación de la identidad de una persona física 54
3.2.3.1. En los certificados 54
3.2.3.2. Necesidad de presencia personal 54
3.2.3.3. Vinculación de la persona física 55
La justificación documental de la vinculación de una persona física identificada en un certificado con la entidad, empresa u organización de derecho público o privado viene dada por su constancia en los registros internos (contrato de trabajo como empleado, o el contrato mercantil que lo vincula, o el

acta donde se indique su cargo, o la solicitud como miembro de la organización…) de cada una de las personas púbicas y privadas a las que están vinculadas.Información de suscriptor no verificada 55
3.2.4. Autenticación de la identidad de una RA y sus operadores 55
3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITUDES DE RENOVACIÓN 56
3.3.1. Validación para la renovación rutinaria de certificados 56
3.3.2. Identificación y autenticación de la solicitud de revocación 56
3.4. IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE REVOCACIÓN 57
3.5. AUTENTICACIÓN DE UNA PETICIÓN DE SUSPENSIÓN 58

4. REQUISITOS DE OPERACIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS 59

4.1. SOLICITUD DE EMISIÓN DE CERTIFICADO 59
4.1.1. Legitimación para solicitar la emisión 59
4.1.2. Procedimiento de alta y responsabilidades 59
4.2. PROCESAMIENTO DE LA SOLICITUD DE CERTIFICACIÓN 60
4.2.1. Ejecución de las funciones de identificación y autenticación 60
4.2.2. Aprobación o rechazo de la solicitud 60
4.2.3. Plazo para resolver la solicitud 61
4.3. EMISIÓN DEL CERTIFICADO 61
4.3.1. Acciones de la CA durante el proceso de emisión 61
4.3.2. Notificación de la emisión al suscriptor 62
4.4. ENTREGA Y ACEPTACIÓN DEL CERTIFICADO 62
4.4.1. Responsabilidades de la CA 62
4.4.2. Conducta que constituye aceptación del certificado 63
4.4.3. Publicación del certificado 63
4.4.4. Notificación de la emisión a terceros 63
4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO 63
4.5.1. Uso por el firmante 63
4.5.2. Uso por el subscriptor 65
4.5.2.1. Obligaciones del suscriptor del certificado 65
4.5.2.2. Responsabilidad civil del suscriptor de certificado 65
4.5.3. Uso por el tercero que confía en certificados 66
4.5.3.1. Obligaciones del tercero que confía en certificados 66
4.5.3.2. Responsabilidad civil del tercero que confía en certificados 67
4.6. RENOVACIÓN DE CERTIFICADOS 67
4.7. RENOVACIÓN DE CLAVES Y CERTIFICADOS 67
4.7.1. Causas de renovación de claves y certificados 67
4.7.2. Legitimación para solicitar la renovación 68
4.7.3. Procedimientos de solicitud de renovación 68
4.7.3.1. Realización de la solicitud 68
4.7.3.2. Ejecución de las funciones de identificación y autenticación 68
4.7.3.3. Aprobación o rechazo de la solicitud 68
4.7.3.4. Plazo para resolver la solicitud 69
4.7.4. Notificación de la emisión del certificado renovado 69

4.7.5. Conducta que constituye aceptación del certificado 69
4.7.6. Publicación del certificado 69
4.7.7. Notificación de la emisión a terceros 69
4.8. MODIFICACIÓN DE CERTIFICADOS 70
4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS 70
4.9.1. Causas de revocación de certificados 70
4.9.2. Legitimación para solicitar la revocación 71
4.9.3. Procedimientos de solicitud de revocación 72
4.9.4. Plazo temporal de solicitud de revocación 72
4.9.5. Plazo temporal de procesamiento de la solicitud 73
4.9.6. Obligación de consulta de información de revocación de certificados 73
4.9.7. Frecuencia de emisión de listas de revocación de certificados (LRCs) 73
4.9.8. Plazo máximo de publicación de LRCs 74
4.9.9. Disponibilidad de servicios de comprobación en línea de estado de certificados 74
4.9.10. Obligación de consulta de servicios de comprobación de estado de certificados 75
4.9.11. Otras formas de información de revocación de certificados 75
4.9.12. Requisitos especiales en caso de compromiso de la clave privada 75
4.9.13. Causas de suspensión de certificados 75
4.9.14. Solicitud de suspensión 76
4.9.15. Procedimientos para la petición de suspensión 76
4.9.16. Período máximo de suspensión 77
4.10. FINALIZACIÓN DE LA SUSCRIPCIÓN 77
4.11. SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS 77
4.11.1. Características operativas de los servicios 77
4.11.2. Disponibilidad de los servicios 77
4.12. DEPÓSITO Y RECUPERACIÓN DE CLAVES 77
4.12.1. Política y prácticas de depósito y recuperación de claves 77
4.12.2. Política y prácticas de encapsulado y recuperación de claves de sesión 78

5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES 79

5.1. CONTROLES DE SEGURIDAD FÍSICA 79
5.1.1. Localización y construcción de las instalaciones 80
5.1.2. Acceso físico 80
5.1.3. Electricidad y aire acondicionado 81
5.1.4. Exposición al agua 81
5.1.5. Prevención y protección de incendios 81
5.1.6. Almacenamiento de soportes 81
5.1.7. Tratamiento de residuos 82
5.1.8. Copia de respaldo fuera de las instalaciones 82
5.2. CONTROLES DE PROCEDIMIENTOS 82
5.2.1. Funciones fiables 82
5.2.2. Número de personas por tarea 83

5.2.3. Identificación y autenticación para cada función 83
5.2.4. Roles que requieren separación de tareas 84
5.2.5. Sistema de gestión PKI 84
5.3. CONTROLES DE PERSONAL 84
5.3.1. Requisitos de historial, calificaciones, experiencia y autorización 84
5.3.2. Procedimientos de investigación de historial 85
5.3.3. Requisitos de formación 86
5.3.4. Requisitos y frecuencia de actualización formativa 87
5.3.5. Secuencia y frecuencia de rotación laboral 87
5.3.6. Sanciones para acciones no autorizadas 87
5.3.7. Requisitos de contratación de profesionales 87
5.3.8. Suministro de documentación al personal 88
5.4. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD 88
5.4.1. Tipos de eventos registrados 88
5.4.2. Frecuencia de tratamiento de registros de auditoría 89
5.4.3. Período de conservación de registros de auditoría 90
5.4.4. Protección de los registros de auditoría 90
5.4.5. Procedimientos de copia de respaldo 90
5.4.6. Localización del sistema de acumulación de registros de auditoría 91
5.4.7. Notificación del evento de auditoría al causante del evento 91
5.4.8. Análisis de vulnerabilidades 91
5.5. ARCHIVOS DE INFORMACIONES 91
5.5.1. Tipos de registros archivados 92
5.5.2. Período de conservación de registros 92
5.5.3. Protección del archivo 92
5.5.4. Procedimientos de copia de respaldo 93
5.5.5. Requisitos de sellado de fecha y hora 93
5.5.6. Localización del sistema de archivo 93
5.5.7. Procedimientos de obtención y verificación de información de archivo 93
5.6. RENOVACIÓN DE CLAVES 94
5.7. COMPROMISO DE CLAVES Y RECUPERACIÓN DE DESASTRE 94
5.7.1. Procedimientos de gestión de incidencias y compromisos 94
5.7.2. Corrupción de recursos, aplicaciones o datos 94
5.7.3. Compromiso de la clave privada de la entidad 94
5.7.4. Continuidad del negocio después de un desastre 95
5.8. TERMINACIÓN DEL SERVICIO 95

6. CONTROLES DE SEGURIDAD TÉCNICA 97

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES 97
6.1.1. Generación del par de claves 97
6.1.1.1. Generación del par de claves del firmante 99
6.1.2. Envío de la clave privada al firmante 99

6.1.3. Envío de la clave pública al emisor del certificado 100
6.1.4. Distribución de la clave pública del prestador de servicios de certificación 100
6.1.5. Tamaños de claves 100
6.1.6. Generación de parámetros de clave pública 100
6.1.7. Comprobación de calidad de parámetros de clave pública 101
6.1.8. Generación de claves en aplicaciones informáticas o en bienes de equipo 101
6.1.9. Propósitos de uso de claves 101
6.2. PROTECCIÓN DE LA CLAVE PRIVADA 101
6.2.1. Estándares de módulos criptográficos 101
6.2.2. Control por más de una persona (n de m) sobre la clave privada 101
6.2.3. Depósito de la clave privada 102
6.2.4. Copia de respaldo de la clave privada 102
6.2.5. Archivo de la clave privada 102
6.2.6. Introducción de la clave privada en el módulo criptográfico 103
6.2.7. Método de activación de la clave privada 103
6.2.8. Método de desactivación de la clave privada 103
6.2.9. Método de destrucción de la clave privada 103
6.2.10. Clasificación de módulos criptográficos 103
6.2.11. Clasificación de módulos criptográficos 104
6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES 104
6.3.1. Archivo de la clave pública 104
6.3.2. Períodos de utilización de las claves pública y privada 104
6.4. DATOS DE ACTIVACIÓN 104
6.4.1. Generación e instalación de datos de activación 105
6.4.2. Protección de datos de activación 105
6.5. CONTROLES DE SEGURIDAD INFORMÁTICA 105
6.5.1. Requisitos técnicos específicos de seguridad informática 106
6.5.2. Evaluación del nivel de seguridad informática 106
6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA 106
6.6.1. Controles de desarrollo de sistemas 106
6.6.2. Controles de gestión de seguridad 107
6.6.2.1. Clasificación y gestión de información y bienes 107
6.6.2.2. Operaciones de gestión 107
6.6.2.3. Tratamiento de los soportes y seguridad 108
Planificación del sistema 108
Reportes de incidencias y respuesta 108
Procedimientos operacionales y responsabilidades 108
6.6.2.4. Gestión del sistema de acceso 108
AC General 108
Generación del certificado 109
Gestión de la revocación 109
Estado de la revocación 109
6.6.2.5. Gestión del ciclo de vida del hardware criptográfico 109

6.7. CONTROLES DE SEGURIDAD DE RED 110
6.8. CONTROLES DE INGENIERÍA DE MÓDULOS CRIPTOGRÁFICOS 111
6.9. FUENTES DE TIEMPO 111

7. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS 112

7.1. PERFIL DE CERTIFICADO 112
7.1.1. Número de versión 112
7.1.2. Extensiones del certificado 112
7.1.3. Identificadores de objeto (OID) de los algoritmos 112
7.1.4. Formato de Nombres 113
7.1.5. Restricción de los nombres 113
7.1.6. Identificador de objeto (OID) de los tipos de certificados 113
7.2. PERFIL DE LA LISTA DE REVOCACIÓN DE CERTIFICADOS 113
7.2.1. Número de versión 113
7.2.2. Perfil de OCSP 113

8. AUDITORÍA DE CONFORMIDAD 114

8.1. FRECUENCIA DE LA AUDITORÍA DE CONFORMIDAD 114
8.2. IDENTIFICACIÓN Y CALIFICACIÓN DEL AUDITOR 114
8.3. RELACIÓN DEL AUDITOR CON LA ENTIDAD AUDITADA 114
8.4. LISTADO DE ELEMENTOS OBJETO DE AUDITORÍA 114
8.5. ACCIONES A EMPRENDER COMO RESULTADO DE UNA FALTA DE CONFORMIDAD 115
8.6. TRATAMIENTO DE LOS INFORMES DE AUDITORÍA 115

