DECLARACION DE PRÁCTICAS DE CERTIFICACIÓN SERVICIO ESTAMPADO CRONOLOGICO

Andes SCD S.A.

Versión 1.0
2017

Tabla de contenido

1. Introducción

ANDES SCD es una entidad de certificación Abierta autorizada por la Superintendencia de Industria y Comercio el 23 de marzo de 2011 según resolución 14349 para prestar sus servicios de certificación digital en el territorio Colombiano y de conformidad con la normatividad colombiana vigente. Según se establece en la ley 527 de 1999 artículo 30, las Entidades de Certificación se encuentran autorizadas para prestar el servicio de estampado cronológico.

ANDES SCD dispone de la plataforma tecnológica para el suministro del servicio de estampado cronológico a través del protocolo TSP conforme al estándar RFC 3161

2. Presentación del documento

Este documento reúne la Declaración de Prácticas de Certificación (DPC) que describe el funcionamiento del servicio de estampado cronológico y en general especifica las condiciones de uso, obligaciones y responsabilidades de las partes que intervienen.

2.1. Nombre del documento e Identificación

Documento	DECLARACION DE PRÁCTICAS DE CERTIFICACION SERVICIO DE ESTAMPADO CRONOLÓGICO
Descripción	Este documento presenta las declaraciones de la Autoridad de Certificación ANDES SCD respecto a las operaciones y procedimientos empleados como soporte al servicio de estampado cronológico en cumplimiento con la normatividad vigente.
Identificador OID	1.3.6.1.4.1.31304.1.1.2.1.1
Versión	V 1.1
Fecha de emisión	19 Octubre 2017
Ubicación	http://www.andesscd.com.co/docs/DPC_TSA_AndesSCD_V1.1.pdf

2.2. Identificación de la Entidad de Certificación Digital

Nombre	Andes Servicio de Certificación Digital S.A.
Razón Social	Andes Servicio de Certificación Digital S.A.
NIT	900.210.800 - 1
Número de Matrícula Cámara de Comercio	01774848 del 15 de febrero de 2008
Fecha de emisión	Noviembre 24 de 2015
Certificado de existencia y representación legal	https://www.andesscd.com.co/images/Certificado_de_existencia_y_representacion_legal.pdf

Domicilio Social y Correspondencia	Carrera 27 # 86 – 43 B. El Polo, Bogotá D.C.
Teléfono	(571) 7953430
FAX	(571) 7953430
Dirección de correo electrónico	pqrs@andesscd.com.co
Dirección de peticiones, consultas y reclamos	Carrera 27 No. 86 -43. Barrio El Polo. Bogotá. D.C.

La anterior información está disponible en la página web de Andes SCD sección Quiénes somos.

2.3. Alcance

Este documento establece las normas y reglas a seguir por la Autoridad Certificadora ANDES SCD en la prestación del servicio de estampado cronológico, estipula los procedimientos y el régimen jurídico aplicado a los integrantes del modelo de confianza.

2.4. Referencias

El suministro del servicio de estampado cronológico se realiza conforme al estándar RFC 3161 Time-Stamp Protocol (TSP)

El contenido de esta Declaración de Prácticas de Certificación fue elaborado teniendo en cuenta las recomendaciones de la RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs) y del estándar ETSI TS 102 023 V 1.2.2: Policy Requirements for Time-Stamping Authorities.

2.5. Administración de la Política

El contenido de esta Declaración de Prácticas de Certificación es administrado por el comité de Políticas y Seguridad encargado de su elaboración, registro, mantenimiento y actualización. A continuación, se detallan los datos del comité de políticas y seguridad y de una persona de contacto disponibles para responder preguntas respecto a este documento.

2.5.1. Organización que administra este documento

Nombre : Comité de Políticas y Seguridad
Dirección : Carrera 27 No 86 – 43
Email : comite.politicas.seguridad@andesscd.com.co
Teléfono : PBX 571 795 3430

2.5.2. Persona de contacto

Razón social : ANDES Servicio de Certificación Digital S.A SIGLA ANDES SCD SA.
Nombre : Martín Vargas Linares – Gerente General
Dirección : Carrera 27 No 86 - 43
Email : gerencia@andesscd.com.co
Teléfono : PBX 571 795 3430

2.5.3. Procedimientos de aprobación de la política

La Declaración de Prácticas de Certificación de ANDES SCD es administrada por el Comité de Políticas y Seguridad y es aprobada por la Dirección de ANDES SCD, siguiendo el Protocolo de Análisis y Aprobación de la Política identificado con el OID 1.3.6.1.4.1.31304.100.2.1.

