# POLITICA DE CERTIFICACIÓN COMUNIDAD ACADEMICA

Andes SCD S.A.

2018

## Tabla de Contenido

**Introducción**

La presente Política para Certificados de Comunidad académica complementa las disposiciones establecidas en la Declaración de Prácticas de Certificación y concretamente expresa el conjunto de reglas definidas por la Autoridad de Certificación Andes SCD para la aplicación de los certificados a una comunidad, los usos que se le pueden dar a este tipo de certificado y los requerimientos técnicos, legales y de seguridad exigidos para su emisión y revocación.

Se recomienda leer este documento antes de solicitar un Certificado de Comunidad académica o hacer uso del mismo para comprobación de firmas electrónicas con el fin de conocer el ámbito de aplicación y los efectos legales asociados al uso de este tipo de certificado.

## 1. Presentación del documento

### 1.1. Nombre del documento e Identificación

| | |
|---|---|
| Documento | POLITICA DE CERTIFICACION COMUNIDAD ACADEMICA |
| Descripción | El certificado de Comunidad Académica acredita la identidad del suscriptor y su calidad como docente, estudiante o miembro de una comunidad académica, y le permite al suscriptor firmar documentos digitalmente en su propio nombre e interés. |
| Identificador OID | 1.3.6.1.4.1.31304.1.2.2.2.6 |
| Versión | V 2.6 |
| Fecha de emisión | 14 Septiembre 2018 |
| Ubicación | http://www.andesscd.com.co/docs/PC2.6/pc_comunidadacademica_v2.6.pdf |

### 1.2. Referencias

El desarrollo del contenido de las Políticas de Certificación y la Declaración de Prácticas de Certificación se emite teniendo en cuenta las recomendaciones de la (Request for comments) **RFC 3647**: Internet X.509 Public Key Infraestructure: Certificate Policy and Certification Practices Framework y de los siguientes estándares europeos:

- ETSI TS 101 456: Policy Requirements for certification authorities issuing qualified certificates.
- ETSI TS 102 042: Policy Requirements for certification authorities issuing public key certificates.

### 1.3. Administración de la política

El contenido de esta Política 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.

#### *1.3.1.* Organización que administra el 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

### *1.3.2.* Persona de contacto

**Razón social** : Andes Servicio de Certificación Digital S.A SIGLA ANDES SCD SA.
**Nombre** : Adriana Lucia Monroy Londoño – Gerente General
**Dirección** : Carrera 27 No 86 - 43
**Email** : adriana.monroy@andesscd.com.co
**Teléfono** : PBX 571 795 3430

### *1.3.3.* Procedimientos de aprobación de la política

La Política de Certificación de Comunidad académica 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.

### *1.3.4.* Publicación del documento

Las Políticas de Certificación de Comunidad académica y la Declaración de Prácticas de Certificación son documentos de uso público que se encuentran disponibles en la página web de Andes SCD. Cualquier modificación en estos documentos se publica de forma inmediata manteniendo un histórico de versiones.

## 1.4. Comunidad de usuarios y aplicabilidad

Los certificados de Comunidad Académica son emitidos a personas Físicas, acreditan la identidad del titular y su calidad como docente, estudiante o miembro de una comunidad académica en la firma de documentos electrónicos garantizando la autenticidad del emisor de la comunicación, el no repudio del origen y la integridad del contenido. El poseedor de un certificado de Comunidad Académica actúa en su propio nombre e interés.

*Autoridad de certificación (CA)*

La Autoridad de Certificación Andes SCD es la entidad que actúa como tercera parte de confianza entre el suscriptor y los usuarios en el medio electrónico y es responsable de emitir y gestionar los certificados digitales para Comunidad Académica conforme a la presente Política de Certificación. En la Declaración de Prácticas de Certificación se detalla la jerarquía de las Autoridades Certificadoras que conforman Andes SCD

*Autoridad de registro (RA)*

Las Autoridades de Registro son las entidades delegadas por la Autoridad de Certificación Andes SCD para gestionar las solicitudes, corroborar presencialmente la identidad de los solicitantes y realizar un registro completo de los solicitantes que deseen adquirir un certificado digital de Comunidad Académica conforme a la presente Política de Certificación.

*Suscriptores*

El suscriptor es aquella persona física que ha adquirido un certificado de Comunidad Académica emitido por la Autoridad de Certificación Andes SCD para obrar en el entorno electrónico en su propio nombre y se considera suscriptor mientras dicho certificado se encuentre vigente.

