DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Información general

Control documental

Clasificación de seguridad:	Público
Versión:	1.0
Fecha edición:	18/03/2024
Fichero:	**PSC-1-DPC_CER_UCO_v1.r1**
Código	**PSC-1-**

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Alejandro Grande Fecha: 18/03/2024	Nombre: Fabiola Ortega Fecha: 20/4/2024	Nombre: Elias Barzallo Fecha: 08/8/2024

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	Alejandro Grande	18/03/2024

Índice

1 Introducción 11
1.1 Presentación 11
1.2 Nombre del documento e identificación 14
1.5.1 Organización que administra el documento 39
1.5.2 Datos de contacto de la organización 39
1.5.3 Procedimientos de gestión del documento 39
2 Publicación de información y depósito de certificados 40
2.1 Depósito(s) de certificados 40
2.2 Publicación de información del proveedor de servicios de certificación 40
2.3 Frecuencia de publicación 40
2.4 Control de acceso 41
3 Identificación y autenticación 42
3.1 Registro inicial 42
3.1.1 Tipos de nombres 42
3.1.2 Significado de los nombres 49
3.1.3 Emisión de certificados del set de pruebas y certificados de pruebas en general 49
3.1.4 Empleo de anónimos y seudónimos 49
3.1.5 Interpretación de formatos de nombres 49
3.1.6 Unicidad de los nombres 50
3.1.7 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 Validación de la Identidad 52
3.2.3 Autenticación de la identidad de una persona jurídica (organización, empresa o entidad) 52
3.2.4 Autenticación de la identidad de una Persona natural 55
3.2.5 Información de suscriptor no verificada 58
3.2.6 Autenticación de la identidad de una RA y sus operadores 58

3.3 Identificación y autenticación de solicitudes de renovación 58
3.4 Modificación del certificado 59
3.5 Identificación y autenticación de la solicitud de revocación y/o suspensión 59
4 Requisitos de operación del ciclo de vida de los certificados 61
4.1 Solicitud de emisión de certificado 61
4.1.1 Legitimación para solicitar la emisión 61
4.1.2 Procedimiento de alta y responsabilidades 61
4.2 Procesamiento de la solicitud de certificación 62
4.2.1 Ejecución de las funciones de identificación y autenticación 62
4.2.2 Aprobación o rechazo de la solicitud 62
4.2.3 Plazo para resolver la solicitud 63
4.3 Emisión del certificado 64
4.3.1 Acciones de la ECD, durante el proceso de emisión 64
4.3.2 Notificación de la emisión al suscriptor 64
4.4 Entrega y aceptación del certificado 65
4.4.1 Responsabilidades de la ECD 65
4.4.2 Conducta que constituye aceptación del certificado 66
4.4.3 Publicación del certificado 66
4.4.4 Notificación de la emisión a terceros 66
4.5 Uso del par de claves y del certificado 66
4.5.1 Uso por el firmante 66
4.5.2 Uso por el subscriptor 68
4.5.3 Uso por el tercero que confía en certificados 69
4.6 Renovación de certificados 70
4.7 Modificación de Certificados 71
4.8 Revocación y suspensión de certificados 71
4.8.1 Causas de revocación de certificados 71
4.8.2 Causas de suspensión de un certificado 74
4.8.3 Causas de reactivación de un certificado 74
4.8.4 Quién puede solicitar la revocación 74
4.8.5 Procedimientos de solicitud de revocación 74
4.8.6 Plazo temporal de solicitud de revocación 75

4.8.7 Plazo temporal de procesamiento de la solicitud de revocación 75
4.8.8 Obligación de consulta de información de revocación de certificados 75
4.8.9 Frecuencia de emisión de listas de revocación de certificados (CRLs) y (ARLs) 76
4.8.10 Plazo máximo de publicación de CRLs 76
4.8.11 Disponibilidad de servicios de comprobación en línea de estado de certificados 76
4.8.12 Obligación de consulta de servicios de comprobación de estado de certificados 77
4.8.13 Requisitos especiales en caso de compromiso de la clave privada 77
4.9 Finalización de la suscripción 77
4.10 Depósito y recuperación de claves 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 80
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 81
5.1.8 Copia de respaldo fuera de las instalaciones 81
5.2 Controles de procedimientos 82
5.2.1 Funciones (Roles) fiables 82
5.2.2 Número de personas por tarea 83
5.2.3 Identificación y autenticación para cada función 84
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 85
5.3.2 Procedimientos de investigación de historial 86
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 87
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 89
5.4.4 Protección de los registros de auditoría 89
5.4.5 Procedimientos de copia de respaldo 90
5.4.6 Localización del sistema de acumulación de registros de auditoría 90
5.4.7 Notificación del evento de auditoría al causante del evento 90
5.4.8 Análisis de vulnerabilidades 90
5.5 Archivos de informaciones 91
5.5.1 Tipos de registros archivados 91
5.5.2 Periodo de Conservación de registros 91
5.5.3 Protección del archivo 92
5.5.4 Procedimientos de copia de respaldo 92
5.5.5 Requisitos de sellado de fecha y hora 92
5.5.6 Localización del sistema de archivo 92
5.5.7 Procedimientos de obtención y verificación de información de archivo 93
5.6 Renovación de claves 93
5.7 Compromiso de claves y recuperación de desastre 93
5.7.1 Procedimientos de gestión de incidencias y compromisos 93
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 94
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
6.1.2 Entrega (envío) de la clave privada al firmante 98
6.1.3 Entrega (envío) de la clave pública al emisor del certificado 99
6.1.4 Distribución de la clave pública de la ECD 99

6.1.5 Tamaños de claves 99
6.1.6 Generación de parámetros de clave pública 99
6.1.7 Comprobación de calidad de parámetros de clave pública 99
6.1.8 Generación de claves en aplicaciones informáticas o en bienes de equipo 99
6.1.9 Propósitos de uso de claves (Campo Key Usage de X.509V3) 100
6.2 Protección de la clave privada 100
6.2.1 Estándares de módulos criptográficos 100
6.2.2 Control por más de una persona (n de m) sobre la clave privada 100
6.2.3 Depósito de la clave privada 101
6.2.4 Copia de respaldo de la clave privada 101
6.2.5 Archivo de la clave privada 102
6.2.6 Introducción (trasferencia) de la clave privada en el módulo criptográfico 102
6.2.7 Método de activación de la clave privada 102
6.2.8 Método de desactivación de la clave privada 102
6.2.9 Método de destrucción de la clave privada 103
6.2.10 Clasificación de módulos criptográficos 103
6.3 Otros aspectos de gestión del par de claves 103
6.3.1 Archivo de la clave pública 103
6.3.2 Períodos de utilización de las claves pública y privada 103
6.4 Datos de activación 104
6.4.1 Generación e instalación de datos de activación 104
6.4.2 Protección de datos de activación 104
6.5 Controles de seguridad informática 104
6.5.1 Requisitos técnicos específicos de seguridad informática 105
6.5.2 Evaluación del nivel de seguridad informática 105
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 106
6.6.3 Clasificación y gestión de información y bienes 106
6.6.4 Operaciones de gestión 106
6.6.5 Tratamiento de los soportes y seguridad 107
6.7 Gestión del sistema de acceso 107

6.8 Gestión del ciclo de vida del hardware criptográfico 108
6.9 Controles de seguridad de red 108
6.10 Controles de ingeniería de módulos criptográficos 109
6.11 Fuentes de Tiempo 109
6.12 Cambio de estado de un Dispositivo Seguro de Creación de Firma (SSCD) 109
7. Perfiles de certificados y listas de certificados revocados 111
7.1 Perfil de certificado 111
7.1.1 Número de versión 111
7.1.2 Extensiones del certificado 111
7.1.3 Identificadores de objeto (OID) de los algoritmos 111
7.1.4 Formato de Nombres 111
7.1.5 Restricción de los nombres 112
7.1.6 Identificador de objeto (OID) de los tipos de certificados 112
7.2 Perfil de la lista de revocación de certificados (CRL) 112
7.2.1 Número de versión 112
7.2.2 Perfil de OCSP 112
8. Auditoría de conformidad 113
8.1 Frecuencia de la auditoría de conformidad 113
8.2 Identificación y calificación del auditor 113
8.3 Relación del auditor con la entidad auditada 113
8.4 Listado de elementos objeto de auditoría 113
8.5 Acciones a emprender como resultado de una falta de conformidad 114
8.6 Tratamiento de los informes de auditoría 114
9. Requisitos comerciales y legales 115
9.1 Tarifas 115
9.1.1 Tarifa de emisión o renovación de certificados 115
9.1.2 Tarifa de acceso a los certificados 115
9.1.3 Tarifa de revocación o acceso a la información de estado 115
9.1.4 Tarifas de otros servicios 115
9.1.5 Política de reintegro 115
9.2 Capacidad financiera 115
9.2.1 Cobertura 116

9.2.2 Otros activos 116
9.2.3 Cobertura para terceros que confían en certificados 116
9.3 Confidencialidad 117
9.3.1 Informaciones confidenciales 117
9.3.2 Informaciones no confidenciales 117
9.3.3 Divulgación de información de suspensión y revocación 118
9.3.4 Divulgación legal de información 118
9.3.5 Divulgación de información por petición de su titular 118
9.3.6 Otras circunstancias de divulgación de información 118
9.4 Protección de datos personales 118
9.5 Derechos de propiedad intelectual 123
9.5.1 Propiedad de los certificados e información de revocación 123
9.5.2 Propiedad de la información relativa a nombres 124
9.5.3 Propiedad de claves 124
9.6 Obligaciones y responsabilidad civil 124
9.6.1 Obligaciones de UANATACA COLOMBIA 124
9.6.2 Obligaciones de los Proveedores 126
9.6.3 Garantías ofrecidas a suscriptores y terceros que confían en certificados 127
9.6.4 Rechazo de otras garantías 128
9.6.5 Limitación de responsabilidades 128
9.6.6 Indemnización y Cláusulas de indemnidad 129
9.6.6.1 Cláusula de indemnidad de suscriptor 129
9.6.7 Caso fortuito y fuerza mayor 130
9.7 Legislación 130
9.7.1 Ley aplicable 130
9.7.2 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación 130
9.7.3 Cláusula de jurisdicción competente 131
9.7.4 PQRS – Disputas 131
9.7.5 Resolución de conflictos 131
9.8 CLÁUSULA DE ACEPTACIÓN COMPLETA 132
9.9 Otras estipulaciones 132
Anexo I - Acrónimos 133
Anexo 2 – Modelo de contrato de suscripción 134

1 Introducción

1.1 Presentación

Este documento declara las prácticas de certificación para la emisión de certificados digitales de Uanataca Colombia, S.A.S, en adelante "*UANATACA COLOMBIA*", dando cumplimiento a lo previsto en la Ley 527 de 1999, Decreto Ley 019 de 2012 y demás normas y decretos reglamentarios aplicables a la prestación de servicios de certificación digital. Así como de los requisitos contenidos en la *CEA-3.0-07 Criterios Específicos De Acreditación Entidades De Certificación Digital* –vigente y establecido por el Organismo Nacional de Acreditación de Colombia – ONAC para la prestación de servicios de certificación digital.

El presente documento es de carácter público y se encuentra dirigido a todas las personas naturales y jurídicas, suscriptores, firmantes, usuarios, terceros que confían y público en general.

Los certificados digitales en relación con las firmas electrónicas o digitales que se emiten serán conforme a lo siguiente:

- **De Persona natural:** El certificado digital de persona natural sirve para identificar a una persona natural, que permite su uso y firma para realizar todo tipo de trámites como Persona Natural sin vinculación a ninguna empresa o entidad.
    - Certificado de Persona Natural en tarjeta o token
    - Certificado de Persona Natural en HSM centralizado

- **De Profesional titulado:** Son certificados que permiten identificar al suscriptor y su título profesional y le permite al Suscriptor firmar en su propio nombre e interés.
    - Certificado Profesional titulado en tarjeta o token
    - Certificado de Profesional titulado en HSM centralizado

- **De Persona Natural - Miembro de Empresa u organización**: Son certificados que permiten identificar al Suscriptor y firmante, este último también podrá firmar como Persona Natural vinculada a una empresa o entidad (persona jurídica), ya sea como empleado, asociado, colaborador, cliente, etc.

- Certificado de persona natural miembro de Empresa en tarjeta o token
- Certificado de persona natural miembro de Empresa en HSM Centralizado

- **De Representante:** Son certificados que permiten identificar y firmar como Persona Natural vinculada a una empresa o entidad (Persona Jurídica), como su representante legal. Por lo que el titular del certificado se identifica no únicamente como persona física, sino que añade su cualificación como representante legal o apoderado de la misma.

  - Certificado de Representante en tarjeta o token
  - Certificado de Representante en HSM centralizado

- **De Función Pública:** Son certificados emitidos a una Persona Natural vinculada al servicio de la Administración Pública y se identifica en su condición de funcionario público o de particular en ejercicio de una función pública. En concreto, el certificado identifica al funcionario público o de particular en ejercicio de una función pública, la identidad de la entidad pública y la vinculación que la persona natural tiene con esta. Solamente, otorgará a su titular las facultades que posee por el desempeño de sus competencias, de su trabajo o de los servicios prestados para la entidad pública correspondiente. Este certificado contiene en sus campos la referencia al cargo o puesto y al área o unidad de destino, pero no informa acerca de la existencia de poderes de representación.

  - Certificado de Función Pública en tarjeta o token
  - Certificado de Función Pública en HSM centralizado

- **De Persona jurídica – sello de empresa:** Se trata de un certificado digital emitido a favor de una Persona jurídica (entidad, empresa, etc.) y podrá ser utilizado en la identificación, autenticación y gestión concerniente dentro del giro normal de sus negocios.

  - Certificado de Persona Jurídica Sello Electrónico en tarjeta o token
  - Certificado de Persona Jurídica Sello Electrónico en HSM centralizado

- **De facturación electrónica:** Se trata de un certificado digital emitido a favor de una Persona jurídica (entidad, empresa, etc.) o natural para realizar la facturación electrónica atendiendo la necesidad de las empresas y/o personas naturales que buscan la seguridad del certificado para la emisión de las facturas electrónicas, entre otros documentos y podrá ser utilizado en la identificación, autenticación y gestión concerniente dentro del giro normal de sus negocios.

    - Certificado para Facturación Electrónica de Persona Natural en tarjeta o token.
    - Certificado para Facturación Electrónica de Persona Natural en HSM centralizado.
    - Certificado para Facturación Electrónica de Persona Jurídica en tarjeta o token
    - Certificado para Facturación Electrónica de Persona Jurídica en HSM centralizado.

- **De Sello de Tiempo:** Se tratan de certificados emitidos para la operación de autoridades de sellado de tiempo y hora, para la firma de los sellos de tiempo que éstas producen. Certifica la fecha y hora exacta en las que se produjo la firma del documento tomando la referencia horaria en la República de Colombia.

    - Certificado de Estampado Cronológico (sello de tiempo)

1.2 Nombre del documento e identificación

Este documento es la "*Declaración de Prácticas de Certificación de UANATACA COLOMBIA*" identificándose a los efectos bajo el ***OID 1.3.6.1.4.1.47286.201.0.1.***

1.2.1 Identificadores de certificados

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

Número OID	Tipo de certificados
1.3.6.1.4.1.47286.201.1.1	**Persona Natural**
1.3.6.1.4.1.47286.201.1.1.1	*Certificado de Persona Natural ciudadano en tarjeta o token*
1.3.6.1.4.1.47286. 201.1.1.2	*Certificado de Persona Natural ciudadano en HSM centralizado*
1.3.6.1.4.1.47286.201.1.2	**Profesional titulado**
1.3.6.1.4.1.47286.201.1.2.1	*Certificado de persona natural profesional titulado en tarjeta o token*
1.3.6.1.4.1.47286.201.1.2.2	*Certificado de persona natural profesional titulado en HSM centralizado*
1.3.6.1.4.1.47286.201.1.3	**Persona Natural - Miembro de Empresa u organización**
1.3.6.1.4.1.47286.201.1.3.1	*Certificado de Persona Natural miembro de Empresa u organización en tarjeta o token*
1.3.6.1.4.1.47286.201.1.3.2	*Certificado de Persona Natural miembro de Empresa u organización en HSM Centralizado*
1.3.6.1.4.1.47286.201.1.4	**Persona Natural Representante de Persona Jurídica**
1.3.6.1.4.1.47286.201.1.4.1	*Certificado de Persona Natural Representante de Persona Jurídica en tarjeta o token*
1.3.6.1.4.1.47286.201.1.4.2	*Certificado de Persona Natural Representante de Persona Jurídica en HSM centralizado*
1.3.6.1.4.1.47286.201.1.6	**De función Pública**
1.3.6.1.4.1.47286.201.1.6.1	*Certificado de Persona Natural Función Pública en tarjeta o token*
1.3.6.1.4.1.47286.201.1.6.2	*Certificado de Persona Natural Función Pública en HSM centralizado*
1.3.6.1.4.1.47286.201.1.7	**Persona Jurídica - Sello De Empresa**
1.3.6.1.4.1.47286.201.1.7.1	*Certificado de Sello Electrónico en tarjeta o token*
1.3.6.1.4.1.47286.201.1.7.2	*Certificado de Sello Electrónico en HSM Centralizado*
1.3.6.1.4.1.47286.201.1.8	**Persona Natural - Facturación Electrónica**
1.3.6.1.4.1.47286.201.1.8.1	*Certificado para Facturación Electrónica de Persona Natural en tarjeta o token*
1.3.6.1.4.1.47286.201.1.8.2	*Certificado para Facturación Electrónica de Persona Natural en HSM centralizado*

1.3.6.1.4.1.47286.201.1.9	**Persona Jurídica - Facturación Electrónica**
1.3.6.1.4.1.47286.201.1.9.1	*Certificado para Facturación Electrónica de Persona Jurídica en tarjeta o token*
1.3.6.1.4.1.47286.201.1.9.2	*Certificado para Facturación Electrónica de Persona Jurídica en HSM CENTRALIZADO*
1.3.6.1.4.1.47286.201.1.10	**Estampado Cronológico** *(De sello 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 Entidad de Certificación Digital

La Entidad de Certificación Digital o indistintamente el Proveedor de Servicios electrónicos de certificación es la persona autorizada y facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

UANATACA COLOMBIA en su papel de Entidad de Certificación Digital (ECD) abierta, es la persona jurídica privada que presta indistintamente en el país servicios y actividades inherentes a la certificación digital, que actúa de acuerdo con la legislación de Colombia, conformada por la Ley 527 de 1999, el Decreto Ley No. 019 de 2012, Decreto Único del Sector Comercio, Industria y Turismo – DURCSIT, 1074 de 2015, así como las normas técnicas del ETSI aplicables a la expedición y gestión de certificados principalmente, EN 319 401, EN 319 411-1 y EN 319 412, y los mejores estándares internacionales, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

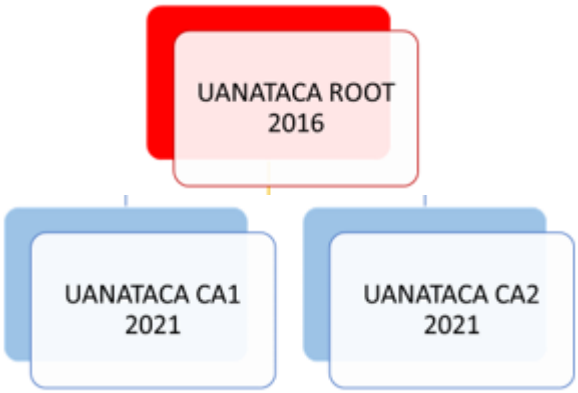
UANATACA COLOMBIA, le corresponderá la realización de todos los trámites y procedimientos administrativos necesarios ante el ONAC, a fin de lograr y mantener la acreditación correspondiente.

Asimismo, UANATACA COLOMBIA, en su papel de autoridad de certificación, emite y revoca los certificados, presta los servicios de comprobación de revocación mediante CRL (*Certificate Revocation List*) y OCSP (*Online Certificate Status Protocol*).

Es de resaltar que UANATACA COLOMBIA y su correspondiente jerarquía de certificación asociada en esta Declaración de Prácticas (DPC) seguirá lo indicado en este documento.

Asimismo, en aquellos aspectos en los que UANATACA COLOMBIA emplee un proveedor de servicios de certificación, se entenderá que las obligaciones derivadas como Autoridad de Certificación también le serán aplicables a dicho proveedor a través del acuerdo contractual suscrito entre ambas partes.

