



DECLARACION DE PRÁCTICAS DE CERTIFICACIÓN SERVICIO ESTAMPADO CRONOLOGICO

Andes SCD S.A.

Versión1.3
2018

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
		Fecha:	14/09/2018
		Versión:	1.3
		Clasificación	Público
		Elaboró:	Coordinador de Seguridad
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

Tabla de contenido

1.	Introducción.....	4
2.	Presentación del documento	4
2.1.	Nombre del documento e Identificación	4
2.2.	Identificación de la Entidad de Certificación Digital	4
2.3.	Alcance	5
2.4.	Referencias	5
2.5.	Administración de la Política	5
2.5.1.	Organización que administra este documento	5
2.5.2.	Persona de contacto	5
2.5.3.	Procedimientos de aprobación de la política	6
2.5.4.	Publicación del documento	6
3.	Definiciones y abreviaturas	6
3.1.	Definiciones.....	6
3.2.	Lista de acrónimos y abreviaturas.....	6
4.	Políticas del servicio.....	6
4.1.	Servicio de estampado cronológico (TSS)	7
4.2.	Autoridad de estampado cronológico (TSA).....	8
4.3.	Solicitante.....	9
4.4.	Suscriptor	9
4.5.	Usuario o tercero aceptante	10
5.	Obligaciones y responsabilidades	10
5.1.	Obligaciones	10
5.1.1.	Obligaciones generales de la TSA	10
5.1.2.	Obligaciones de la TSA con los suscriptores	10
5.1.3.	Obligaciones de los suscriptores.....	11
5.1.4.	Obligaciones de los usuarios que confían.....	11
5.2.	Responsabilidades.....	12
5.2.1.	Responsabilidades de la TSA	12
5.2.2.	Responsabilidades del suscriptor.....	12
5.2.3.	Responsabilidades de los usuarios que confían	12
6.	Requisitos sobre prácticas de la TSA.....	12
6.1.	Declaraciones de prácticas y divulgación.....	12
6.1.1.	Declaración de prácticas de la TSA	12
6.1.2.	Declaración de divulgación de la TSA.....	12
6.2.	Ciclo de vida de administración de la llave.....	12

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	
	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
	Fecha:	14/09/2018
	Versión:	1.3
	Clasificación	Público
	Elaboró:	Coordinador de Seguridad
	Revisó:	Comité Políticas y Seguridad
Aprobó:	Gerente General	

6.2.1.	Generación de llave de la TSU	12
6.2.2.	Protección de la llave de la TSU	13
6.2.3.	Distribución de la llave publica TSU	13
6.2.4.	Fin del ciclo de vida de la llave TSU.....	13
6.2.5.	Gestión del ciclo de vida del módulo criptográfico para firmar estampas cronológicas.....	13
6.3.	Estampado cronológico.....	13
6.3.1.	Solicitud del servicio.....	13
6.3.2.	Solicitud de estampado.....	14
6.3.3.	Proceso de estampado cronológico	14
6.3.4.	Proceso de verificación	14
6.3.5.	Sincronización de reloj con UTC	14
6.4.	Administración y operación de la TSA.....	14
6.4.1.	Administración de seguridad	14
6.4.2.	Terminación de la TSA.....	14
6.4.3.	Cumplimiento de requisitos legales.....	15
6.4.4.	Información operación de servicio estampado cronológico.....	15
7.	Procedimiento para administrar incidentes	15
8.	Plan de continuidad.....	16
9.	Controles de seguridad	16
10.	Condiciones exigidas a proveedores críticos	16
11.	Minutas y contratos	17
12.	Tarifas	17
13.	Control de cambios	18

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
		Fecha:	14/09/2018
		Versión:	1.3
		Clasificación	Público
		Elaboró:	Coordinador de Seguridad
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

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 CRONOLOGICO
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	1.3.6.1.4.1.31304.1.1.2.1.3
Versión	V1.3
Fecha de emisión	14 septiembre de 2018
Ubicación	http://www.andesscd.com.co/docs/DPC_TSA_AndesSCD_V1.3.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
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 – 43B. El Polo, Bogotá D.C.
Teléfono	(571) 7953430
FAX	(571) 7953430

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
		Fecha:	14/09/2018
		Versión:	1.3
		Clasificación	Público
		Elaboró:	Coordinador de Seguridad
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

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-StampProtocol (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), recomendaciones de la (Requestforcomments) RFC 3647 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 : Carrera27No86-43
Email : comite.politicas.seguridad@andesscd.com.co
Teléfono : PBX571 7953430