*Solicitantes*

El solicitante es aquella persona física que desea acceder a los servicios de certificación digital al adquirir un certificado de Comunidad Académica emitido por Andes SCD. Bajo ninguna circunstancia se aceptan solicitudes de este tipo de certificados a nombre de personas que no demuestren estar vinculadas como estudiantes, docentes o miembros de una comunidad académica.

*Usuarios*

El usuario es cualquier persona que voluntariamente deposita su confianza en los certificados de Comunidad Académica emitidos por la Autoridad Certificación Andes SCD y que utiliza el servicio de certificación como medio para acreditar la autenticidad e integridad de un documento firmado por un tercero.

## 1.5. Ámbito de aplicación

### *1.5.1. Usos del certificado*

El certificado de Comunidad Académica emitido bajo esta política puede ser utilizado para los siguientes propósitos:

*Autenticación de identidad*

El certificado puede utilizarse para identificar a una persona física como estudiante, docente o miembro de una Comunidad Académica en el ámbito de su actividad.

*Firma digital*

Las firmas digitales realizadas con certificados de Comunidad Académica ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio

- **Autenticidad del origen**: En una comunicación electrónica el suscriptor puede acreditar válidamente su identidad ante otra persona demostrando la posesión de la llave privada asociada con la respectiva llave pública contenida en el certificado
- **Integridad del documento**: Existe la garantía de que el documento no fue alterado o modificado después de firmado por el suscriptor puesto que el resumen del documento es cifrado con la llave privada del emisor el cual es el único que está en posesión de la misma.
- **No repudio**: Evita que el emisor del documento firmado pueda negar en un determinado momento la autoría o la integridad del documento, puesto que la firma a través del certificado digital puede demostrar la identidad del emisor sin que este pueda repudiarlo.

*Cifrado de información*

Es el proceso de transformar la información para hacerla incomprensible para todos excepto para el receptor a quien va dirigida

### *1.5.2. Límites de uso de los certificados*

Los certificados de Comunidad Académica no pueden ser usados para actuar ni como Autoridad de Registro ni como Autoridad de Certificación, firmando otros certificados de llave pública de ningún tipo ni listas de certificados revocados (CRL). Tampoco pueden ser usados para fines contrarios a la legislación vigente.

Las limitaciones de uso de los certificados de Comunidad académica emitidos en convenios se encuentran especificadas en los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5. correspondiente a convenios

### *1.5.3. Prohibiciones de uso de los certificados*

La realización de operaciones no autorizadas según esta política de certificación, por parte de terceros o suscriptores del servicio eximirá a la Autoridad de Certificación Andes SCD de cualquier responsabilidad por este uso prohibido.

- No se permite el uso del certificado de Comunidad Académica para firmar otros certificados o listas de revocación (CRL)
- Está prohibido utilizar el certificado para usos distintos a los estipulados en el apartado "Usos permitidos del certificado" y "Limites de uso de los certificados" de la presente Política de Certificación.
- Las alteraciones sobre certificados no están permitidas y el certificado debe usarse tal y como fue suministrado por la Autoridad Certificadora Andes SCD.
- Se prohíbe el uso de certificados en sistemas de control o sistemas intolerantes a fallos que puedan ocasionar daños personales o medioambientales.
- Se considera prohibida toda aquella acción que infrinja las disposiciones, obligaciones y requisitos estipulados en la presente Política de Certificación.
- No es posible por parte de Andes SCD emitir valoración alguna sobre el contenido de los documentos que firma el suscriptor, por lo tanto la responsabilidad del contenido del mensaje es responsabilidad única del signatario.
- No es posible por parte de Andes SCD recuperar los datos cifrados en caso de pérdida de la llave privada del suscriptor porque la CA por seguridad no guarda copia de la llave privada de los suscriptores, por lo tanto es responsabilidad del suscriptor la utilización de cifrado de datos.

### *1.5.4.* Minutas y contratos

Al registrar la solicitud de emisión de certificados el suscriptor manifiesta que conoce y acepta los términos y condiciones de prestación del servicio descrito en la página Web.

No se requiere confirmación explicita por parte del suscriptor para dar por aceptado los términos y condiciones del servicio. Se considera que los términos y condiciones de prestación del servicio son aceptados en el momento que se registra la solicitud.