Para la prestación de los servicios de certificación, UANATACA COLOMBIA 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 pública ha sido auto firmado. Su función es firmar el certificado de las otras CA pertenecientes a la Jerarquía de Certificación.

Asimismo, la CA Raíz de UANATACA podrá emitir certificados de otras CA Subordinadas del grupo y/o que sea de su interés, lo cual quedará reflejado en las correspondientes DPC de estas CA Subordinadas. Por tanto, UANATACA ROOT 2016 también podrá ser la CA Raíz de otras PKI del grupo y/o aquellas en las que persiga algún interés particular.

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 2021

Se trata de la Autoridad de Certificación Subordinada (CA Sub) dentro de la jerarquía que emite los certificados a las entidades finales y los certificados de estampado cronológico (sellado de tiempo), y cuyo certificado de clave pública ha sido firmado digitalmente por UANATACA ROOT 2016.

Datos de identificación:

CN:	UANATACA CA1 2021
Huella digital:	a1 db ea 6c 10 7a a3 e8 1e 16 c9 af 8e 55 7f ed 3d 90 cf 98
Válido desde:	jueves, 3 de junio de 2021
Válido hasta:	sábado, 3 de junio de 2034
Longitud de clave RSA:	4.096 bits

1.3.1.3 UANATACA CA2 2021

Se trata de la entidad de certificación Subordinada (CA Sub) dentro de la jerarquía que emite los certificados a las entidades finales y los certificados de estampado cronológico (sellado de tiempo), y cuyo certificado de clave pública ha sido firmado digitalmente por UANATACA ROOT 2016.

Datos de identificación:

CN:	UANATACA CA2 2021
Huella digital:	2d 35 17 27 f4 5b 01 2a a4 88 03 4b db 01 1c da 4f 61 a4 2e
Válido desde:	jueves, 3 de junio de 2021
Válido hasta:	sábado, 3 de junio de 2034
Longitud de clave RSA:	4.096 bits

1.3.2 Autoridad de Registro

La Autoridad de Registro (RA) son las encargadas de recibir las solicitudes relacionadas con certificación digital, para registrar las peticiones que hagan los solicitantes para obtener un certificado, comprobar la veracidad y corrección de los datos que aportan los usuarios en las peticiones, enviar las peticiones que cumplen los requisitos a una CA para que sean procesadas.

Una Autoridad de Registro (RA) de UANATACA COLOMBIA es la entidad encargada de:

- Tramitar las solicitudes de certificados.
- Identificar al solicitante y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados.
- Validar las circunstancias personales de la persona que constará como firmante del certificado.
- Gestionar la generación de claves y la emisión del certificado
- Hacer entrega del certificado al suscriptor o de los medios para su generación.
- Custodiar la documentación relativa a la identificación y registro de los firmantes y/o suscriptores y gestión del ciclo de vida de los certificados.

Teniendo en cuenta las funciones de la RA, UANATACA COLOMBIA formalizará contractualmente las relaciones entre ella misma y cada una de las entidades que actúen como Autoridad de Registro de UANATACA COLOMBIA garantizando que las funciones de comprobación de veracidad, y corrección de datos que aportan los usuarios, así como el envío a una CA de las peticiones cumplen con los requisitos exigidos en la CEA-3.0-07 siendo responsable total de las actividades realizadas por terceros debido a que mantiene como función propia de UANATACA COLOMBIA

Podrán actuar como RA de UANATACA COLOMBIA:

- Cualquier entidad autorizada por UANATACA COLOMBIA.
- UANATACA COLOMBIA directamente.

La entidad que actúe como Autoridad de Registro de UANATACA COLOMBIA podrá autorizar a una o varias personas como Operador de la RA para operar con el sistema de emisión de certificados de UANATACA COLOMBIA en nombre de la Autoridad de Registro.

La Autoridad de Registro podrá delegar las funciones de identificación de los suscriptores y/o firmantes, previo acuerdo de colaboración en el que se acepte la delegación de estas funciones. UANATACA COLOMBIA deberá autorizar de manera expresa dicho acuerdo de colaboración.

También podrán ser Autoridades de Registro sujetas a esta Declaración de Prácticas de Certificación de UANATACA COLOMBIA, 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.

1.3.3 Entidades finales

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

Serán entidades finales de los servicios de certificación de UANATACA COLOMBIA las siguientes:

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

1.3.3.1 Suscriptores del servicio de certificación

A la persona a cuyo nombre la Entidad de Certificación Digital UANATACA COLOMBIA expide un certificado digital, se le conoce como el suscriptor del servicio de certificación.

A los efectos, pueden ser las personas naturales, empresas, entidades, corporaciones u organizaciones (directamente o a través de un tercero) que desplegará su uso en el ámbito personal, corporativo empresarial u organizativo, entre otros usos, los cuales se encuentran debidamente identificados en los certificados.

El suscriptor del servicio de certificación adquiere una licencia de uso del certificado, para su uso propio 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. En este último caso, esta persona figura identificada en el certificado.

El suscriptor del servicio de certificación digital es, por tanto, el cliente de la entidad de certificación digital (ECD), de acuerdo con la legislación privada, y tiene los derechos y obligaciones que se definen por la entidad de certificación digital, 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 aplicables a la expedición de certificados digitales, en especial ETSI EN 319 411.

1.3.3.2 Firmantes

Los firmantes son las personas naturales que poseen de forma exclusiva las claves de firma para autenticación y/o firma digital; siendo típicamente los empleados, representantes legales o voluntarios, así como otras personas vinculadas a los suscriptores; incluyendo las personas al servicio de la Administración, en los certificados de función pública.

Los firmantes se encuentran debidamente autorizados por el suscriptor y debidamente identificados en el certificado mediante su nombre y apellidos, y número de identificación inequívoco, así como todos aquellos datos exigidos por la ley, sin que sea posible, en general, el empleo de seudónimos.

La clave privada de un firmante no puede ser recuperada o deducida por la Entidad de certificación digital, por lo que las personas naturales 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 digital según corresponda, como la autenticación, también se emplea el término más genérico de "Persona natural identificada en el certificado", siempre con pleno respeto al cumplimiento de la regulación de firma digital 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 a través de certificados digitales.

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, dicha comprobación, se realiza a través del acceso a las listas de revocación (CRL) o a servicios de consulta en línea (OCSP) tal y como se establece, en esta declaración de prácticas de certificación y en las correspondientes instrucciones disponibles en la página web de la Autoridad de Certificación.

1.3.4 Proveedor de Servicios de Infraestructura de Clave Pública

Los proveedores de Servicios de Infraestructura de Clave Pública son terceros que prestan su infraestructura y/o servicios tecnológicos a la Entidad de Certificación Digital (ECD) para el óptimo desarrollo de sus operaciones, a su vez, garantizan la continuidad del servicio a las entidades finales, suscriptores y firmantes durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

Que entre "Uanataca Colombia SAS" y "Uanataca, S.A." han suscrito un contrato de prestación de servicios de tecnología en el que Uanataca, S.A., proveerá la infraestructura de clave pública (PKI) que sustenta el servicio de certificación de UANATACA COLOMBIA.

Así mismo, Uanataca, S.A., pone a disposición de UANATACA COLOMBIA el personal técnico necesario para el correcto desempeño de las funciones fiables propias de una Entidad de Certificación Digital (ECD).

Dicho lo cual, Uanataca, S.A., se configura como el proveedor de servicios de Infraestructura para servicios de certificación y provee sus servicios tecnológicos a UANATACA COLOMBIA, para que éste pueda llevar a cabo los servicios inherentes como una Entidad de Certificación Digital (ECD), garantizando en todo momento la continuidad de los servicios en las condiciones y bajo los requisitos exigidos por la normativa.

En relación con lo anterior, se informa que Uanataca, S.A., a nivel internacional es un **Proveedor de Servicios de Certificación Europeo** (Entidad de Certificación Digital) cuya PKI se somete a auditorías anuales para la evaluación de la conformidad de prestadores de servicios de certificación de acuerdo con la normativa aplicable, bajo las normas:

a) ISO/IEC 17065:2012
b) ETSI EN 319 403
c) ETSI EN 319 421
d) ETSI EN 319 401
e) ETSI EN 319 411-2
f) ETSI EN 319 411-1

Adicionalmente, la PKI de Uanataca, S.A., se somete también a auditorías anuales bajo los estándares de seguridad:

a) ISO 9001:2015
b) ISO/IEC 27001:2014

En razón a lo anterior, se indican los datos de identificación del proveedor de servicios de infraestructura tecnológica de clave pública para la provisión de los servicios y actividades de certificación digital por parte de UANATACA COLOMBIA.

Nombre (Razón Social): UANATACA SA
NIF (NIT): A66721499
Datos de Inscripción en Registro Mercantil (Número de matrícula de Cámara de Comercio Colombia): Registro Mercantil de Barcelona, Hoja B-482242 Tomo 45264 Folio 12
Consulta el Estado de vigencia en el Registro Mercantil (Estado activo en Cámara de Comercio de Colombia) en: https://sede.registradores.org/site/mercantil buscando por sociedad introduciendo el NIF A66721499
Domicilio social y correspondencia: Avenida Meridiana Núm. 350 P.3 Barcelona (08027)
Teléfono: (+34) 935 27 22 90
Email: info@uanataca.com
Web: https://web.uanataca.com/es/

1.4 Tipos y Usos de los certificados

Esta DPC cumple e incluye las Políticas de Certificación de los certificados indicados en el apartado 1.2.1. 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, disponibles en el web https://web.uanataca.com/co/politicas-practicas

1.4.1.1 Certificado de persona natural ciudadano en tarjeta o token.

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.1.1**. Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2, lo cual se declara en el certificado. Este certificado emitido en dispositivo seguro de creación de firma es un certificado de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o Common Criteria (EAL4+), de conformidad con lo establecido en la normativa nacional.

Garantiza únicamente la identidad de la persona natural firmante y permite la generación de la "firma digital" entendido como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

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

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

La información de usos en el perfil de certificado indica lo siguiente:
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 commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.2 Certificado de persona natural ciudadano en HSM centralizado

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.1.2**. Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2, lo cual se declara en el certificado. Este certificado emitido en dispositivo seguro de creación de firma es un certificado de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 19 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o Common Criteria (EAL4+), de conformidad con lo establecido en la normativa nacional.

Garantiza únicamente la identidad de la persona natural firmante y permite la generación de la "firma digital", es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial

no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

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

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

La información de usos en el perfil de certificado indica lo siguiente:
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 commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.3 Certificado de persona natural profesional titulado en tarjeta o token

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.2.1**. Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2, lo cual se declara en el certificado. Este certificado emitido en dispositivo seguro de creación de firma es un certificado de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o Common Criteria (EAL4+), de conformidad con lo establecido en la normativa nacional.

Garantiza la identidad de la persona natural titular del certificado, así como su condición de profesional titulado (vinculación con un título profesional). Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual en el ámbito de su profesión permitiendo la generación de la "firma digital", es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la

transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

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

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

La información de usos en el perfil de certificado indica lo siguiente:
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 commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.4 Certificado de persona natural profesional titulado en HSM centralizado

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.2.2**. Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2., lo cual se declara en el certificado. Este certificado emitido en dispositivo seguro de creación de firma es un certificado de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 19 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 19 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 *Level* 3 o *Common Criteria (EAL4+)*, de conformidad con lo establecido en la normativa nacional.

Garantiza la identidad de la persona natural titular del certificado, así como su condición de profesional titulado (vinculación con un título profesional). Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual en el ámbito de su profesión permitiendo la generación de la "firma digital", es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la

transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

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

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

La información de usos en el perfil de certificado indica lo siguiente:
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 commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.5 Certificado de persona natural miembro de empresa u organización en tarjeta o token

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.3.1.** Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado emitido en dispositivo seguro de creación de firma es un certificado de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria (EAL4+)*, de conformidad con lo establecido en la normativa nacional.

Garantiza la identidad del suscriptor y firmante, certificando la vinculación de la persona natural a una entidad, quien actúa como suscriptor y descrita en el campo "O" (Organization), con ocasión a la relación y/o funciones que, como empleado, asociado, colaborador, etc., ocupa en la misma. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual, permitiendo la generación de la "firma digital" es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la

transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

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

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

La información de usos en el perfil de certificado indica lo siguiente:
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 commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.6 Certificado de persona natural miembro de empresa u organización en HSM centralizado

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.3.2.** Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2, lo cual se declara en el certificado. Este certificado emitido en dispositivo seguro de creación de firma es un certificado de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria (EAL4+)*, de conformidad con lo establecido en la normativa nacional.

Garantiza la identidad del suscriptor y firmante, certificando la vinculación de la persona natural a una entidad, quien actúa como suscriptor y descrita en el campo "O" (Organization), con ocasión a la relación y/o funciones que, como empleado, asociado, colaborador, etc., ocupa en la misma. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual, permitiendo la generación de la "firma digital" es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del

iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

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 electrónica.

La información de usos en el perfil de certificado indica lo siguiente:
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 commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.7. Certificado de persona natural representante de persona jurídica en tarjeta o token

Este certificado dispone del OID **1.3.6.1.4.1.47286.201.1.4.1.** Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado de representante de persona jurídica es emitido en un dispositivo seguro de creación de firma de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria (EAL4+)*, de conformidad con lo establecido en la normativa nacional.

Garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una persona jurídica, entidad u organización en el campo "O" (Organization), y permite la generación de la "firma digital" es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

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

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

La información de usos en el perfil de certificado indica lo siguiente:
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 commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.8. Certificado de persona natural Representante de persona jurídica en HSM centralizado

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.4.2.** Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado de representante de persona jurídica es emitido en un dispositivo seguro de creación de firma de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria (EAL4+)*, de conformidad con lo establecido en la normativa nacional.

Garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una persona jurídica, entidad u organización en el campo "O" (Organization), y permite la generación de la "firma digital" es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

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

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

La información de usos en el perfil de certificado indica lo siguiente:
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 commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.9 Certificado de persona natural función pública en token o tarjeta

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.6.1.** Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2, lo cual se declara en el certificado. Este certificado de función pública es emitido en un dispositivo seguro de creación de firma de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria (EAL4+)*, de conformidad con lo establecido en la normativa nacional.

Garantiza la identidad del suscriptor y del firmante, y una relación entre el firmante y una Institución descrita en el campo “O” (Organization) que pertenece a la administración pública, en virtud del rango de funcionario público y/o que presta una función de carácter público, permite la generación de la “firma digital” es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

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

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

La información de usos en el perfil de certificado indica lo siguiente:
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 commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.10 Certificado de persona natural función pública en HSM centralizado

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.6.2.** Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2, lo cual se declara en el certificado. Este certificado de función pública es emitido en un dispositivo seguro de creación de firma de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria (EAL4+)*, de conformidad con lo establecido en la normativa nacional.

Garantiza la identidad del suscriptor y del firmante, y una relación entre el firmante y una Institución descrita en el campo "O" (Organization) que pertenece a la administración pública, en virtud del rango de funcionario público y/o que presta una función de carácter público, permite la generación de la "firma digital" es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

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

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

La información de usos en el perfil de certificado indica lo siguiente:
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 commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.11 Certificado de Sello Electrónico en tarjeta o token (Persona Jurídica)

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.7.1**. Es un certificado que se emite de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado de sello electrónico es emitido en un dispositivo seguro de creación de firma de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria (EAL4+)*, de conformidad con lo establecido en la normativa nacional.

Los certificados de sello electrónico en dispositivo seguro de creación de firma garantizan la identidad de la entidad suscriptora vinculada. La información de usos en el perfil de certificado indica lo siguiente:

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 commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.12 Certificado de Sello Electrónico en HSM centralizado (Persona Jurídica)

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.7.2**. Es un certificado que se emite de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado de sello electrónico es emitido en un dispositivo seguro de creación de firma de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único

reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria (EAL4+)*, de conformidad con lo establecido en la normativa nacional.

Los certificados de sello electrónico en dispositivo seguro de creación de firma garantizan la identidad de la entidad suscriptora vinculada. La información de usos en el perfil de certificado indica lo siguiente:
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 commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.13 Certificado para facturación electrónica de persona natural en tarjeta o token

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.8.1**. Es un certificado que se emite de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado es exclusivo para facturación electrónica atendiendo a la necesidad de las personas naturales que buscan la seguridad del certificado para la emisión de facturas electrónicas. Certificado exclusivo para la firma digital de facturas electrónicas, notas crédito, notas débito, soportes de pago de nómina electrónica, notas de ajuste del documento soporte de pago de nómina electrónica y otros documentos producto de los procesos de las plataformas desatendidas de los proveedores tecnológicos aprobados por la DIAN, el sistema de facturación gratuita de la DIAN y la plataforma RADIAN, en cumplimiento de los anexos técnicos emitidos por dicha entidad

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria (EAL4+)*, de conformidad con lo establecido en la normativa nacional.

Los certificados de sello electrónico en dispositivo seguro de creación de firma garantizan la identidad del responsable del sello y de la entidad vinculada, incluidos en el certificado.

Estos certificados garantizan la identidad de la entidad suscriptora vinculada, y en su caso la del responsable de gestionar el sello identificado en el mismo. La información de usos en el perfil de certificado indica lo siguiente:
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 commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.14 Certificado para facturación electrónica de persona natural en HSM centralizado

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.8.2**. Es un certificado que se emite de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado es exclusivo para facturación electrónica atendiendo a la necesidad de las personas naturales que buscan la seguridad del certificado para la emisión de facturas electrónicas. Certificado exclusivo para la firma digital de facturas electrónicas, notas crédito, notas débito, soportes de pago de nómina electrónica, notas de ajuste del documento soporte de pago de nómina electrónica y otros documentos producto de los procesos de las plataformas desatendidas de los proveedores tecnológicos aprobados por la DIAN, el sistema de facturación gratuita de la DIAN y la plataforma RADIAN, en cumplimiento de los anexos técnicos emitidos por dicha entidad

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria (EAL4+)*, de conformidad con lo establecido en la normativa nacional.

Los certificados de sello electrónico en dispositivo seguro de creación de firma garantizan la identidad del responsable del sello y de la entidad vinculada, incluidos en el certificado.

Estos certificados garantizan la identidad de la entidad suscriptora vinculada, y en su caso la del responsable de gestionar el sello identificado en el mismo. La información de usos en el perfil de certificado indica lo siguiente:
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 commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.15 Certificado para facturación electrónica de persona jurídica en tarjeta o token

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.9.1**. Es un certificado que se emite de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado es exclusivo para facturación electrónica atendiendo a la necesidad de las personas jurídicas que buscan la seguridad del certificado para la emisión de facturas electrónicas. Certificado exclusivo para la firma digital de facturas electrónicas, notas crédito, notas débito, soportes de pago de nómina electrónica, notas de ajuste del documento soporte de pago de nómina electrónica y otros documentos producto de los procesos de las plataformas desatendidas de los proveedores tecnológicos aprobados por la DIAN, el sistema de facturación gratuita de la DIAN y la plataforma RADIAN, en cumplimiento de los anexos técnicos emitidos por dicha entidad.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria (EAL4+)*, de conformidad con lo establecido en la normativa nacional.

Los certificados de sello electrónico en dispositivo seguro de creación de firma garantizan la identidad del responsable del sello y de la entidad vinculada, incluidos en el certificado.

Estos certificados garantizan la identidad de la entidad suscriptora vinculada, y en su caso la del responsable de gestionar el sello identificado en el mismo. La información de usos en el perfil de certificado indica lo siguiente:
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 commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.16 Certificado para facturación electrónica de persona jurídica en HSM centralizado

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.9.2**. Es un certificado que se emite de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado es exclusivo para facturación electrónica atendiendo a la necesidad de las personas jurídicas que buscan la seguridad del certificado para la emisión de

facturas electrónicas. Certificado exclusivo para la firma digital de facturas electrónicas, notas crédito, notas débito, soportes de pago de nómina electrónica, notas de ajuste del documento soporte de pago de nómina electrónica y otros documentos producto de los procesos de las plataformas desatendidas de los proveedores tecnológicos aprobados por la DIAN, el sistema de facturación gratuita de la DIAN y la plataforma RADIAN, en cumplimiento de los anexos técnicos emitidos por dicha entidad.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria (EAL4+)*, de conformidad con lo establecido en la normativa nacional.

Los certificados de sello electrónico en dispositivo seguro de creación de firma garantizan la identidad del responsable del sello y de la entidad vinculada, incluidos en el certificado.

