Declaración de Prácticas de Certificación de estampado cronológico

Información general

Control documental

Clasificación de seguridad:	Público
Versión:	1.0
Fecha edición:	18/03/2024
Fichero:	**PSC-2-DPC_TSA_UCO_v1.r1**
Código	PSC-2-

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Alejandro Grande Fecha: 18/03/2024	Nombre: Fabiola Ortega Fecha: 20/04/2024	Nombre: Elias Barzallo Fecha: 08/08/2024

Control de versiones

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

Índice

1. Introducción

1.1. Presentación

Este documento declara las prácticas de certificación para el servicio de estampado cronológico (Expedición de Sellos de Tiempo Electrónico) de *Uanataca Colombia, S.A.S*, en lo sucesivo "*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.

1.2. Nombre del documento e identificación

Este documento es la "Declaración de Prácticas de Certificación de Estampado Cronológico (Sellado de Tiempo)" de UANATACA COLOMBIA identificado con el OID 1.3.6.1.4.1.47286.201.0.3

1.3. Participantes en los servicios de certificación

1.3.1. Entidad de Certificación Digital

La Entidad de Certificación Digital, en adelante "ECD" 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 condición de Entidad de Certificación Digital (ECD), en cumplimiento de su Declaración de Prácticas de Certificación (DPC), en los términos de la legislación colombiana, así como las normas técnicas ETSI aplicables a la prestación del servicio de Estampado Cronológico (expedición de sellos de tiempo electrónicos), principalmente EN 319 421, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

1.3.2. Autoridad de Sellado de Tiempo

La Autoridad de Sellado de Tiempo, en lo sucesivo "*TSA*" es el tercero que presta el servicio de Estampado Cronológico (expedición de sellos de tiempo electrónicos). UANATACA COLOMBIA es la Entidad de Certificación Digital (ECD) que actúa como Autoridad de Sellado de Tiempo para la expedición de sellos de tiempo electrónicos.

1.3.3. Suscriptores del servicio de certificación

Los suscriptores son los usuarios finales de la estampa cronológica (sellos de tiempo electrónicos) expedidos por UANATACA COLOMBIA. Los suscriptores del servicio pueden ser:

- Empresas, entidades, corporaciones u organizaciones que solicitan a UANATACA COLOMBIA (directamente o a través de un tercero) para su uso en su ámbito corporativo empresarial, corporativo u organizativo.
- Las personas físicas que solicitan el servicio para sí mismas.

El suscriptor del servicio de estampado cronológico, por tanto, el cliente de la Entidad de Certificación UANATACA COLOMBIA con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en esta DPC y habiendo firmado el respectivo Contrato de Prestación de Servicios acepta las condiciones del servicio de estampado cronológico prestado por éste.

1.3.4. Partes usuarias

Las partes usuarias son las personas y organizaciones que reciben y deciden aceptar y confiar en un sello de tiempo emitido por la ECD UANATACA COLOMBIA.

Como paso previo a confiar en los sellos de tiempo, las partes usuarias deben verificarlos, como se establece en esta Declaración de Prácticas de Certificación.

1.3.5. 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.

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 Sellado de Tiempo también le serán aplicables a dicho proveedor a través del acuerdo contractual suscrito entre ambas partes.

Que entre "Uanataca Colombia, S.A.S" 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, S.A.
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. características - Uso del Servicio de Sellado de Tiempo

1.4.1. Características de los Sellos de tiempo (Estampado cronológico)

Los sellos de tiempo emitidos por la TSA de UANATACA COLOMBIA cumplen lo siguiente:

- Los sellos de tiempo son conformes a la RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”.
- El sello de tiempo incluye un identificador de la política de sello de tiempo, en concordancia con la TSA y la TSU de UANATACA COLOMBIA. (ver sección 1.4.2).
- El sello de tiempo incluye el resumen de los datos firmados (HASH) incluido en la correspondiente petición de sello de tiempo.

- El sello de tiempo está firmado por una clave generada para este propósito, correspondiente a la TSU de la TSA UANATACA COLOMBIA.
- El algoritmo de hash de firma de los sellos de tiempo es SHA-256.
- El tiempo incluido en los sellos de tiempo está provisto mediante consulta al Instituto Nacional de Metrología (INM) de Colombia (fuente de tiempo confiable).
- Se utiliza un servicio de sincronización a la fuente de tiempo confiable.
- El tiempo incluido en el sello de tiempo está sincronizado con la hora UTC de la fuente de tiempo confiable dentro de la precisión de +/- 1 segundo, la cual se incluye en el sello de tiempo (el valor del campo accuracy en el sello de tiempo es 1 segundo).
- Si se detecta que el reloj del proveedor del sello de tiempo se encuentra fuera de la precisión indicada, los sellos de tiempo no se emiten.

1.4.2. Usos permitidos

El servicio de Estampado Cronológico (Sellado de Tiempo) expide sellos de tiempo con el fin de probar que una serie de datos han existido y no han sido alterados a partir de un instante específico en el tiempo. Su uso se limita a las aplicaciones y/o sistemas de los clientes (personas físicas o jurídicas) que han contratado estos servicios.