9. REQUISITOS COMERCIALES Y LEGALES 117

9.1. TARIFAS 117
9.1.1. Tarifa de emisión o renovación de certificados 117
9.1.2. Tarifa de acceso a certificados 117
9.1.3. Tarifa de acceso a información de estado de certificado 117
9.1.4. Tarifas de otros servicios 117
9.1.5. Política de reintegro 117
9.2. CAPACIDAD FINANCIERA 117
9.2.1. Cobertura de seguro 118
9.2.2. Otros activos 118
9.2.3. Cobertura de seguro para suscriptores y terceros que confían en certificados 118
9.3. CONFIDENCIALIDAD 118
9.3.1. Informaciones confidenciales 118
9.3.2. Informaciones no confidenciales 119
9.3.3. Divulgación de información de suspensión y revocación 119
9.3.4. Divulgación legal de información 120
9.3.5. Divulgación de información por petición de su titular 120
9.3.6. Otras circunstancias de divulgación de información 120
9.4. PROTECCIÓN DE DATOS PERSONALES 120

9.5. DERECHOS DE PROPIEDAD INTELECTUAL 121
9.5.1. Propiedad de los certificados e información de revocación 121
9.5.2. Propiedad de la Declaración de Prácticas de Certificación 122
9.5.3. Propiedad de la información relativa a nombres 122
9.5.4. Propiedad de claves 122
9.6. OBLIGACIONES Y RESPONSABILIDAD CIVIL 122
9.6.1. Obligaciones de UANATACA 123
9.6.2. Garantías ofrecidas a suscriptores y terceros que confían en certificados 124
9.6.3. Rechazo de otras garantías 125
9.6.4. Limitación de responsabilidades 126
9.6.5. Cláusulas de indemnidad 126
9.6.5.1. Cláusula de indemnidad de suscriptor 126
9.6.5.2. Cláusula de indemnidad de tercero que confía en el certificado 126
9.6.6. Caso fortuito y fuerza mayor 127
9.6.7. Ley aplicable 127
9.6.8. Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación 127
9.6.9. Cláusula de jurisdicción competente 128
9.6.10. Resolución de conflictos 128

1. Introducción

1.1. Presentación

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

Los certificados que se emiten son los siguientes:

- **De Persona Física**
  - De Persona Física en SOFT
  - De Persona Física en DCCF Identificación
  - De Persona Física en DCCF firma
  - De Persona Física en DCCF cifrado

- **De Representante**
  - De Representante en SOFT
  - De Representante en DCCF identificación
  - De Representante en DCCF firma
  - De Representante en DCCF cifrado

- **De Representante de Persona Jurídica ante las Administraciones Públicas**
  - De persona física representante ante las Administraciones de Persona Jurídica emitido en SOFT
  - De persona física representante ante las Administraciones de Persona Jurídica emitido en DCCF identificación
  - De persona física representante ante las Administraciones de Persona Jurídica emitido en DCCF firma
  - De persona física representante ante las Administraciones de Persona Jurídica emitido en DCCF cifrado

- **De Representante de Entidad sin Personalidad Jurídica ante las Administraciones Públicas**
  - De persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica emitido en SOFT

- De persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica emitido en DCCF identificación
- De persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica emitido en DCCF firma

De persona física representante ante las Administraciones Entidad sin Personalidad Jurídica emitido en DCCF cifrado

- **De Empleado Público**
  - De Empleado Público nivel Medio
  - De Empleado Público nivel Alto (identificación)
  - De Empleado Público nivel Alto (firma)
  - De Empleado Público nivel Alto (cifrado)

1.2. Nombre del documento e identificación

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

1.2.1. Identificadores de certificados

UANATACA ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por las aplicaciones.

Número OID	Tipo de certificados
	PERSONA FÍSICA
1.3.6.1.4.1.47286.1.1.1	*De Persona Física en SOFT*
1.3.6.1.4.1.47286.1.1.2.1	*De Persona Física en DCCF Identificación*
1.3.6.1.4.1.47286.1.1.2.2	*De Persona Física en DCCF firma*
1.3.6.1.4.1.47286.1.1.2.3	*De Persona Física en DCCF cifrado*
	REPRESENTANTE
1.3.6.1.4.1.47286.1.2.1	*De Representante en SOFT*
1.3.6.1.4.1.47286.1.2.2.1	*De Representante en DCCF identificación*
1.3.6.1.4.1.47286.1.2.2.2	*De Representante en DCCF firma*

1.3.6.1.4.1.47286.1.2.2.3	*De Representante en DCCF cifrado*
	REPRESENTANTE ANTE ADMINISTRACIONES DE PERSONA JURÍDICA
1.3.6.1.4.1.47286.1.7.1	*De persona física representante ante las Administraciones de Persona Jurídica emitido en SOFT*
1.3.6.1.4.1.47286.1.7.2.1	*De persona física representante ante las Administraciones de Persona Jurídica emitido en DCCF identificación*
1.3.6.1.4.1.47286.1.7.2.2	*De persona física representante ante las Administraciones de Persona Jurídica emitido en DCCF firma*
1.3.6.1.4.1.47286.1.7.2.3	*De persona física representante ante las Administraciones de Persona Jurídica emitido en DCCF cifrado*
	REPRESENTANTE ANTE ADMINISTRACIONES DE ENTIDAD SIN PERSONALIDAD JURÍDICA
1.3.6.1.4.1.47286.1.8.1	*De persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica emitido en SOFT*
1.3.6.1.4.1.47286.1.8.2.1	*De persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica emitido en DCCF identificación*
1.3.6.1.4.1.47286.1.8.2.2	*De persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica emitido en DCCF firma*
1.3.6.1.4.1.47286.1.8.2.3	*De persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica Persona Jurídica emitido en DCCF cifrado*
	EMPLEADO PÚBLICO
1.3.6.1.4.1.47286.1.4.1	*De Empleado Público nivel Medio*
1.3.6.1.4.1.47286.1.4.2.1	*De Empleado Público nivel Alto (identificación)*

1.3.6.1.4.1.47286.1.4.2.2	*De Empleado Público nivel Alto (firma)*
1.3.6.1.4.1.47286.1.4.2.3	*De Empleado Público nivel Alto (cifrado)*
1.3.6.1.4.1.47286.1.5	**Unidad de Sellado de tiempo electrónico**

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

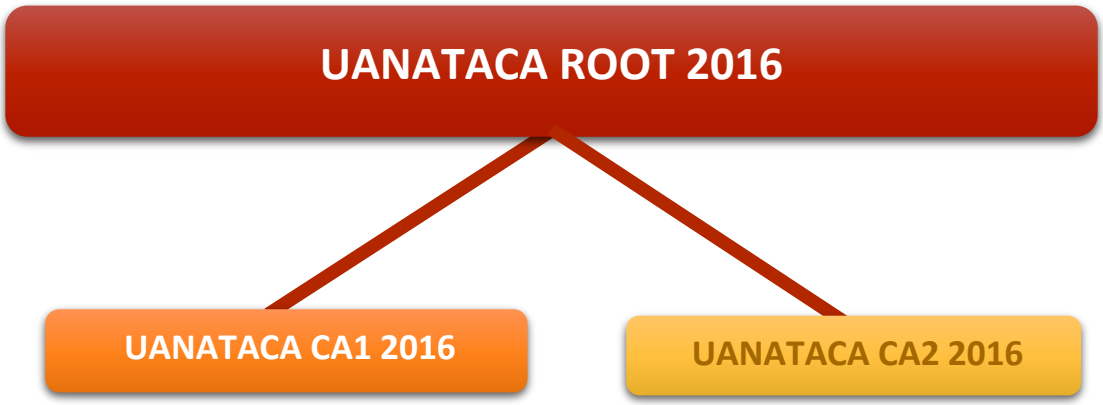
1.3. Participantes en los servicios de certificación

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 presta otros servicios relacionados con la firma electrónica.

UANATACA es un prestador de servicios de certificación, que actúa de acuerdo con lo dispuesto en la Ley 59/2003, de 19 de diciembre, de firma electrónica, y las normas técnicas del ETSI aplicables a la expedición y gestión de certificados cualificados, principalmente ETSI TS 101 456, EN 319 411-1 y 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, UANATACA ha establecido una jerarquía de entidades de certificación:



1.3.1.1. UANATACA ROOT 2016

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

Datos de identificación:

CN:	UANATACA ROOT 2016
Huella digital:	6d c0 84 50 a9 5c d3 26 62 c0 91 0f 8c 2d ce 23 0d 74 66 ad
Válido desde:	Viernes, 11 de marzo de 2016
Válido hasta:	Lunes, 11 de marzo de 2041
Longitud de clave RSA:	4.096 bits

1.3.1.2. UANATACA CA1 2016

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 la UANATACA ROOT 2016.

Datos de identificación:

CN:	UANATACA CA1 2016
Huella digital:	7f 2c b4 f7 69 22 4c b0 cf 8b 69 27 51 cb d4 cc 64 a2 c4 50
Válido desde:	Viernes, 11 de marzo de 2016
Válido hasta:	Domingo, 11 de marzo de 2029
Longitud de clave RSA:	4.096 bits

1.3.1.3. UANATACA CA2 2016

Se trata de la entidad de certificación dentro de la jerarquía que emite los certificados de sellado de tiempo electrónico, entre otros de entidad final, y cuyo certificado de clave pública ha sido firmado digitalmente por la UANATACA ROOT 2016.

Datos de identificación:

CN:	UANATACA CA2 2016
Huella digital:	0e ce 52 78 03 c9 db 6e 63 bc ea 55 36 b9 3a e8 28 4e 8d 2d
Válido desde:	Viernes, 11 de marzo de 2016
Válido hasta:	Domingo, 11 de marzo de 2029
Longitud de clave RSA:	4.096 bits

1.3.2. Registradores

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

También son registradores 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 un departamento de personal, 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 del artículo 13.5 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, 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 UANATACA las siguientes:

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

1.3.3.1. Suscriptores del servicio de certificación

Los suscriptores del servicio de certificación son:

- las empresas, entidades u organizaciones que los adquieren a UANATACA para su uso en su ámbito corporativo empresarial u organizativo, y se encuentran identificados en los certificados.
- Las personas físicas que adquieren los certificados para sí mismas, 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 privada, 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, en especial ETSI TS 101 456, sección 4.4, mantenida en sus versiones posteriores, y actualmente, en ETSI EN 319 411, secciones 5.4.2 y 6.3.4.e)

1.3.3.2. Firmantes

Los firmantes son las personas físicas que poseen de forma exclusiva las claves de firma digital para identificación y firma electrónica avanzada o cualificada; siendo típicamente los empleados, clientes y otras personas vinculadas a los suscriptores, en los certificados de persona física; los representantes legales y voluntarios, en los certificados de representante; o las personas al servicio de las Administraciones Públicas, en los certificados de empleado público.

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, sin que sea posible, en general, el empleo de seudónimos.