Estos certificados garantizan la identidad de la entidad suscriptora vinculada, y en su caso la del responsable de gestionar el sello identificado en el mismo. La información de usos en el perfil de certificado indica lo siguiente:
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 commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.17 Certificado de Estampado Cronológico (sello de tiempo)

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.10,** y se emite de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2.

Los certificados de Estampado Cronológico (sello de tiempo) se tratan de certificados emitidos para la operación de autoridades de sellado de tiempo y hora, para la firma de las estampas cronológicas (sellos de tiempo) que éstas producen, el cual permite establecer con una prueba que estos datos existían en ese momento o periodo de tiempo y que no sufrieron ninguna modificación a partir del momento en que se realizó el estampado.

Estos certificados permiten la firma de la estampa cronológica (sello de tiempo) que se emiten, desde el momento que hayan obtenido un certificado de estampado cronológico (sello de tiempo) válido y mientras éste se encuentre vigente.

La sincronización de los tiempos en UANATACA COLOMBIA se realiza mediante un servicio del servidor de tiempo NTP Stratum 3 v4 conforme al estándar RFC 5905 “Network Time Protocol Version 4: Protocol and Algorithms Specification”. Los registros tienen una fuente de tiempo que se mantiene actualizado conforme al Instituto Nacional de Metrología (INM) de Colombia. Como fuente de sincronización secundaria, corresponderá a la originada en UANATACA S.A que se basa en antenas y receptores GPS que permiten un nivel de confianza de STRATUM 1 (con dos sistemas en alta disponibilidad).

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.

Dentro de la documentación técnica y de configuración de la ECD existe un apartado sobre la configuración de tiempos de los equipos utilizados en la emisión de certificados.

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 regulación aplicable.

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

Se puntualiza la prohibición de utilizar la certificación digital de manera que contravenga la ley, documentos relacionados con el servicio de certificación u ocasione mala reputación para la Entidad de Certificación Digital de UANATACA COLOMBIA. Lo que a su vez implica, que no debe monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica del ONAC y de la ECD UNATACA COLOMBIA; así como comprometer intencionadamente la seguridad de la Jerarquía del ONAC y la Entidad de Certificación.

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, disponibles en la web de UNATACA COLOMBIA.

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 COLOMBIA, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

UANATACA COLOMBIA 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 COLOMBIA 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 Colombia, S.A.S.
RUT: 9016714475
Dirección: Calle 93 B 12 28 OF 203 204 Bogotá, Colombia

1.5.2 Datos de contacto de la organización

Uanataca Colombia, S.A.S
Dirección: Calle 93 B 12 28 OF 203 204 Bogotá, Colombia
Correo electrónico: info@uanataca.co
Teléfono: +593 99 970 3430
Dirección web: https://web.uanataca.com/co/

1.5.3 Procedimientos de gestión del documento

El sistema documental y de organización de UANATACA COLOMBIA 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.

Además, publicará en su página web cada nueva versión aprobada de la DPC y el Contrato de Suscripción incluido como ANEXO 2, sustituyendo a la anterior versión.

2 Publicación de información y depósito de certificados

2.1 Depósito(s) de certificados

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

Dicho servicio se encuentra disponible en el sitio web de UANATACA COLOMBIA, durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de UANATACA COLOMBIA, 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 proveedor de servicios de certificación

UANATACA COLOMBIA publica las siguientes informaciones, en su Depósito:

- Los certificados emitidos indistintamente del método de identificación, de los que se ha obtenido previamente el consentimiento de la Persona natural 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.

2.3 Frecuencia de publicación

La información de la Entidad de Certificación Digital, 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 4.9.9 y 4.9.10 de esta Declaración de Prácticas de Certificación.

2.4 Control de acceso

UANATACA COLOMBIA 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 COLOMBIA 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 natural 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 distintivo (DN o *distinguished name*) conforme al estándar X.509 en el campo *Subject*, incluyendo un componente *Common Name* (CN=), relativo a la identidad del suscriptor y de la Persona natural identificada en el certificado, así como diversas informaciones de identidad adicionales en el campo *SubjectAlternativeName.*

Los campos de **DN** del titular del certificado referentes a Nombre y Apellidos y/o a nombre o razón social serán idénticos a los datos que consten en la cédula de Ciudadanía, Cédula de Extranjería o Pasaporte y/o en el Certificado de existencia y representación legal en Cámara de Comercio y/o Registro único Tributario (o documentos equivalentes)

Los nombres contenidos en los certificados son los siguientes:

3.1.1.1 Certificado de persona natural ciudadano en tarjeta o token

Country Name (C)	CO
Surname	Apellidos del Suscriptor (como consta en el documento de identificación)
Given Name	Nombre del Suscriptor (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del SUSCRIPTOR codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	NOMBRE Y APELLIDOS DEL SUSCRIPTOR
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor

3.1.1.2 Certificado de persona natural ciudadano en HSM centralizado

Country Name (C)	CO
Surname	Apellidos del Suscriptor (como consta en el documento de identificación)
Given Name	Nombre del Suscriptor (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del SUSCRIPTOR codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	NOMBRE Y APELLIDOS DEL SUSCRIPTOR
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor

3.1.1.3 Certificado de persona natural profesional titulado en tarjeta o token

Country Name (C)	CO
Organization Name (O)	Se especificará el nombre de la entidad habilitante (Emisor de la tarjeta profesional o entidad/institución educativa que otorga el título)
Title	Se especificará el título o especialidad del suscriptor y el número de profesional si dispone. (Ejemplo: ABOGADO - NUMERO DE PROFESIONAL)
Surname	Apellidos del suscriptor (como consta en el documento de identificación)
Given Name	Nombre del suscriptor (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del suscriptor codificado acorde a ETSI EN 319 412-1 ejemplo ("IDCCO-[CC]" o "PASCO-[PASAPORTE]")
Common Name	Nombre y apellido del Suscriptor + Título (Ejemplo: "Given name" + "Surname" + "Title")
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor

3.1.1.4 Certificado de persona natural profesional titulado en HSM centralizado

Country Name (C)	CO
Organization Name (O)	Se especificará el nombre de la entidad habilitante (Emisor de la tarjeta profesional o entidad/institución educativa que otorga el título)
Title	Se especificará el título o especialidad del suscriptor y el número de profesional si dispone. (Ejemplo: ABOGADO - NUMERO DE PROFESIONAL)
Surname	Apellidos del suscriptor (como consta en el documento de identificación)
Given Name	Nombre del suscriptor (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del suscriptor codificado acorde a ETSI EN 319 412-1 ejemplo ("IDCCO-[CC]" o "PASCO-[PASAPORTE]")
Common Name	Nombre y apellido del Suscriptor + Título (Ejemplo: "Given name" + "Surname" + "Title")
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor

3.1.1.5 Certificado de persona natural miembro de empresa u organización en tarjeta o token

Country Name (C)	CO
Organizational Unit Name (OU)	Se especificará el Departamento al que pertenece el Firmante o el tipo de vinculación con la Empresa
Organization Name (O)	Se especificará el nombre de la Empresa u Organización
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: "VATCO-00000")
Title	Se especificará el nombre del título o puesto que la persona ocupa en la Empresa u Organización
Surname	Apellidos del firmante (como consta en el documento de identificación)
Given Name	Nombre del firmante (como consta en el documento de identificación)

Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad a la que está vinculado el firmante

3.1.1.6 Certificado de persona natural miembro de empresa u organización en HSM centralizado

Country Name (C)	CO
Organizational Unit Name (OU)	Se especificará el Departamento al que pertenece el Firmante o el tipo de vinculación con la Empresa
Organization Name (O)	Se especificará el nombre de la Empresa u Organización
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: “VATCO-00000”)
Title	Se especificará el nombre del título o puesto que la persona ocupa en la Empresa u Organización
Surname	Apellidos del firmante (como consta en el documento de identificación)
Given Name	Nombre del firmante (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad a la que está vinculado el firmante

3.1.1.7 Certificado de persona natural representante de persona jurídica en tarjeta o token

Country Name (C)	CO
Organization Name (O)	Nombre de la organización de la que el firmante es representante
Organizational Unit Name (OU)	Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: “VATCO-00000”)
Title	REPRESENTANTE LEGAL
Surname	Apellidos del representante (como consta en el documento de identificación)
Given Name	Nombre del representante (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)

Common Name	NOMBRE Y APELLIDOS DEL REPRESENTANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la persona jurídica a la que está vinculado el firmante

3.1.1.8 Certificado de persona natural representante de persona jurídica en HSM centralizado

Country Name (C)	CO
Organization Name (O)	Nombre de la organización de la que el firmante es representante
Organizational Unit Name (OU)	Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: "VATCO-00000")
Title	REPRESENTANTE LEGAL
Surname	Apellidos del representante (como consta en el documento de identificación)
Given Name	Nombre del representante (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo ("IDCCO-[CC]" o "PASCO-[PASAPORTE]")
Common Name	NOMBRE Y APELLIDOS DEL REPRESENTANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la persona jurídica a la que está vinculado el firmante

3.1.1.9 Certificado de persona natural función pública en tarjeta o token

Country Name (C)	CO
Organizational Unit Name (OU) –	Se especificará el Departamento al que pertenece el firmante o el tipo de vinculación con la Institución
Organization Name (O)	Se especificará el nombre de la Institución
Organization Identifier	Número oficial de identificación de la institución a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: "VATCO-00000")
Title	Se especificará el cargo o puesto que la persona ocupa en la Institución
Surname	Apellidos del firmante (como consta en el documento de identificación)
Given Name	Nombre del firmante (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo ("IDCCO-[CC]" o "PASCO-[PASAPORTE]")
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la institución

3.1.1.10 Certificado de persona natural función pública en HSM centralizado

Country Name (C)	CO
Organizational Unit Name (OU) –	Se especificará el Departamento al que pertenece el firmante o el tipo de vinculación con la Institución
Organization Name (O)	Se especificará el nombre de la Institución
Organization Identifier	Número oficial de identificación de la institución a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: “VATCO-00000”)
Title	Se especificará el cargo o puesto que la persona ocupa en la Institución
Surname	Apellidos del firmante (como consta en el documento de identificación)
Given Name	Nombre del firmante (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la institución

3.1.1.11 Certificado de Sello Electrónico en tarjeta o token

Country Name (C)	CO
Organization Name (O)	Denominación (nombre “oficial” de la organización o entidad)
Organizational Unit Name (OU) –	Denominación (nombre “oficial” de la unidad) del solicitante del sello (Ej: Subdirección de explotación)
Organization Identifier	Número oficial de identificación de la organización o entidad a la que está vinculado el sello en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: “VATCO-00000”)
Common Name	NOMBRE DESCRIPTIVO DEL CREADOR DEL SELLO, ASEGURANDO QUE DICHO NOMBRE TENGA SENTIDO Y NO DÉ LUGAR A AMBIGÜEDADES
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad

3.1.1.12 Certificado de Sello Electrónico en HSM centralizado

Country Name (C)	CO
Organization Name (O)	Denominación (nombre “oficial” de la organización o entidad)

Organizational Unit Name (OU) –	Denominación (nombre “oficial” de la unidad) del solicitante del sello (Ej: Subdirección de explotación)
Organization Identifier	Número oficial de identificación de la organización o entidad a la que está vinculado el sello en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: “VATCO-00000”)
Common Name	NOMBRE DESCRIPTIVO DEL CREADOR DEL SELLO, ASEGURANDO QUE DICHO NOMBRE TENGA SENTIDO Y NO DÉ LUGAR A AMBIGÜEDADES
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad

3.1.1.13 Certificado para facturación electrónica de persona natural en tarjeta o token

Country Name (C)	País de residencia o nacionalidad del Suscriptor
Surname	Apellidos del Suscriptor (como consta en el documento de identificación)
Given Name	Nombre del Suscriptor (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del Suscriptor codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	Certificado de facturación electrónica de [Nombre del Suscriptor] (Ejemplo "Certificado de facturación electrónica de + [Given Name] + [Surname])
Description	Número de documento de identificación del Suscriptor + digito de verificación (sin puntos) (Ejemplo: [Núm. Documento de identificación del Suscriptor] + "digito de verificación").
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor

3.1.1.14 Certificado para facturación electrónica de persona natural en HSM centralizado

Country Name (C)	País de residencia o nacionalidad del Suscriptor
Surname	Apellidos del Suscriptor (como consta en el documento de identificación)
Given Name	Nombre del Suscriptor (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del Suscriptor codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	Certificado de facturación electrónica de [Nombre del Suscriptor] (Ejemplo "Certificado de facturación electrónica de + [Given Name] + [Surname])
Description	Número de documento de identificación del Suscriptor + digito de verificación (sin puntos)

	(Ejemplo: [Núm. Documento de identificación del Suscriptor] + "digito de verificación").
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor

3.1.1.15 Certificado para facturación electrónica de persona jurídica en tarjeta o token

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Organization Name (O)	Denominación (nombre "oficial" de la organización o entidad)
Organizational Unit Name (OU)	Denominación (nombre "oficial" de la unidad) del solicitante del sello (área en la empresa que hará uso del certificado (Ej: Subdirección de explotación)
Organization Identifier	Número oficial de identificación de la organización o entidad a la que está vinculado el sello en formato ETSI EN 319412-1 (Ejemplo: "VATCO-[NIT-DE-LA-ENTIDAD]")
Common Name	Número de identificación empresa + digito de verificación (sin puntos) (Ejemplo: [Num. NIT de la entidad] + "digito de verificación").
Description	Certificado de facturación electrónica de [Nombre de la Organización] (Ejemplo "Certificado de facturación electrónica de + [Organization Name])
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor

3.1.1.16 Certificado para facturación electrónica de persona jurídica en HSM centralizado

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Organization Name (O)	Denominación (nombre "oficial" de la organización o entidad)
Organizational Unit Name (OU)	Denominación (nombre "oficial" de la unidad) del solicitante del sello (área en la empresa que hará uso del certificado (Ej: Subdirección de explotación)
Organization Identifier	Número oficial de identificación de la organización o entidad a la que está vinculado el sello en formato ETSI EN 319412-1 (Ejemplo: "VATCO-[NIT-DE-LA-ENTIDAD]")
Common Name	Número de identificación empresa + digito de verificación (sin puntos) (Ejemplo: [Num. NIT de la entidad] + "digito de verificación").
Description	Certificado de facturación electrónica de [Nombre de la Organización] (Ejemplo "Certificado de facturación electrónica de + [Organization Name])
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad

3.1.1.17 Certificado de Estampado Cronológico (sello de tiempo electrónico)

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada [CO]
Locality Name (L)	Nombre de la LOCALIDAD donde resida el proveedor del servicio de certificación. (No incluir información adicional al nombre de la localidad)

Organizational Unit Name (OU))	TSP- UNIDAD DEL PRESTADOR
Organization Name (O)	NOMBRE ORGANIZACIÓN
Common Name (CN)	Estampado cronológico de [NOMBRE DEL PRESTADOR DE SERVICIO]
Organization Identifier (other name)	VATCO-[NIT DEL PRESTADOR DEL SERVICIO]
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio del proveedor del servicio de certificación

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 Emisión de certificados del set de pruebas y certificados de pruebas en general

En el caso que los datos indicados en el DN o Subject fueran ficticios (ej. “Test Organization”, “Test Nombre”, “Apellido1”) o se indique expresamente palabras que denoten su invalidez (ej. “TEST”, “PRUEBA” o “INVALIDO”), se considerará al certificado sin validez legal y por lo tanto sin responsabilidad alguna sobre UANATACA COLOMBIA. Estos certificados se emiten para realizar pruebas técnicas de interoperabilidad y permitir al ente regulador su evaluación.

3.1.4 Empleo de anónimos y seudónimos

En ningún caso se pueden utilizar seudónimos para identificar una entidad, empresa u organización, suscriptor, ni a un firmante. Así mismo, en ningún caso se emiten certificados anónimos.

3.1.5 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” o “estado” será el del suscriptor del certificado.

Los certificados cuyos suscriptores sean personas jurídicas, entidades u organismos de la administración pública, muestran la relación entre estas y una Persona natural, con independencia de la nacionalidad de la Persona natural.

En el campo “número de serie” se incluye el número de identificación de la Cédula de Ciudadanía, Cédula de Extranjería Pasaporte u otro número de identificación idóneo del firmante, reconocido en derecho.

3.1.6 Unicidad de los nombres

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

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 documento de identidad y/o el Número de Identificación Fiscal, o equivalente, en el esquema de nombres, permitiendo distinguir entre dos identidades cuando exista algún problema de duplicidad 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:

- Cédula de Ciudadanía, Cédula de Extranjería, Pasaporte u otro identificador legalmente válido de la Persona natural.
- Número de Identificación Tributaria (NIT) u otro identificador legalmente válido del suscriptor.
- Tipo de certificado (OID de identificador de política de certificación).
- El certificado anterior no conste como vigente.

Como excepción esta DPC permite emitir un certificado cuando coincida NIT del suscriptor, documento de identidad del suscriptor (firmante), tipo de certificado, con un certificado activo, siempre que exista algún elemento diferenciador entre ambos, en los campos cargo (*title*) y/o departamento (*Organizational Unit*).

3.1.7 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.

No existirá ninguna obligación 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, la Entidad de Certificación Digital se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres y no está obligada a tener evidencia de la posesión de marcas registradas antes de la emisión de los certificados.

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 los organismos competentes para la realización de un arbitraje en la República de Colombia a los 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 identificación de los suscriptores se realiza mediante comparecencia personal o remota según la necesidad del usuario y las políticas de UANATACA COLOMBIA, cuya identidad resulta fijada en el momento de la firma del contrato entre UANATACA COLOMBIA y el suscriptor, momento en el que queda verificada fehacientemente la identidad del suscriptor mediante los procedimientos de reconocimiento establecidos, su documento nacional de identidad y/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 únicamente la consulta directa a los registros públicos correspondientes.

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

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 suscriptor (firmante), en certificados de firma.

Asimismo, en la Política de Certificación se especifica el método de prueba de posesión de la clave privada para cada uno de los tipos de soporte en los que se pueden emitir los correspondientes certificados

3.2.2 Validación de la Identidad

Para la solicitud de certificados los Operadores de Registro de UANATACA COLOMBIA verificarán la identidad del suscriptor a la que se le expide el certificado (véase la persona física o representante autorizado de la persona jurídica), así como cualquier atributo especifico de la persona física o jurídica con la que tenga relación o vinculación.

Para la verificación se procederá a través de un operador de registro o persona autorizada de la Autoridad de Registro, de acuerdo con los siguientes métodos:

a. De forma presencial por parte de la persona física o de un representante autorizado de la persona jurídica, quien deberá aportar la Cédula de Ciudadanía, Cédula de Extranjería, Pasaporte u otro medio idóneo reconocido en derecho para su identificación.
b. Por medio del procedimiento de identificación a distancia a través del sistema de validación de identificación remota de UANATACA COLOMBIA o utilizando otros métodos de identificación a distancia que cumplan las condiciones y requisitos de seguridad determinados por el ONAC.

3.2.3 Autenticación de la identidad de una persona jurídica (organización, empresa o entidad)

La Autoridad de registro verificará la información para poder autenticar la identidad de la persona jurídica, empresa o entidad (u otro tipo de entidad pública o privada) que desempeñe una actividad económica para la cual esté obligada a inscribirse en un registro de carácter fiscal o tributario identificada en el certificado digital mediante la siguiente documentación:

- Solicitud de Certificado de existencia y representación legal en Cámara de Comercio o documento equivalente, en los casos que sea aplicable; expedido en Colombia (por defecto) o en otro país un máximo de 30 días antes.
- Solicitud de Registro Único Tributario o documento equivalente, en todos los casos; expedido en Colombia (por defecto) o en otro país.
- Si no se incluye en la documentación anterior, solicitud de un documento oficial adicional en el que conste una dirección completa actual de la empresa o entidad (por

ejemplo, un Certificado de Residencia para Personas Naturales), en el caso de que el Suscriptor desee que figure en el certificado una dirección distinta a las incluidas en el Certificado de existencia y representación legal en Cámara de Comercio y/o en el Registro Único Tributario o documentos equivalentes; expedido en Colombia (por defecto) o en otro país un máximo de 30 días antes.
- Para aquellos casos en los que sea posible, consulta del número de identificación tributaria de la empresa o entidad en una base de datos online (en Colombia, para las empresas del tipo Persona Jurídica o Persona Natural, base de datos RUES), para verificar la existencia de la empresa o entidad y que se encuentra activa.