2.5.4. Publicación del documento

ANDES SCD divulga en el sitio WEB de forma inmediata cualquier modificación en la Declaración de Prácticas de Certificación DPC para el servicio de estampado cronológico, manteniendo un histórico de versiones.

3. Definiciones y abreviaturas

3.1. Definiciones

Termino	Descripción
Autoridad de estampado cronológico (TSA)	Es la autoridad de confianza que emite y gestiona estampas cronológicas a través de una o más unidades de estampado cronológico (TSU)
Estampa cronológica	Es un tipo especial de firma digital emitida por una entidad prestadora de servicios de certificación digital que permite garantizar la integridad de un documento en una fecha y hora determinada.
HASH	Es el resumen codificado que se calcula sobre un objeto digital de cualquier tamaño, y que tiene la propiedad de estar asociado unívocamente al objeto digital.
HSM	Hardware Secure Module. Componente que ofrece una mayor seguridad para la generación y almacenamiento de Llaves
Tiempo universal coordinado (UTC)	Es el tiempo determinado por la referencia a una zona horaria
Unidad de estampado cronológico (TSU)	Es el conjunto de hardware y software que es gestionado como una unidad para ofrecer el servicio de estampado cronológico. Cada TSU cuenta con un par de llaves avaladas por un certificado de firma digital

3.2. Lista de acrónimos y abreviaturas

Abrev.	Descripción
DPC	Declaración de prácticas de certificación
TSA	Autoridad de Estampado Cronológico
TSP	Protocolo de Estampado Cronológico
TST	Token de Estampa Cronológica
TSS	Servicio de Estampado Cronológico
TSU	Unidad de Estampado Cronológico
UTC	Hora Universal coordinada

4. Políticas del servicio

4.1. Servicio de estampado cronológico (TSS)

El servicio de estampado cronológico que proporciona la TSA Andes SCD se divide en 2 componentes:

a. Mecanismo on-line para emisión de estampa cronológica que consiste en la asignación de la fecha y hora actual a un objeto digital (documento, video, audio, etc.), por parte de una entidad prestadora de servicios de certificación que asegura la exactitud e integridad de la marca de tiempo del documento.

El servicio de emisión de estampas cronológicas es comercializado por paquetes de peticiones. Al suscriptor del servicio se le asigna una cuenta de usuario con la cantidad de peticiones contratadas.

El proceso para emitir una estampa cronológica es el siguiente:

1. Petición de Estampado cronológico
   El suscriptor posee un objeto digital como un documento, video, audio o cualquier formato de archivo y desea obtener una estampa cronológica para probar que el objeto digital existía en un determinado momento. El suscriptor prepara la petición de estampado cronológico realizando lo siguiente:
   - Obtiene el HASH del objeto digital para el cual desea obtener la estampa
   - Se autentica con la URL **https://tsa.andesscd.com.co**, suministra el nombre de usuario y contraseña de su cuenta y envía el HASH del objeto digital en la petición de estampado cronológico según protocolo TSP de RFC 3161
2. Verificación de la solicitud de Estampado cronológico
   La TSA Andes SCD recibe la petición de estampado cronológico y verifica que cumple los requisitos. Si cumple los requisitos la petición es procesada para emisión de la estampa cronológica.
3. Emisión de la estampa cronológica
   La TSA Andes SCD genera una estampa cronológica que incluye el HASH del objeto digital, un número de serie único y la fecha y hora actual obtenida del reloj del servidor que se encuentra sincronizado con UTC (ver sección 6.3.4. Sincronización de reloj con UTC).
   La estampa cronológica está firmada digitalmente por una de las unidades de estampado cronológico TSU pertenecientes a la TSA Andes SCD.