La clave privada de un firmante no es almacenada y, por tanto, no puede ser recuperada por el prestador de servicios de certificación, por lo que las personas físicas identificadas en los correspondientes certificados son las únicas responsables de su protección y deberían considerar las implicaciones de perder una clave privada.

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.

1.3.3.3. 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.

1.4. 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 el web https://www.uanataca.com

1.4.1.1. Certificado de persona física, emitido en software

Este certificado dispone del OID 1.3.6.1.4.1.47286.1.1.1.

Este certificado se emite de acuerdo con la política de certificación QCP-n con el OID 0.4.0.194112.1.0, lo cual se declara en el certificado.

Los certificados de persona física emitidos en software, son certificados cualificados de acuerdo con lo establecido en los artículos 24 y 28 del Reglamento (UE) 910/2014, todo ello en concordancia con el artículo 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Los certificados de persona física emitidos en software no garantizan su funcionamiento con dispositivos cualificados de creación de firma, a los que se refieren los artículos 29 y 51 del Reglamento (UE) 910/2014, en concordancia con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

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 cualificados".

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma digital, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

Estos certificados permiten el cifrado de documentos, contenidos y mensajes de datos, bajo la exclusiva responsabilidad del firmante, dado que UANATACA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, UANATACA 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 (Digital Signature, para realizar la función de autenticación)
    b. Compromiso con el contenido (Content commintment, para realizar la función de firma electrónica)
    c. Key Encipherment
    d. Data Encipherment

1.4.1.2. Certificado de persona física, emitido en DCCF

Este certificado dispone del OID 1.3.6.1.4.1.47286.1.1.2.1 para la autenticación, del OID 1.3.6.1.4.1.47286.1.1.2.2 para la firma y del OID 1.3.6.1.4.1.47286.1.1.2.3 para el cifrado.

El certificado cualificado para firma con OID 1.3.6.1.4.1.47286.1.1.2.2, se emite de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2, lo cual se declara en el certificado.

El certificado para firma de persona física emitido en DCCF, es un certificado cualificado de acuerdo con lo establecido en los artículos 24 y 28 del Reglamento (UE) 910/2014, todo ello en concordancia con el artículo 11.1, con el contenido prescrito por el artículo 11.2, y dando cumplimiento a las obligaciones previstas para su emisión, contenidas en los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

El certificado cualificado para firma de persona física emitido en DCCF, funciona con dispositivos cualificados de creación de firma, de acuerdo con los artículos 29 y 51 del Reglamento (UE) 910/2014, en concordancia con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Este certificado cualificado para firma garantiza la identidad del firmante y su vinculación con el suscriptor del servicio de certificación, y permite la generación de la "firma electrónica cualificada"; es decir, la firma electrónica avanzada que se basa en un certificado cualilficado y que ha sido generada empleando un dispositivo cualificado, por lo cual se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

También se puede 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.

Estos certificados permiten el cifrado de documentos, contenidos y mensajes de datos, bajo la exclusiva responsabilidad del firmante, dado que UANATACA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, UANATACA 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. En el perfil de autenticación:
        i. Firma digital (Digital Signature, para realizar la función de autenticación)
    b. En el perfil de firma:
        i. Compromiso con el contenido (Content commintment, para realizar la función de firma electrónica)
    c. En el perfil de cifrado:
        i. Key Encipherment
        ii. Data Encipherment

1.4.1.3. Certificado de representante, emitido en software

Este certificado dispone del OID 1.3.6.1.4.1.47286.1.2.1.

Este certificado se emite de acuerdo con la política de certificación QCP-n con el OID 0.4.0.194112.1.0, lo cual se declara en el certificado.

Los certificados de representante emitidos en software son certificados cualificados de acuerdo con lo establecido en los artículos 24 y 28 del Reglamento (UE) 910/2014, todo ello en concordancia con el artículo 11.1, con el contenido prescrito por el artículo 11.2 y

11.4, y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica y que dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Los certificados de representante en software no garantizan su funcionamiento con dispositivos cualificados de creación de firma, a los que se refieren los artículos 29 y 51 del Reglamento (UE) 910/2014, en concordancia con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Estos certificados garantizan la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una entidad, empresa u organización descrita en el campo "O" (Organization), y permiten la generación de la "firma electrónica avanzada basada en certificado electrónico cualificado".

Por otra parte, los certificados de representante emitido en software se pueden utilizar en otras aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma digital.

Estos certificados permiten el cifrado de documentos, contenidos y mensajes de datos, bajo la exclusiva responsabilidad del firmante, dado que UANATACA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, UANATACA 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 (Digital Signature, para realizar la función de autenticación)
    b. Compromiso con el contenido (Content commintment, para realizar la función de firma electrónica)
    c. Key Encipherment
    d. Data Encipherment

1.4.1.4. Certificado de representante, emitido en DCCF

Este certificado dispone del OID 1.3.6.1.4.1.47286.1.2.2.1 para la autenticación, del OID 1.3.6.1.4.1.47286.1.2.2.2 para la firma y del OID 1.3.6.1.4.1.47286.1.2.2.3 para el cifrado.

El certificado cualificado para firma con OID 1.3.6.1.4.1.47286.1.2.2.2, se emite de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2, lo cual se declara en el certificado.

El certificado para firma de representante emitido en DCCF, es un certificado cualificado de acuerdo con lo establecido en los artículos 24 y 28 del Reglamento (UE) 910/2014, todo ello en concordancia con el artículo 11.1, con el contenido prescrito por el artículo 11.2, y dando cumplimiento a las obligaciones previstas para su emisión, contenidas en los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

El certificado de representante emitido en DCCF, funciona con dispositivos cualificados de creación de firma, de acuerdo con los artículos 29 y 51 del Reglamento (UE) 910/2014, en concordancia con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Este certificado cualificado para firma garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una entidad, empresa u organización descrita en el campo “O” (Organization), y permite 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 se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

También se puede 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.

Estos certificados permiten el cifrado de documentos, contenidos y mensajes de datos, bajo la exclusiva responsabilidad del firmante, dado que UANATACA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, UANATACA 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. En el perfil de autenticación:
        i. Firma digital (Digital Signature, para realizar la función de autenticación)
    b. En el perfil de firma:
        i. Compromiso con el contenido (Content commintment, para realizar la función de firma electrónica)
    c. En el perfil de cifrado:
        i. Key Encipherment
        ii. Data Encipherment

1.4.1.5. Certificado de persona física representante ante las Administraciones de Persona Jurídica emitido en software

Este certificado dispone del OID 1.3.6.1.4.1.47286.1.7.1.

Este certificado se emite de acuerdo con la política de certificación QCP-n con el OID 0.4.0.194112.1.0, lo cual se declara en el certificado.

Los certificados de representante emitidos en software son certificados cualificados de acuerdo con lo establecido en los artículos 24 y 28 del Reglamento (UE) 910/2014, todo ello en concordancia con el artículo 11.1, con el contenido prescrito por el artículo 11.2 y 11.4, y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica y que dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Los certificados de representante en software no garantizan su funcionamiento con dispositivos cualificados de creación de firma, a los que se refieren los artículos 29 y 51 del Reglamento (UE) 910/2014, en concordancia con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Estos certificados garantizan la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una entidad, empresa u organización descrita en el campo "O" (Organization), y permiten la generación de la "firma electrónica avanzada basada en certificado electrónico cualificado".

Por otra parte, los certificados de representante emitido en software se pueden utilizar en otras aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma digital.

Estos certificados permiten el cifrado de documentos, contenidos y mensajes de datos, bajo la exclusiva responsabilidad del firmante, dado que UANATACA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, UANATACA 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 (Digital Signature, para realizar la función de autenticación)
    b. Compromiso con el contenido (Content commintment, para realizar la función de firma electrónica)
    c. Key Encipherment
    d. Data Encipherment

1.4.1.6. Certificado de persona física representante ante las Administraciones de Persona Jurídica emitido en DCCF

Este certificado dispone del OID 1.3.6.1.4.1.47286.1.7.2.1 para la autenticación, del OID 1.3.6.1.4.1.47286.1.7.2.2 para la firma y del OID 1.3.6.1.4.1.47286.1.7.2.3 para el cifrado.

El certificado cualificado para firma con OID 1.3.6.1.4.1.47286.1.7.2.2, se emite de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2, lo cual se declara en el certificado.

El mencionado certificado de firma emitido en DCCF, es un certificado cualificado de acuerdo con lo establecido en los artículos 24 y 28 del Reglamento (UE) 910/2014, todo ello en concordancia con el artículo 11.1, con el contenido prescrito por el artículo 11.2, y dando cumplimiento a las obligaciones previstas para su emisión, contenidas en los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

El certificado de representante emitido en DCCF, funciona con dispositivos cualificados de creación de firma, de acuerdo con los artículos 29 y 51 del Reglamento (UE) 910/2014, en concordancia con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Este certificado de firma garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una entidad, empresa u organización descrita en el campo "O" (Organization), y permite 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 se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

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.

Estos certificados permiten el cifrado de documentos, contenidos y mensajes de datos, bajo la exclusiva responsabilidad del firmante, dado que UANATACA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, UANATACA 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. En el perfil de autenticación:
        i. Firma digital (Digital Signature, para realizar la función de autenticación)
    b. En el perfil de firma:
        i. Compromiso con el contenido (Content commintment, para realizar la función de firma electrónica)
    c. En el perfil de cifrado:
        i. Key Encipherment
        ii. Data Encipherment

1.4.1.7. Certificado de persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica emitido en software

Este certificado dispone del OID 1.3.6.1.4.1.47286.1.8.1.

Este certificado se emite de acuerdo con la política de certificación QCP-n con el OID 0.4.0.194112.1.0, lo cual se declara en el certificado.

Los certificados de representante emitidos en software son certificados cualificados de acuerdo con lo establecido en los artículos 24 y 28 del Reglamento (UE) 910/2014, todo ello en concordancia con el artículo 11.1, con el contenido prescrito por el artículo 11.2 y 11.4, y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica y que dan cumplimiento a lo dispuesto

por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Los certificados de representante en software no garantizan su funcionamiento con dispositivos cualificados de creación de firma, a los que se refieren los artículos 29 y 51 del Reglamento (UE) 910/2014, en concordancia con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Estos certificados garantizan la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una entidad, empresa u organización descrita en el campo "O" (Organization), y permiten la generación de la "firma electrónica avanzada basada en certificado electrónico cualificado".

Por otra parte, los certificados de representante emitido en software se pueden utilizar en otras aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma digital.

Estos certificados permiten el cifrado de documentos, contenidos y mensajes de datos, bajo la exclusiva responsabilidad del firmante, dado que UANATACA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, UANATACA 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 (Digital Signature, para realizar la función de autenticación)
    b. Compromiso con el contenido (Content commintment, para realizar la función de firma electrónica)
    c. Key Encipherment
    d. Data Encipherment

1.4.1.8. Certificado de persona física representante ante las Administraciones de Persona Jurídica emitido en DCCF

Este certificado dispone del OID 1.3.6.1.4.1.47286.1.8.2.1 para la autenticación, del OID 1.3.6.1.4.1.47286.1.8.2.2 para la firma y del OID 1.3.6.1.4.1.47286.1.8.2.3 para el cifrado.