En el caso de las personas naturales con capacidad de actuar en nombre de las personas jurídicas o entidades sin personalidad jurídica, públicas o privadas, que sean suscriptoras de certificados, podrán actuar como representantes de estas, siempre y cuando exista una situación previa de representación legal o voluntaria entre la Persona natural y la organización de la que se trate, que exige su reconocimiento por UANATACA COLOMBIA, la cual se realizará mediante el siguiente procedimiento:

1. El representante del suscriptor deberá acreditar su identidad por uno de los métodos de identificación especificados en el apartado 3.2.2., de tal manera que:
   i. Si se identifica presencialmente ante un operador o persona autorizada de una Autoridad de Registro de UANATACA COLOMBIA:
      - Mostrando su documento nacional de identificación (la Cédula de Ciudadanía, Cédula de Extranjería, pasaporte u otro medio idóneo reconocido en derecho para su identificación).
      - Acreditando el carácter y facultades que alegue poseer.

   ii. Si se identifica electrónicamente a través del sistema de video identificación remota de UANATACA COLOMBIA:
      - Mostrando su documento nacional de identificación (la Cédula de Ciudadanía, Cédula de Extranjería, pasaporte u otro medio idóneo reconocido en derecho para su identificación).
      - Proveyendo prueba de vida mediante el uso de medios técnicos de captación de imágenes y vídeo utilizando algoritmos de criptografía biométrica facial e inteligencia artificial para el cotejo inequívoco de la identidad del solicitante y la verificación de la prueba de vida de éste, así como de la autenticidad del documento de identidad exhibido.
      - Acreditando el carácter y facultades que alegue poseer.

2. El representante proporcionará la siguiente información y sus correspondientes soportes acreditativos:
   - Sus datos de identificación, como representante:
     - Nombre y apellidos

- Lugar y fecha de nacimiento
- Documento: Cédula de Ciudadanía, Cédula de Extranjería, Pasaporte u otro medio idóneo reconocido en derecho para la identificación 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: NIT o documento acreditativo de la identificación fiscal de la entidad.
  - 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) si resulta aplicable.
  - 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. El operador o personal autorizado de la Autoridad de Registro de UANATACA COLOMBIA comprobará la identidad del representante actuando del siguiente modo:
   - Cuando la identificación se haya realizado presencialmente, a través de la revisión de:
     - Documento de identidad aportado.
     - Documentación que acredite su representación.

- Cuando la identificación se haya realizado a través del método de identificación electrónica a través del sistema de validación de identificación remota de UANATACA COLOMBIA mediante:
  - Revisión de los vídeos e imágenes captadas del documento de identificación aportado y del propio solicitante.
  - Revisión de la prueba de vida del solicitante, a través de los resultados facilitados por el sistema de validación de identificación remota.
  - Revisión del cotejo producido por el sistema de validación de identificación remota de la fotografía del documento de identidad con las imágenes o vídeo obtenido durante el registro del solicitante.
  - Revisión producida por el sistema de validación de identificación remota, a través de inteligencia artificial para la detección de documentos de identidad falsos.
  - Documentación que acredite su representación.

4. El operador o personal autorizado de la Autoridad de Registro de UANATACA COLOMBIA verificará la información suministrada para la autenticación y le devolverá cuando corresponda la documentación original aportada.

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

La ECD se reserva el derecho de no emitir el certificado si considera que la documentación aportada no es suficiente o adecuada para la comprobación de los datos anteriormente citados.

La Autoridad de Registro guardará la documentación relativa al sustento de la validación de la identidad de la empresa o entidad identificada en el certificado.

3.2.4 Autenticación de la identidad de una Persona natural

La autoridad de Registro verificará de forma fehaciente la identidad de la Persona Natural individual identificada en el certificado, y validará que el documento de identidad presentado sea aparentemente legítimo y que los datos contenidos en el mismo (país de expedición, tipo y número de documento de identidad, nombres y apellidos) son conformes a los datos de la solicitud o la consulta directa a los registros públicos correspondientes. Asimismo, en los casos que sea aplicable, la RA verificará que el documento estaba vigente cuando se presentó. Está sección describe los métodos de comprobación de la identidad de la persona identificada en un certificado.

3.2.4.1 En los certificados

La identidad de las personas naturales suscriptoras (firmantes) identificados en los certificados, se valida a través de los métodos de identificación especificados en el apartado 3.2.2 de esta DPC, de tal manera que:

- (i) Si se identifica presencialmente ante un operador o persona autorizada de una Autoridad de Registro de UANATACA COLOMBIA:
  - Mostrando su Documento de Identidad (Cédula de Ciudadanía, Cédula de Extranjería, pasaporte u otro medio idóneo reconocido en derecho).

- (ii) Si se identifica electrónicamente a través del sistema de validación de identidad remota usado por UANATACA COLOMBIA, o sistemas aprobados previamente por UANATACA COLOMBIA que garanticen el reconocimiento de identidad del titular:
  - Mostrando su Documento de Identidad (Cédula de Ciudadanía, Cédula de Extranjería, pasaporte u otro medio idóneo reconocido en derecho).
  - Proveyendo prueba de vida mediante el uso de medios técnicos de captación de imágenes o vídeo utilizando algoritmos de criptografía biométrica facial e inteligencia artificial para el cotejo inequívoco de la identidad del solicitante y la verificación de la prueba de vida de éste.

La información de identificación de las personas naturales identificadas en los certificados cuyo suscriptor sea una entidad con o sin personalidad jurídica, la información podrá ser validada 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, o bien con la documentación que esta haya suministrado sobre la Persona natural que identifica como firmante, asegurando la corrección de la información a certificar.

3.2.4.2 Validación de la Identidad

Para la solicitud de certificados, el operador o personal autorizado de la Autoridad de Registro UANATACA COLOMBIA comprobará la identidad de la persona física identificada en la solicitud del certificado, actuando del siguiente modo:

- Cuando la identificación se haya realizado presencialmente, a través de la revisión de:

- Documento de identidad aportado.

- Cuando la identificación se haya realizado a través del método de identificación electrónica a través de video identificación de UANATACA COLOMBIA mediante:
  - Revisión de los vídeos e imágenes captadas del documento de identificación aportado y del propio solicitante.
  - Revisión de la prueba de vida del solicitante, a través de los resultados facilitados por el sistema de video identificación remota.
  - Revisión del cotejo producido por el sistema de video identificación remota de la fotografía del documento de identidad con las imágenes y vídeo obtenido durante el registro del solicitante.
  - Revisión producida por el sistema de video identificación remota, a través de inteligencia artificial para la detección de documentos de identidad falsos.

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 natural y entidad, empresa u organización de derecho público o privado a la que está vinculada. 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 natural identificada en el certificado mediante su presencia física o siguiendo el procedimiento de validación de identidad establecido por UANATACA COLOMBIA.

Durante este trámite se confirma rigurosamente la identidad de la Persona natural identificada en el certificado. Por este motivo, en todos los casos en que se expide un certificado se acredita mediante un operador de registro la identidad de la Persona natural firmante.

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

3.2.4.3 Vinculación de la Persona natural

La justificación documental de la vinculación de una Persona natural 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 públicas y privadas a las que están vinculadas.

3.2.5 Información de suscriptor no verificada

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

3.2.6 Autenticación de la identidad de una RA y sus operadores

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

Igualmente, UANATACA COLOMBIA directamente a través de su Autoridad de Registro, verifica y valida la identidad de los operadores de las Autoridades de Registro, para lo cual estas últimas envían a UANATACA COLOMBIA la documentación de identificación correspondientes al nuevo operador, juntamente con su autorización para actuar como tal.

UANATACA COLOMBIA se asegura que los operadores de la Autoridad de Registro reciben la formación suficiente para el desarrollo de sus funciones, lo cual verifica con la evaluación correspondiente. Dicha formación y evaluación puede ser ejecutada por la Autoridad de Registro previamente autorizada por UANATACA COLOMBIA.

Para la prestación de los servicios, UANATACA COLOMBIA se asegura de que los operadores de Autoridad de Registro acceden al sistema mediante autenticación fuerte con certificado digital.

En ese sentido, UANATACA COLOMBIA conservará como propias las funciones de comprobación de veracidad, y corrección de los datos que aportan los usuarios, así como el envío a una CA de las peticiones que cumplen los requisitos exigidos por la Entidad de Certificación Digital.

3.3 Identificación y autenticación de solicitudes de renovación

La renovación se entenderá como la emisión de un nuevo certificado digital, por lo cual implica el registro de una nueva solicitud, la cual estará sujeta a validación de identidad por parte de la autoridad de registro según lo especificado en la sección 3.2., con la respectiva generación de un nuevo par de claves.

La ECD UANATACA COLOMBIA notificará con al menos treinta (30) días calendario de anticipación a sus suscriptores y/o firmantes la terminación de la vigencia de su certificado digital. Esta notificación podrá realizarse por correo electrónico a la dirección proporcionada por el suscriptor o por cualquier otro medio idóneo de comunicación cuando UANATACA COLOMBIA lo considere pertinente.

Sin embargo, no es obligación de UANATACA COLOMBIA garantizar la efectividad de la notificación sobre la terminación de la vigencia de su certificado o confirmar la recepción de esta, pues es una obligación del Suscriptor y/o firmante conocer la vigencia de su certificado digital y adelantar los trámites pertinentes ante UANATACA COLOMBIA para la emisión del certificado

Los casos en los que se requiera un nuevo certificado digital con cambio de claves, por expiración, próxima expiración o revocación de un certificado, se tratan como una nueva emisión de certificado, realizándose la misma validación de identidad que se hizo inicialmente para el primer certificado digital, según lo especificado en la sección 3.2.

3.4 Modificación del certificado

Durante el ciclo de vida de un certificado, no se tiene prevista la modificación/actualización de los campos contenidos en el certificado. Si se requiere un cambio en los datos del certificado emitido, será necesario revocar el certificado y emitir uno nuevo con las modificaciones correspondientes, registrando adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 3.2.

3.5 Identificación y autenticación de la solicitud de revocación y/o suspensión

UANATACA COLOMBIA o un operador o personal autorizado de la Autoridad de Registro autentica las peticiones e informes relativos a la revocación, comprobando que provienen de una persona autorizada.

La identificación de los suscriptores y/o firmantes en el proceso de revocación de certificados podrá ser realizada por:

- El suscriptor y/o firmante:

- Identificándose y autenticándose de manera online mediante el uso del Código de Revocación (CRE o ERC) a través de la página web de UANATACA COLOMBIA en horario 24x7.
- Otros medios de comunicación, como el teléfono, correo electrónico, etc. cuando existan garantías razonables de la identidad del solicitante de la revocación, a juicio de UANATACA COLOMBIA y/o Autoridades de Registro.

- Las autoridades de registro de UANATACA COLOMBIA: deberán identificar al firmante ante una petición de revocación según los propios medios que considere necesarios.

UANATACA COLOMBIA no permite la suspensión de certificados, debiendo proceder conforme lo estipulado para la revocación de certificados.

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

Están autorizados para solicitar la emisión de un certificado digital cualquier persona mayor de edad en plena capacidad de asumir las obligaciones y responsabilidades inherentes a la posesión y uso del certificado y que sustente correctamente la información requerida por la Autoridad de Registro.

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 natural, o bien en nombre del suscriptor en el caso de que el suscriptor sea la entidad, empresa u organización de derecho público o privado.

El solicitante del certificado indistintamente del método de identificación empleado por UANATACA COLOMBIA, sea persona natural o jurídica, debe firmar un contrato de prestación de servicios de certificación con UANATACA COLOMBIA.

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

4.1.2 Procedimiento de alta y responsabilidades

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

Las solicitudes se instrumentan mediante un formulario en formato papel o electrónico, de manera individual o por lotes, o mediante la conexión con bases de datos externas, o a través de una capa de *Web Services* cuyo destinatario es UANATACA COLOMBIA. En el caso de certificados cuyo suscriptor sea una entidad, empresa u organización de derecho público o privado que actúe como una Autoridad de Registro de UANATACA COLOMBIA, podrá gestionar directamente las solicitudes accediendo a los sistemas informáticos de UANATACA COLOMBIA y generar los certificados correspondientes para la propia entidad, empresa u organización o para sus miembros.

A la solicitud se deberá acompañar documentación justificativa de la identidad y otras circunstancias de la persona natural identificada en el certificado, de acuerdo con lo establecido en la sección 3.2.4. También se deberá acompañar una dirección física, u otros datos, que permitan contactar a la persona natural 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 COLOMBIA se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

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

La documentación justificativa de la aprobación de la solicitud debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante el periodo que establezca la legislación vigente cuando sea aplicable y hasta por un plazo máximo de 10 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

Tras realizar la identificación de la persona de manera presencial o a distancia, siguiendo las políticas y procedimientos de UANATACA COLOMBIA, se procederá a su verificación. En caso de que los datos se verifiquen correctamente, UANATACA COLOMBIA debe aprobar la solicitud del certificado y proceder a su emisión y entrega.

Siempre que lo considere oportuno, el operador de registro podrá solicitar la subsanación de la información inicialmente proporcionada por el solicitante en su solicitud, necesaria para la correcta validación y aprobación del servicio. En caso de que de las comprobaciones adicionales no se desprenda la corrección de las informaciones a verificar, la solicitud quedará denegada definitivamente.

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 Autoridad de Certificación, de las Autoridades de Registro o de los suscriptores, UANATACA COLOMBIA denegará la petición, o detendrá su aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

Igualmente, se declinará una solicitud de un servicio de certificación digital, si el mismo no se encuentra en el alcance de la acreditación que le fue otorgado por ONAC.

Asimismo, de conformidad con el numeral 10.11.3.7 de la CEA-3.0-07 el operador de registro de la RA podrá declinar la aceptación de una solicitud cuando existan razones fundamentadas y demostradas, por ejemplo, la participación del solicitante y/o suscriptor en actividades ilegales, o temas relacionados con el suscriptor.

En atención a criterios de imparcialidad y no discriminación dentro de la Autoridad de Registro se dejará un registro interno en la aplicación (CMS) de la RA a efectos de evidenciar que quien realiza la función de la revisión de la solicitud (Operador de Registro) ha emitido una recomendación documentada positiva para que se tenga en cuenta en la decisión sobre la certificación, siendo el Operador de Decisión quien deberá tomar la decisión final sobre la emisión del certificado.

De otra parte, cuando se emita una recomendación documentada negativa será obligatorio para el Operador de Registro justificar y registrar esta debido a que no satisface algún requisito establecido en este documento, en la Política de Certificación correspondiente o en las normas o leyes vigentes aplicables.

En el caso de no otorgar la certificación digital, la autoridad de registro, a quien corresponda, enviará un correo electrónico al Solicitante y al Suscriptor notificando las razones de la decisión de no emitir el certificado.

Podrá automatizarse 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

Las solicitudes de certificados se atienden 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 ECD, 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 COLOMBIA:

- Protege la confidencialidad e integridad de los datos de registro de que dispone provenientes tanto de la identificación realizada de manera presencial como de la realizada a distancia.
- 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.
- Indica la fecha y la hora en que se expidió un certificado.
- Garantiza el control exclusivo de las claves por parte del usuario, no pudiendo la propia UANATACA COLOMBIA o sus Autoridades de Registro deducirlas o utilizarlas en ningún modo.

4.3.2 Notificación de la emisión al suscriptor

UANATACA COLOMBIA notifica la emisión del certificado al suscriptor y/o a la Persona natural identificada en el certificado y el método de generación/descarga.

4.4 Entrega y aceptación del certificado

UANATACA COLOMBIA, pondrá a disposición de las partes relevantes los certificados emitidos por la CA a través de los medios y procedimientos indicados al efecto según corresponda.

4.4.1 Responsabilidades de la ECD

UANATACA COLOMBIA suministra al interesado la documentación formal de los servicios de certificación digital que adquirió, de forma que indique claramente el contenido del certificado digital o las características del servicio adquirido como lo establece esta Declaración de Prácticas de Certificación y Política de certificación respectivamente.

Las Autoridades de Registro, durante este proceso, el operador o personal autorizado de la Autoridad de Registro UANATACA COLOMBIA debe realizar las siguientes actuaciones:

- Independientemente del método de identificación realizado por UANATACA COLOMBIA se deberá acreditar definitivamente la identidad de la Persona natural identificada en el certificado, de acuerdo con lo establecido en las secciones 3.2.2 y 3.2.4.
- Disponer del Contrato de Prestación de Servicios de Certificación debidamente firmado por el Suscriptor.
- Entregar la hoja de entrega y aceptación del certificado a la Persona natural identificada en el certificado con los siguientes contenidos mínimos.
    - Nombre y dirección de la ECD
    - Nombre y dirección del Suscriptor
    - Fecha de expiración de los servicios de certificación digital.
    - Alcance de los servicios de certificación digital
    - Información básica acerca del uso del certificado, incluyendo especialmente información acerca de la Entidad de Certificación Digital 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/o los mecanismos para su generación/descarga 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. Fecha en la que se otorga el servicio de certificación digital (esta fecha no debe ser anterior a la fecha en la cual se tomó la decisión sobre la certificación digital) o fecha de activación del servicio.

Toda esta información podrá incluirse en el propio Contrato de Prestación de Servicios de Certificación. Dicho lo cual, cuando se produzca la firma del Contrato Prestación de Servicios de Certificación por el Suscriptor, se entenderá perfeccionada la entrega y aceptación del certificado.

- Obtener la firma de la persona identificada en el certificado.

En ese sentido, se registrará documentalmente los anteriores actos y conservará los citados documentos originales (hojas de entrega y aceptación) según corresponda, remitiendo copia electrónica a UANATACA COLOMBIA, así como los originales cuando UANATACA COLOMBIA precise de acceso a los mismos.

4.4.2 Conducta que constituye aceptación del certificado

Indistintamente del método de identificación utilizada para la emisión del certificado cuando se haga entrega de la hoja de aceptación en formato digital o físico según corresponda, dicha aceptación del certificado por la persona natural identificada en el certificado se produce mediante la firma de la hoja de entrega y aceptación.

Cuando la generación y entrega del certificado se lleve a cabo a través del procedimiento automatizado definido por UANATACA COLOMBIA, la aceptación del certificado por la Persona natural identificada en el mismo se produce mediante la firma del contrato de Prestación de Servicios de Certificación utilizando el propio certificado.

4.4.3 Publicación del certificado

UANATACA COLOMBIA publica el certificado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes, siempre con la autorización de la persona natural identificada en el certificado mediante la firma del contrato.

4.4.4 Notificación de la emisión a terceros

UANATACA COLOMBIA no realiza ninguna notificación de la emisión a terceras entidades.

4.5 Uso del par de claves y del certificado

Los certificados y las respectivas claves podrán ser utilizados según lo estipulado en esta DPC y política de certificación correspondiente.

4.5.1 Uso por el firmante

UANATACA COLOMBIA obliga a:

- Facilitar a UANATACA COLOMBIA 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 juntamente con un dispositivo seguro de creación de firmas, reconocer su capacidad de producción de firmas digitales 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 6.3.
- Comunicar a UANATACA COLOMBIA, Autoridades de Registro 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 COLOMBIA obliga al firmante a responsabilizarse de:

- Que todas las informaciones suministradas por el mismo 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 una Entidad de Certificación Digital, 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 Proveedor de Servicios de certificación (entidad de certificación digital) ni en ningún otro caso.

4.5.2 Uso por el subscriptor

4.5.2.1 Obligaciones del suscriptor del certificado

UANATACA COLOMBIA obliga contractualmente al suscriptor a:

- Facilitar a la Autoridad 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 COLOMBIA, Autoridades de Registro y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:

  a) La pérdida, el robo o el compromiso potencial de su clave privada.

  b) 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.

  c) Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

  d) La pérdida, la alteración, el uso no autorizado, el robo o el compromiso, cuando exista, de la tarjeta.

  e) Trasladar a las personas naturales identificadas en el certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de estas.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de UANATACA COLOMBIA, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de la Entidad de certificación digital de UANATACA COLOMBIA.
- No utilizar la clave privada ni el certificado desde el momento en que se solicita o es advertido por la ECD o la RA de la revocación de este, o una vez expirado el plazo de validez del certificado.
- Informar a la mayor brevedad la existencia de alguna causa de revocación señaladas en los numerales 4.9.1 conforme al 4.9.4 de esta Declaración de Prácticas de Certificación.

4.5.2.2 Responsabilidad civil del suscriptor del certificado

UANATACA COLOMBIA obliga contractualmente al suscriptor a responsabilizarse por:

- 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 una Entidad de Certificación Digital (ECD), 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 Entidad de Certificación Digital ni en ningún otro caso.