La TSA de UANATACA COLOMBIA dispone de una Unidad de Sellado de Tiempo (TSU) para firmar los sellos de tiempo que emite. La TSA de UANATACA COLOMBIA dispone de un certificado de la firma de sellos de tiempo que ha sido emitido por la CA de la jerarquía de certificados de la PKI de Uanataca, S.A.

El Servicio de Sellado de Tiempo de UANATACA COLOMBIA se identifica con el OID 1.3.6.1.4.1.47286.201.1.10., y emite todos los sellos de tiempo bajo una misma política identificada por un OID específico contenido en los sellos de tiempo conforme a la política de sellado de tiempo respectiva.

1.4.3. Límites y prohibiciones de uso

El Servicio de Sellado de Tiempo no se utilizará para fines distintos de los especificados en el presente documento. Del mismo modo, el servicio deberá emplearse únicamente de acuerdo con la regulación aplicable.

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, sustituyendo a la anterior versión que no se mantendrá en la página web.

2. Publicación y preservación

2.1. Depósito

UANATACA COLOMBIA custodia de manera segura todas las estampas cronológicas (sellos de tiempo) generadas conservándose durante un periodo de 10 años y/o por el término que establezca la legislación vigente. Asimismo, dispone de un Depósito, en el que se publican las informaciones relativas al servicio de expedición de sellos de tiempo electrónicos.

Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de UANATACA COLOMBIA, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo de acuerdo con los plazos y procedimientos establecidos con respecto de la continuidad del negocio.

2.2. Publicación de Información de la Entidad de Certificación Digital

UANATACA COLOMBIA publica las siguientes informaciones, en su Depósito:

- La Declaración de Prácticas de Certificación de Sellado de Tiempo.
- La clave pública del certificado de sello de tiempo electrónico.
- Referencias a los mecanismos de validación de los Sellos de Tiempo.

2.3. Frecuencia de Publicación

La información de la Entidad de Certificación, incluyendo la Declaración de Prácticas de Certificación de Sellado de Tiempo, se publica en cuanto se encuentra disponible.

Los cambios en la Declaración de Prácticas de Certificación de Sellado de Tiempo se rigen por lo establecido en el procedimiento de gestión de este documento y de acuerdo la normativa de aplicación.

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.

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.
- 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

Los Certificados digitales utilizados en el servicio de estampado cronológico (expedición de sellos de tiempo electrónicos), son denominados Certificados de la Unidad de Sellado de Tiempo, en adelante "Certificado/s de TSU", contienen un nombre distintivo (DN o distinguished name) conforme al estándar X.501 en el campo Subject, incluyendo un componente Common Name (CN=) de la siguiente manera:

- 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

Los Certificados de TSU son emitidos por UANATACA COLOMBIA en su calidad de Entidad de Certificación de Información de acuerdo con su Declaración de Prácticas de Certificación, siendo estos certificados emitidos conforme los términos de la ley de conformidad con 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 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 parla prestación de servicios de certificación digital, siguiendo además las normativas técnicas identificadas con las referencias ETSI EN 319 412-3 y ETSI EN 319 421.

3.1.2. Significado de los nombres

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

3.1.3. Empleo de anónimos y seudónimos

N/A

3.1.4. Interpretación de formatos de nombres

UANATACA COLOMBIA cumple con los requisitos del estándar X500.

3.1.5. Unicidad de los nombres

El nombre distintivo de los certificados de TSU será único.

3.2. Validación inicial de la identidad

N/A

3.3. Identificación y autenticación de solicitudes de renovación

N/A

3.4. Identificación y autenticación de la solicitud de revocación, suspensión o reactivación

N/A

4. Requisitos de Operaciones

4.1. Solicitud de emisión de sello de tiempo

4.1.1. Legitimación para solicitar el servicio de sellado de tiempo

El solicitante o usuario del servicio de estampado cronológico (sellado de tiempo), sea persona natural o jurídica, puede realizar la solitud de emisión de estampas cronológicas (sellos de tiempo) mediante petición directa a UANATACA COLOMBIA o bien a través de los servidores de TSA disponibles, que permiten el sellado de tiempo de los documentos que desee.

El solicitante o usuario del servicio de sellado de tiempo puede usar su propio aplicativo o software, todo ello conectándose a una dirección web y mediante unas credenciales proporcionadas por UANATACA COLOMBIA.

UANATACA COLOMBIA es responsable de la decisión tomada con respecto a la certificación digital. En ese sentido, una vez que se ha realizado la revisión de la solicitud, tomará la decisión de otorgar o de cancelar el servicio solicitado y realizará según corresponda las comunicaciones oportunas para comunicar su decisión. Asimismo, le suministrará la documentación relacionada con la prestación del servicio de certificación digital.

Una vez que la solicitud ha sido aceptada y registrada y se han llevado a cabo las comprobaciones adecuadas, se realizará la configuración en el servicio de estampado cronológico para su uso, se genera la marca de tiempo y la envía al solicitante.

4.1.2. Procedimiento de alta y responsabilidades

UANATACA COLOMBIA recibe solicitudes para el servicio de sellado de tiempo, realizadas por personas, entidades, empresas u organizaciones de derecho público o privado.