Este certificado cualificado para firma con OID 1.3.6.1.4.1.47286.1.8.2.2, se emite de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2, lo cual se declara en el certificado.

El certificado para firma de representante de persona jurídica emitido en DCCF, es un certificado cualificado de acuerdo con lo establecido en los artículos 24 y 28 del Reglamento (UE) 910/2014, todo ello en concordancia con el artículo 11.1, con el contenido prescrito por el artículo 11.2, y dando cumplimiento a las obligaciones previstas para su emisión, contenidas en los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

El certificado de representante de persona jurídica emitido en DCCF, funciona con dispositivos cualificados de creación de firma, de acuerdo con los artículos 29 y 51 del Reglamento (UE) 910/2014, en concordancia con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Este certificado garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una entidad u organización descrita en el campo “O” (Organization), y permite 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 se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

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.

Estos certificados permiten el cifrado de documentos, contenidos y mensajes de datos, bajo la exclusiva responsabilidad del firmante, dado que UANATACA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, UANATACA 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. En el perfil de autenticación:
        i. Firma digital (Digital Signature, para realizar la función de autenticación)
    b. En el perfil de firma:
        i. Compromiso con el contenido (Content commintment, para realizar la función de firma electrónica)
    c. En el perfil de cifrado:
        i. Key Encipherment
        ii. Data Encipherment

1.4.1.9. Certificado de empleado público, nivel medio

Este certificado dispone del OID 1.3.6.1.4.1.47286.1.4.1.

Este certificado se emite de acuerdo con la política de certificación QCP-n con el OID 0.4.0.194112.1.0, lo cual se declara en el certificado.

Los certificados de persona física empleado público nivel medio son certificados cualificados de acuerdo con lo establecido en los artículos 24 y 28 del Reglamento (UE) 910/2014, todo ello en concordancia con en el artículo 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Estos certificados se emiten a empleados públicos para identificarlos como personas al servicio de la Administración Pública, 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.

Los certificados de persona física empleado público nivel medio no garantizan su funcionamiento con dispositivos cualificados de creación de firma, a los que se refieren los artículos 29 y 51 del Reglamento (UE) 910/2014, en concordancia con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Los certificados de persona física empleado público nivel medio se emiten de acuerdo con el Esquema de identificación y firma electrónica de las Administraciones públicas en su versión vigente a fecha de este documento.

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.

Estos certificados permiten el cifrado de documentos, contenidos y mensajes de datos, bajo la exclusiva responsabilidad del firmante, dado que UANATACA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, UANATACA 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 (Digital Signature, para realizar la función de autenticación)

b. Compromiso con el contenido (Content commintment, para realizar la función de firma electrónica)
c. Key Encipherment
d. Data Encipherment

1.4.1.10. Certificado de empleado público, nivel alto

Este certificado dispone del OID 1.3.6.1.4.1.47286.1.4.2.1 para la identificación, del OID 1.3.6.1.4.1.47286.1.4.2.2 para la firma y del OID 1.3.6.1.4.1.47286.1.4.2.3 para el cifrado.

Este certificado cualificado para firma con OID 1.3.6.1.4.1.47286.1.4.2.2, se emite de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2., lo cual se declara en el certificado.

El certificado de firma de persona física empleado público nivel alto, es un certificado cualificado de acuerdo con lo establecido en los artículos 24 y 28 del Reglamento (UE) 910/2014, todo ello en concordancia con el artículo 11.1, con el contenido prescrito por el artículo 11.2, y dando cumplimiento a las obligaciones previstas para su emisión, contenidas en los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Este certificado cualificado de firma se emite a empleados públicos para identificarlos como personas al servicio de la Administración Pública, 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.

El certificado cualificado de firma de persona física empleado público nivel alto, funciona con dispositivos cualificados de creación de firma, de acuerdo con los artículos 29 y 51 del Reglamento (UE) 910/2014, en concordancia con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Asimismo, los certificados de persona física empleado público nivel alto se emiten de acuerdo con el Esquema de identificación y firma electrónica de las Administraciones públicas en su versión vigente a fecha de este documento.

Este certificado cualificado para firma garantiza la identidad del suscriptor y del firmante, y permite 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 en concordancia con el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

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.

Estos certificados permiten el cifrado de documentos, contenidos y mensajes de datos, bajo la exclusiva responsabilidad del firmante, dado que UANATACA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, UANATACA 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. En el perfil de autenticación:
        i. Firma digital (Digital Signature, para realizar la función de autenticación)
    b. En el perfil de firma:
        i. Compromiso con el contenido (Content commintment, para realizar la función de firma electrónica)
    c. En el perfil de cifrado:
        i. Key Encipherment

ii. Data Encipherment

1.4.1.11. Certificado de la Unidad de Sellado de tiempo electrónico

Este certificado dispone del OID 1.3.6.1.4.1.47286.1.5.

Este certificado se emite de acuerdo con la política de certificación QCP-l con el OID 0.4.0.194112.1.1.

Los certificados de sello de tiempo electrónico se tratan de certificados electrónicos emitidos para la operación de autoridades de sellado de tiempo y hora para la firma de los sellos de tiempo que éstas producen.

Estos certificados permiten la firma de los sellos de tiempo que se emiten, desde el momento que hayan obtenido un certificado de sello de tiempo electrónico válido y mientras éste se encuentre vigente.

La sincronización de los tiempos en UANATACA se realiza con un servidor de tiempo NTP stratum 1.

Este servidor, un Meinberg Lantime M300/GPS, con oscilador TCXO de alta estabilidad, receptor GPS, formado por una tarjeta GPS interna para sincronizarse simultáneamente con los satélites con los que tiene visibilidad en cada momento (entre 3 y 8), y protección anti-rayos.

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 (LRC).

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 UANATACA (https://www.uanataca.com).

El empleo de los certificados digitales en operaciones que contravienen esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos con las entidades de registro o con sus firmantes/suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a UANATACA, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

UANATACA no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de UANATACA 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 Declaración de Prácticas de Certificación, 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.

1.5. Administración de la política

1.5.1. Organización que administra el documento

Uanataca, S.A.
Calle Riera de Can Todà, 24-26, 6º, 1ª
08024 Barcelona

1.5.2. Datos de contacto de la organización

Uanataca, S.A.
Calle Riera de Can Todà, 24-26, 6º, 1ª
08024 Barcelona

1.5.3. Procedimientos de gestión del documento

El sistema documental y de organización de UANATACA S.A. 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.

2. Publicación de información y depósito de certificados

2.1. Depósito(s) de certificados

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

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 UANATACA, 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 del prestador de servicios de certificación

UANATACA publica las siguientes informaciones, en su Depósito:

- Los certificados emitidos, cuando se haya obtenido consentimiento de la persona física identificada en el certificado.
- 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 (Policy 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

UANATACA 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.

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

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Los certificados sólo estén disponibles para consulta si la persona física identificada en el certificado ha prestado su consentimiento.
- Pueda detectarse 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 persona física, emitido en software

Country (C)	Estado[1]
Organization (O)	Organización a la que está vinculado el firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	DNI/NIE del firmante
Common Name (CN)	Nombre, apellidos del firmante

3.1.1.2. Certificado de persona física, emitido en DCCF

Country (C)	Estado[2]
Organization (O)	Organización a la que está vinculado el firmante
Surname	Apellidos del firmante

[1] El campo "país" corresponderá al del estado donde se produzca la relación contractual entre el firmante y la entidad a la que está vinculado (por ser empleado, miembro, socio u otra vinculación), con independencia de la nacionalidad del trabajador.

[2] El campo "país" corresponderá al del estado donde se produzca la relación contractual entre el firmante y la entidad a la que está vinculado (por ser empleado, miembro, socio u otra vinculación), con independencia de la nacionalidad del trabajador.

Given Name	Nombre del firmante
Serial Number	DNI/NIE del firmante
Common Name (CN)	Nombre, apellidos del firmante

3.1.1.3. Certificado de representante, emitido en software

Country (C)	Estado[3]
Organization (O)	Organización a la que representa el firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	DNI/NIE del firmante
Common Name (CN)	Nombre, apellidos del firmante

3.1.1.4. Certificado de representante, emitido en DCCF

Country (C)	Estado[4]
Organization (O)	Organización a la que representa el firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	DNI/NIE del firmante
Common Name (CN)	Nombre, apellidos del firmante

[3] El campo "país" corresponderá al del estado donde se produzca la relación contractual entre el firmante y la entidad a la que representa con independencia de la nacionalidad del representante.

[4] El campo "país" corresponderá al del estado donde se produzca la relación contractual entre el firmante y la entidad a la que representa con independencia de la nacionalidad del representante.

3.1.1.5. Certificado de persona física representante ante las Administraciones de Persona Jurídica emitido en software

Country (C)	Estado[5]
Organization (O)	Organización a la que representa el firmante
Organizationidentifier	NIF de la persona jurídica representada en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)
Surname	Apellidos del firmante (como consta en el DNI/NIE)
Given Name	Nombre del firmante (como consta en el DNI/NIE)
Serial Number	NIF del titular (NIF es el número y letra que aparece en el DNI o NIE según corresponda "123456789Z") o codificación acorde a ETSI EN 319 412-1 "IDCES-123456789Z")
Common Name (CN)[6]	Ej. 00000000T Pedro Rull (R: Q0000000J)

3.1.1.6. Certificado de persona física representante ante las Administraciones de Persona Jurídica emitido en DCCF

Country (C)	Estado[7]
Organization (O)	Organización a la que representa el firmante
Organizationidentifier	NIF de la persona jurídica representada en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)

[5] El campo "país" corresponderá al del estado donde se produzca la relación contractual entre el firmante y la entidad a la que representa con independencia de la nacionalidad del representante.

[6] De acuerdo con la propuesta del apartado 14.1.3.3 (codificación del atributo Common Name) del documento de "Perfiles de certificados Electrónicos (abril del 2016)" del Ministerio de Hacienda y Administraciones Públicas: DNI/NIE, Nombre y Apellido, "(R:", Nif de la empresa representada, ")". Máximo 64 caracteres según la RFC 5280

[7] El campo "país" corresponderá al del estado donde se produzca la relación contractual entre el firmante y la entidad a la que representa con independencia de la nacionalidad del representante.

Surname	Apellidos del firmante (como consta en el DNI/NIE)
Given Name	Nombre del firmante (como consta en el DNI/NIE)
Serial Number	NIF del titular (NIF es el número y letra que aparece en el DNI o NIE según corresponda "123456789Z") o codificación acorde a ETSI EN 319 412-1 "IDCES-123456789Z")
Common Name (CN)[8]	Ej. 00000000T Pedro Rull (R: Q0000000J) AUTENTIC
	Ej. 00000000T Pedro Rull (R: Q0000000J) FIRMA
	Ej. 00000000T Pedro Rull (R: Q0000000J) CIFRADO

3.1.1.7. Certificado de persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica emitido en software

Country (C)	Estado[9]
Organization (O)	Organización a la que representa el firmante
Organizationidentifier	NIF de la persona jurídica representada en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)
Surname	Apellidos del firmante (como consta en el DNI/NIE)
Given Name	Nombre del firmante (como consta en el DNI/NIE)
Serial Number	NIF del titular (NIF es el número y letra que aparece en el DNI o NIE según corresponda "123456789Z") o codificación acorde a ETSI EN 319 412-1 "IDCES-123456789Z")

[8] De acuerdo con la propuesta del apartado 14.1.3.3 (codificación del atributo Common Name) del documento de "Perfiles de certificados Electrónicos (abril del 2016)" del Ministerio de Hacienda y Administraciones Públicas: DNI/NIE, Nombre y Apellido, "(R:", Nif de la empresa representada, ")". Máximo 64 caracteres según la RFC 5280

[9] El campo "país" corresponderá al del estado donde se produzca la relación contractual entre el firmante y la entidad a la que representa con independencia de la nacionalidad del representante.