2.5.2. Persona de contacto

Razón social : ANDES Servicio de Certificación Digital S.A SIGLA ANDES SCD SA.
Nombre : Adriana Lucia Monroy Londoño- Gerente General
Dirección : Carrera27No 86- 43
Email : adriana.monroy@andesscd.com.co
Teléfono : PBX571 7953430

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
		Fecha:	14/09/2018
		Versión:	1.3
		Clasificación	Público
		Elaboró:	Coordinador de Seguridad
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

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 ANDESSCD, 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

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
		Fecha:	14/09/2018
		Versión:	1.3
		Clasificación	Público
		Elaboró:	Coordinador de Seguridad
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

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. Peticion 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

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
		Fecha:	14/09/2018
		Versión:	1.3
		Clasificación	Público
		Elaboró:	Coordinador de Seguridad
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

el protocolo TSP en lenguaje C.

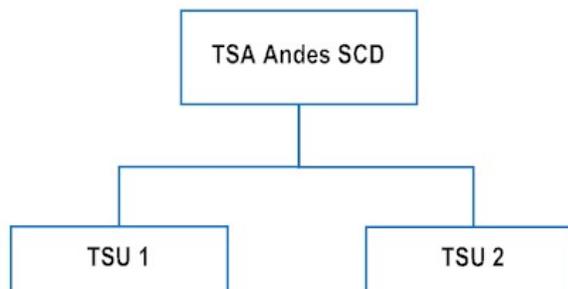
- Digistamp (<http://digistamp.com/toolkitDoc/MSToolKit.htm>): Toolkit basado en la librería criptográfica CryptoAPI de Microsoft que implementa el protocolo TSP en Visual Basic
- Adobe Reader: La aplicación Adobe Reader permite validar estampas cronológicas incluidas en documentos PDF.

- 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.

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
		Fecha:	14/09/2018
		Versión:	1.3
		Clasificación	Público
		Elaboró:	Coordinador de Seguridad
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

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	fingerpint
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. Solicitante

Es la persona que ha solicitado el servicio de estampado cronológico a Andes SCD.

4.4. 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).

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
		Fecha:	14/09/2018
		Versión:	1.3
		Clasificación	Público
		Elaboró:	Coordinador de Seguridad
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

4.5. 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

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
		Fecha:	14/09/2018
		Versión:	1.3
		Clasificación	Público
		Elaboró:	Coordinador de Seguridad
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

- 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.
- h. Pagar la remuneración pactada en el momento que lo indique Andes SCD
- i. Respetar los derechos de terceras personas y responsabilizarse frente a las mismas por los perjuicios que la utilización, exposición, publicación y/o presentación del mensaje de datos objeto de estampa cronológica pueda causar, así como salir en defensa de ANDES SCD si ésta es demandada por cualquier circunstancia relacionada con tal situación.
- j. Seguir en todo caso las instrucciones que le imparta ANDES SCD para el desarrollo del proceso de estampado cronológico
- k. Contar de manera permanente con toda la infraestructura tecnológica y de seguridad necesaria para la utilización adecuada del servicio de estampado cronológico de acuerdo con los requerimientos que haga ANDES SCD.
- l. Abstenerse de:
 - 1) Alterar o modificar, en todo o en parte, el software entregado por ANDES SCD, o permitir que terceras personas lo hagan.
 - 2) Copiar o reproducir en cualquier forma el servicio de estampado cronológico, como todos sus componentes o procesos, o permitir su copia o reproducción.
 - 3) Realizar ingeniería inversa, decodificar, desensamblar o realizar cualquier tipo de acción tendiente a conocer o descifrar el código fuente, el código objeto u otra información relevante respecto del software que se relacione con la prestación del servicio de ANDES SCD.
 - 4) Transferir, ceder o negociar los derechos otorgados por los presentes términos y condiciones.
 - 5) Permitir que terceras personas se beneficien de o utilicen, directa o indirectamente, los derechos que se derivan de la prestación de servicios de certificación digital, bajo las condiciones de este documento.

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.

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
		Fecha:	14/09/2018
		Versión:	1.3
		Clasificación	Público
		Elaboró:	Coordinador de Seguridad
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

- 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

El servicio de estampado cronológico está disponible para consumo en línea en la URL <https://tsa.andesscd.com.co>

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.