Las solicitudes se realizan directamente a través de los sistemas informáticos de UANATACA COLOMBIA.

4.2. Procesamiento de la Solicitud

El solicitante presenta a través de los procedimientos establecidos, la solicitud del sello de tiempo para un documento electrónico directamente al servicio de sellado / servidor encargado del sellado. Se hace la petición, se envía al documento, apuntando a la dirección correspondiente y se retorna sellado.

4.3. Emisión del Sello de Tiempo

Los sellos de tiempo electrónicos se generan automáticamente a través del sistema o del servidor encargado del servicio de estampado cronológico (sellado de tiempo). Tras la aprobación de la solicitud se procede a la emisión del sello de tiempo de forma segura y se pone a disposición del suscriptor.

Durante el proceso, UANATACA COLOMBIA:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Indica la fecha y la hora en que se expidió un sello de tiempo.

4.4. Entrega y aceptación del certificado

La entrega y aceptación de los Certificados de TSU siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación de UANATACA COLOMBIA como Entidad de Certificación de Información, todo ello disponible en la página web: https://web.uanataca.com/co/

4.5. Uso del Par de Claves y del Certificado

El Certificado de TSU únicamente se utiliza exclusivamente el servicio de expedición de sellos de tiempo electrónicos.

4.6. Modificación de Certificados

N/A

4.7. Revocación de certificados

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

Los procedimientos de revocación de los Certificados de TSU siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación de UANATACA COLOMBIA como Entidad de Certificación de Información, todo ello disponible en la página web: https://web.uanataca.com/co/

4.7.1. Causas de revocación de certificados

UANATACA COLOMBIA procederá a la revocación de los Certificados de TSU cuando concurra alguna de las siguientes causas:

1. Circunstancias que afectan a la información contenida en el certificado:
    a. Modificación de alguno de los datos contenidos en el certificado, después de la correspondiente emisión del certificado que incluye las modificaciones.
    b. Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.
2. Circunstancias que afectan a la seguridad de la clave o del certificado:
    a. Compromiso de la clave privada, de la infraestructura o de los sistemas del prestador de servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.

b. Infracción, por UANATACA COLOMBIA, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas de Certificación de Sellado de Tiempo.

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

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

3. Otras circunstancias:

a. La terminación del servicio de certificación de UANATACA COLOMBIA.

b. 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:

i. La naturaleza y el número de quejas recibidas.

ii. La identidad de las entidades que presentan las quejas.

iii. La legislación relevante vigente en cada momento.

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

4.7.2. Causas de suspensión de un certificado

Los Certificados de TSU no pueden ser suspendidos, de acuerdo con la Declaración de Prácticas de Certificación de UANATACA COLOMBIA en calidad de entidad de certificación para la expedición de certificados.

4.7.3. Causas de reactivación de un certificado

Los Certificados de TSU no pueden ser reactivados, de acuerdo con la Declaración de Prácticas de Certificación de UANATACA COLOMBIA en calidad de entidad de certificación para la expedición de certificados

4.7.4. Quién puede solicitar la revocación

La revocación será solicitada por UANATACA COLOMBIA.

4.7.5. Procedimientos de solicitud de revocación

El Procedimiento de solicitud de la revocación de los certificados de TSU siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación de UANATACA COLOMBIA como Entidad de Certificación de Información, todo ello disponible en la página web: https://web.uanataca.com/co/

4.7.6. Plazo temporal de solicitud y procesamiento de la revocación

El Procedimiento de solicitud de la revocación de los certificados de TSU siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación de UANATACA COLOMBIA como Entidad de Certificación de Información, todo ello disponible en la página web: https://web.uanataca.com/co/

4.7.7. Obligación de consulta de información de revocación de certificados

Los terceros deben comprobar el estado de los sellos de tiempo electrónicos en los cuales desean confiar, para ello deberán consultar el estado del Certificado de TSU. Un método por el cual se puede verificar el estado de los certificados de TSU es consultando la Lista de Revocación de Certificados más reciente emitida por de UANATACA COLOMBIA como Entidad de Certificación de Información, responsable de la emisión de estos.

Las Listas de Revocación de Certificados o LRC se publican en la página web de UANATACA COLOMBIA, así como en las siguientes direcciones web, indicadas dentro de los certificados:

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

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

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

4.7.8. Frecuencia de emisión de listas de revocación de certificados (LRCs) en inglés CRLs.

UANATACA COLOMBIA como Entidad de Certificación de Información emisora de los certificados de TSU, emite una LRC al menos cada 24 horas.

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

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

4.7.9. Plazo máximo de publicación de LRCs

Las LRCs se publican en https://web.uanataca.com/co/ y en las direcciones web indicadas, en un periodo inmediato razonable tras su generación, que en ningún caso no supera unos pocos minutos.

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

De forma alternativa, los terceros que confían en los sellos de tiempo electrónicos cualificados 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/public/pki/dpc-ec/

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 Intermedia 2 (UANATACA CA2 2016):
  - http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl
  - http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl

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

Resulta obligatorio consultar el estado de los Certificados de TSU antes de confiar en los sellos de tiempo electrónicos de UANATACA COLOMBIA.