Common Name (CN)[10]	Ej. 00000000T Pedro Rull (R: Q0000000J)

3.1.1.8. Certificado de persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica emitido en DCCF

Country (C)	Estado[11]
Organization (O)	Organización a la que representa el firmante
Organizationidentifier	NIF de la persona jurídica representada en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)
Surname	Apellidos del firmante (como consta en el DNI/NIE)
Given Name	Nombre del firmante (como consta en el DNI/NIE)
Serial Number	NIF del titular (NIF es el número y letra que aparece en el DNI o NIE según corresponda "123456789Z") o codificación acorde a ETSI EN 319 412-1 "IDCES-123456789Z")
Common Name (CN)[12]	Ej. 00000000T Pedro Rull (R: Q0000000J) AUTENTIC
	Ej. 00000000T Pedro Rull (R: Q0000000J) FIRMA
	Ej. 00000000T Pedro Rull (R: Q0000000J) CIFRADO

[10] De acuerdo con la propuesta del apartado 14.1.3.3 (codificación del atributo Common Name) del documento de "Perfiles de certificados Electrónicos (abril del 2016)" del Ministerio de Hacienda y Administraciones Públicas: DNI/NIE, Nombre y Apellido, "(R:", Nif de la empresa representada, ")". Máximo 64 caracteres según la RFC 5280

[11] El campo "país" corresponderá al del estado donde se produzca la relación contractual entre el firmante y la entidad a la que representa con independencia de la nacionalidad del representante.

[12] De acuerdo con la propuesta del apartado 14.1.3.3 (codificación del atributo Common Name) del documento de "Perfiles de certificados Electrónicos (abril del 2016)" del Ministerio de Hacienda y Administraciones Públicas: DNI/NIE, Nombre y Apellido, "(R:", Nif de la empresa representada, ")". Máximo 64 caracteres según la RFC 5280

3.1.1.9. Sello de órgano, de nivel medio

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial" de la organización) del suscriptor
Surname	Apellidos del responsable creador de sellos
Given Name	Nombre del responsable creador de sellos
Serial Number	DNI/NIE de la organización suscriptora
Common Name (CN)	Denominación de sistema o aplicación de proceso automático.
DNI/NIE del responsable OID: 2.16.724.1.3.5.2.2.4	DNI o NIE del responsable del sello
Nombre de pila OID: 2.16.724.1.3.5.2.2.6	Nombre de pila del responsable del sello
Primer apellido OID: 2.16.724.1.3.5.2.2.7	Primer apellido del responsable del sello
Segundo apellido OID: 2.16.724.1.3.5.2.2.8	Segundo apellido del responsable del sello
Correo electrónico OID: 2.16.724.1.3.5.2.2.9	Correo electrónico del responsable del sello

3.1.1.10. Sello de órgano, de nivel alto

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial" de la organización) del suscriptor
Surname	Apellidos del responsable creador de sellos
Given Name	Nombre del responsable creador de sellos
Serial Number	DNI/NIE de la organización suscriptora
Common Name (CN)	Denominación de sistema o aplicación de proceso automático.
DNI/NIE del responsable OID: 2.16.724.1.3.5.2.1.4	DNI o NIE del responsable del sello

Nombre de pila OID: 2.16.724.1.3.5.2.1.6	Nombre de pila del responsable del sello
Primer apellido OID: 2.16.724.1.3.5.2.1.7	Primer apellido del responsable del sello
Segundo apellido OID: 2.16.724.1.3.5.2.1.8	Segundo apellido del responsable del sello
Correo electrónico OID: 2.16.724.1.3.5.2.1.9	Correo electrónico del responsable del sello

3.1.1.11. Certificado de empleado público, nivel medio

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
Surname	Primer y segundo 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
Title	Puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado.
Common Name (CN)	Nombre Apellido1 Apellido2 – NIF del empleado
DNI/NIE del responsable OID: 2.16.724.1.3.5.3.2.4	DNI o NIE del responsable
Número de autenticación personal OID: 2.16.724.1.3.5.3.2.5	NRP o NIP del responsable del suscriptor del certificado
Nombre de pila OID: 2.16.724.1.3.5.3.2.6	Nombre de pila del responsable del certificado

Primer apellido OID: 2.16.724.1.3.5.3.2.7	Primer apellido del responsable del certificado
Segundo apellido OID: 2.16.724.1.3.5.3.2.8	Segundo apellido del responsable del certificado
Correo electrónico OID: 2.16.724.1.3.5.3.2.9	Correo electrónico del responsable del certificado

3.1.1.12. Certificado de empleado público, nivel alto

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
Surname	Primer y segundo 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
Title	Puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado.
Common Name (CN)	Nombre Apellido1 Apellido2 – NIF del empleado
DNI/NIE del esponsable OID: 2.16.724.1.3.5.3.1.4	DNI o NIE del responsable
Número de autenticación personal OID: 2.16.724.1.3.5.3.1.5	NRP o NIP del responsable del suscriptor del certificado
Nombre de pila OID: 2.16.724.1.3.5.3.1.6	Nombre de pila del responsable del certificado
Primer apellido OID: 2.16.724.1.3.5.3.1.7	Primer apellido del responsable del certificado

Segundo apellido OID: 2.16.724.1.3.5.3.1.8	Segundo apellido del responsable del certificado
Correo electrónico OID: 2.16.724.1.3.5.3.1.9	Correo electrónico del responsable del certificado

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, ni a un firmante.

En ningún caso se emiten certificados anónimos.

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 campo “país” será el del país del suscriptor, y siempre será España en los certificados emitidos a las Administraciones Públicas españolas.

El certificado muestra la relación entre una persona física y la empresa, entidad u organización 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 entidad, empresa u organización, y la persona física vinculada la persona autorizada a su uso.

En los certificados emitidos a suscriptores españoles, el campo "número de serie" debe incluir el NIF del 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 UANATACA.

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 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.

UANATACA 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 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 UANATACA y el suscriptor, momento en el que se verifica la existencia del suscriptor mediante su documento oficial de identidad o las escrituras correspondientes, al igual que los poderes de actuación de la persona que presente como representante si fuese el caso. Para esta verificación, se podrá emplear documentación pública o notarial, o la consulta directa a los registros públicos correspondientes.

En el caso de personas físicas identificadas en certificados cuyo suscriptor sea una persona jurídica, sus identidades se validarán mediante los registros corporativos de la entidad, empresa u organización de derecho público o privado, suscriptoras de los certificados. El suscriptor producirá una certificación de los datos necesarios, y la remitirá a UANATACA, por los medios que ésta habilite, para el registro de la identidad de los firmantes.

Los ficheros de datos personales de cada entidad, empresa u organización de derecho público o privado deberán estar inscritos en la Agencia de Protección de Datos correspondiente, por cada una de ellas, siendo su responsabilidad, y no la de UANATACA, que actúa como encargado del tratamiento.

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 suscriptor, en certificados de sello, o por el firmante, en certificados de firma.

3.2.2. Autenticación de la identidad de una organización, empresa o entidad mediante representante

Las personas físicas con capacidad de actuar en nombre de las persona públicas o privadas suscriptoras, podrán actuar como representantes de las mismas, siempre y cuando exista una situación previa de representación legal o voluntaria entre la persona física y la persona pública o privada, que exige su reconocimiento por UANATACA, la cual se realizará mediante el siguiente procedimiento presencial:

1. El representante del suscriptor se reunirá presencialmente con un representante autorizado de UANATACA, donde dispondrá de un formulario de autenticación.

   Alternativamente, el representante del suscriptor podrá obtener el formulario de la página web de UANATACA para su cumplimentación previa.

2. El representante cumplimentará el formulario, con las siguientes informaciones y a la que acompañará los siguientes documentos:

   - Sus datos de identificación, como representante:
     - Nombre y apellidos
     - Lugar y fecha de nacimiento
     - Documento: NIF del representante

   - Los datos de identificación del suscriptor al que representa:
     - Denominación o razón social.
     - Toda información de registro existente, incluyendo los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante.

- Documento: NIF de la persona pública o privada.
- Documento: Documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

- Los datos relativos a la representación o la capacidad de actuación que ostenta:

  - La vigencia de la representación o la capacidad de actuación (fecha de inicio y fin).
  - El ámbito y los límites, en su caso, de la representación o de la capacidad de actuación:
    - TOTAL. Representación o capacidad total. Esta comprobación se podrá realizar mediante consulta telemática al registro público donde conste inscrita la representación.
    - PARCIAL. Representación o capacidad parcial. Esta comprobación se podrá realizar mediante copia auténtica electrónica de la escritura notarial de apoderamiento, en los términos de la normativa notarial.

3. Cumplimentado y firmado el formulario, se firmará y entregará a UANATACA junto con la documentación justificativa indicada.

4. El personal de UANATACA comprobará la identidad del representante mediante la presentación del DNI, así como el contenido de la representación con la documentación.

5. El personal de UANATACA entregará un justificante de la autenticación y le devolverá la documentación aportada.

6. Alternativamente, de acuerdo con lo establecido en el artículo 13.1 de la Ley 59/2003, de 19 de diciembre, se podrá legitimar notarialmente la firma del formulario, y hacerse llegar a UANATACA por correo postal certificado, en cuyo caso los pasos 3 a 5 anteriores no serán precisos.

La prestación del servicio de certificación digital se formaliza mediante el oportuno contrato entre UANATACA y el suscriptor, debidamente representado.

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.

3.2.3.1. En los certificados

La información de identificación de las personas físicas identificadas en los certificados cuyo suscriptor sea una persona jurídica, se valida comparando la información de la solicitud con los registros de la entidad, empresa u organización de derecho público o privado a la que está vinculado, asegurando la corrección de la información a certificar.

La identidad de los firmantes identificados en los certificados cuyo suscriptor sea una persona física, se valida mediante la presentación de su documento oficial de identificación (Documento Nacional de Identidad, tarjeta de identidad, pasaporte u otro medio idóneo reconocido en derecho para su identificación).

3.2.3.2. Necesidad de presencia personal

Para la solicitud de certificados de persona física, UANATACA valida la identidad del solicitante, para lo cual la persona física deberá personarse y exhibir su documento oficial de identidad ante la Autoridad de Registro o el lugar que se haya indicado para tal fin.