Emitida la estampa cronológica se realiza lo siguiente

- La estampa cronológica es enviada al suscriptor del servicio.
- Se resta la estampa utilizada del paquete de peticiones disponibles en la cuenta del suscriptor
- Andes SCD almacena registro que evidencia la emisión de estampa cronológica para posible verificación posterior.

4. Recepción y verificación de la estampa cronológica
   - El suscriptor recibe la estampa cronológica y la almacena
   - El suscriptor verifica la autenticidad de la estampa cronológica

El suscriptor debe adaptar su sistema para poder realizar peticiones de estampado cronológico, recepción y verificación de la estampa cronológica. Existen librerías públicas que implantan el protocolo TSP en diversos lenguajes de programación:

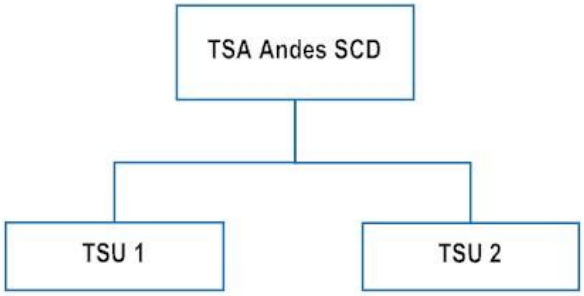
- BouncyCastle (http://www.bouncycastle.org): Librerías criptográficas que implementan protocolo TSP en los lenguajes Java y C#
- OpenTSA (http://www.opentsa.org): Ampliación de librería criptográfica OpenSSL que implementa el protocolo TSP en lenguaje C.
- Digistamp (http://digistamp.com/toolkitDoc/MSToolKit.htm): Toolkit basado en la librería criptográfica CryptoAPI de Microsoft que implementa el protocolo TSP en Visual Basic
- Adobe Reader: La aplicación Adobe Reader permite validar estampas cronológicas incluidas en documentos PDF.

b. Administración del servicio de estampado cronológico que incluye procedimientos para la gestión de las cuentas habilitadas a suscriptores y tareas para monitorear y controlar la correcta operación del servicio.

   El documento de uso interno Procedimientos de administración del servicio de estampado cronológico identificado con el OID 1.3.6.1.4.1.31304.100.1.45 se detallan los procesos para la administración del servicio.

4.2. Autoridad de estampado cronológico (TSA)

La Autoridad de estampado cronológico TSA Andes SCD actúa como tercera parte de confianza entre el suscriptor del servicio y los usuarios en el medio electrónico; es responsable de recibir la solicitud de estampado cronológico, verificar los parámetros de la solicitud y emitir estampas cronológicas conforme a la presente Declaración de prácticas de certificación.
La Autoridad de estampado cronológico TSA Andes SCD dispone de 2 Unidades de estampado Cronológico (TSU) para garantizar la alta disponibilidad del servicio, donde la TSU 1 es la principal y la TSU 2 es la de respaldo.



Las unidades de estampado cronológico TSU 1 y TSU 2 cuentan cada una con un par de llaves diferente avalado por certificado de firma digital emitido por la CA Andes SCD Clase II. A continuación se detallan los campos del perfil del certificado de cada TSU.

Perfil de certificado de TSU		
Campo	**Descripción**	**Valor**
Versión	Versión del certificado	V3
Serial number	Número que identifica al certificado	Ver Número de serie en el certificado emitido a TSU
Algoritmo de firma	Algoritmo usado por Andes SCD para firmar el certificado	SHA256WithRSA
Algoritmo hash de firma	Algoritmo usado para obtener el resumen de los datos	Sha256
Emisor	Datos de la CA Andes SCD Clase II.	Ver en el certificado los datos de la CA Clase II
Valido desde	Fecha y hora UTC inicio validez	Ver en el certificado la fecha de inicio de vigencia
Válido hasta	Fecha y hora UTC fin validez	Ver en el certificado la fecha final de vigencia
Asunto	CN	Sellado de Tiempo Andes SCD Clase II
	OU	Unidad de sellado de tiempo Andes SCD TSU #
	C	CO
	S	Cundinamarca
	L	Bogota D.C
	STREET	Cra 27 No 86 – 43
	E	info@andesscd.com.co
Llave Pública	Llave pública de la TSU	RSA (2048 Bits)
Extensiones	Acceso a la información de la entidad emisora	Método de acceso=Protocolo de estado de certificado en línea Dirección URL=http://ocsp.andesscd.com.co
	Puntos de distribución CRL	[1]Punto de distribución CRL URL=http://www.andesscd.com.co/includes/getCert.php?crl=1