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

El compromiso de la clave privada de los Certificados de TSU 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.

4.8. Finalización de la suscripción

N/A

4.9. Depósito y Recuperación de Claves

4.9.1. Política y práctivas de depósito y recuperación de claves

N/A

4.9.2. Política y práctivas de encapsulado y recuperación de claves de sesión

N/A

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

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 sistemas, los propios sistemas y los equipamientos empleados para las operaciones para 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:

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

Estas medidas resultan aplicables a las instalaciones 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 de UANATACA COLOMBIA 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 a los administradores del servicio de hospedaje que disponen de la llave para abrir la jaula.

5.1.3. Electricidad y aire acondicionado

Las instalaciones 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 utiliza 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

Se garantiza que los 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, para la administración y la operación de las plataformas de la TSA de UANATACA COLOMBIA destinadas a la generación de las claves y a la administración y la operación del servicio de estampado cronológico de la TSA de UANATACA COLOMBIA.

5.2.1. Funciones fiables

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

- **Auditor Interno:** Responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de Sistemas de Información. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas.
- **Administrador de Sistemas**: Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de sellado.
- **Operador de Sistemas**: Responsable necesario juntamente 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.

- **Responsable de Seguridad**: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de UANATACA COLOMBIA. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

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

5.2.2. Identificación y autenticación para cada función

Cada rol de confianza de las plataformas de la TSA se autentica mediante la utilización de mecanismos de autenticación seguros. La autenticación dentro de estas plataformas permite el acceso a determinados activos de información de UANATACA COLOMBIA.

Cada persona 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. 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.

5.2.3. Número de personas por tarea

Se garantiza al menos dos personas para realizar las tareas que requieren control multipersona relativas a la generación de las claves de la TSU, la recuperación de un *back-up* de la clave privada de la TSU y la emisión del certificado de la TSU, la revocación del certificado de la TSU y la activación de la clave privada de la TSU.

5.2.4. Roles que requieren separación de tareas

Las funciones fiables se establecen bajo el principio del mínimo privilegio, garantizado una segregación de funciones, de modo que la persona que ostente un rol no tenga un control total o especialmente amplio de todas las funciones de certificación, asegurando el debido control y vigilancia, limitando así cualquier tipo de comportamiento fraudulento a nivel interno.

La concesión del mínimo privilegio para las funciones de confianza, se hará teniendo en cuenta el mejor desarrollo de la actividad y será lo más limitado posible, considerando la estructura organizativa en cada momento.

5.3. Controles de personal

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.

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.

UANATACA COLOMBIA no 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.

5.3.2. Procedimientos de investigación de historial

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

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

UANATACA 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

UANATACA COLOMBIA forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación. Se imparten los cursos necesarios al personal para garantizar la ejecución adecuada de las tareas asignadas a sus roles respectivos, teniendo en cuenta los conocimientos individuales de cada persona.

Los programas de formación son sometidos a revisiones periódicas y se actualizan regularmente para mejorar y perfeccionar su contenido.

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.

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, 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 por UANATACA COLOMBIA. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la Declaración de Prácticas de Certificación, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios, no obstante, lo cual, 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

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

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipos de eventos registrados

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

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la TSA 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 TSA.
- Encendido y apagado de la aplicación de la TSA.
- Cambios en los detalles de la TSA y/o sus claves.
- 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 de la TSA.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal que realiza tareas de confianza.
- 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
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al servicio.
- Eventos relativos a la sincronización y recalibración del reloj.

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

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

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:

- Están protegidos de manipulación mediante la firma de los ficheros que los contienen asegurando su integridad.
- Son almacenados en dispositivos ignífugos.
- Se protege su disponibilidad mediante su almacenamiento en instalaciones externas al centro.

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

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 externas e internas 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

Los registros especificados entre ellos los registros de auditoría (logs) y demás datos del sistema que tengan lugar dentro de la prestación del servicio de estampado cronológico serán archivados durante un período de tiempo apropiado, según lo establecido en la sección 5.5.1 y 5.4.3 de esta política.

UANATACA COLOMBIA es responsable del correcto archivo de todo este material y documentación.

5.5.1. Período de conservación de registros

Se archivan los registros especificados en el numeral 5.5. de manera general durante al menos 10 años según corresponda, o el período que establezca la legislación vigente cuando sea aplicable.

5.5.2. Protección del archivo

Se protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo asegurando que únicamente individuos debidamente autorizados tengan acceso. El archivo es protegido contra posibles amenazas, tales como visualización no autorizada, modificaciones, borrados o cualquier otra manipulación indeseada, al ser almacenado en un sistema confiable.

La información que se recopila con el fin de expedir los sellos de tiempo se realiza mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en instalaciones externas a los Centros de Datos de la ECD en los casos en que así se requiera. Además, se dispone de documentos técnicos y de configuración donde se detallan todas las acciones tomadas para garantizar la protección de los archivos.

5.5.3. 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, en los casos que exista la necesidad de guardar copia de documentos en papel, los mismos se almacenan en un lugar seguro.

5.5.4. 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.

5.5.5. 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.

5.5.6. 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. UANATACA COLOMBIA proporciona la información y medios de verificación al auditor.