4.5.3 Uso por el tercero que confía en certificados

Los terceros de buena fe sólo pueden depositar su confianza en los certificados para aquello que establece esta DPC, la PC y la normativa aplicable. En ese sentido, pueden realizar operaciones de clave pública de manera satisfactoria confiando en el certificado emitido por la cadena de confianza.

Así mismo, deben tener a precaución y asumir la responsabilidad de verificar el estado del certificado utilizando los medios y servicios ofrecidos por UANATACA COLOMBIA y que se establecen en esta DPC.

4.5.3.1 Obligaciones del tercero que confía en certificados

UANATACA COLOMBIA 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 vigencia, validez o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados, lo cual, incluirá comprobar que los certificados no han expirado ni han sido revocados (mediante consulta de la CRL o del servicio OCSP).
- 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
- Reconoce que las firmas generadas en un dispositivo seguro de creación de firma tienen la consideración legal de firmas digitales; 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 COLOMBIA, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de UANATACA COLOMBIA.
- Notificar a UANATACA COLOMBIA cualquier situación irregular con respecto al servicio prestado por la Entidad de Certificación Digital (ECD).

4.5.3.2 Responsabilidad civil del tercero que confía en certificados

UANATACA COLOMBIA 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

UANATACA COLOMBIA notificará con al menos treinta (30) días calendario de anticipación a sus suscriptores y/o firmantes la terminación de la vigencia de su certificado digital. Esta notificación podrá realizarse por correo electrónico a la dirección proporcionada por el suscriptor o por cualquier otro medio idóneo de comunicación cuando UANATACA COLOMBIA lo considere pertinente.

No obstante, es de resaltar que no constituye una obligación para UANATACA COLOMBIA garantizar la efectividad de la notificación sobre la terminación de la vigencia de su certificado o confirmar la recepción de esta, pues es una obligación de Suscriptor y/o firmante conocer la vigencia de su certificado digital y adelantar los trámites pertinentes ante UANATACA COLOMBIA para la emisión de su nuevo certificado.

La renovación se entenderá como la emisión de un nuevo certificado digital, por lo cual implica el registro de una nueva solicitud, la cual estará sujeta a la validación de identidad por parte de la autoridad de registro, y la generación de un nuevo par de claves.

4.7 Modificación de Certificados

UANATACA COLOMBIA no atiende requerimientos de modificación de certificados digitales.

Los casos en los que se requiera modificar algún dato en un certificado digital (actualización de la información contenida en un certificado) se tratan como una revocación de certificado y una nueva emisión de certificado, con cambio de claves.

4.8 Revocación y suspensión de certificados

La revocación de un certificado supone la pérdida de validez definitiva del mismo, y es irreversible.

Los certificados de UANATACA COLOMBIA no permiten la suspensión, debiendo proceder con la revocación del mismo.

4.8.1 Causas de revocación de certificados

Un certificado será revocado o cancelado ya sea por solicitud del suscriptor, o cuando la ECD conoce, tiene indicios o confirmación de alguna de las siguientes situaciones conforme al numeral 10.11.5.1 de la CEA-3.0-07:

a) Por compromiso de la seguridad en cualquier motivo, modo, situación o circunstancia.
b) Por muerte o incapacidad sobrevenida del suscriptor.
c) Por liquidación de la persona jurídica representada que consta en el servicio de certificación digital.
d) Por la confirmación de que alguna información o hecho contenido en el certificado digital es falso.
e) Por la ocurrencia de hechos nuevos que provoquen que los datos originales no correspondan a la realidad.
f) Por orden judicial o de entidad administrativa competente.
g) Por pérdida, inutilización del certificado digital que haya sido informado a la ECD.

h) Por la terminación del contrato de suscripción, de conformidad con las causales establecidas en el contrato
i) Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto de que se ponga en duda la confiabilidad del servicio.
j) Por el manejo indebido por parte del suscriptor del certificado digital.
k) Por el incumplimiento del suscriptor o de la persona jurídica que representa o la que está vinculado a través del Contrato del Servicio de Certificación Digital proporcionado por la ECD,

A continuación, a efectos meramente orientativos, se describen algunas circunstancias específicas derivadas de las causales anteriormente citadas, de manera que si concurre alguna de las siguientes circunstancias se revocará o cancelará el certificado digital conforme a los términos indicados en esta DPC.

4.8.1.1 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 falso o incorrecto.
c) Descubrimiento de que alguno de los datos contenidos en el certificado es falso o incorrecto.
d) Liquidación de la persona jurídica que consta en el certificado y/o bien cese del desempeño de la actividad económica para la cual estaba obligada a inscribirse en un registro de carácter fiscal o tributario, por la persona natural que consta en el certificado como empresa o entidad.

4.8.1.2 Circunstancias que afectan a la seguridad de la clave privada o del certificado:

a) Compromiso de la clave privada, de la infraestructura o de los sistemas de la ECD que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
b) Infracción, por UANATACA COLOMBIA, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas de Certificación o en la Política de certificación correspondiente.
c) Compromiso o sospecha de compromiso de la seguridad de la clave privada 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 natural identificada en el certificado, o la falta de diligencia en la custodia de la clave privada.
f) Cualquier causa que induzca a creer razonablemente que el servicio de certificación haya sido comprometido, poniendo en duda la confiabilidad del certificado digital.
g) En caso de que se advierta que los mecanismos criptográficos utilizados para la generación de la clave privada o el certificado no cumplen los estándares de seguridad mínimos necesarios para garantizar su seguridad.

4.8.1.3 Circunstancias que afectan al suscriptor o a la persona natural identificada en el certificado:

a) Finalización de la relación jurídica de prestación de servicios entre UANATACA COLOMBIA y el suscriptor.
b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado a la persona natural identificada en el certificado.
c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de este.
d) Infracción por el suscriptor, la entidad que se encuentra vinculado al 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, total o parcial, o el fallecimiento del suscriptor 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.

4.8.1.4 Otras circunstancias:

a) Por resolución judicial o administrativa que lo ordene.
b) La terminación del servicio de certificación de la Entidad de Certificación Digital UANATACA COLOMBIA
c) Cualquier otra causa lícita especificada en la presente DPC o en la PC que corresponda, entre ellas, el uso del certificado que sea dañino y continuado para UANATACA COLOMBIA. En este caso, se considera que un uso es dañino en función de los siguientes criterios:
    1. La naturaleza y el número de quejas recibidas.
    2. La identidad de las entidades que presentan las quejas.
    3. La legislación relevante vigente en cada momento.

4. La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.

4.8.2 Causas de suspensión de un certificado

Los certificados de UANATACA COLOMBIA no pueden ser suspendidos.

4.8.3 Causas de reactivación de un certificado

Los certificados de UANATACA no pueden ser reactivados.

4.8.4 Quién puede solicitar la revocación

Pueden solicitar la revocación de un certificado de acuerdo con esta DPC los siguientes:

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

4.8.5 Procedimientos de solicitud de revocación

La entidad que precise la revocación de un certificado puede solicitarlo directamente a UANATACA COLOMBIA o a la Autoridad de Registro del suscriptor o realizarlo él mismo a través del servicio online disponible en la página web de UANATACA COLOMBIA. La solicitud de revocación deberá incorporar la siguiente información:

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

La solicitud debe ser autenticada, por UANATACA COLOMBIA, 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 COLOMBIA en la dirección: https://www.web.uanataca.com/co/

En caso de que el destinatario de una solicitud de revocación por parte de una persona natural identificada en el certificado fuera la entidad suscriptora, una vez autenticada la solicitud debe remitir una solicitud en este sentido a UANATACA COLOMBIA.

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

Tanto el servicio de gestión de revocación 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 COLOMBIA.

4.8.6 Plazo temporal de solicitud de revocación

Las solicitudes de revocación se remitirán de forma inmediata en cuanto se tenga conocimiento.

4.8.7 Plazo temporal de procesamiento de la solicitud de revocación

La revocación se producirá inmediatamente cuando sea recibida. Si se realiza a través de un operador, se ejecutará dentro del horario ordinario de operación de UANATACA COLOMBIA o en su caso de la Autoridad de Registro. Si se realiza a través del servicio online, será inmediata.

4.8.8 Obligación de consulta de información de revocación de certificados

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

La verificación del estado de los certificados es obligatoria para cada uso de los certificados, ya sea mediante la consulta de la CRL o del servicio OCSP.

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 COLOMBIA o del servicio OCSP.

Las **Listas de Revocación de Certificados** se publican en el Depósito de la Entidad de Certificación, así como en los certificados emitidos, en sus respectivas extensiones CRL Distribution Points y *Authority Information Access* y en las direcciones web de acceso a ambos sistemas en línea así:

UANATACA CA1 2021

- http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
- http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

UANATACA CA2 2021

- http://crl1.uanataca.com/public/pki/crl/2021CA2sub.crl
- http://crl2.uanataca.com/public/pki/crl/2021CA2sub.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/

4.8.9 Frecuencia de emisión de listas de revocación de certificados (CRLs) y (ARLs)

UANATACA COLOMBIA emite una CRL al menos cada 24 horas.

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

La CRL mantiene obligatoriamente el certificado revocado hasta que expira.

La Lista de revocación de Autoridades de Certificación (ARLs) se actualizará cada 180 días.

4.8.10 Plazo máximo de publicación de CRLs

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

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

UANATACA COLOMBIA tiene disponibles dos sistemas en línea de verificación del estado de los certificados, uno mediante comprobación de revocación por CRL y otro por OCSP, ambos gratuitos y sin restricciones de acceso.

De forma alternativa, los terceros que confían en certificados podrán consultar el Depósito de certificados de UANATACA COLOMBIA, que se encuentra disponible las 24 horas de los 7 días de la semana en el web https://www.uanataca.com/co/

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

- *Autoridad de Certificación Raíz (UANATACA ROOT 2016):*
  - http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
  - http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

- *Autoridad de Certificación Subordinada (UANATACA CA1 2021):*

  - http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
  - http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

- *Autoridad de Certificación Subordinada (UANATACA CA2 2021):*

  - http://crl1.uanataca.com/public/pki/crl/2021CA2sub.crl
  - http://crl2.uanataca.com/public/pki/crl/2021CA2sub.crl

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de UANATACA COLOMBIA, 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 COLOMBIA suministra información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

4.8.12 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.

4.8.13 Requisitos especiales en caso de compromiso de la clave privada

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

4.9 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.

4.10 Depósito y recuperación de claves

UANATACA COLOMBIA únicamente custodia las claves de los certificados expedidos en formato HSM Centralizado. Estas claves no son exportables y están bajo el control exclusivo del titular del certificado. No ofrece servicios de recuperación de las claves privadas.

5 Controles de seguridad física, de gestión y de operaciones

UANATACA COLOMBIA y Uanataca, S.A., han suscrito un contrato de prestación de servicios de tecnología en el que UANATACA provee la infraestructura de clave pública (PKI) que sustenta el servicio de certificación de UANATACA COLOMBIA.

En el presente apartado, se describen los sistemas de seguridad con que cuenta el Centro de Procesamiento de Datos donde se aloja el sistema que contiene la infraestructura de clave pública PKI del servicio de la Autoridad de Certificación de Información de UANATACA COLOMBIA.

La Infraestructura de Clave Pública PKI de la Autoridad de Certificación de UANATACA COLOMBIA, está ubicada en un rack / armario aislado físicamente del resto de infraestructuras hospedados en el Centro de Procesamiento de Datos del proveedor de servicios de tecnología ADAM Ecotech (en lo sucesivo ADAM).

El Centro de Procesamiento de Datos de producción y contingencia se encuentra ubicado en una instalación segura dentro del edificio de ADAM. El mismo ha sido diseñado con tecnología TIER 3, el cual permite tener un esquema redundante para garantizar la continuidad en la operación y disponibilidad de los sistemas y cuenta con los controles de seguridad que se definen a continuación.

5.1 Controles de seguridad física

Se han establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran, los propios sistemas y los equipamientos empleados para las operaciones y la prestación de los servicios electrónicos de certificación.

En concreto, la política de seguridad aplicable a los servicios electrónicos de certificación establece prescripciones sobre lo siguiente:

- Control 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 antirrobo.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del Proveedor de Servicios de certificación.

Estas medidas resultan aplicables a las instalaciones desde donde se prestan los servicios electrónicos de certificación, en sus entornos de producción y contingencia, las cuales son auditadas periódicamente de acuerdo con la normativa aplicable y a las políticas propias destinadas a este fin.

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, así como varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.

Se 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 estos.

5.1.2 Acceso físico

Se dispone de tres niveles de seguridad física (Entrada del Edificio donde se ubica el CPD, acceso a la sala del CPD y acceso al Rack) 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 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 de este, 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 los administradores del servicio de hospedaje que disponen de la llave para abrir la jaula.

5.1.3 Electricidad y aire acondicionado

Las instalaciones 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 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 garantizan la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se desechan en cuyo caso se destruyen físicamente, o se reutilizan previo proceso de borrado permanente o formateo. 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

Se realiza el uso de un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del centro de operaciones.

5.2 Controles de procedimientos

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 ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad. Por razones de seguridad, la información relativa a los controles de procedimiento se considera materia confidencial y solo se explican de forma resumida.

5.2.1 Funciones (Roles) fiables

Se cuenta con roles de confianza distintos tanto para la administración y operación de las plataformas de la CA Raíz y la CA Subordinada., destinadas a la generación de las claves y a la administración de los perfiles de certificados, la Lista de Revocación de Autoridades de Certificación de la CA Raíz, CRL de la CA Subordinada como para la administración y la operación de las plataformas de la RA, destinadas a la administración y la operación de la Autoridad de Registro.

De esta forma, se garantiza una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de registro y certificación.

Se ha identificado, de acuerdo con la política de recursos humanos y de seguridad, las siguientes funciones o roles con la condición de fiables:

- **Auditor Interno:** Serán las únicas personas autorizadas a acceder a los logs de la CA y auditarlos. Deberá encargarse de comprobar el seguimiento de incidencias y eventos, comprobar la protección de los sistemas (vulnerabilidades, logs de acceso, usuarios, etc.), comprobar alarmas y elementos de seguridad física. 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.
- **Administrador de Sistemas**: responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación que componen la PKI.
- **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 Sistemas:** responsable necesario conjuntamente con el administrador de sistemas del funcionamiento correcto del hardware y software soporte de la plataforma de certificación. El operador es responsable de los procedimientos de copia de respaldo y mantenimiento de las operaciones diarias de los sistemas.

- **Operador de CA:** responsable necesario juntamente 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 (backup), de operación y mantenimiento de los sistemas en general de la CA.
- **Responsable de Seguridad**: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de la CA. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.
- **Agentes de la RA:** Son responsables por las operaciones diarias, tales como la revisión y aprobación de solicitudes. Usuarios de la RA con privilegios, integrado por:
    - **Operador de Registro**: Gestión y revisión la solicitud para la emisión de servicios de certificación digital, informar al cliente de la documentación necesaria para realizar el proceso de certificación digital, de la toma de datos, de la gestión del acuerdo contractual de prestación de servicios de certificación digital, la revisión de la información obtenida y la validación de la identidad del solicitante y/o suscriptor del servicio.
    - **Operador de Decisión**: Persona responsable de la toma de decisión sobre la emisión del certificado, solicitará la emisión en la CA, y firmará y entregará la documentación formal. También se encargará de gestionar la revocación de los certificados digitales mediante la aplicación correspondiente. Para la autenticación ante la CA para la solicitud de creación del certificado, el operador de Decisión utilizará su certificado y credenciales para identificarse a la entidad emisora (CA).
- **Administrador de la RA:** La persona responsable de administrar y configurar la RA, realizando cuando sea necesario el mantenimiento y actualización de la RA**.**
- **System Auditor**: auditor de los sistemas de información de la RA y evaluar las desviaciones encontradas, entre ellos, auditar los LOGs de la Autoridad de Registro dentro de la plataforma de la Autoridad de Registro, planificar la auditoría interna y ejecutarla reuniendo las evidencias suficientes utilizando metodología de muestras y técnicas de observación, inspección, investigación, entre otras.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Adicionalmente, se implementan criterios en sus políticas para la segregación de las funciones, como medida de prevención de actividades fraudulentas.

5.2.2 Número de personas por tarea

Se garantiza al menos dos personas para realizar las tareas relativas a la generación, recuperación y back-up de la clave privada de las Autoridades de Certificación. Igual criterio se aplica para la ejecución de tareas de emisión y activación de certificados y claves privadas de las

Autoridades de Certificación, y en general cualquier manipulación del dispositivo de custodia de las claves de las Autoridades de certificación 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 usuario/contraseña, certificado digital, tarjeta de acceso físico y/o llaves.

5.2.4 Roles que requieren separación de tareas

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

- Las tareas propias del rol de Auditor serán incompatibles con la operación y administración de sistemas, y en general aquellas dedicadas a la prestación directa de los servicios electrónicos de certificación.
- Emisión y revocación de certificados, serán tareas incompatibles con la Administración y operación de los sistemas.
- La administración y operación de los sistemas y las CAs, serán incompatibles entre sí.
- Los roles de la RA (Operador de Registro, Operador de Decisión, Auditor de la RA, Administrador de la RA) son incompatibles entre ellos y entre los roles de la CA, garantizando la independencia e imparcialidad entre las funciones de revisión y de decisión sobre la emisión de los certificados digitales.

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 de la Autoridad de Validación (servicios de OCSP).

5.3 Controles de personal

UANATACA COLOMBIA tiene en cuenta en los controles de personal los siguientes aspectos:

- Se mantiene la confidencialidad de la información, poniendo los medios necesarios y manteniendo una actitud adecuada en el desarrollo de sus funciones y, fuera del ámbito laboral en aquello referente a la seguridad de las infraestructuras.
- Se es diligente y responsable en el tratamiento, mantenimiento y custodia de los activos de la infraestructura.
- No se revela información no pública fuera del ámbito de la infraestructura, ni se extraen soportes de información a niveles de seguridad inferiores.
- Se reporta al Responsable de Seguridad, lo más pronto posible, cualquier incidente que se considere que afecta a la seguridad de la infraestructura, o limita la calidad del servicio.
- Se utilizan los activos de la infraestructura para las finalidades que les han sido encomendadas.
- No se accede voluntariamente, ni se elimina o altera información no destinada a su persona o perfil profesional.

5.3.1 Requisitos de historial, calificaciones, experiencia y autorización

Todo el personal está cualificado y/o 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.

Se asegura de que el personal de registro es confiable para realizar las tareas de registro. A tal efecto se exige una Autorización para su rol dentro de UANATACA COLOMBIA. El Administrador y Agentes de la RA, reciben formación para realizar las tareas de registro y validación de las peticiones.

En general, se retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de conflictos de interés y/o la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

No se asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por una 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.
- Referencias profesionales.

En todo caso, las Autoridades de Registro podrán establecer procesos de comprobación de antecedentes diferentes, siempre preservando las políticas establecidas, siendo responsables por la actuación de las personas que autoricen en sus operaciones.

5.3.2 Procedimientos de investigación de historial

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

- Información suministrada en la Hoja de Vida
- Referencias de los trabajos de los últimos años
- Referencias profesionales
- Estudios, incluyendo titulación alegada.

UANATACA COLOMBIA obtiene el consentimiento inequívoco del afectado para dicha investigación previa, y procesa y protege todos sus datos personales en cumplimiento de la normativa vigente en materia de protección de datos personales.

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.

5.3.3 Requisitos de formación

Se forma al personal para asegurar la correcta realización de las tareas asignadas a sus respectivos roles, y en función de los conocimientos que requiera cada uno de los puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.

Los programas de formación son revisados, 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 COLOMBIA. 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

Se actualiza la formación del personal de acuerdo con las necesidades, y con la frecuencia suficiente para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación, ante cambios tecnológicos, normativos, introducción de nuevas herramientas o modificación de procedimientos operativos, se llevará a cabo la formación adecuada para el personal afectado.

5.3.5 Secuencia y frecuencia de rotación laboral

No aplicable.

5.3.6 Sanciones para acciones no autorizadas

Se dispone de un sistema sancionador interno, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable.

Las acciones disciplinarias incluyen la suspensión, separación de las funciones y hasta 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. Cualquier acción que comprometa la seguridad de los procesos aceptados podría, 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 COLOMBIA.

5.3.8 Suministro de documentación al personal

La ECD 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

Se produce y guarda registro de los logs, en especial, 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 que realizan tareas de certificación.
- 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 natural identificada en el certificado, en caso de certificados de organización, si se gestiona esa información.
- 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

Se revisan los 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.

Se 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

Los LOGs de cada uno de los servicios de certificación digital con fines de auditoria se retendrán como mínimo tres (3) años y hasta diez (10) años en función del tipo de información registrada para garantizar la seguridad del sistema.