Para la solicitud de los certificados cuyo suscriptor sea una persona jurídica no se requiere la presencia física directa, debido a la relación ya acreditada entre la persona física y entidad, empresa u organización de derecho público o privado a la que está vinculada, siempre que no hubiesen transcurrido más de cinco (5) años desde la identificación, de

conformidad con lo previsto en el artículo 13.4.a) de la Ley 59/2003. Sin embargo, antes de la entrega de un certificado, la entidad, empresa u organización de derecho público o privado suscriptora, por medio de su responsable de certificación, de tenerlo, u otro miembro designado, deberá contrastar la identidad de la persona física identificada en el certificado mediante su presencia física.

Durante este trámite se confirma rigurosamente la identidad de la persona física identificada en el certificado.Por este motivo, en todos los casos en que se expide un certificado se verifica presencialmente la identidad de la persona física firmante.

La Autoridad de Registro verificará mediante la exhibición de documentos o a través de sus propias fuentes de información, el resto de datos y atributos a incluir en el certificado, guardando documentación acreditativa de la validez de estos.

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 entidad, empresa u organización de derecho público o privado viene dada por su constancia en los registros internos (contrato de trabajo como empleado, o el contrato mercantil que lo vincula, o el acta donde se indique su cargo, o la solicitud como miembro de la organización…) de cada una de las personas púbicas y privadas a las que están vinculadas.Información de suscriptor no verificada

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

3.2.4. Autenticación de la identidad de una RA y sus operadores

Para la constitución de una nueva Autoridad de Registro, UANATACA realiza las verificaciones necesarias para confirmar la existencia de la entidad u organización de la que se trate. Para ello, UANATACA podrá utilizar exhibición de documentos o utilizar sus propias fuentes de información.

Igualmente, UANATACA verifica y valida la identidad de los operadores de las Autoridades de Registro, para lo cual estas últimas envían a UANATACA la documentación de

identificación correspondientes al nuevo operador, conjuntamente con su autorización para actuar como tal.

UANATACA se asegura que los operadores de la RA reciben la formación suficiente para el desarrollo de sus funciones, lo cual verifica con la evaluación correspondiente. Para la prestación de los servicios, UANATACA se asegura de que los operadores de RA se autentican para su comunicación a través de certificados digitales.

3.3. Identificación y autenticación de solicitudes de renovación

3.3.1. Validación para la renovación rutinaria de certificados

Antes de renovar un certificado, UANATACA o una Entidad de Registro comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y de la persona física identificada en el certificado continúan siendo válidos.

Los métodos aceptables para dicha comprobación son:

- El uso de una "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 renovar de forma automática su certificado, siempre que no se haya superado el plazo máximo legalmente establecido.
- El empleo del certificado vigente para su renovación, siempre que se trate de un certificado expedido por UANATACA y no se haya superado el plazo máximo legalmente establecido para esta posibilidad.

Si cualquier información del suscriptor o de la persona física identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una autenticación completa, de acuerdo con lo establecido en la sección 3.2.

3.3.2. Identificación y autenticación de la solicitud de revocación

Antes de generar un certificado a un suscriptor cuyo certificado fue revocado, UANATACA o una Entidad de Registro comprobará que la información empleada en su día para

verificar la identidad y los restantes datos del suscriptor y de la persona física identificada en el certificado continúa siendo válida, en cuyo caso se aplicará lo dispuesto en la sección anterior.

La renovación de certificados tras la revocación no será posible en los siguientes casos:

- El certificado fue revocado por emisión errónea a una persona diferente a la identificada en el certificado.
- El certificado fue revocado por emisión no autorizada por la persona física identificada en el certificado.
- El certificado revocado puede contener información errónea o falsa.

Si cualquier información del suscriptor o de la persona física identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una autenticación completa, de acuerdo con lo establecido en la sección 3.2.

3.4. Identificación y autenticación de la solicitud de revocación

UANATACA o una Entidad de Registro autentica 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", 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 empresa, entidad u Organización subscriptora.
- Otros medios de comunicación, como el teléfono, cuando existan garantías razonables de la identidad del solicitante de la revocación, a juicio de UANATACA.

3.5. Autenticación de una petición de suspensión

La petición de suspensión se realizará por el suscriptor utilizando el formulario existente en la web de UANATACA indicando la opción de suspensión (https://www.uanataca.com) en horario de 24x7.

Cuando en horario de oficina el suscriptor desee iniciar una petición de revocación y existan dudas para su identificación, su certificado pasa a estado de suspensión.

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

4.1. Solicitud de emisión de certificado

4.1.1. Legitimación para solicitar la emisión

El solicitante del certificado, sea persona física o jurídica, debe firmar un contrato de prestación de servicios de certificación con UANATACA.

Asimismo, con anterioridad a la emisión y entrega de un certificado, debe existir una solicitud de certificados ya sea en el mismo contrato, o en un documento específico de hoja de solicitud de certificados.

Cuando el solicitante es una persona distinta al suscriptor, debe existir 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 propio en el caso de certificados para persona física, o bien en nombre del suscriptor en el caso de que el suscriptor sea la por entidad, empresa u organización de derecho público o privado.

4.1.2. Procedimiento de alta y responsabilidades

UANATACA recibe solicitudes de certificados, realizadas por personas, entidades, empresas u organizaciones de derecho público o privado.

Las solicitudes se instrumentan mediante un documento en formato electrónico, cumplimentado por el solicitante, cuyo destinatario es UANATACA, el cual incluirá los datos de las personas a las que se expedirán certificados. En el caso de certificados cuyo suscriptor sea una entidad, empresa u organización de derecho público o privado, 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 UANATACA.

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, UANATACA se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

En caso afirmativo, UANATACA verifica la información proporcionada, verificando los aspectos descritos en la sección 3.2

En caso de un certificado cualificado, 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 expiración del certificado, incluso en caso de pérdida anticipada de vigencia por revocación.

4.2.2. Aprobación o rechazo de la solicitud

En caso que los datos se verifiquen correctamente, UANATACA debe aprobar la solicitud del certificado y proceder a su emisión y entrega.

Si la verificación indica que la información no es correcta, o si se sospecha que no es correcta o que puede afectar a la reputación de la Entidad de Certificación, de las Entidades de Registro o de los suscriptores, UANATACA denegará la petición, o detendrá su aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

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

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

UANATACA 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

UANATACA 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.

Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, dado que la misma implica la emisión de un nuevo certificado.

Durante el proceso, UANATACA:

- 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 artículo 11 de la Ley 59/2003, de 19 de diciembre, 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

UANATACA notifica la emisión del certificado al suscriptor y a la persona física identificada en el certificado.

4.4. Entrega y aceptación del certificado

4.4.1. Responsabilidades de la CA

Durante este proceso, UANATACA debe realizar las siguientes actuaciones:

- Acreditar definitivamente la identidad de la persona física identificada en el certificado, con la colaboración de la Entidad de Registro o subscriptor, de acuerdo con lo establecido en las secciones 3.2.2 y 3.2.3.
- Entregar a la persona física identificada en el certificado con la colaboración, cuando exista, de la Entidad de Registro, la hoja de entrega y aceptación del certificado con 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.

La Entidad de Registro colabora en estos procesos, debiendo registrar documentalmente los anteriores actos y conserva los citados documentos originales (hojas de entrega y aceptación), remitiendo copia electrónica a UANATACA, así como los originales cuando UANATACA precise de acceso a los mismos.

4.4.2. Conducta que constituye aceptación del certificado

La aceptación del certificado por la persona física identificada en el certificado se produce mediante la firma de la hoja de entrega y aceptación.

4.4.3. Publicación del certificado

UANATACA publica el certificado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes y siempre que UANATACA disponga de la autorización de la persona física identificada en el certificado.

4.4.4. Notificación de la emisión a terceros

UANATACA 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 firmante

UANATACA obliga a:

- Facilitar a UANATACA información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- 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 UANATACA 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.

UANATACA obliga al firmante a responsabilizarse de:

- 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 subscriptor

4.5.2.1. Obligaciones del suscriptor del certificado

UANATACA 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 registro.
- 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 UANATACA 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 UANATACA, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación del prestador de servicios de certificación de UANATACA, sin permiso previo por escrito.

4.5.2.2. Responsabilidad civil del suscriptor de certificado

UANATACA obliga contractualmente al suscriptor a responsabilizarse de:

- 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

4.5.3.1. Obligaciones del tercero que confía en certificados

UANATACA 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 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 UANATACA, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de la UANATACA, sin permiso previo por escrito.

4.5.3.2. Responsabilidad civil del tercero que confía en certificados

UANATACA 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

La renovación de los certificados exige la renovación de claves, por lo que debe atenderse a lo establecido en la sección 4.7.

4.7. Renovación de claves y certificados

4.7.1. Causas de renovación de claves y certificados

Los certificados vigentes se pueden renovar mediante un procedimiento específico y simplificado de solicitud, al efecto de mantener la continuidad del servicio de certificación.

4.7.2. Legitimación para solicitar la renovación

Con anterioridad a la emisión y entrega de un certificado renovado, debe existir una solicitud de renovación de certificado, que puede producirse de oficio o a instancia de parte interesada.

Asimismo, se contempla una autorización del suscriptor para que el solicitante pueda realizar la solicitud, que se instrumenta jurídicamente mediante una hoja de renovación de certificados suscrita por la empresa, entidad u organización.

4.7.3. Procedimientos de solicitud de renovación

4.7.3.1. Realización de la solicitud

UANATACA recibe solicitudes de certificados, realizadas por las personas físicas, entidades, empresas u organizaciones de derecho público o privado.

Existe un documento, ya sea en soporte papel o en formato electrónico, referente a la solicitud de renovación de certificados, realizada por la entidad, empresa u organización de derecho público o privado, el cual incluirá los datos de las personas a las que se expedirán certificados.

La solicitud debe indicar que los datos de los certificados no han cambiado, pudiendo únicamente indicar cambios en la dirección física, u otros datos, que permitan contactar a la persona física identificada en el certificado.

4.7.3.2. Ejecución de las funciones de identificación y autenticación

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

4.7.3.3. Aprobación o rechazo de la solicitud

En caso que los datos se verifiquen correctamente, UANATACA debe aprobar la solicitud de renovación del certificado y proceder a su emisión y entrega.

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

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

4.7.3.4. Plazo para resolver la solicitud

UANATACA atiende las solicitudes de renovación de certificados por orden de llegada, en un plazo razonable anterior a la expiración de los certificados a revocar, pudiendo especificarse una garantía de plazo máximo en el convenio de emisión de certificados.
Las solicitudes de renovación se mantienen activas hasta su aprobación o rechazo.

4.7.4. Notificación de la emisión del certificado renovado

UANATACA notifica la emisión del certificado al suscriptor y a la persona física identificada en el certificado.

4.7.5. Conducta que constituye aceptación del certificado

La aceptación del certificado por la persona física identificada en el certificado se produce mediante la firma, escrita o electrónica, de la hoja de entrega y aceptación ante el responsable de certificación de la entidad, empresa u organización de derecho público o privado.

4.7.6. Publicación del certificado

UANATACA publica el certificado renovado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes.

4.7.7. Notificación de la emisión a terceros

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

4.8. Modificación de certificados

La modificación de certificados, excepto la modificación de la clave pública certificada, que se considera renovación, 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

UANATACA revoca un certificado cuando concurre 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 UANATACA, 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 UANATACA 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 la Entidad de Certificación de UANATACA, de acuerdo con lo establecido en la sección 5.8.

b) El uso del certificado que sea dañino y continuado para UANATACA. 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.