5.6. Renovación de claves

Cada par de claves de los Certificados de TSU utilizados en el servicio de sellado de tiempo es únicamente asociado con el sistema que presta dicho servicio. Con anterioridad a que el uso de la clave privada de los Certificados de TSU caduquen, se realizará un cambio de claves antes de la caducidad o revocación de las actuales.

Las claves privadas con las cuales se firman los sellos de tiempo emitidos por UANATACA COLOMBIA, no serán usadas luego de terminado su ciclo de vida sino que será emitida una nueva clave privada de la TSU y puesta en operación, realizando el cambio de un certificado digital por otro, incluyendo la generación segura y la distribución del nuevo certificado. La clave privada de la TSU cuyo certificado ha expirado o ha sido revocado, o cualquier parte de ella, incluyendo cualquier copia, será destruida de modo que no pueda ser recuperada.

En consecuencia, el nuevo certificado de TSU conteniendo su nueva clave pública estará contenido en los sellos de tiempo emitidos con esa nueva clave.

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.

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.

5.7.3. Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso de la clave privada de la TSA o de la CA que ha emitido el certificado de la TSA (CA Raíz de UANATACA COLOMBIA), la seguridad del servicio de estampado cronológico se verá afectada, y 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 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.
- 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.
- 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.

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.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

El par de claves del Certificado de TSU son generadas por UANATACA COLOMBIA como Entidad de Certificación Digital, de acuerdo con su Declaración de Prácticas de Certificación, encontrándose disponibles en la página web: https://web.uanataca.com/co/

Asimismo, se han seguido los procedimientos de ceremonia de claves, 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.

Para la generación de la clave privada de la TSU se utiliza un dispositivo criptográfico hardware (HSM) con las certificaciones FIPS 140-2 level 3 y Common Criteria EAL4+.

- Certificados de la Unidad de Sello de tiempo (TSU)	2.048 bits	Hasta 8 años

6.1.2. Envío de la clave pública al emisor del certificado

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

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

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

Las claves 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.

6.1.4. Tamaños de claves

La longitud de las claves de los Certificados de TSU es de 2048 bits.

6.1.5. Generación de parametros de clave pública

La clave pública de los certificados de TSU está codificada de acuerdo con RFC 5280.

6.1.6. Comprobación de calidad de parámetros de clave pública

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

6.1.7. Comprobación de calidad de parámetros de clave pública

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

6.2. Protección de la clave privada

6.2.1. Estándares de módulos criptográficos

Los módulos que gestionan claves cumplen con las certificaciones FIPS 140-2 level 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 el acceso a la clave privada del Certificado de TSU. Cómo mínimo se requerirán dos personas autenticadas al mismo tiempo. Dicho control garantiza que una persona no posea el control individual, ni la responsabilidad de activar y usar la clave privada de la TSU.

Asimismo, los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

6.2.3. Copia de respaldo de la clave privada

Se realiza copia de backup de las claves privadas de los certificados de TSU, de tal manera que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de estas. 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.

6.2.4. Introducción de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos que conforman la infraestructura de clave pública.

6.2.5. Metodo de activación de la clave privada

Las claves privadas de los Certificados de TSU se almacenan cifradas en los módulos criptográficos que conforman la infraestructura de clave pública.

6.2.6. Método de desactivacion de la clave privada

Los procedimientos de gestión de la clave privada del Certificado de TSU se activan mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por personas que desempeñen funciones fiables.

6.2.7. Método de destruccion de la clave privada

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

Se realizará un borrado seguro de la clave privada de la TSU, utilizando las funciones que proveen los dispositivos criptográficos hardware empleados (HSM), de forma que no resulten afectadas el resto de claves gestionadas por los dispositivos. Asimismo, se realizará un borrado seguro de todas las copias de seguridad de la clave privada de la TSU, las cuales habrán sido identificadas.

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 COLOMBIA. Para el reinicio se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

Finalmente se destruirán de forma segura las copias de seguridad.

6.2.8. Clasificación de módulos criptográficos

Los módulos criptográficos empleados para generar y almacenar las claves de la TSU (HSM) están certificados con la norma FIPS 140-2 level 3 y/o Common Criteria EAL4+.

6.3. Controles de Seguridad Informática

Se emplean sistemas fiables para ofrecer sus servicios de certificación digital. Para ello se han 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 S.A., como proveedor de la infraestructura de clave pública aplica los controles del esquema de certificación sobre sistemas de gestión de la información ISO 27001.

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

Cada servidor incluye las siguientes funcionalidades:

- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Auditoria de eventos relativos a la seguridad.
- Mecanismos de recuperación de claves y del sistema de la TSA.

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

6.4. Controles Técnicos del Ciclo de Vida

6.4.1. Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas 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.

6.4.2. Controles de gestión de seguridad

Se llevan a cabo actividades precisas para la formación y concienciación de los empleados en materia de seguridad. En la realización de esta función dispone de un plan de formación anual.

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

6.4.2.1 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 tres niveles: SIN CLASIFICAR, USO INTERNO y CONFIDENCIAL.

6.4.2.2 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.

Se 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.