5.4.4 Protección de los registros de auditoría

Los logs de los sistemas son protegidos mediante mecanismos que aseguran su integridad:

- 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

Se dispone de un procedimiento adecuado de copia de seguridad 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.

Se 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

La ECD realiza periódicamente una revisión de vulnerabilidades y test de intrusión para analizar la infraestructura que utiliza la ECD. El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de UANATACA S.A., proveedor de tecnología.

Los análisis de vulnerabilidad deben ser ejecutados, repasadas y revisadas por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados periódicamente de acuerdo con el procedimiento interno previsto para este fin.

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

Se 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 COLOMBIA (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 suscriptores, firmantes y/o solicitantes 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.
- CRLs emitidas o registros del estado de los certificados generados (Consultas OCSP).
- 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 COLOMBIA y/o las Autoridades de Registro según corresponda, serán responsables del correcto archivo de todo este material.

5.5.2 Periodo de Conservación de registros

Se archivan los registros especificados en el numeral 5.5.1 de manera general durante al menos 10 años, o el período que establezca la legislación vigente cuando sea aplicable.

En particular, los registros de certificados revocados estarán accesibles para su libre consulta durante al menos 10 años o el periodo que establezca la legislación vigente desde su cambio de estado.

5.5.3 Protección del archivo

Se 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.

Se asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en instalaciones seguras externas.

5.5.4 Procedimientos de copia de respaldo

Se 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.

Como mínimo se realizan copias de respaldo incrementales diarias de todos sus documentos electrónicos y realizar copias de respaldo completas semanalmente para casos de recuperación de datos.

Además, se (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

Se dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados interno, también se dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos

5.5.7 Procedimientos de obtención y verificación de información de archivo

Se dispone de un procedimiento donde se describe el proceso para verificar que la información archivada es correcta y accesible. Sólo el personal autorizado para ello tiene acceso a los archivos físicos de soportes y archivos informáticos, para obtener y llevar a cabo verificaciones de integridad de dichos archivos. Se proporcionan tanto la información y medios de verificación al auditor.

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

Se han desarrollado políticas, un procedimiento de seguridad y plan de continuidad del negocio que le permiten la gestión y recuperación de los sistemas en caso de incidentes y compromiso de sus operaciones, asegurando los servicios críticos de revocación y publicación del estado de los certificados.

El procedimiento de seguridad para la gestión de incidencias cumple con el anexo A de la norma ISO 27001.

De conformidad con la normativa, UANATACA COLOMBIA que ante los siguientes eventos y/o incidentes de seguridad, actuará de la siguiente manera:

- Compromiso de la clave privada de la ECD. En el caso que una clave de CA se viera comprometida, UANATACA COLOMBIA procedería con la revocación de la clave de CA afectada y de todos los certificados activos emitidos por ésta.
  Asimismo procedería a informar en un plazo máximo de 24 horas desde que tuviese conocimiento a la ONAC, así como a todos los suscriptores y firmantes.
  UANATACA COLOMBIA mantendría en todo momento vigente el servicio de validación de certificación.

- Vulneración del sistema de seguridad de la ECD. En caso que el sistema de seguridad haya sido vulnerado, se procederá con el procedimiento de gestión de brechas de seguridad. En ese caso, el protocolo establece una serie de procedimientos por tal de detectar, comunicar, auditar, evaluar y mitigar cualquier afectación a la seguridad. Asimismo se procederá de acuerdo con el procedimiento de comunicación para advertir a las partes afectadas, así como la ONAC.

- Fallas en el sistema de la ECD que comprometan la prestación de servicio. Ante escenarios que pudieran comprometer la prestación del servicio, UANATACA COLOMBIA dispone de un plan de continuidad de negocio con los distintos escenarios plausibles de interrupción de las actividades como prestador de servicios de certificación. Asimismo, se detalla el equipo de respuesta y las instrucciones para poder restaurar la normalidad de la actividad.

- Cuando los sistemas de cifrado pierdan vigencia no pudiendo ofrecer el nivel de seguridad contratado por el suscriptor. El compromiso de algoritmos destinados a la prestación del servicio o a la seguridad en el mismo, son escenarios contemplados en el plan de continuidad de negocio de UANATACA COLOMBIA.

5.7.2 Corrupción de recursos, aplicaciones o datos

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se seguirán los procedimientos de gestión oportunos de acuerdo con las políticas de seguridad y gestión de incidentes, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres.

5.7.3 Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso de UNATACA COLOMBIA, se activarán los procedimientos de compromiso de claves de acuerdo con las políticas de seguridad, gestión de incidencias y continuidad del negocio, que permita la recuperación de los sistemas críticos, si fuera necesario en un centro de datos alternativo.

5.7.4 Continuidad del negocio después de un desastre

Se restablecerán los servicios críticos (revocación, y publicación de información de estado de certificados) de acuerdo con el plan de incidencias y continuidad de negocio existente

restaurando la operación normal de los servicios anteriores en las 24 horas siguientes al desastre.

Se 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

Se asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios de la ECD. En este sentido, se garantiza un mantenimiento continuo de los registros definidos en el apartado 5.5.1, por el tiempo establecido en el apartado 5.5.2 de esta Declaración de Prácticas de Certificación.

No obstante, lo anterior, si procede se ejecutará todas las acciones que sean necesarias para transferir a un tercero o a un depósito notarial, las obligaciones de mantenimiento de los registros especificados durante el periodo correspondiente según esta Declaración de Prácticas de Certificación o la previsión legal que corresponda.

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

- Informar en primera instancia a ONAC y a la Superintendencia de Industria y Comercio acerca del cese de actividades con una anticipación de treinta (30) días y solicitar su autorización.
- Luego de haber sido autorizado, informar por medio de dos avisos publicados en diarios de amplia difusión y por el correo electrónico declarado, a todos los Suscriptores con un intervalo de quince (15) días sobre la autorización y terminación de su actividad o actividades, la fecha precisa de cesación y las consecuencias jurídicas de ésta respecto de los certificados expedidos. Además, informar la posibilidad de que el suscriptor obtenga el reembolso equivalente al valor del tiempo de vigencia restante sobre el servicio contratado. En todo caso, los suscriptores podrán solicitar la revocación y el reembolso equivalente al valor del tiempo de vigencia restante de los servicios, si lo solicitan dentro de los dos (2) meses siguientes a la segunda publicación del aviso.
- En cualquier caso, se garantiza la continuidad del servicio a los usuarios quienes ya hayan contratado los servicios de la ECD, directamente o por medio de terceros, sin ningún costo adicional a los servicios que contrató.
- Proveerá de los fondos necesarios, incluyendo un seguro de responsabilidad civil, para continuar la finalización de las actividades de revocación.
- 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.

6 Controles de seguridad técnica

Se emplean 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. Uanataca S.A cuenta con una organización de seguridad encargada de su gestión sobre la base la norma UNE-ISO/IEC 27001:2017 sometida a auditorías de seguimiento cada año. Los procedimientos y controles de seguridad del proveedor de infraestructura de la ECD se realizan bajo los controles aplicables de dicho estándar de seguridad.

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 2021" y "UANATACA CA2 2021" han sido creadas por la entidad de certificación raíz "UANATACA ROOT 2016" de acuerdo con los procedimientos de ceremonia de UANATACA S.A, 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. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por UANATACA S.A.

Para la generación de la clave de la entidad de certificación intermedia se utilizan dispositivos con las certificaciones FIPS 140-2 level 3 y Common Criteria EAL4+.

UANATACA CA1 2021	4.096 bits	13 años
• Certificados de entidad final	2.048 bits	Hasta 2 años
• Certificados de Estampado Cronológico (Sello de tiempo)	2.048 bits	Hasta 8 años
• UANATACA CA2 2021	4.096 bits	13 años
• Certificados de entidad final	2.048 bits	Hasta 2 años
• Certificados de Estampado Cronológico (Sello de tiempo)	2.048 bits	Hasta 8 años

6.1.1.1 Generación del par de claves del firmante

Las claves del firmante pueden ser generadas por él mismo mediante dispositivos hardware y/o software autorizados por la ECD. Nunca se generan claves fuera de un dispositivo seguro de creación de firma para ser enviadas al firmante.

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

La generación de las claves de la CA Raíz y la CA Subordinada se realiza, de acuerdo con un procedimiento documentado de ceremonia de claves, dentro de una sala de seguridad, en un dispositivo criptográfico hardware (HSM) certificado FIPS 140-2 nivel 3, por personal autorizado con un control dual, y en presencia de testigos y de un auditor externo.

La ECD garantiza que las claves de firma de la CA Raíz y la CA Subordinada no son empleadas para otro supuesto que los indicados en el presente documento.

Para los certificados de Entidad final, la generación de claves se realizará en dispositivos seguros de creación de firma que aseguren razonablemente que la clave privada únicamente puede ser utilizada por el Suscriptor, bien por medios físicos, bien estableciendo el Suscriptor los controles y medidas de seguridad adecuadas.

En los casos en que la ECD pueda garantizar que las claves criptográficas del Suscriptor han sido creadas en un dispositivo criptográfico que cumpla con los requisitos mínimos (si el tipo de soporte es HSM Centralizado), se indicará en el propio certificado mediante la inclusión del identificador OID correspondiente en la extensión *Certificate Policies.*

6.1.2 Entrega (envío) de la clave privada al firmante

En certificados en dispositivo seguro de creación de firma la clave privada se genera y se almacena debidamente protegida en el interior de dicho dispositivo. Las credenciales de acceso a la clave privada son introducidas por el propio firmante, no siendo almacenadas ni susceptibles de capacidad de deducción o intercepción por el sistema de generación y custodia remota. En los casos en que la ECD genera la clave privada de los certificados (si el tipo de soporte es HSM Centralizado), la ECD no entrega la clave privada al Solicitante o al Suscriptor (firmante) pero garantizará el acceso seguro a la misma por el mismo. La clave privada no se envía al firmante, es decir, nunca abandona el entorno de seguridad que garantiza el control exclusivo de la clave privada por parte del firmante.

6.1.3 Entrega (envío) de la clave pública al emisor del certificado

El método de remisión de la clave pública a la Entidad de Certificación Digital es PKCS#10, otra prueba criptográfica equivalente o cualquier otro método aprobado por UANATACA COLOMBIA.

6.1.4 Distribución de la clave pública de la ECD

Las claves de UANATACA COLOMBIA 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 Autoridades de Certificación Raíz y Subordinadas estará a disposición de los usuarios en la página web de UANATACA COLOMBIA.

6.1.5 Tamaños de claves

- La longitud de las claves de las Autoridad de Certificación subordinadas es de 4096 bits.
- La longitud de las claves de los Certificados de Entidad final es de 2048 bits.
-

6.1.6 Generación de parámetros de clave pública

La clave pública de la Autoridades de Certificación raíz, subordinadas y de los certificados de los suscriptores está codificada de acuerdo con RFC 5280 y PKCS#1.

6.1.7 Comprobación de calidad de parámetros de clave pública

- Longitud del Módulo = 4096 bits
- 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 (Campo Key Usage de X.509V3)

Todos los certificados incluyen las extensiones Key Usage y Extended Key Usage, excepto los propios certificados de la CA Raíz y de la CA Subordinada que sólo incluyen la extensión Key Usage, indicando en ambas extensiones los usos habilitados de las claves. En este último caso, los usos de las claves para los certificados de las CA son exclusivamente para la firma de certificados y de CRLs.

Los usos admitidos de la clave para cada tipo de certificado de entidad final están definidos en la Política de Certificados correspondiente. De manera general, los usos de las claves para los certificados de entidad final son exclusivamente para la firma digital, el no repudio y cifrado de datos.

6.2 Protección de la clave privada

En el presente apartado se recogen los controles relativos a la clave privada de la Autoridad de Certificación Subordinada, por tal de garantizar el control exclusivo por parte de UANATACA.

6.2.1 Estándares de módulos criptográficos

En relación con los módulos que gestionan claves de UANATACA COLOMBIA y de los suscriptores de certificados de firma digital, se asegura el nivel exigido por los estándares indicados en las secciones anteriores, específicamente, los módulos criptográficos empleados para generar y almacenar las claves de la CA Raíz y la CA Subordinada (HSM) están certificados con la norma FIPS 140-2 nivel 3 y/o Common Criteria (EAL4+). Las claves de los Suscriptores de certificados en HSM Centralizado, Smartcard y token son generadas de forma segura en un dispositivo criptográfico con certificación FIPS 140-2 nivel 3 y/o Common Criteria (EAL4+).

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 autorizadas para la activación de las claves, con uso de sus respectivos dispositivos criptográficos protegidos con un PIN, para el acceso y activación de las mencionadas claves privadas. Dicho control garantiza que una persona no posea el control individual, descentralizando la responsabilidad de activar y usar las claves privadas de la CA Raíz y la CA Subordinada.

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

6.2.3 Depósito de la clave privada

No se almacenan copias utilizables por medios propios de las claves privadas de los firmantes.

La clave privada de la CA Raíz está custodiada por dispositivos criptográficos hardware (HSM) certificados con la norma FIPS 140-2 nivel 3 y/o Common Criteria (EAL4+), garantizando que la clave privada nunca está en claro fuera del dispositivo criptográfico. La activación y posterior uso de la clave privada requiere el control multi-persona detallado en la sección 6.2.2. Con posterioridad a la operación realizada, la sesión se cierra, quedando desactivada la clave privada.

La clave privada de la CA Subordinada está custodiada por dispositivos criptográficos hardware (HSM) certificados con la norma FIPS 140-2 nivel 3 y/o Common Criteria (EAL4+),, garantizando que la clave privada nunca está en claro fuera del dispositivo criptográfico. La activación de la clave privada requiere el control multi-persona detallado en la sección 6.2.2.

En el caso de certificados de suscriptores en HSM Centralizado, la ECD custodia las claves privadas protegidas mediante métodos de cifrado robustos en dispositivos criptográficos hardware (HSM) certificados FIPS 140-2 nivel 3 y/o Common Criteria (EAL4+), que utilizan una clave que reside en los HSM y otra clave derivada de una contraseña definida por el Suscriptor (firmante) o el solicitante.

Para certificados generados en dispositivos criptográficos como token o tarjeta deben ostentar las certificaciones en estándares criptográficos como FIPS 140-2 Level 3 o superior, o Common Criteria (EAL4+) o superior relacionado a seguridad y almacenamiento de llaves.

Las claves en hardware de los suscriptores se crean dentro del dispositivo criptográfico entregado por la SubCA.

6.2.4 Copia de respaldo de la clave privada

UANATACA COLOMBIA realiza copia de seguridad 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.

Claves generadas en dispositivo seguro de creación de firma: No es posible realizar backups de las claves, ya que no es posible su exportación. Si estas se encuentran en un HSM, es posible realizar backups de un bloob cifrado con la clave Security World del HSM utilizado, siendo imposible su descifrado sin el uso de las credenciales que sólo el titular del certificado conoce.

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 también se guardará copia de la clave privada asociada al certificado de cifrado.

6.2.6 Introducción (trasferencia) de la clave privada en el módulo criptográfico

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

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 COLOMBIA. 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.

6.2.8 Método de desactivación 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.

La clave privada de la CA Raíz se desactivará en sus HSM después de su uso, por procedimiento. La clave privada de la CA Subordinada sólo se desactivará en sus HSM en situaciones extraordinarias debidamente documentado. En el caso de certificados de Suscriptores en HSM Centralizado, la clave privada se desactivará después de cada uso.

6.2.9 Método de destrucción de la clave privada

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 hardware y podrán ser destruidas mediante una aplicación informática especial en las dependencias de las RA o de UANATACA.

6.2.10 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.

Los certificados emitidos por la ECD por tanto las claves públicas, se conservarán durante el periodo exigido por la legislación vigente cuando sea aplicable, o al menos durante 10 años desde su expiración.

6.3.2 Períodos de utilización de las claves pública y privada

La clave privada no debe ser usada después del periodo de validez o la revocación del certificado.

La clave pública no debe ser usada después del periodo de validez o la revocación del certificado, excepto por los Terceros que confían para verificar datos históricos.

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

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de 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, se 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 subordinadas están 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 o varias contraseñas lo más completas y complejas posible. El firmante debe recordar dicha(s) contraseña(s).

6.5 Controles de seguridad informática

UANATACA COLOMBIA emplea sistemas fiables para ofrecer sus servicios de certificación. Asimismo, UANATACA COLOMBIA 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 COLOMBIA aplica los controles del esquema de certificación sobre sistemas de gestión de la información ISO 27001.

La documentación técnica y de configuración de UANATACA detalla la arquitectura de los equipos que ofrecen el servicio de certificación tanto en su seguridad física como lógica.

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

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

6.5.1 Requisitos técnicos específicos de seguridad informática

Cada servidor incluye las siguientes funcionalidades:

1. Control de acceso a los servicios de las Autoridades de Certificación subordinadas y gestión de privilegios.
2. Imposición de separación de tareas para la gestión de privilegios.
3. Identificación y autenticación de roles asociados a identidades.
4. Archivo del historial del suscriptor, de las Autoridades de Certificación subordinadas y datos de auditoría.
5. Auditoria de eventos relativos a la seguridad.
6. Auto-diagnóstico de seguridad relacionado con los servicios de las Autoridades de Certificación subordinadas.
7. Mecanismos de recuperación de claves y del sistema de las Autoridades de Certificación subordinadas.

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. La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan dar lugar a brechas de seguridad. La seguridad física está garantizada por las instalaciones ya definidas anteriormente y la gestión de

personal está controlado debido al reducido número de personas (autorizadas) que realizan sus trabajos en los Centros de Datos subcontratados.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por UANATACA COLOMBIA 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 COLOMBIA 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 COLOMBIA exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de servicios electrónicos de certificación.

6.6.3 Clasificación y gestión de información y bienes

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

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

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

6.6.4 Operaciones de gestión

Se 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 se desarrolla en detalle el proceso de gestión de incidencias.

UANATACA COLOMBIA 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.

6.6.5 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 mantiene un registro de las capacidades de los equipos. Juntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

Reportes de incidencias y respuesta

Se 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

Se definen 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.

6.7 Gestión del sistema de acceso

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

UANATACA COLOMBIA 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 Gestión del ciclo de vida del hardware criptográfico

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 COLOMBIA 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 COLOMBIA 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 la CA Raíz y de la CA Subordinada de UANATACA COLOMBIA almacenada en el hardware criptográfico se eliminarán una vez se hayan retirado los dispositivos.

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

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.

6.9 Controles de seguridad de red

UANATACA COLOMBIA 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.

6.10 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 COLOMBIA son realizadas en módulos con las certificaciones FIPS 140-2 nivel 3 y/o Common Criteria (EAL4+),.

6.11 Fuentes de Tiempo

UANATACA COLOMBIA tiene un procedimiento de sincronización de tiempo coordinado vía NTP, que accede a dos servicios independientes:

- La primera sincronización del tiempo para los servicios de la ECD se obtiene mediante consulta al Instituto Nacional de Metrología (INM) de Colombia, institución encargada de mantener, coordinar y difundir la hora legal de la República de Colombia. Los servidores se mantienen actualizados con la hora UTC, mediante sincronización a través del protocolo NTP v4, conforme al estándar RFC 5905 "*Network Time Protocol Version 4: Protocol and Algorithms Specification*".

- La segunda dispone de una sincronización complementaria, vía NTP, Servicio basado en antenas y receptores GPS que permite un nivel de confianza de STRATUM 1 (con dos sistemas en alta disponibilidad)

6.12 Cambio de estado de un Dispositivo Seguro de Creación de Firma (SSCD)

UANATACA COLOMBIA en el caso de modificación del estado de la certificación de los dispositivos seguros de creación de firma (SSCD), procederá de la siguiente manera:

- UANATACA COLOMBIA dispone de una lista de varios SSCD certificados, así como una estrecha relación con proveedores de dichos dispositivos, con el fin de garantizar alternativas a posibles pérdidas de estado de certificación de dispositivos SSCD.
- En el supuesto de finalización del periodo de validez o pérdida de la certificación, UANATACA COLOMBIA no utilizará dichos SSCD para la emisión de nuevos certificados

electrónicos, bien sea en nuevas emisiones como eventualmente en posibles renovaciones.

- Procederá de inmediato a cambiar a de dispositivos SSCD con certificación válida.
- En el supuesto caso que un dispositivo SSCD haya demostrado no haberlo sido nunca, por falsificación o cualquier otro tipo de fraude, se procederá de inmediato a comunicárselo a sus clientes y al ente regulador, revocar los certificados electrónicos emitidos en estos dispositivos y reemplazarlos emitiéndolos en SSCD válidos.