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
		Fecha:	14/09/2018
		Versión:	1.3
		Clasificación	Público
		Elaboró:	Coordinador de Seguridad
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

La llave privada de la unidad de estampado cronológico (TSU 2) de la TSA Andes SCD 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) y (TSU 2) 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.

6.2.3. Distribución de la llave pública 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. Solicitud del servicio

El cliente realiza la solicitud a través del formulario de solicitud dispuesto en la página web de ANDES SCD (Solicitud de estampas) proporcionando la siguiente información necesaria para el proceso.

- Tipo de solicitud
- Razón social
- NIT de la entidad
- Nombre contacto
- Identificación contacto
- Teléfono contacto
- Email contacto
- Cantidad de estampas

Las solicitudes son direccionadas automáticamente al sistema de Tickets OTRS5.

Un representante comercial de ANDES SCD recibe la solicitud a través de un ticket generado por la herramienta OTRS, establece comunicación con el cliente verificando y validando los requerimientos técnicos y comerciales para la prestación del servicio, remite ticket al director de operaciones para la habilitación del servicio.

Dentro de la TSA se crean las credenciales y se asigna el cupo, a través de correo electrónico se realiza la entrega de las credenciales de uso de la TSA al cliente para que pueda hacer consumo del servicio.

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
		Fecha:	14/09/2018
		Versión:	1.3
		Clasificación	Público
		Elaboró:	Coordinador de Seguridad
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

6.3.2. Solicitud de estampado.

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

6.3.3. 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.

6.3.4. Proceso de verificación

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

6.3.5. 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/>) de conformidad con el RFC 5905.

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 el procedimiento de gestión de incidentes y el plan de continuidad del negocio.

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:

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
		Fecha:	14/09/2018
		Versión:	1.3
		Clasificación	Público
		Elaboró:	Coordinador de Seguridad
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

- 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

7. Procedimiento para administrar incidentes

ANDES SCD dispone del siguiente procedimiento para gestionar incidentes o eventos que puedan afectar la confidencialidad, integridad y disponibilidad de la información y los servicios:

1. **Detección y reporte del incidente:** conocimiento del incidente a través de sistemas de monitorización, sistemas de detección de intrusos, registros del sistema, aviso por parte del personal o por parte de los clientes.
2. **Análisis y evaluación del incidente:** una vez detectado el incidente se determina el procedimiento de respuesta y se contacta con las personas responsables para evaluar y documentar las acciones a tomar según la gravedad de la incidencia. Se efectúa una investigación para determinar cuál fue el alcance del incidente, es decir averiguar hasta donde llegó el ataque y la máxima información posible de la incidencia.
3. **Control de daños ocasionados por incidente:** reaccionar rápidamente para contener la incidencia y evitar que se propague tomando medidas como bloquear accesos al sistema.
4. **Investigación y recopilación de evidencias:** revisar registros de auditoría para realizar un seguimiento de lo ocurrido.
5. **Recuperación y medidas contra incidencia:** restaurar el sistema a su correcto funcionamiento y documentar el procedimiento y formas de evitar que vuelva a presentarse la incidencia.

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
		Fecha:	14/09/2018
		Versión:	1.3
		Clasificación	Público
		Elaboró:	Coordinador de Seguridad
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

6. **Análisis posterior de la incidencia para mejorar el procedimiento:** realizar un análisis de todo lo ocurrido, detectar la causa de la incidencia, corregir la causa para el futuro, analizar la respuesta y corregir errores en la respuesta.

ANDES SCD dentro del procedimiento de gestión de incidentes de seguridad de la información contempla el manejo de eventos que puedan afectar la prestación del servicio de estampado cronológico. Los eventos considerados son los siguientes:

- Compromiso de llave privada de alguna de las CA de ANDES SCD
- Compromiso del sistema de seguridad de ANDES SCD
- Compromiso en la prestación del servicio por fallas en el sistema
- Compromiso de sistemas de cifrado

8. Plan de continuidad

ANDES SCD tiene establecido y probado un plan de continuidad y contingencia que especifica las acciones a ejecutar, componentes o recursos a utilizar y como debe reaccionar el personal en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación.