6.4.2.3 Tratamiento de los soportes y seguridad

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

6.4.2.4 Planificación del sistema

El departamento de Sistemas al cargo de la infraestructura de clave pública 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.

6.4.2.5 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 del proceso de resolución de la incidencia.

6.4.2.6 Procedimientos operacionales y responsabilidades

Se han definido 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.

6.4.2.7 Gestión del sistema de Acceso

Se llevan a cabo todas las actividades necesarias para confirmar que el sistema de acceso está limitado a las personas autorizadas.

En particular:

- Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con autenticación fuerte.
- Se dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.

- Se dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones de certificación.
- El personal es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

6.4.2.8 Gestión del ciclo de vida del hardware criptográfico

Se asegura que el hardware criptográfico usado para el servicio de sellado de tiempo no se manipula durante su transporte mediante la inspección del material entregado.

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

Se registran todo tipo de información pertinente con respecto del dispositivo para añadir al catálogo de activos.

El uso del hardware criptográfico de sellado de tiempo requiere el uso de al menos dos empleados de confianza.

Se llevan a cabo test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

La clave privada del certificado de TSU almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema, 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.

6.5. Controles de Seguridad de Red

Se 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.

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

6.7. Estampado Cronológico - Fuentes de Tiempo

UANATACA COLOMBIA tiene un procedimiento de sincronización de tiempo coordinado vía NTP, que accede y que realizan el registro del instante de tiempo en los que tienen lugar los eventos. El tiempo de los sistemas proviene de una fuente fiable de hora. Todos los sistemas de UANATACA COLOMBIA sincronizan su instante de tiempo con esta fuente. Las fuentes de tiempos utilizadas, basadas en el protocolo NTP (Network Time Protocol) se auto calibran por distintos caminos, utilizando como referencia la Hora Legal de la

República de Colombia tomada directamente de los patrones de referencia del Instituto Nacional de Metrología de Colombia (INM).

- 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)

6.8. Cambio de estado de un Dispositivo Seguro de Creación de Firma (SSCD)

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

1. Se 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.

2. En el supuesto de finalización del periodo de validez o pérdida de la certificación, no utilizarán dichos SSCD para la emisión de nuevos certificados digitales, bien sea en nuevas emisiones como eventualmente en posibles renovaciones.

3. Procederá de inmediato a cambiar a de dispositivos SSCD con certificación válida.

4. 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 digitales emitidos en estos dispositivos y reemplazarlos emitiéndolos en SSCD válidos.

7. Perfil del Certificado de TSU

El perfil de certificado de TSU para la prestación del servicio de sellado de tiempo sigue los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación de UANATACA COLOMBIA como Entidad de Certificación de Información, todo ello disponible en la página web: https://web.uanataca.com/es/.

7.1. Perfil de certificado

Los certificados de TSU cumplen con el estándar X.509 versión 3, el RFC 3739 y la norma EN 319 422.

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 los documentos de perfiles que son accesibles desde la página web de UANATACA COLOMBIA https://web.uanataca.com/es/.

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 del certificado de TSU es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública en certificado de TSU 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.

7.2. Perfil de la lista de revocación de certificados

El estado del certificado de TSU de la TSA de la ECD UANATACA COLOMBIA se puede verificar mediante la consulta de la última CRL emitida por la CA de la jerarquía de certificados de la PKI de UANATACA COLOMBIA.

El perfil de esta CRL es conforme a lo especificado en la DPC para la emisión de certificados de UANATACA COLOMBIA.

El Procedimiento de revocación, suspensión y/o reactivación de los certificados de TSU siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación de UANATACA COLOMBIA como Entidad de Certificación de Digital, todo ello disponible en la página web: https://web.uanataca.com/co/

7.2.1. Número de versión

Las CRL emitidas por UANATACA COLOMBIA son de la versión 2.

7.2.2. Perfil de OCSP

Según el estándar IETF RFC 6960.

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 COLOMBIA se somete a auditoría interna y auditoría de tercera parte en los términos previstos en dicho documento. En caso de requerirse, UANATACA COLOMBIA 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 cualificación 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 COLOMBIA.

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.
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 Entidades de Certificación, Entidades 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 la firma que ha 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 del Certificado de TSU y regenerar la infraestructura.
- Terminar el servicio de la Autoridad de sellado de tiempo.
- Otras acciones complementarias que resulten necesarias.

8.6. Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se entregan al Comité de Seguridad de UANATACA 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 de sellos de tiempo

UANATACA COLOMBIA establecerá una tarifa (precio final con IVA) por la emisión de sellos de tiempo, de la que, en su caso, se informará oportunamente a los suscriptores.

9.1.2. Tarifa de acceso

N/A

9.1.3. Tarifa de acceso a información de estado de certificado de TSU

UANATACA COLOMBIA no ha establecido ninguna tarifa por el acceso a la información de estado del certificado de TSU.

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

Sin estipulación.

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 de seguro

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 de seguro para suscriptores y terceros que confían

UANATACA COLOMBIA dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional, para los servicios de Certificación Digital prestados atendiendo al mínimo establecido por la legislación de la República de Colombia.