7. Perfiles de certificados y listas de certificados revocados

7.1 Perfil de certificado

Todos los certificados emitidos bajo esta política cumplen con el estándar X.509 versión 3 y el RFC 3739 y los diferentes perfiles descritos en la norma ETSI EN 319 412.

La documentación relativa a los perfiles de la norma ETSI EN 319 412 puede solicitarse a UANATACA COLOMBIA.

7.1.1 Número de versión

UANATACA COLOMBIA emite certificados X.509 Versión 3.

7.1.2 Extensiones del certificado

Las extensiones de los certificados se encuentran detalladas en la política de certificación disponible en la página web https://web.uanataca.com/co/

En la DPC para el estampado cronológico de UANATACA se especifican las extensiones del certificado de TSU de la TSA de la ECD.

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 de certificados, CRL y respuestas OCSP es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública en certificados 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 (CRL)

7.2.1 Número de versión

Las CRL emitidas por UANATACA COLOMBIA son CRL de la versión 2., conforme a los siguientes estandares: - RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. - ITU-T X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

7.2.2 Perfil de OCSP

El certificado OCSP de la CA Subordinada de la ECD es coherente con lo dispuesto en los siguientes estándares: - RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

8. Auditoría de conformidad

UANATACA COLOMBIA se somete a las auditorías de acreditación que realiza ONAC de conformidad con los dispuesto en el artículo 162 del Decreto-ley 19 de 2012. Asimismo, de acuerdo con lo exigido en los Criterios Específicos de Acreditación de ONAC, UANATACA se somete a auditoría interna y auditoría de tercera parte en los términos previstos en dicho documento. En caso de requerirse, UANATACA permite y facilita la realización de auditorías por parte de la Superintendencia de Industria y Comercio de Colombia siempre y cuando este organismo considere necesarias y sea comunicada previamente con un término prudencial de anticipación.

8.1 Frecuencia de la auditoría de conformidad

Se 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 de acreditación que competen a UANATACA COLOMBIA son realizadas por auditores que cumplen con lo establecido en los Criterios Específicos de ONAC vigentes y siguiendo el procedimiento aplicable.

8.3 Relación del auditor con la entidad auditada

Se declara que no existe ningún conflicto de intereses entre las empresas que realizan auditorías externas que puedan desvirtuar su actuación en su relación con UANATACA.

8.4 Listado de elementos objeto de auditoría

Las auditorías verifican de forma general que se cumple con los principios establecidos en los requisitos de acreditación (Criterios Específicos de ONAC vigentes), la legislación vigente aplicable y la documentación establecida en el sistema de gestión de la ECD. La auditoría verifica respecto a UANATACA COLOMBIA:

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, así como, los métodos de identificación previstos por la legislación de la República de Colombia tanto presenciales como a distancia
c. Que la Declaración de Prácticas de Certificación y demás documentación jurídica vinculada, se ajusta a lo acordado por UANATACA COLOMBIA 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 las Autoridades de Certificación, Autoridades de Registro 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 los auditores que han ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta las medidas correctivas que solventen dichas deficiencias.

Si UANATACA COLOMBIA 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 COLOMBIA que podrá ejecutar las siguientes acciones:

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

8.6 Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se comunicarán a UANATACA COLOMBIA 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

Se 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.

Se podrán especificar las tarifas de emisión para los correspondientes certificados en la página web de UANATACA COLOMBIA.

9.1.2 Tarifa de acceso a los certificados

El acceso a los certificados emitidos por los respectivos Suscriptores y/o Solicitantes es libre y gratuito.

9.1.3 Tarifa de revocación o acceso a la información de estado

No se establece ninguna tarifa para la revocación de certificados, ni para el acceso a la información de estado de los certificados.

UANATACA COLOMBIA provee un acceso gratuito a la información relativa al estado de los certificados, por medio de la publicación de las correspondientes CRL y del servicio OCSP.

9.1.4 Tarifas de otros servicios

Las tarifas aplicables a otros posibles servicios se negociarán entre UANATACA COLOMBIA y los clientes de los servicios ofrecidos.

9.1.5 Política de reintegro

Sin estipulación.

9.2 Capacidad financiera

UANATACA COLOMBIA dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones garantizando sus responsabilidades en su actividad como

Entidad de Certificación Digital tal como se define en la legislación colombiana vigente, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios ante los usuarios de sus servicios y a terceros, garantizando sus responsabilidades en su actividad como Entidad de Certificación Digital tal como se define en la legislación colombiana vigente.

9.2.1 Cobertura

UANATACA COLOMBIA de acuerdo con el artículo 9 del decreto 333 de 2014 establece mediante un Seguro de Responsabilidad Civil vigente con la cobertura igual o superior a la exigida por la normativa aplicable y expedida por una entidad aseguradora vigilada por la Superintendencia Financiera de Colombia.

La garantía citada tiene las siguientes características:

- Cubre todos los riesgos u perjuicios contractuales y extracontractuales de suscriptores y terceros de buena fe de las actividades para las cuales cuenta con acreditación.
- Cubre los anteriores riesgos por una cuantía asegurada por evento igual o superior a 7.500 salarios mínimos mensuales por evento.
- Cubre la restitución automática del valor asegurado.
- La Entidad aseguradora, el tomador y el asegurado están obligados a informar previamente a ONAC la terminación del contrato de seguro o las modificaciones que reducen el alcance o monto de la cobertura.
- El seguro se hará cargo de todas las cantidades que UANATACA COLOMBIA resulte lealmente obligado a pagar, hasta el límite de cobertura contratado, como resultado de un procedimiento judicial en el que pueda declararse su responsabilidad, derivada de cualquier acto negligente, error u incumplimiento no intencionado de la legislación vigente entre otros.

9.2.2 Otros activos

Sin estipulación.

9.2.3 Cobertura para terceros que confían en certificados

No existe cobertura para los terceros aceptantes.

9.3 Confidencialidad

9.3.1 Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales:

- 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 de la CA raíz y la CA subordinada de UANATACA generadas y/o almacenadas por la ECD.
- Procedimiento y Acta de Ceremonia de generación de las claves de la CA Raíz y la CA subordinada.
- 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 Autoridad de Certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- 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:

- La contenida en la presente DPC.
- La contenida en la Política de Certificado (PC)
- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por la Entidad de Certificación.
- La información contenida en los certificados, así como cualquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado, puesto que para su emisión el Suscriptor y/o Solicitante otorga previamente su consentimiento, incluyendo los diferentes estados o situaciones del certificado.
- Los usos y límites reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de expiración.
- 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 o caducado y el motivo que provocó el cambio de estado.

- Las listas de revocación de certificados (CRLs), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Cualquier otra información que no esté indicada en la sección anterior y cuya publicidad sea impuesta normativamente.

9.3.3 Divulgación de información de suspensión y revocación

Véase la sección anterior.

9.3.4 Divulgación legal de información

UANATACA COLOMBIA no divulga la información confidencial, ni la información que contiene de datos personales 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.

Se indicarán estas circunstancias en la política de privacidad prevista en la sección 9.4.

9.3.5 Divulgación de información por petición de su titular

Se 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 natural 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 COLOMBIA garantiza el cumplimiento de la normativa vigente en materia de protección de datos personales de los Suscriptores y/o Solicitantes de los servicios de certificación digital, especialmente en cumplimiento de la Ley Estatutaria 1581 de 2012 y demás decretos reglamentarios relacionados. De acuerdo al Régimen General de Protección de Datos Personales, cuyo objeto es "(...) *desarrollar el derecho constitucional que tienen todas las*

personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma" y de los Criterios Específicos de Acreditación Entidades de Certificación Digital - CEA-3.0-07 vigente.

Serán considerados como datos personales, la información de nombres, dirección, correo electrónico, y toda información que pueda vincularse a la identidad de una persona natural o jurídica, contenidos en los contratos y solicitudes de los Suscriptores y/o Solicitantes. Esta información será considerada como confidencial y será de uso exclusivo para las operaciones de certificación digital estipuladas, a excepción que exista un previo consentimiento del usuario final de dichos datos o medie una orden judicial o administrativa que así lo determine, en cuyo caso, a menos que lo prohíba la ley, el Suscriptor o la persona implicada será notificada de la información suministrada.

Es responsabilidad de los Suscriptores y/o Solicitantes garantizar que la información provista a la Entidad de certificación sea veraz y vigente. Asimismo, son responsables del perjuicio que pudieran causar por aportar datos falsos, incompletos o inexactos.

UANATACA COLOMBIA cuenta con una Política de Privacidad de datos personales que detalla los principios, recolección y tratamiento de datos personales y que se encuentra publicada en la página web. En cumplimiento de esta, UANATACA COLOMBIA ha documentado en esta Declaración de Prácticas de Certificación los aspectos y procedimientos de seguridad y organizativos, con el fin de garantizar que todos los datos personales a los que tenga acceso son protegidos ante su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, asegurando la confidencialidad e integridad de estos.

A continuación, se detalla la política de privacidad aplicable a todos los servicios de certificación de UANATACA COLOMBIA en el que se detalla toda la información necesaria con respecto al tratamiento de datos personales realizado por UANATACA COLOMBIA.

Finalidad del tratamiento

UANATACA COLOMBIA trata los datos de carácter personal facilitados para llevar a cabo los servicios electrónicos solicitados, concretamente la expedición de certificados digitales, todo ello de acuerdo con lo previsto en la Declaración de Prácticas de Certificación (DPC) de UANATACA COLOMBIA, la cual se encuentra disponible en el siguiente enlace: (https://web.uanataca.com/co/).

Las finalidades de tratamiento de datos relativos al SERVICIO son las siguientes:

- Identificación de los suscriptores y/o firmantes de los certificados electrónicos.

- Expedición y gestión de certificados digitales.

- Gestión del ciclo de vida del certificado (emisión, renovación, y revocación).
- Comunicaciones relativas al servicio.
- Custodia y mantenimiento del archivo relativo al certificado electrónico.
- Gestión administrativa, contable y de facturación derivada de la contratación.

UANATACA COLOMBIA informa que los datos personales facilitados únicamente se tratarán para las finalidades anteriormente descritas y no serán tratados de manera incompatible con las mismas.

Los datos serán obtenidos directamente de los solicitantes de los certificados.

Legitimación del tratamiento

De acuerdo con las finalidades de tratamiento indicadas, la base legal para el tratamiento de los datos personales de los usuarios es:

- La legitimación del tratamiento para la Prestación de Servicios de Certificación es la ejecución del contrato de los servicios solicitados, donde el usuario es parte de este.
- La legitimación del tratamiento para atender las consultas y solicitudes se basa en el consentimiento del interesado, el cual lo presta expresa e inequívocamente, mediante acción positiva y previa al envío, al aceptar las condiciones y la política de privacidad. Dicho consentimiento puede ser retirado en cualquier momento mediante el envío de un correo electrónico a **info@uanataca.co**

Transferencia de datos

Los datos personales no se cederán a terceros sin la autorización del Titular salvo obligación legal, conforme al artículo 10 de la Ley 1581 de 2012

Los casos previstos son los siguientes:

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;

b) Datos de naturaleza pública;

c) Casos de urgencia médica o sanitaria;

d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;

e) Datos relacionados con el Registro Civil de las Personas.

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley.

Transferencia Internacional de Datos

Con ocasión de las actividades desarrolladas por la organización podrá servirse de transferir información para que ésta sea tratada por terceros responsables dentro y fuera del territorio nacional, este último, a un país que ofrezcas un nivel adecuado de protección de datos. Esta transferencia de datos personales deberá llevarse a cabo con estricta sujeción a lo dispuesto por la presente política de tratamiento y a los estándares de seguridad implementados por la organización. Para la transferencia la organización solicitará autorización del Titular de la información.

Datos tratados y conservación

Las categorías de datos personales tratados por UANATACA COLOMBIA, a título enunciativo, pero no limitativo, comprenden:

- Datos identificativos: nombre, apellidos y número oficial de identidad.
- Datos profesionales: organización, departamento y/o cargo.
- Datos de contacto: dirección postal, correo electrónico y número de teléfono.
- Datos relativos a la identidad o identificación de los usuarios: fotografías, vídeos y/o cuando corresponda el patrón biométrico facial, con la finalidad de poder llevar a cabo el proceso de validación de identidad remota de UANATACA COLOMBIA o sistemas aprobados previamente por UANATACA COLOMBIA que garanticen el reconocimiento de identidad del titular .

Los datos personales se conservarán hasta la finalización de la relación contractual y posteriormente, durante los plazos legalmente exigidos acorde a cada caso. Como norma general, los datos personales relativos al servicio se conservarán durante 10 años desde la revocación del certificado correspondiente.

Derechos de los usuarios - Titulares de la Información

Conforme con el artículo 8 de la Ley Estatutaria 1581 de 2012 los derechos de los titulares son:

a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado;

b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley;

c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales;

d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución;

f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

Para ejercer sus derechos, los usuarios (titulares) pueden contactar con UANATACA COLOMBIA a través del formulario de contacto disponible en la página web, mediante el envío de una petición a la dirección de correo electrónico de **info@uanataca.co** o bien dirigir un escrito a la dirección indicada en el apartado de información del responsable del tratamiento.

En dicha petición, deberán adjuntar copia de su documento de identidad e indicar claramente cuál es el derecho y solicitud que se desea ejercer.

Recibida una petición, UANATACA COLOMBIA le dará el trámite oportuno, entregando la misma al responsable que corresponda en función del área que se vea afectada o del derecho que se desee ejercer.

Las solicitudes para el ejercicio de los derechos y consulta de información personal por parte del titular de los registros que tiene UANATACA COLOMBIA se responderán dentro del plazo de diez (10) días hábiles contados a partir de la fecha de recibo de esta. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

El Titular que considere que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en el Estatuto para la protección de datos personales, podrán presentar un reclamo ante el Responsable del Tratamiento o el Encargado del Tratamiento el cual será tramitado bajo las siguientes reglas:

- El reclamo se formulará mediante solicitud dirigida a UANATACA COLOMBIA, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.
- El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

9.5 Derechos de propiedad intelectual

9.5.1 Propiedad de los certificados e información de revocación

Todos los derechos en materia de propiedad intelectual e industrial relacionados con los sistemas, documentos, procedimientos, certificados, listas de certificados revocados y cualesquiera otros, relacionados con su actividad como ECD, incluida la presente DPC y las PC asociadas, corresponderán en exclusiva y únicamente a UANATACA COLOMBIA. 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 electrónicos 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 COLOMBIA contienen un aviso legal relativo a la propiedad de estos.

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

9.5.2 Propiedad de la información relativa a nombres

El suscriptor y, en su caso, la Persona natural 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 (DN) del certificado, formado por las informaciones especificadas en la sección 3.1.1.

9.5.3 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 COLOMBIA

UANATACA COLOMBIA garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la Declaración de Prácticas de Certificación y en la PC asociada, siendo el responsable del cumplimiento de los procedimientos descritos, de acuerdo con las indicaciones contenidas en este documento. Así como de los Criterios Específicos de Acreditación Entidades de Certificación Digital – CEA-3.0-07 vigente. Asimismo, informa a sus proveedores de que hace extensivo a ellos el cumplimiento de los requisitos dispuestos por el ONAC, cuando les corresponda.

UANATACA COLOMBIA informa en su página web a los Solicitantes, Suscriptores, Firmantes, Terceros que confían y al público en general de la información general de la empresa, como es su naturaleza, el tipo de empresa, etc.

UANATACA COLOMBIA presta los servicios electrónicos de certificación conforme con esta Declaración de Prácticas de Certificación e informa sobre las modificaciones de esta y de la Política de Certificación asociada a los Suscriptores, Solicitantes y público en general, incluyendo dichas modificaciones en la tabla inicial de historial de versiones.

UANATACA COLOMBIA dispone de un seguro de responsabilidad civil que cubra el valor mínimo exigido por la normativa vigente.

UANATACA COLOMBIA 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.

UANATACA COLOMBIA archivará por el periodo dispuesto en la legislación vigente, los documentos suministrados por el Suscriptor y/o Solicitante

UANATACA COLOMBIA vincula a suscriptores, poseedores de claves y terceros que confían en certificados, mediante la Declaración de Prácticas de Certificación y Política de Certificación, 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 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.

UANATACA COLOMBIA deberá atender y dar respuesta a las peticiones, quejas, reclamos y apelaciones de los Suscriptores, Firmantes y demás partes relacionadas.

UANATACA COLOMBIA en cuanto a sus actividades como RA actuará de acuerdo con la normativa aplicable, respetará lo dispuesto en este DPC y en la PC correspondiente al tipo de certificado que emita. Así como lo señalado en los contratos firmados por el suscriptor.

UANATACA COLOMBIA actuará de forma imparcial de acuerdo a sus políticas, en las que se incluyen los principios de Imparcialidad y de No Discriminación en la prestación de los servicios de certificación digital.

UANATACA COLOMBIA hará uso de los símbolos que caractericen su acreditación como Entidad de Certificación Digital, los cuales estarán restringidos al alcance y servicios acreditados, y no podrán ser transferidos a terceros ni heredados fuera de los servicios de certificación digital, personas, procesos y terceros evaluados por el ONAC. En ese sentido, UANATACA COLOMBIA ejercerá el control que le corresponda, respecto a la propiedad y el uso de símbolos, certificados y/o cualquier otro mecanismo para indicar que el servicio de certificación digital está acreditado.

Las referencias al alcance de acreditación otorgado, o el uso engañoso del alcance de acreditación otorgado, los símbolos, los certificados, y cualquier otro mecanismo para indicar que un servicio de certificación digital, o que la ECD está acreditada, en la documentación o en otra publicidad estarán sujetas al cumplimiento de las Reglas de Acreditación de ONAC RAC-3.0-01 (*Reglas del Servicio de acreditación*) y RAC-3.0-03 (*Reglamento de uso de los símbolos de acreditado y/o asociado*) vigentes.

9.6.2 Obligaciones de los Proveedores

Los proveedores de la Entidad de Certificación Digital (ECD) UANATACA COLOMBIA no afectarán la confianza de calidad y seguridad de los servicios de certificación digital debido a que se encuentran obligados a cumplir con los requisitos mínimos exigidos por ONAC, dispuestos en el documento CEA-3.0-07. Asimismo, UANATACA COLOMBIA ejerce el control, evalúa y hace el

seguimiento del desempeño del proveedor de acuerdo con la política y procedimientos internos de la ECD según les corresponda.

9.6.3 Garantías ofrecidas a suscriptores y terceros que confían en certificados

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

UANATACA COLOMBIA como mínimo, garantiza **al suscriptor**:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Autoridad de Certificación 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 COLOMBIA como mínimo, garantiza **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 COLOMBIA garantiza al suscriptor y al tercero que confía en el certificado:

- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, Persona natural identificada en el certificado, se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la Entidad de Certificación, con los límites que se establezcan.

9.6.4 Rechazo de otras garantías

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

9.6.5 Limitación de responsabilidades

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

UANATACA COLOMBIA no será responsable en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

a) Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el Suscriptor, el Solicitante o por los Terceros que confían, o cualquier otro caso de fuerza mayor.
b) Por el uso indebido de la información contenida en el certificado, en la CRL o en el servicio OCSP.
c) Por el contenido de los mensajes o documentos firmados o cifrados mediante los certificados.
d) En relación con acciones u omisiones del Solicitante y/o Suscriptor:

- Falta de veracidad o exactitud de la información suministrada para emitir el certificado.
- Retraso en la comunicación de las causas de revocación del certificado.
- Ausencia de solicitud de revocación del certificado cuando proceda.
- Negligencia en la conservación de sus datos de creación de firma datos o los datos de activación de estos, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
- Uso del certificado fuera de su periodo de vigencia, o cuando la ECD UANATACA COLOMBIA y/o la RA le notifique la revocación de este.
- Extralimitación en el uso del certificado, según lo dispuesto en la normativa vigente y en la DPC de la ECD, en particular, superar los límites que figuren en el certificado en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al Solicitante y/o Suscriptor por la ECD.

e) En relación con acciones u omisiones del Tercero que confía:

- Falta de comprobación de las restricciones que figuren en el certificado o en la DPC de la ECD en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.

- Falta de comprobación de la perdida de vigencia del certificado publicada en el servicio de consulta sobre la vigencia de los certificados o falta de verificación de la firma digital.

9.6.6 Indemnización y Cláusulas de indemnidad

UANATACA COLOMBIA asumirá las indemnizaciones correspondientes por daños efectuados a Solicitantes, Suscriptores en base a los términos establecidos en la normativa reguladora de la prestación de los servicios de emisión, revocación y distribución de los certificados digitales, así como a la presente DPC y las PC asociadas.