9. Controles de seguridad

Los sistemas y equipamientos empleados por ANDES SCD para ofrecer el servicio de estampado cronológico se encuentran ubicados físicamente en el Data Center Triara, un centro de datos de clase mundial ubicado en la Sabana de Bogotá en un lugar estratégico de gran desarrollo empresarial. El Data Center Triara es un sitio que ha sido diseñado con especificaciones TIA/EIA 942 – Tier IV 1, cumple con estrictas normas de construcción y seguimiento a rigurosos estándares de operación para garantizar que los equipos e información allí alojados cuenten con el máximo nivel de seguridad. Sus instalaciones están localizadas en una zona nula de actividad sísmica y se encuentran dentro de un bunker de concreto armado y acero, las edificaciones son resistentes a inundaciones, vendavales, descargas eléctricas y precipitaciones atmosféricas y están dotadas con un subsistema arquitectónico, un subsistema de telecomunicaciones, un subsistema eléctrico, un subsistema mecánico y un sistema de seguridad física articulado por metodologías de administración de riesgo y seguridad.

Los servicios de seguridad que ofrece el Data Center Triara han sido integrados a las políticas y procedimientos de seguridad de ANDES SCD describiendo cada uno de los controles implementados para evitar el riesgo, alteración, sustracción, daño o pérdida de los activos involucrados en la prestación del servicio de certificación digital.

Para garantizar la prestación de los servicios críticos en caso de presentarse un incidente con su Data Center principal, ANDES SCD cuenta con un centro de datos alternativo contratado con IFX NETWORKS. Este centro de datos está ubicado Carrera 69 25b 44 edificio World Business Port Piso 8, Bogotá. WPB DATA CENTER está calificado como tipo TIERIII y cuenta con óptimos mecanismos de seguridad para la prestación de los servicios.

10. Condiciones exigidas a proveedores críticos

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
		Fecha:	14/09/2018
		Versión:	1.3
		Clasificación	Público
		Elaboró:	Coordinador de Seguridad
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

Para Andes SCD, es un deber la prestación de un excelente servicio, por esta razón, los proveedores han de ser la primera línea para poder sustentar nuestro compromiso de servicio y con la calidad de este, así bien nuestros proveedores son evaluados de forma anual para validar el cumplimiento de los niveles de servicio definidos contractualmente.

El centro de datos principal debe cumplir con una disponibilidad de sitio del 99,9% para la prestación de los servicios de certificación digital, además debe cumplir con los demás requisitos tanto administrativos como técnicos definidos contractualmente.

11. Minutas y contratos

Al registrar la solicitud de emisión de estampas cronológicas desde el formulario dispuesto en página web, el suscriptor manifiesta que conoce y acepta los términos y condiciones de prestación del servicio descritos en el siguiente enlace: [términos y condiciones de uso](#)

Una vez registrada la solicitud el solicitante será contactado por personal de ANDES SCD con el fin de validar los requerimientos del servicio (Condiciones contractuales, particularidades del servicio, entre otras)

ANDES SCD entregará mediante correo electrónico al suscriptor una notificación con las credenciales de uso de la TSA para que pueda hacer consumo del servicio.

12. Tarifas

Las tarifas aquí indicadas son valores de referencia y se encuentran definidos por rangos. Las tarifas podrán variar según acuerdos comerciales especiales suscritos con clientes, entidades o solicitantes, o en desarrollo de campañas promocionales adelantadas por ANDES SCD.

Rango	Valor Unitario IVA Incluido
Hasta 100.000	\$ 105.91
100.001 – 500.000	\$ 81.2
500.001 – 1.000.000	\$ 65.45
1.000.001 – 3.000.000	\$ 49.98
3.000.001 en adelante	\$ 35.7

Rango de paquetes de estampas

Los precios anteriormente mencionados son valores unitarios y tienen el IVA (19%) incluido

	DECLARACION DE PRACTICAS DE CERTIFICACION SERVICIO ESTAMPADO CRONOLOGICO	IdentificadorOID	1.3.6.1.4.1.31304.1.1.2.1.3
		Fecha:	14/09/2018
		Versión:	1.3
		Clasificación	Público
		Elaboró:	Coordinador de Seguridad
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

Control de cambios

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
1.2	20/03/2018	-5.1.3. Se incluye el apartado obligaciones de los suscriptores. -6.3.1 Se describe proceso de solicitud del servicio -7. Se adiciona información relacionada con el manejo de incidentes. planes de continuidad y contingencia, controles de seguridad. - 9. Se incluyen condiciones exigidas a proveedores críticos. -10. Se incluye el apartado minutas y contratos. -11. Se incluye el apartado tarifas de los servicios.	Comité políticas y seguridad
1.3	14/09/2018	- 2.1 Se actualiza identificador OID, versión y url de descarga de la DPC. -2.5.2 Se actualiza nombre e email de Gerente General.	Comité políticas y seguridad