9.3. Confidencialidad

9.3.1. Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales:

- Las solicitudes del servicio, así como toda otra información personal obtenida para la prestación de este, excepto las informaciones indicadas en la sección siguiente.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa.
- 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. Divulgación legal de información

La siguiente información se considera no confidencial:

- La contenida en la presente DPC.
- La información contenida en los sellos de tiempo, puesto que para su emisión el Suscriptor y/o solicitante otorga previamente su consentimiento.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado de TSU
- Las listas de revocación de certificados (LRCs), así como las restantes informaciones de estado de revocación.

- La información contenida en los depósitos de certificados.
- Cualquier otra información que no esté indicada en la sección anterior.

9.3.3. Divulgación de información de suspensión y revocación

Véase la sección anterior.

9.3.4. Divulgación legal de información

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

9.3.5. Divulgación de información por petición de su titular

UANATACA COLOMBIA 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 el servicio de estampado cronológico (Expedición de Sellos de Tiempo Electrónico), todo ello de acuerdo con lo previsto en este documento, el 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 del servicio de estampado cronológico (Expedición de Sellos de Tiempo Electrónico).
- Comunicaciones relativas al servicio.
- Custodia y mantenimiento del archivo relativo al servicio.
- 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 del servicio de estampado cronológico (Expedición de Sellos de Tiempo Electrónico) 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.co@uanataca.com**

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.

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

De conformidad con lo dispuesto por las leyes nacionales y los tratados internacionales, todos los derechos en materia de propiedad intelectual e industrial relacionados con los sistemas, documentos, procedimientos, sellos de tiempo y cualesquiera otros, relacionados con su actividad como Entidad de Certificación Digital, incluida la presente DPC, corresponderán en exclusiva a UANATACA COLOMBIA.

9.6. Obligaciones y responsabilidad civil

9.6.1. Obligaciones de UANATACA COLOMBIA

Se garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la Declaración de Prácticas de Certificación, siendo el responsable del cumplimiento de los procedimientos descritos, de acuerdo con las indicaciones contenidas en este documento.

UANATACA COLOMBIA presta los servicios de Certificación Digital conforme con esta Declaración de Prácticas de Certificación de Estampado Cronológico (Sellado de Tiempo) y a los estándares de aplicación. Asimismo, emite los sellos de tiempo según la información que obra en su poder y libres de errores de entrada de datos entregando los servicios con la confiabilidad y exactitud establecida en los respectivos contratos y en el presente documento.

UANATACA COLOMBIA informa al suscriptor de los términos y condiciones relativos al uso del sello, de su precio y de sus limitaciones de uso, mediante un contrato de suscriptor.

UANATACA COLOMBIA vincula a suscriptores, poseedores de claves y terceros que confían en certificados, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en el presente documento.
- Límites de uso de los sellos de tiempo.
- Información sobre cómo validar un sello de tiempo, incluyendo el requisito de comprobar el estado de este, y las condiciones en las cuales se puede confiar razonablemente en él, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial del Prestador de Servicios de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Prestador de Servicios de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.

9.6.2. Obligaciones de los Suscriptores

El Suscriptor estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

a) Integrar, configurar y utilizar el servicio de estampado cronológico de la ECD, conforme a las instrucciones enviadas por la ECD al Solicitante.
b) Utilizar sistemas cliente que envíen peticiones al servicio de estampado cronológico de la ECD e interpreten sus respuestas conforme al formato establecido en la RFC 3161, y que realicen las verificaciones del estado del certificado de la TSA.
c) Respetar lo dispuesto en los instrumentos jurídicos vinculantes con la ECD.

9.6.3. Obligaciones de los terceros que confían

Los Terceros que confían estarán obligados a verificar que los documentos hayan sido firmados con un sello de tiempo, y que éste haya sido firmado con la clave privada asociada a un certificado de TSU de la TSA de la ECD de UANATACA COLOMBIA vigente en el momento de la verificación (para comprobar que la clave privada usada para firmar el sello de tiempo no ha sido comprometida).

Además, será obligación de los Terceros que confían cumplir con lo dispuesto por la normativa vigente y también: a) Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los sellos de tiempo en los que confían, y aceptar sujetarse a los mismos. b) Notificar a UANATACA COLOMBIA cualquier situación irregular con respecto al servicio prestado por la ECD.

9.6.4. 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.

9.6.5. 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. Además, garantiza al suscriptor que los sellos de tiempo cumplen con todos los requisitos materiales establecidos en esta Declaración de Prácticas de Certificación, así como las normas de referencia.

UANATACA COLOMBIA garantiza al tercero que confía en el sello de tiempo que la información contenida o incorporada por referencia en el sello es correcta, excepto cuando se indique lo contrario.

9.6.6. Rechazo de otras garantías

UANATACA COLOMBIA rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en el presente documento.

9.6.7. Limitación de responsabilidades

Se limita la responsabilidad a la prestación del servicio de expedición de sellos de tiempo el cual se regulará por el contrato oportuno.

No se realiza ninguna verificación del documento para el que se solicita el Sello de tiempo, ya que el mismo se envía directamente por el Suscriptor bajo su propia y exclusiva responsabilidad.