Algoritmo de identificación	Algoritmo utilizado para obtener la huella digital del certificado	Sha1
Huella digital	La síntesis o huella digital de los datos del certificado	fingerprint
Uso de la llave	Propósitos para los cuales se debe utilizar el certificado.	Firma Digital Impresión de fecha (1.3.6.1.5.5.7.3.8)

4.3. Suscriptor

El suscriptor es la persona o entidad que ha contratado el servicio de estampado cronológico ofrecido por TSA Andes SCD y cuenta con paquete de peticiones disponibles para su uso.
El suscriptor contrata el servicio por paquetes de peticiones y se le asigna una cuenta de usuario con el número de peticiones disponibles para usar, autenticándose con los datos de la cuenta puede realizar peticiones del servicio y recibe estampas cronológicas siguiendo el protocolo RFC 3161 Time Stamp Protocol (TSP).

4.4. Usuario o tercero aceptante

Es cualquier usuario que comprueba las estampas cronológicas, basado en la confianza en Andes SCD

5. Obligaciones y responsabilidades

5.1. Obligaciones

5.1.1. Obligaciones generales de la TSA

La TSA Andes SCD tiene las siguientes obligaciones como Autoridad de estampado cronológico:

a. Respetar y cumplir las disposiciones reglamentadas en este documento y en la normatividad Colombiana vigente.
b. Emitir estampas cronológicas que cumplen las especificaciones de la RFC 3161
c. Custodiar la llave privada que se utiliza cada una de las TSU para firma de estampas cronológicas de forma que se garantice su confidencialidad e integridad.
d. Usar una fuente fiable de tiempo como referencia temporal en el proceso de emisión de estampas cronológicas.
e. Hacer público este documento en la página web de Andes SCD manteniendo histórico de versiones.
f. Implementar y mantener la infraestructura necesaria y sistemas de seguridad en función del servicio de estampado cronológico.
g. Atender las solicitudes, quejas y reclamos presentadas por suscriptores del servicio de estampado cronológico
h. Mantener servicio de consulta del estado de los certificados emitidos para TSU
i. Publicar en la CRL CA Andes SCD Clase II los certificados de TSU que hayan sido revocados
j. En caso de compromiso de la referencia temporal informar a todas las partes proporcionando una descripción de la situación.

k. No emitir estampas cronológicas en caso de que se vea comprometida la seguridad del servicio (compromiso de las llaves de TSU, compromiso de referencia temporal, etc.).
l. Proteger la información personal de los suscriptores, de acuerdo a lo establecido en la Ley 1581 de 2012

5.1.2. Obligaciones de la TSA con los suscriptores

La TSA Andes SCD garantiza lo siguiente a los suscriptores del servicio de estampado cronológico

a. El tiempo UTC incluido en las estampas cronológicas tienen una desviación máxima de 1 segundo de la referencia temporal obtenida del servicio de publicación de hora legal colombiana proporcionado por la Superintendencia de Industria y Comercio.
b. Las estampas cronológicas son firmadas usando la llave privada generada exclusivamente para ese propósito y avalada por certificado digital vigente emitido por la CA Andes SCD clase II.
c. Garantizar acceso permanente al servicio de estampado cronológico contratado excluyendo el tiempo mínimo de suspensión requerido para el mantenimiento de los sistemas y equipos
d. Notificar a los suscriptores sobre las interrupciones del servicio debidas a mantenimiento utilizando medios de difusión disponibles.
e. No usar datos personales en las estampas cronológicas generadas
f. Incluir un número de serie único para cada estampa cronológica generada
g. Emitir estampa cronológica una vez que se reciba una petición valida de un suscriptor del servicio.