4.9.2. Legitimación para solicitar la revocación

Pueden solicitar la revocación de un certificado:

- La persona identificada en el certificado.
- El suscriptor del certificado por medio responsable del servicio de certificación.

4.9.3. Procedimientos de solicitud de revocación

La entidad que precise revocar un certificado debe solicitarlo a UANATACA. La solicitud de revocación comprenderá la siguiente información:

- Fecha de solicitud de la revocación.
- Identidad del suscriptor.
- Razón detallada para la petición de revocación.
- Nombre y título de la persona que pide la revocación.
- Información de contacto de la persona que pide la revocación.

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

El servicio de revocación se encuentra en la página web de UANATACA en la dirección: https://www.uanataca.com

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 debe remitir una solicitud en este sentido a UANATACA.

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

UANATACA no reactiva el certificado una vez ha sido revocado.

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

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.

4.9.5. Plazo temporal de procesamiento de la solicitud

La revocación se producirá inmediatamente cuando sea recibida, dentro del horario ordinario de operación de UANATACA.

4.9.6. Obligación de consulta de información de revocación de certificados

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 UANATACA.

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:

- http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl
- http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl

- http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl
- http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl

El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSP.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

4.9.7. Frecuencia de emisión de listas de revocación de certificados (LRCs)

UANATACA emite una LRC al menos cada 24 horas.

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

La LRC mantiene obligatoriamente el certificado revocado o suspendido hasta que expira.

4.9.8. Plazo máximo de publicación de LRCs

Las LRCs se publican en el Depósito en un periodo inmediato razonable tras su generación, que en ningún caso no supera unos pocos minutos.

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

De forma alternativa, los terceros que confían en certificados podrán consultar el Depósito de certificados de UANATACA, que se encuentra disponible las 24 horas de los 7 días de la semana en el web:

- https://www.uanataca.com/public/pki/crtlist

Para comprobar la última CRL emitida en cada CA se debe descargar:

- *CA ROOT:*
  - http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
  - http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

- *CA1 INTERMEDIA:*
  - http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl
  - http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl

- *CA2 INTERMEDIA:*
  - http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl
  - http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl

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

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

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.

4.9.11. Otras formas de información de revocación de certificados

UANATACA también 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://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

4.9.12. Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de UANATACA 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 UANATACA, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

4.9.13. Causas de suspensión de certificados

Los certificados de UANATACA pueden ser suspendidos a partir de las siguientes causas:

- Cuando así sea solicitado por el suscriptor o la persona física identificada en el certificado.
- Cuando la documentación requerida en la solicitud de revocación sea suficiente pero no se pueda identificar razonablemente al suscriptor o la persona física identificada en el certificado.

- Cuando la documentación requerida en la solicitud de revocación no sea suficiente, aunque se pueda identificar razonablemente al suscriptor o la persona física identificada en el certificado.
- Cuando la documentación requerida en la solicitud de revocación no sea suficiente y tampoco permitan identificar razonablemente al suscripto o la persona física identificada en el certificado.
- La falta de uso del certificado durante un periodo prolongado de tiempo, conocido previamente.
- Si se sospecha el compromiso de una clave, hasta que éste sea confirmado. En este caso, UANATACA tiene que asegurarse de que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.

4.9.14. Solicitud de suspensión

Pueden solicitar la suspensión del certificado:

- La persona física identificada en el certificado.
- El suscriptor del certificado por medio de representantes autorizados.

4.9.15. Procedimientos para la petición de suspensión

El procedimiento consiste en:

- El usuario accede a un formulario web que se encuentra en la web de UANATACA.
- Una vez rellenado el formulario con su número y letra de DNI/NIE, se envía una contraseña temporal al correo electrónico con el que el usuario solicitó el certificado.
- El usuario debe confirmar con esa contraseña su solicitud de suspensión.
- Una vez confirmada la solicitud, UANATACA procede a la suspensión del certificado.

Se informa al suscriptor y, todo caso, a la persona física identificada en el certificado, acerca del cambio de estado del certificado suspendido.

4.9.16. Período máximo de suspensión

El plazo máximo de suspensión será de una semana.

4.10. Finalización de la suscripción

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

Como excepción, el suscriptor puede mantener el servicio vigente, solicitando la renovación del certificado, con la antelación que determina esta Declaración de Prácticas de Certificación.

UANATACA puede emitir de oficio un nuevo certificado, mientras los suscriptores mantengan dicho estado.

4.11. Servicios de comprobación de estado de certificados

4.11.1. 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.uanataca.com

4.11.2. Disponibilidad de los servicios

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

4.12. Depósito y recuperación de claves

4.12.1. Política y prácticas de depósito y recuperación de claves

UANATACA 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

UANATACA 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 UANATACA, 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.
- Disponibilidad del 99,99%.

UANATACA 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

UANATACA dispone de tres niveles de seguridad física (Entrada del Edificio donde se ubica el CPD, acceso a la sala del CPD y acceso al RAC) para la protección del servicio de generación de certificados, debiendo accederse desde los niveles inferiores a los niveles superiores.

El acceso físico a las dependencias de UANATACA 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 y gestionado por un sistema informático que mantiene un log de entradas y salidas automático.
- Para el acceso al rack donde se ubican los procesos criptográficos es necesario la autorización previa de UANATACA 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 UANATACA 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 UANATACA 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

UANATACA 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

UANATACA 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 UANATACA ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

5.2.1. Funciones fiables

UANATACA 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.
- **Administrador 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 UANATACA. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

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

UANATACA 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 e intermedias.

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.

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.

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

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

En general, UANATACA 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.

UANATACA 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. Por este motivo, previamente se realiza una investigación **hasta donde permita la legislación aplicable**, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales y comprobación que realmente se realizó el trabajo alegado.
- Morosidad.

5.3.2. Procedimientos de investigación de historial

UANATACA, antes de contratar a una persona o de que ésta acceda al puesto de trabajo, realiza las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años
- Referencias profesionales
- Estudios, incluyendo titulación alegada.

UANATACA obtiene el consentimiento inequívoco del afectado para dicha investigación previa, y procesa y protege todos sus datos personales de acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de

desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

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

UANATACA forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.

Los programas de formación son actualizados y mejorados de forma periódica.

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 UANATACA. 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

UANATACA, 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

UANATACA 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 UANATACA. 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 Declaración de Prácticas de Certificación, 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 UANATACA.

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

UANATACA 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.
- 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.

5.4.2. Frecuencia de tratamiento de registros de auditoría

UANATACA 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.

UANATACA 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

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

5.4.4. Protección de los registros de auditoría

Los logs de los sistemas:

- Están protegidos de manipulación 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 solo 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

UANATACA 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.

UANATACA 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 auditoria 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 UANATACA.

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.

5.5. Archivos de informaciones

UANATACA, 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 UANATACA (o por las entidades de registro):

- Todos los datos de auditoría de sistema.
- 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.
- 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.

UANATACA es responsable del correcto archivo de todo este material.

5.5.2. Período de conservación de registros

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

5.5.3. Protección del archivo

UANATACA 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.

UANATACA 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

UANATACA 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 solo a personal autorizado.

UANATACA 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, UANATACA (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.

No es necesario que esta información se encuentre firmada digitalmente.

5.5.6. Localización del sistema de archivo

UANATACA 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

UANATACA 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 caduque, será realizado un cambio de claves. La antigua AC y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por dicha AC. Se generará una nueva AC con una clave privada nueva y un nuevo DN.

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 UANATACA, 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 UANATACA 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 UANATACA.

5.7.3. Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso de UANATACA, 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.

UANATACA 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

UANATACA restablecerá los servicios críticos (suspensión y revocación, y publicación de información de estado de certificados) de acuerdo con el plan de contingencias y continuidad de negocio existente restaurando la operación normal de los servicios anteriores en las 24 horas siguientes al desastre.

UANATACA 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.

5.8. Terminación del servicio

UANATACA 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, mediante su transferencia a un depósito notarial.

Antes de terminar sus servicios, UANATACA desarrolla un plan de terminación, con las siguientes provisiones:

- Proveerá de los fondos necesarios (mediante seguro de responsabilidad civil) para continuar la finalización de las actividades de revocación.
- Informará a todos Firmantes/Suscriptores, Tercero que confían y otras AC's con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 6 meses.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.
- Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios.
- Destruirá o deshabilitará para su uso las claves privadas de la AC.
- Mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos.
- Ejecutará las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros que confían en certificados.
- Comunicará al Ministerio de Industria, Energía y Turismo, com una antelación mínima de 2 meses, 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 Industria, Energía y Turismo, la apertura de cualquier proceso concursal que se siga contra UANATACA así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

6. Controles de seguridad técnica

UANATACA emplea sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

El par de claves de las entidades de certificación intermedias "UANATACA CA1 2016" y "UANATACA CA2 2016" son creadas por la entidad de certificación raíz "UANATACA ROOT 2016" de acuerdo con los procedimientos de ceremonia de UANATACA, 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 UANATACA.

Para la generación de la clave de las entidades de certificación raíz e intermedia se utilizan dispositivos con las certificaciones FIPS 140-2 level 3.

UANATACA ROOT 2016	**4.096 bits**	**25 años**
UANATACA CA1 2016	4.096 bits	13 años
- Certificados de entidad final	2.048 bits	Hasta 3 años*
UANATACA CA2 2016	4.096 bits	13 años
- Certificados de la Unidad de Sello de tiempo	2.048 bits	Hasta 3 años

* Los certificados de entidad final emitidos por UANATACA CA1 2016, tendrán una validez máxima de 3 años, a excepción de los certificados digitales relativos a los perfiles de: a) Empleado Publico emitido en software y dccf y; b) Sello de Órgano Nivel Medio y Alto, los cuales podrán emitirse con una validez máxima de hasta 5 años.
Más información en las siguientes ubicaciones de las PDS:

CERTIFICADO	URLs
De Persona Física en SOFT	http://www.uanataca.com/public/pki/PDS-PFsoft-EN/
De Persona Física en DCCF autenticación	http://www.uanataca.com/public/pki/PDS-PFDCCF-EN/
De Persona Física en DCCF firma	
De Persona Física en DCCF cifrado	
De REPRESENTANTE en SOFT	http://www.uanataca.com/public/pki/PDS-REPsoft-EN/
De REPRESENTANTE en DCCF identificación	http://www.uanataca.com/public/pki/PDS-REPDCCF-EN/
De REPRESENTANTE en DCCF firma	
De REPRESENTANTE en DCCF cifrado	
De persona física representante ante las Administraciones de Persona Jurídica emitido en SOFT	https://www.uanataca.com/public/pki/PDS-REPafirma-soft-ES/
De persona física representante ante las Administraciones de Persona Jurídica emitido en DCCF identificación	https://www.uanataca.com/public/pki/PDS-REPafirma-DCCF-ES/
De persona física representante ante las Administraciones de Persona Jurídica emitido en DCCF firma	
De persona física representante ante las Administraciones de Persona Jurídica emitido en DCCF cifrado	
De persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica emitido en SOFT	
De persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica emitido en DCCF identificación	

De persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica emitido en DCCF firma	
De persona física representante ante las Administraciones de Entidad sin Personalidad Jurídica emitido en DCCF cifrado	
De Empleado Público nivel Medio	http://www.uanataca.com/public/pki/PDS-EPmedio-EN/
De Empleado Público nivel Alto (identificación)	http://www.uanataca.com/public/pki/PDS-EPalto-EN/
De Empleado Público nivel Alto (firma)	
De Empleado Público nivel Alto (cifrado)	
De Unidad de Sello de Tiempo	http://www.uanataca.com/public/pki/TSA-DS/

6.1.1.1. Generación del par de claves del firmante

Las claves del firmante pueden ser creadas por él mismo mediante dispositivos hardware o software autorizados por UANATACA.
UANATACA puede crear las claves únicamente por medio de un DCCF o en un HSM para su importación posterior a un DCCF.
UANATACA nunca genera claves en software para ser enviadas al firmante.

Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

6.1.2. Envío de la clave privada al firmante

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

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 en este caso no existe envío de clave privada.

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 UANATACA.

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

Las claves de UANATACA 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 UANATACA.

6.1.5. Tamaños de claves

La longitud de las claves de la Entidad de Certificación raíz es de 4096 bits.

La longitud de las claves de la Entidad de Certificación subordinada es de 4096 bits.

Las claves de los certificados de entidad final son de 2048 bits.

6.1.6. Generación de parámetros de clave pública

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.

6.1.7. Comprobación de calidad de parámetros de clave pública

- Longitud del Módulo = 4096
- Algoritmo de generación de claves: rsagen1
- Funciones criptográficas de Resumen: SHA256.

6.1.8. Generación de claves en aplicaciones informáticas o en bienes de equipo

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

6.1.9. 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

6.2.1. Estándares de módulos criptográficos

En relación a los módulos que gestionan claves de UANATACA 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. En el caso de esta Declaración de Prácticas de Certificación, en concreto existe una política de **3 de 6** personas para la activación de las claves.

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

6.2.3. Depósito de la clave privada

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

6.2.4. Copia de respaldo de la clave privada

UANATACA 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 suscriptor en software pueden ser almacenadas para su posible recuperación en caso de contingencia, en un dispositivo de almacenamiento externo separado de la clave de instalación.

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 **10 años** después de la emisión del último certificado. Se almacenarán en archivos ignífugos seguros y en el centro de custodia externo. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de las AC en el dispositivo criptográfico inicial.
Solo en caso de certificados de cifrado, el suscriptor podrá almacenar la clave privada el tiempo que crea oportuno. En este caso UANATACA también guardará copia de la clave privada asociada al certificado de cifrado.

UANATACA no genera ni archiva claves de certificados, emitidas en software.

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 UANATACA.

6.2.7. Método de activación de la clave privada

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

6.2.8. Método de desactivación de la clave privada

La clave privada de UANATACA 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 (3 de 6)

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 destrucción de la clave privada

Para la desactivación de la clave privada de UANATACA 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. Clasificación de módulos criptográficos

Con anterioridad a la destrucción de las claves, se emitirá una revocación del 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 UANATACA. 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 UANATACA.

6.2.11. Clasificación de módulos criptográficos

Ver la sección 6.2.1

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

UANATACA 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.

Como excepción, la clave privada de descifrado puede continuar empleándose incluso tras la expiración del certificado.

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 UANATACA 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, UANATACA 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.

6.5. Controles de seguridad informática

UANATACA emplea sistemas fiables para ofrecer sus servicios de certificación. UANATACA ha realizado controles y auditorias 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.

Respecto a la seguridad de la información, UANATACA aplica los controles del esquema de certificación sobre sistemas de gestión de la información ISO 27001.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de UANATACA, 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 trafico de red.

6.5.1. Requisitos técnicos específicos de seguridad informática

Cada servidor de UANATACA 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 auditoria.
- Auditoria 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.

6.5.2. Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas por UANATACA 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 UNATACA 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

UANATACA 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.

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

6.6.2.1. Clasificación y gestión de información y bienes

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

La política de seguridad de UANATACA detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: SIN CLASIFICAR, USO INTERNO y CONFIDENCIAL.

6.6.2.2. Operaciones de gestión

UANATACA 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.

En el documento de seguridad de UANATACA se desarrolla en detalle el proceso de gestión de incidencias.

UANATACA 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.

6.6.2.3. 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 UANATACA 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

UANATACA dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

Procedimientos operacionales y responsabilidades

UANATACA 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.

6.6.2.4. Gestión del sistema de acceso

UANATACA 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.
- UANATACA dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- UANATACA 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 UANATACA 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 UANATACA.

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 UANATACA.

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.

6.6.2.5. Gestión del ciclo de vida del hardware criptográfico

UANATACA 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.

UANATACA 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.

UANATACA 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 UANATACA almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

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

UANATACA 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

UANATACA 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 trasfiere 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. Controles de ingeniería de módulos criptográficos

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 UANATACA son realizadas en módulos con las certificaciones FIPS 140-2 nivel 3.

6.9. Fuentes de Tiempo

UANATACA tiene un procedimiento de sincronización de tiempo coordinado vía NTP.

7. Perfiles de certificados y listas de certificados revocados

7.1. Perfil de certificado

Todos los certificados cualificados emitidos bajo esta política cumplen el estándar X.509 versión 3, RFC 3739 y ETSI 101 862 "Qualified Certificate Profile".

7.1.1. Número de versión

UANATACA 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 UANATACA (https://www.uanataca.com).

De esta forma se permite mantener unas versiones más estables de la Declaración de Prácticas de Certificación y desligarlos de los frecuentes ajustes en los perfiles.

7.1.3. Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública es:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4. Formato de Nombres

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

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

7.2. Perfil de la lista de revocación de certificados

7.2.1. Número de versión

Las CRL emitidas por UANATACA son de la versión 2.

7.2.2. Perfil de OCSP

Según el estándar IETF RFC 6960.

8. Auditoría de conformidad

UANATACA ha comunicado el inicio de su actividad como prestador de servicios de certificación por el Ministerio de Industria y se encuentra sometida a las revisiones de control que este organismo considere necesarias.

8.1. Frecuencia de la auditoría de conformidad

UANATACA 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.

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 UANATACA.

8.4. Listado de elementos objeto de auditoría

La auditoría verifica respecto a UANATACA:

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 Declaración de Prácticas de Certificación y otra documentación vinculada con la emisión de los distintos certificados digitales.
c) Que la Declaración de Prácticas de Certificación y demás documentación jurídica vinculada, se ajusta a lo acordado por UANATACA 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 las medidas correctivas que solventen dichas deficiencias.

Si la UANATACA es incapaz de desarrollar y/o ejecutar las medidas correctivas o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicarlo inmediatamente al Comité de Seguridad de UANATACA 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 al Comité de Seguridad de UANATACA 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

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

9.1.2. Tarifa de acceso a certificados

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

9.1.3. Tarifa de acceso a información de estado de certificado

UANATACA 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. Capacidad financiera

UANATACA 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 319 401-1 7.12 c), en relación a la gestión de la finalización de los servicios y plan de cese.

9.2.1. Cobertura de seguro

UANATACA 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 artículo 20.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, 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

UANATACA 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 artículo 20.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, con un mínimo asegurado de 3.000.000 de euros.

9.3. Confidencialidad

9.3.1. Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales por UANATACA:

- 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, 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 (LRCs), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- 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

UANATACA 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 serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

UANATACA 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

UANATACA 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. Protección de datos personales

UANATACA se obliga a cumplir la normativa sobre protección de datos de carácter personal, con las medidas de seguridad correspondientes según se relaciona en la Ley Orgánica 15/1999 de Protección de Datos Personales, y en el Real Decreto 1720/2007 de desarrollo de la citada Ley.

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

UANATACA tiene la condición de encargado del tratamiento en tanto que no decide sobre la finalidad, contenido y uso del tratamiento de dichos datos de carácter personal, mientras que el SUSCRIPTOR es el responsable del fichero.

UANATACA utilizará los datos contenidos en sus ficheros, única y exclusivamente para los fines que figuran en esta Declaración de Prácticas de Certificación.

Asimismo, UANATACA ha desarrollado una política de privacidad, de acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y ha documentado en esta Declaración de Prácticas de Certificación los aspectos y procedimientos de seguridad correspondientes al documento de seguridad en cumplimiento de lo previsto en el artículo 19.3 de Ley 59/2003, de 19 de diciembre, de firma electrónica, y los artículos 82 y 88 del Real Decreto Real Decreto 1720/2007, de 21 de diciembre, por el cual se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de trece de diciembre de 1999, de protección de datos de carácter personal. Esta Declaración de Prácticas de Certificación tiene, por tanto, la consideración de documento de seguridad.

UANATACA 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.

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 cumplen las obligaciones previstas en el Real Decreto 1720/2007, de 21 de diciembre, por el cual se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de trece de diciembre de 1999, de protección de datos de carácter personal.

9.5. Derechos de propiedad intelectual

9.5.1. Propiedad de los certificados e información de revocación

Únicamente UANATACA 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 UANATACA 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 UANATACA 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 suscriptores 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 UANATACA

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

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

Con anterioridad a la emisión y entrega del certificado al suscriptor, UANATACA 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[13], cumple el contenido del anexo A de la ETSI EN 319 411-1 v1.1.1 (2016-02), documento el cual puede ser transmitido por medios electrónicos, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

UANATACA 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 la publicación del certificado en el depósito y acceso por terceros al mismo.
- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor y para la cesión de dicha información a terceros, en caso

[13] "PKI Disclosure Statement", o declaración de divulgación de PKI aplicable.

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. Garantías ofrecidas a suscriptores y terceros que confían en certificados

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

UANATACA, 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.

UANATACA, 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.
- En caso de certificados publicados en el Depósito, que el certificado ha sido emitido al suscriptor identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 4.4
- 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 y Depósito.

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

- Que el certificado contiene las informaciones que debe contener un certificado cualificados, de acuerdo con el artículo 11 de la Ley 59/2003, de 19 de diciembre.
- 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.

9.6.3. Rechazo de otras garantías

UANATACA rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 9.6.2.

9.6.4. Limitación de responsabilidades

UANATACA limita su responsabilidad a la emisión y gestión de certificados y de pares de claves de suscriptores suministrados por la Entidad de Certificación.

9.6.5. Cláusulas de indemnidad

9.6.5.1. Cláusula de indemnidad de suscriptor

UANATACA 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 domino), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

9.6.5.2. Cláusula de indemnidad de tercero que confía en el certificado

UANATACA 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.

9.6.6. Caso fortuito y fuerza mayor

UANATACA incluye en el texto de divulgación o PDS, cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

9.6.7. Ley aplicable

UANATACA 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.

9.6.8. Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

UANATACA 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.

9.6.9. Cláusula de jurisdicción competente

UANATACA establece, en el contrato de suscriptor y en el texto de divulgación o PDS, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles.

La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

9.6.10. Resolución de conflictos

UANATACA establece, en el contrato de suscriptor, y en el texto de divulgación o PDS, los procedimientos de mediación y resolución de conflictos aplicables.