No se asume ninguna obligación con respecto de la monitorización del contenido, tipo y/o formato de los documentos y del hash enviado por el proceso de sellado de tiempo.

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 o por los Terceros que confían, o cualquier otro caso de fuerza mayor.

b) Por el uso indebido de la información contenida en los sellos de tiempo, en el certificado de la TSU o en la CRL.

c) Por el contenido de los mensajes o documentos con sello de tiempo.

d) En relación a acciones u omisiones del Solicitante y Suscriptor:

- Falta de veracidad de la información suministrada para solicitar el servicio

- Negligencia en conservación de sus datos de acceso al servicio, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.

- Extralimitación en el uso de los sellos de tiempo, según lo dispuesto en la normativa vigente y en la presente Declaración de Prácticas de Certificación.

- Retraso en la comunicación de las causas de cancelación del servicio.

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

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

9.6.8. Caso fortuito y fuerza mayor

Se incluyen cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

9.6.9. Indemnizaciones

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 del servicio de estampado cronológico, así como a la presente DPC.

De otra parte, tanto los Suscriptores, como los Solicitantes, como los Terceros que confían son responsables por apoderarse, destruir, modificar, adulterar indebidamente los datos

de un sello de tiempo durante o después de la fecha de creación del sello de tiempo y estarán sujetos al pago de indemnizaciones por los correspondientes daños causados según lo establecido en la normativa reguladora de la prestación del servicio de estampado cronológico.

9.6.10. 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.

9.6.11. Ley aplicable

UANATACA COLOMBIA establece que la legislación aplicable al presente documento, así como las operaciones que derivan de ellas se establece en el contrato de suscriptor. Sin embargo, la ley aplicable a la prestación de los servicios, a las 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.

9.6.12. 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.
- 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.

9.6.13. 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 de Colombia, con independencia del lugar dónde se hubieran utilizado los sellos de tiempo emitidos.

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

9.6.14. Resolución de conflictos

UANATACA COLOMBIA establece, en el contrato de suscriptor, los procedimientos de mediación y resolución de conflictos aplicables.

Anexo I – Definiciones y Acrónimos

DPC	Documento en el que constan de manera detallada los procedimientos que aplica la ECD para la prestación de sus servicios. Una declaración de las prácticas que la ECD emplea para emitir sellos de tiempo
Estampado cronológico	(Estampa cronológica, Sello de tiempo o Sellado de tiempo, Time stamp o Time stamping en inglés) Es un mensaje de datos firmado digitalmente y marcado con un sello de tiempo por una TSA. Este sello de tiempo vincula el mensaje a un momento específico, proporcionando evidencia de que los datos existían y no se modificaron desde ese instante
Función Hash	Es una operación que toma un conjunto de datos de cualquier tamaño y produce otro conjunto de datos de tamaño fijo, siempre vinculado de manera única a los datos originales
OID	Identificador único de objeto (object identifier). OID. Acrónimo del término en idioma inglés “Object Identifier”, que consiste en un número único de identificación asignado en base a estándares internacionales y comúnmente utilizado para identificar documentos, sistemas, equipos, etc., con la finalidad, entre otras cosas, de conocer el origen, la titularidad y la antigüedad del objeto identificado
TSA	Entidad de confianza que emite sellos de tiempo mediante una o más TSU. Nombrada dentro de la normativa colombiana como Entidad de Certificación Digital – ECD. Los sellos de tiempo emitidos por la ECD, conforme a la regulación establecida por la ONAC, incluyen la fecha y hora referenciada por la fuente de tiempo reportada por el Instituto Nacional de Metrología de Colombia.
TSU	Conjunto de hardware y software que es gestionado como una unidad y tiene una única clave de firma de sellos de tiempo activa en un instante de tiempo.
RFC	Son una serie de publicaciones del Internet Engineering Task Force (IETF) que describen diversos aspectos del funcionamiento del Internet y otras redes de computadoras, como protocolos, procedimientos, etc.
PKI	Entendida como el conjunto de hardware, software, políticas, procedimientos y elementos tecnológicos que, mediante la utilización de un par de claves criptográficas, una privada que sólo posee el suscriptor del servicio y una pública necesario para la prestación de los servicios de certificación digital, entre otros.
SIGLAS	
CP	Certificate Policy
CPS	Certification Practice Statement. Declaración de Prácticas de Certificación
CRL	Certificate Revocation List. Lista de certificados revocados
ECD	Entidad de Certificación Digital
DES	Data Encryption Standard. Estándar de cifrado de datos
DN	Distinguished Name. Nombre distintivo dentro del certificado digital
DSCF	Dispositivo Seguro de Creación de Firma
SSCD	Secure Signature Creation Device. Dispositivo Seguro de Creación de Firma
FIPS	Federal Information Processing Standard Publication. (FIPS, en español Estándares Federales de Procesamiento de la Información). Son estándares desarrollados por el gobierno de los Estados Unidos para el procesamiento y tratamiento de la información.
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.
SHA	Secure Hash Algorithm. Algoritmo seguro de Hash
RFC	Request For Comments
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
TSA	Time Stamping Authority (Autoridad de sellado de tiempo)
TSU	Time Stamping Unit (Unidad de sellado de tiempo)