5.1.3. Obligaciones de los suscriptores

Los suscriptores del servicio de estampado cronológico tienen las siguientes obligaciones

a. Contratar el servicio especificando la cantidad de peticiones que va a utilizar.
b. Respetar los acuerdos contractuales firmados con la TSA Andes SCD.
c. Custodiar confidencialmente los datos de autenticación a la cuenta que le ha sido asignada para hacer uso del cupo de estampas cronológicas contratado.
d. Verificar que el HASH contenido en la estampa cronológica coincide con el HASH que envió
e. Verificar que la firma digital de la estampa cronológica corresponde a una de las TSU que componen la TSA Andes SCD.
f. Verificar que el número de serie del certificado de la TSU que firmo la estampa cronológica no se encuentre en la CRL CA Andes SCD Clase II.
g. Almacenar y conservar las estampas cronológicas entregados por la TSA Andes SCD en caso de considerar que son necesarios en el futuro.

5.1.4. Obligaciones de los usuarios que confían

a. Verificar que la firma digital de la estampa cronológica corresponde a una de las TSU que componen la TSA Andes SCD.
b. Verificar que el número de serie del certificado de la TSU que firmo la estampa cronológica no se encuentre en la CRL CA Andes SCD Clase II.

5.2. Responsabilidades

5.2.1. Responsabilidades de la TSA

La TSA Andes SCD tiene las siguientes responsabilidades como autoridad de estampado cronológico:

a. Emitir estampas cronológicas a suscriptores mientras disponga de peticiones para utilizar del paquete contratado.
b. La TSA no se hace responsable de la veracidad ni del contenido del objeto digital para el cual se ha emitido una estampa cronológica.

5.2.2. Responsabilidades del suscriptor

a. El suscriptor del servicio es responsable de adquirir paquete de peticiones adicionales cuando se haya agotado el paquete de peticiones de su cuenta de usuario.
b. Verificar la firma digital de la estampa cronológica y comprobar el estado de los certificados de la jerarquía de confianza (certificado CA ROOT Andes SCD, certificado CA Andes SCD Clase II y certificado de TSU que firmo la estampa cronológica)

5.2.3. Responsabilidades de los usuarios que confían

a. Verificar la firma digital de la estampa cronológica y comprobar el estado de los certificados de la jerarquía de confianza (certificado CA ROOT Andes SCD, certificado CA Andes SCD Clase II y certificado de TSU que firmo la estampa cronológica)

6. Requisitos sobre prácticas de la TSA

6.1. Declaraciones de prácticas y divulgación

6.1.1. Declaración de prácticas de la TSA

a. Garantizar la confiabilidad para proveer servicio de estampado cronológico.
b. Realizar monitoreo del servicio y realizar controles de seguridad y de operaciones para prevenir riesgos
c. Las estampas cronológicas están firmadas digitalmente con la llave privada asociada a los certificados de TSU

6.1.2. Declaración de divulgación de la TSA

a. El servicio de estampado cronológico está disponible para consumo en línea en la URL **https://tsa.andesscd.com.co**
b. Las tarifas del servicio de estampado cronológico se encuentran publicadas en la página WEB de Andes SCD

6.2. Ciclo de vida de administración de la llave

6.2.1. Generación de llave de la TSU

La llave privada de la unidad de estampado cronológico (TSU 1) de la TSA Andes SCD es generada en un módulo HSM que se rige con el estándar FIPS140-2 del NIST cumpliendo con nivel de seguridad 3.
La llave privada de la unidad de estampado cronológico (TSU 2) de la TSA Andes SCD es generada es generada por software

6.2.2. Protección de la llave de la TSU

La llave privada de la unidad de estampado cronológico (TSU 1) de la TSA Andes SCD se custodia en un módulo HSM que se rige con el estándar FIPS140-2 del NIST cumpliendo con nivel de seguridad 3.
La llave privada de la unidad de estampado cronológico (TSU 2) de la TSA Andes SCD se custodia en un archivo PKCS12

6.2.3. Distribución de la llave publica TSU

La llave pública de la unidad de estampado cronológico (TSU 1 o TSU 2) de la TSA se encuentra en el certificado de la TSU que se adjunta en la estampa cronológica que se emite.

6.2.4. Fin del ciclo de vida de la llave TSU

El periodo de uso de la llave de cada unidad de estampado cronológico (TSU1 y TSU 2) de la TSA Andes SCD es de 2 años. La fecha de inicio y fin esta explicita en el respectivo certificado

6.2.5. Gestión del ciclo de vida del módulo criptográfico para firmar estampas cronológicas

En el documento de uso interno Administración del HSM identificado con el OID 1.3.6.1.4.1.31304.100.1.3 se describen los controles y procedimientos para la gestión y administración de módulos criptográficos HSM.