Tanto los Suscriptores, como los Solicitantes, como los Terceros que confían son responsables por apoderarse, destruir, modificar, adulterar indebidamente los datos de una firma o certificado digital durante o después de la fecha de creación del certificado y estarán sujetos al pago de indemnizaciones por los correspondientes daños causados según lo establecido en la normativa reguladora de la prestación de los servicios de emisión, revocación y distribución de los certificados digitales.

9.6.6.1 Cláusula de indemnidad de suscriptor

UANATACA COLOMBIA 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 extrajudicial 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.

9.6.6.2 Cláusula de indemnidad de tercero que confía en el certificado

UANATACA COLOMBIA informa al tercero que confía en el certificado que 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 extrajudicial 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 revocado.

9.6.7 Caso fortuito y fuerza mayor

UANATACA COLOMBIA incluye en esta DPC y sus contratos cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

9.7 Legislación

9.7.1 Ley aplicable

UANATACA COLOMBIA establece que la legislación aplicable al presente documento, así como a las PC asociadas y a las operaciones que derivan de ellas se establece en el contrato de suscriptor. Sin embargo, la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la ley colombiana, así como los reglamentos que la modifiquen o complementen, a saber: a) Ley 527 de 1999 b) Ley Estatuaria 1581 de 2012 c) Decreto Ley 0019 de 2012 d) Decreto 1074 de 2015 e) Decreto 333 de 2014., entre otros.

9.7.2 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

UANATACA COLOMBIA establece en el contrato de suscriptor 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.

9.7.3 Cláusula de jurisdicción competente

UANATACA COLOMBIA establece en el contrato de suscriptor, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces colombianos.

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.

9.7.4 PQRS – Disputas

Las peticiones, quejas, reclamos y solicitudes (PQRS) sobre los servicios prestados por UANATACA COLOMBIA., son recibidas directamente por el responsable competente.

Los Solicitantes, Suscriptores, Terceros que confían o el público en general indicarán su PQRS con respecto a los servicios de certificación digital ofrecidos por UANATACA COLOMBIA enviando un correo electrónico a la dirección **info@uanataca.co** en el que se detalla la situación por la que se presenta.

Los PQRS serán gestionados por el Responsable de realizar tales funciones., quien se encargará de derivar la incidencia al Departamento o rol respectivo. Dicha gestión se llevará a cabo, dando lugar a una solución en un lapso no mayor a quince (15) días. El usuario recibirá un mensaje de correo electrónico confirmando la recepción de la PQRS y cuando ésta sea resuelta.

UANATACA COLOMBIA cuenta con el procedimiento interno para el tratamiento de PQRS que detalla cada uno de los procesos y se encuentra publicado en la página web.

9.7.5 Resolución de conflictos

UANATACA COLOMBIA establece, a través de los instrumentos jurídicos mediante los que se articule su relación con suscriptores y verificadores, los procedimientos de resolución de conflictos que se consideren oportunos, todo ello sin perjuicio de la legislación nacional que sea aplicable.

Si las Partes no hubiesen resuelto las discrepancias o controversias conforme al procedimiento y en el plazo establecido en la cláusula anterior, acudirán a un tribunal de arbitraje que será integrado por un árbitro designado por las Partes de común acuerdo. Si no se llegara a un acuerdo dentro de los diez (10) días hábiles siguientes a la decisión de una de las Partes de convocar al tribunal de arbitraje, el árbitro será designado por el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá D.C. de las listas que éste tiene para tal efecto. El arbitraje será en derecho y al mismo le serán de aplicación las normas del citado Centro.

9.8 CLÁUSULA DE ACEPTACIÓN COMPLETA

Todos los Solicitantes, Suscriptores, Terceros que confían y cualquier otra parte interesada asumen en su totalidad el contenido de la última versión de esta DPC y de las PC asociadas.

9.9 Otras estipulaciones

No se contemplan

Anexo I - Acrónimos

AC	Autoridad de Certificación
CA	Certification Authority. Autoridad de Certificación
RA	Autoridad de Registro
CP	Certificate Policy
CPS	Certification Practice Statement. Declaración de Prácticas de Certificación
CRL	Certificate Revocation List. Lista de certificados revocados
CSR	Certificate Signing Request. Petición de firma de certificado
DES	Data Encryption Standard. Estándar de cifrado de datos
DN	Distinguished Name. Nombre distintivo dentro del certificado digital
DPC	Declaración de Prácticas de Certificación
DSA	Digital Signature Algorithm. Estándar de algoritmo de firma
ECD	Entidad de Certificación Digital que prestan servicios de certificación digital y equivale a una Entidad Certificadora definida en la Ley 527 de 199.
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
FIPS	Federal Information Processing Standard Publication
ISO	International Organization for Standardization. Organismo Internacional de Estandarización
LDAP	Lightweight Directory Access Protocol. Protocolo de acceso a directorios
OCSP	On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
OID	Object Identifier. Identificador de objeto
ONAC	Organismo Nacional de Acreditación de Colombia
PA	Policy Authority. Autoridad de Políticas
PC	Política de Certificación
PIN	Personal Identification Number. Número de identificación personal
PKI	Public Key Infrastructure. Infraestructura de clave pública
RFC	Request For Commnets.
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
SHA	Secure Hash Algorithm. Algoritmo seguro de Hash
SSL	Secure Sockets Layer. Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.
SSCD	Secure Signature Creation Device. Dispositivo Seguro de Creación de Firma
TCP/IP	Transmission Control Protocol/Internet Protocol Protocolo de control de transmisiones, El protocolo TCP se usa para dividir en origen la información en paquetes, añaden una dirección de destino para luego recomponerla en destino. El Protocolo IP se encarga de direccionar adecuadamente la información hacia su destinatario
TSA	Time Stamping Authority (Autoridad de sellado de tiempo)
TSU	Time Stamping Unit (Unidad de sellado de tiempo)

Anexo 2 – Modelo de contrato de suscripción

Por una parte [*Issuing Officer's Name, Surname1 Surname2*] con CC/CE/Pasaporte nº. [*Issuing Officer's oficial document identification number*], con correo electrónico [*Issuing Officer's email*] actuando como operador autorizado de registro de la Entidad de Certificación UANATACA COLOMBIA SAS., con RUT 9016714475, con dirección CALLE 93 B 12 28 OF 203 204 Bogotá DC., Colombia (UANATACA en lo sucesivo) y;

Por la otra, [Nombre o razón social *Name_of_the_Organisation_Representative"," First_Surname_of_the_Organisation_Representative Second_Surname_of_the_Organisation_Representative*] [if there is not Organisation_Representative, specify: given_name"," surname_1 surname_2] con CC/CE/Pasaporte nº. [*ID_Document_Number_of_the_Organisation_Representative*] [if there is not Organisation_Representative, specify: serial_number], actuando en nombre de *[organization_name "-" organization_identifier (Ess. "Bit4id Ibérica S.L. - B63622252")*] [if there is not organization_name, specify: "Propio"] (EL SUSCRIPTOR en lo sucesivo);

ACUERDAN

1. Que Las Partes que intervienen tienen conocimiento y se encuentran conformes con los siguientes términos y condiciones.

2. Que el alcance del servicio de certificación digital se encuentra sujeto al perfil del certificado emitido por UANATACA de acuerdo con la solicitud realizada por EL SUSCRIPTOR conforme la emisión de un certificado de [*Name of the Certificate Profile y soporte*], con un tiempo de vigencia de [Validity_time] días. Dicho lo cual, se establecen los términos y condiciones a los que UANATACA como Entidad de Certificación está sujeta dentro del ámbito de la emisión de un certificado de este tipo. Asimismo, se informa que las mismas se encuentran publicadas en la página web de la entidad de certificación https://web.uanataca.com/co/ las que se encuentran incorporadas a este contrato por remisión.

3. Que, de acuerdo con la solicitud realizada por el suscriptor, UANATACA emitirá y entregará el certificado digital solicitado en la forma que corresponda de acuerdo con el perfil de certificado solicitado, conforme a la Declaración de Practicas de Certificación, Políticas de Certificación, la Ley 527 de 1999 y sus modificaciones, Decreto Ley 0019 de 2012, Decreto Único del Sector de Comercio, Industria y Turismo, así como las obligaciones especificadas por el Organismo Nacional de Acreditación de Colombia – ONAC mediante los Criterios Específicos de Acreditación Entidades de Certificación Digital – CEA-3.0-07.

4. Que EL SUSCRIPTOR declara que la información detallada a continuación es correcta, y será incluida en el certificado digital solicitado:
- Datos de Identificación del Suscriptor: [*organization_name*] [if there is not an organization_name specify given_name"," surname_1 surname_2]
- NIT/RUT/VAT Nº del Suscriptor: [*organization_identifier*]
- Departamento o Vinculación: [*organizational_unit_1 "-" responsible_position]*
- Nombre y Apellidos del Firmante: [*given_name"," surname_1 surname_2*]
- CC/CE/PASAPORTE Nª del Firmante: [*serial_number*]
- Dirección de correo electrónico del Firmante: [*email*]
- Dirección: [*Address*]
-Título del Firmante: [*title*]

5. Que la emisión del certificado digital se realiza con base a los datos suministrados por EL SUSCRIPTOR, quien declara que son ciertos y de cuya veracidad acepta completa responsabilidad. Debido a lo anterior, EL SUSCRIPTOR acepta sin limitación mantener indemne a UANATACA frente a sí mismo o terceros de toda responsabilidad derivada de la prestación del servicio, a causa de falsedad o manifestación errónea u omisión en la información suministrada a la entidad de certificación en los datos de la solicitud del certificado digital y por el incumplimiento de sus deberes como suscriptor y/o firmante.

6. Que UANATACA gestionará el ciclo de vida del certificado digital, particularmente de los servicios de suspensión y revocación de los certificados en los términos de la legislación aplicable y demás señalados por la ONAC, especialmente cuando se sospeche la producción de las incidencias de seguridad correspondientes. UANATACA gestionará igualmente los mecanismos de comunicación a terceras personas, en relación con el estado de vigencia de los certificados (servicios de validación).

7. Que someten la prestación de los servicios aquí contratados a los pactos instrumentados en este contrato, a las condiciones generales a que se refiere la cláusula 2 de este acuerdo, a la declaración de prácticas de certificación (DPC), Política de Certificación aplicable y que se pueden encontrar actualizadas en la página web de la entidad de certificación https://web.uanataca.com/co/

8. Que UANATACA como Entidad de Certificación dispone de una garantía de cobertura de su responsabilidad civil suficiente para el pago de indemnizaciones o pagos afines, bien mediante un seguro de responsabilidad civil, fianza o aval según corresponda y que cubrirá la cuantía mínima establecida por ONAC en todo momento. UANATACA limita su responsabilidad mediante la inclusión de límites de uso del certificado, de acuerdo con lo establecido en su DPC y demás documentación relacionada.

9. UANATACA limita su responsabilidad respecto de la emisión, gestión de certificados y de pares de claves de suscriptores suministrados por la Autoridad de Certificación, uso del certificado, caso fortuito y fuerza mayor.

10. EL SUSCRIPTOR declara haber sido informado de las condiciones económicas (tarifas) de la prestación del servicio, las cuales acepta y están disponibles en la propuesta comercial informada al cliente y/o publicadas en la web de UANATACA según corresponda para la firma del presente contrato.

11. Las partes acuerdan que se otorga el servicio de certificación digital con la firma del presente documento, el cual entrará en vigor desde el día de su firma (el cual no es anterior a la fecha en la cual se tomó la decisión sobre la certificación digital) y expirará cuando pierda vigencia el certificado o, si ocurriere, cuando se produce la revocación de este. A su vez, el presente documento pierde vigencia en el momento que el SUSCRIPTOR incumpla con las obligaciones del presente documento, con las condiciones generales del servicio descritas en la Declaración de Prácticas de Certificación, Política de Certificación de UANATACA y legislación aplicable.

12. UANATACA de conformidad con la Ley Estatutaria 1581 de 2012, demás decretos y normas reglamentarias relacionados con el régimen General de Protección de Datos Personales, informa que los datos de carácter personal proporcionados serán gestionados por UANATACA configurándose ésta como Responsable del Tratamiento. La finalidad del tratamiento es llevar a cabo la prestación de servicios electrónicos de certificación, de acuerdo con lo previsto en su DPC. La base de legitimación del tratamiento es la ejecución de este contrato. Se informa que los datos personales no se cederán a terceros salvo obligación legal, podrán realizarse transferencias y/o transmisiones internacionales a un país que ofrezca un nivel adecuado de protección de datos cuyo tratamiento de datos deberá llevarse a cabo con estricta sujeción a los dispuesto en la DPC, Política de privacidad y demás estándares de seguridad implementados por la organización. EL SUSCRIPTOR podrá consultar información adicional y detallada sobre Protección de Datos en la Política de privacidad disponible en https://uanataca.com/co/politicas-practicas o bien en el apartado 9.4 de la DPC. Asimismo, los interesados podrán ejercitar sus derechos como titulares de la información siguiendo el procedimiento que se encuentra descrito en dicho apartado antes citado.

13. EL SUSCRIPTOR y en general cualquier interesado podrán remitir un correo electrónico a info@uanataca.co para indicar sus peticiones, quejas, reclamos y sugerencias (PQRS). La resolución de diferencias deberá ser comunicada por medio del correo electrónico brindado por el SUSCRIPTOR a través del presente contrato a UANATACA a info@uanataca.co dentro de los quince (15) días siguientes al envío del mensaje de correo electrónico, se buscará llegar a un arreglo directo entre el SUSCRIPTOR y UANATACA, y se ejecutará el procedimiento de Peticiones, Quejas, Reclamos y Sugerencias (PQRS).En el caso de que no se llegase a un acuerdo entre las partes, intervendría un tercero, mediante arbitraje, bien acudiendo a la jurisdicción que corresponda para su resolución. La jurisdicción aplicable será la del territorio de Colombia independientemente de la nacionalidad o domicilio del SUSCRIPTOR.

14. El procedimiento por el cual las partes se notifican hechos mutuamente es mediante el correo electrónico brindado por el SUSCRIPTOR a través del presente contrato. Si el SUSCRIPTOR desea enviar correspondencia o notificaciones físicas, éstas deberán ser dirigidas a la dirección CALLE 93 B 12 28 OF 203 204 Bogotá, DC Colombia.

15. UANATACA es responsable de mantener la confidencialidad de toda la información obtenida durante el proceso de certificación digital.

16. Que UANATACA informa con respecto del régimen obligatorio de uso de los certificados digitales, el cual incluye las siguientes previsiones:

a) Que la declaración de prácticas de certificación regula la emisión y utilización de los Certificados Digitales de UANATACA, cuyo texto íntegro se puede consultar en la dirección de Internet, https://www.uanataca.com/co/politicas-practicas.
b) Que los certificados digitales y el resto de los elementos que forman parte de la identificación electrónica son únicos para cada usuario. La clave privada de los certificados digitales debe ser protegida por un código o credencial secreta, que sólo conoce el titular. Para utilizar la clave privada del certificado digital es imprescindible conocer este código o credencial secreta.
c) Que los certificados digitales, de acuerdo con su perfil y política de certificación, permite al titular de los certificados digitales generar firmas digitales e identificarse de forma electrónica en aquellos sistemas de información que soporten este tipo de autenticación.
d) Que EL SUSCRIPTOR debe usar el certificado según lo establecido en la Declaración de Practicas de Certificación, Política de Certificación y mantener el control de la firma digital.
e) Que EL FIRMANTE debe custodiar, de forma diligente, el código o credencial secreta que permite utilizarlos, para evitar que otras personas puedan suplantar su identidad y firmar documentos en su nombre, o acceder a mensajes confidenciales o sistemas de información de acceso restringido.

f) Que, si el FIRMANTE detecta cualquier indicio de que su identificación electrónica ha podido ser utilizada por otras personas, tendrá que suspender el uso de los certificados digitales y notificarlo inmediatamente al responsable del servicio de certificación del SUSCRIPTOR, para pedir la revocación de los certificados y, en su caso, la emisión de unos nuevos.
g) Dejar de utilizar la clave privada y el certificado, trascurrido el tiempo de vigencia del certificado, o desde el momento en que se solicita o es advertido por UANATACA de la revocación de este.
h) Que, ante cualquier necesidad de información adicional, respecto de la utilización de los certificados emitidos en nombre de UANATACA, el FIRMANTE se podrá dirigir al SUSCRIPTOR, al responsable del servicio de certificación del SUSCRIPTOR, a la Autoridad de Registro y/o a UANATACA.
i) Que está en conocimiento que de conformidad con la Ley Estatutaria 1581 de 2012, demás decretos y normas reglamentarias relacionados con el régimen General de Protección de Datos Personales, UANATACA será el Responsable del Tratamiento de sus datos personales, con la finalidad de llevar a cabo la prestación de servicios de certificación digital de acuerdo a su Declaración de Practicas de Certificación disponible en https://web.uanataca.com/co/politicas-practicas, y que dispone de información adicional y detallada sobre Protección de Datos en la Política de privacidad disponible en https://web.uanataca.com/co/politicas-practicas o bien en el apartado 9.4 de la DPC. Asimismo, conoce que puede ejercitar sus derechos como titulares de la información.
j) Que sabe que, en cumplimiento de la normativa aplicable y la Declaración de Prácticas de Certificación de UANATACA, los datos contenidos en los certificados digitales están publicados en la página web de UANATACA a efectos del Registro de Certificados y de las listas de revocación, toda vez que ha prestado su consentimiento expreso para ello en el acto de entrega del código o credencial secreta.
k) Que los certificados digitales en función del perfil de certificado serán generados mediante el uso de unas credenciales o códigos, que se enviarán al FIRMANTE a su dispositivo móvil, cuenta de correo electrónico o bien serán entregadas de manera impresa en un soporte físico.

Perfil	OID
[Digital Certificate profile]	Digital certificate OID

17. Que [Certificate holder's name and surnames], con CC/CE/Pasaporte número [Certificate holder's oficial document identification number], dirección electrónica [Certificate holder's e-mail] y número de teléfono celular [mobile_phone_number], identificado en el encabezamiento de este documento, se configura a su vez como FIRMANTE del certificado. En su condición de FIRMANTE declara:
a) Que ha sido informado de las condiciones generales del servicio aplicable a los certificados.
b) Que ha sido informado de los medios para acceder a sus certificados mediante el uso de unas credenciales o códigos, que se le enviarán a su dispositivo móvil, cuenta de correo electrónico, que podrán ser generadas por el mismo usuario a través de un mecanismo de generación de claves o bien serán entregadas de manera impresa en un soporte físico.
c) Que ha sido informado del régimen obligatorio de uso de los certificados.
d) Que ha sido informado de las circunstancias relativas al tratamiento de sus datos personales para la correcta emisión y gestión de los certificados.

18. Que UANATACA se compromete a cumplir su Política de Imparcialidad, la cual se encuentra disponible en su página web, garantizando que durante el desarrollo de sus actividades no permitirá presiones externas de naturaleza comercial, financiera u otras que puedan comprometer la calidad del servicio prestado. De igual manera, UANATACA garantiza que el personal de apoyo contratado para la ejecución del servicio de certificación es idóneo para el desempeño de sus funciones y no presenta ningún tipo de inhabilidad e incompatibilidad que pueda afectar negativamente la integridad de las actividades desarrollada por las partes.

19. En todo aquello no previsto en el presente contrato o en sus condiciones generales, serán aplicables las disposiciones previstas en la legislación civil y mercantil nacional colombiana. En caso de discrepancia entre las partes, en relación con la interpretación o cumplimiento del presente contrato, las partes intentarán la previa resolución amistosa. Si las partes no alcanzasen un acuerdo al respecto, cualquiera de ellas podrá someter si corresponde el conflicto a la jurisdicción civil, de conformidad con las normas de competencia aplicables.

20. En virtud de su condición de SUSCRIPTOR y FIRMANTE, firma el presente contrato habiendo leído y entendido las obligaciones y responsabilidades que asume y haciendo uso del certificado que se expide.

En [*Name of the city where the RA is ubicated*], [dd/mm/aaaa]

Fdo. [*Name_of_the_Organisation_Representative",*" *First_Surname_of_the_Organisation_Representative Second_Surname_of_the_Organisation_Representative*] [if there is not Organisation_Representative, specify: given_name"," surname_1 surname_2]
Suscriptor / Firmante

Fdo. [*Issuing Officer's Name Surname1 Surname2*]
Operador autorizado de registro