6.3. Estampado cronológico

6.3.1. Proceso de solicitud

El suscriptor del servicio se autentica con la URL https://tsa.andesscd.com.co suministrando el usuario y contraseña de la cuenta asignada, genera una petición de estampado cronológico según formato definido en la RFC 3161 sección 2.4.1 cuyo parámetro es el HASH del objeto digital que desea estampar cronológicamente

6.3.2. Proceso de estampado cronológico

La TSA Andes SCD realiza lo siguiente:

- Recibe la petición estampado cronológico y verifica que la estructura de la petición de estampado cronológico contenga los parámetros esperados.
- Se obtiene fecha y hora de la fuente segura de tiempo y se genera el token de tiempo que es firmado digitalmente con la llave privada de una de las TSU que conforman la TSA Andes SCD.

- Se genera respuesta de estampado cronológico según formato definido en la RFC sección 2.4.2
- Se envía al suscriptor la respuesta de estampado cronológico.

6.3.3. Proceso de verificación

El suscriptor recibe la respuesta de estampado cronológico, la valida y extrae los datos necesarios para su almacenamiento.

6.3.4. Sincronización de reloj con UTC

La TSA Andes SCD realiza sincronización de su reloj interno mediante protocolo NTP con el servicio de publicación de hora legal colombiana proporcionado por la Superintendencia de Industria y Comercio (http://horalegal.inm.gov.co/)

6.4. Administración y operación de la TSA

El documento de uso interno Procedimientos de administración del servicio de estampado cronológico identificado con el OID 1.3.6.1.4.1.31304.100.1.45 se detallan los procesos para la administración del servicio.

6.4.1. Administración de seguridad

Los controles procedimentales, de seguridad física, de seguridad personal y de auditoría definidos para trabajar bajo un ambiente seguro y las capacidades de recuperación ante desastres establecidos para garantizar la operación de los servicios de certificación se encuentran especificados en la Declaración de Prácticas de Certificación de Andes SCD identificada con el OID 1.3.6.1.4.1.31304.1.1.1.

6.4.2. Terminación de la TSA

En el caso de cesar las actividades como Autoridad de estampado cronológico se tomarán las siguientes medidas a fin de causar el menor daño posible a suscriptores y usuarios del servicio:

- La TSA Andes SCD notificará con un tiempo 30 días de anticipación a la Superintendencia de Industria y Comercio y al Organismo Nacional de Acreditación la intención de cesar sus actividades como prestador de servicio de estampado cronológico.
- Una vez se haya recibido autorización por parte de la Superintendencia de Industria y Comercio y del Organismo Nacional de Acreditación para el cese de las actividades se hará en la forma y siguiendo el cronograma presentado por la ECD al ente de vigilancia y control y que éste apruebe y se recurrirá a los medios de comunicación para notificar a los usuarios del servicio el cese de la actividad como Prestador de servicio de estampado cronológico.
- La comunicación del cese de actividades a los usuarios del servicio de estampado cronológico se realiza mediante 2 avisos publicados en diarios de amplia circulación nacional, con un intervalo de 15 días, informando sobre la terminación de las actividades y la fecha precisa de la cesación.

6.4.3. Cumplimiento de requisitos legales

El funcionamiento y las operaciones realizadas por la Autoridad Certificadora ANDES SCD, así como la presente Declaración de Prácticas de Certificación están sujetas a la normativa que les sea aplicable y en especial a:

a. Ley 527 de 1999, Por medio de la cual se define y reglamente el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
b. Decreto 1747 de 2000, por el cual se reglamenta parcialmente la ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.

6.4.4. Información operación de servicio estampado cronológico

La TSA Andes SCD almacena y conserva las estampas cronológicas emitidas durante un periodo de 5 años

Versión	Fecha	Detalle	Responsable
1.0	26/09/2016	Versión inicial del documento	Comité políticas y seguridad
1.1	19/10/2017	Se renombro el numeral 4 por Políticas del servicio	Comité políticas y seguridad