Una vez emitido el certificado de firma digital, ANDES SCD entregará mediante correo electrónico al suscriptor una notificación con la información de interés para administrar el ciclo de vida de su certificado. Dicha notificación contiene al menos la siguiente información:

a) Tipo de certificado
b) Referencia PC OID
c) Serial del certificado
d) Inicio de vigencia
e) Fin de vigencia
f) Titular del certificado

g) Entidad
h) Forma entrega certificado
i) Código de Revocación

## 2. Publicación y registro de certificados

Todos los datos del sistema relativos al ciclo de vida de los certificados se conservan de forma digital durante el periodo que establezca la legislación vigente cuando sea aplicable. Los certificados vigentes y caducados se conservan publicados en LDAP de acuerdo con el RFC 4523.

## 3. Identificación y autenticación

A continuación se describen los procedimientos y criterios aplicados para verificar la identidad del solicitante y aprobar la emisión de un certificado de Comunidad académica.

### 3.1. Nombres

#### *3.1.1. Tipos de nombres*

Los certificados de Comunidad Académica tienen una sección denominada Asunto cuyo objetivo es permitir identificar al titular o suscriptor del certificado, esta sección contiene un DN o distinguished name caracterizado por un conjunto de atributos que conforman un nombre inequívoco y único para cada suscriptor de los certificados emitidos por Andes SCD.

| Abrev | Nombre | Descripción |
|---|---|---|
| CN | Nombre | Nombres y apellidos completos del suscriptor |
| S | Serial | Número documento identificación |
| E | Email | Correo electrónico del suscriptor |
| C | País | Abreviatura del país donde reside el suscriptor |
| ST | Departamento | Nombre departamento donde reside el suscriptor |
| L | Ciudad | Nombre municipio donde reside el suscriptor |
| STREET | Dirección | Dirección donde reside el suscriptor |
| T | Titulo | Indica el tipo de vinculación del suscriptor con la comunidad académica |
| O | Organización | Nombre de la universidad o Comunidad Académica. |
| OU | Unidad Organizacional | Nombre de facultad y carrera a la que se encuentra vinculado |
| OU | Unidad Organizacional | Comunidad Académica Emitido por Andes SCD Cra 27 86 43 |

#### *3.1.2. Necesidad para los nombres de ser significativos*

Todo certificado de Comunidad Académica emitido por Andes SCD tiene como característica principal la plena identificación del suscriptor y la asignación de un nombre significativo a su certificado.

#### *3.1.3. Anónimos y pseudónimos en los nombres*

En esta Política de Certificado no se admiten anónimos ni seudónimos para identificar el nombre de una Persona Natural.

En el caso de una persona natural con nacionalidad Colombiana el nombre debe estar conformado por nombres y apellidos tal como figura en la cedula de ciudadanía. Si la persona natural es un extranjero el nombre debe estar conformado por nombres y apellidos tal como figura en el pasaporte o documento equivalente.

#### *3.1.4. Reglas para interpretar los formatos* de nombre

Las reglas para interpretar los formatos de nombre siguen lo señalado por el estándar X.500 de referencia en ISO/IEC 9594.

#### *3.1.5. Singularidad* de los nombres

Se garantiza que los nombres distinguidos de los certificados de Comunidad académica son únicos para cada suscriptor porque contienen atributos serial y email que permiten distinguir entre 2 identidades cuando existan problemas de duplicidad de nombres.

### 3.2. Aprobación de la identidad

#### *3.2.1.Método para demostrar la posesión de la llave privada*

En la Declaración de Prácticas de Certificación de Andes SCD se detalla el procedimiento que utiliza la Autoridad Certificadora para demostrar que el solicitante posee la llave privada correspondiente a la llave pública que se pretende vincular al certificado de Comunidad Académica.

#### *3.2.2.Autenticación de la identidad del solicitante*

El solicitante puede tramitar su solicitud de emisión de certificado de Comunidad académica de las siguientes formas:

1. **Presencial**: El solicitante realiza la solicitud personalmente ante Autoridad de Registro de Andes SCD.
2. **Remota** : El solicitante realiza la solicitud desde la página WEB de Andes SCD.
3. **Convenios**: Las solicitudes de emisión de certificados por convenios son tramitadas por un coordinador designado por la entidad o empresa, de acuerdo con los procedimientos internos definidos por la autoridad de registro

| Requisito | Solicitud presencial | Solicitud remota o convenio |
|---|---|---|
| **Cedula de ciudadanía o documento que acredite la identidad** (Ampliada a 150% y legible) **o evidencias digitales suministrada por un tercero que permitan verificar la identidad del solicitante.** | Presentar original y Fotocopia documento | Se requiere documento escaneado |
| **Documento o evidencia digital emitido por la institución educativa donde haga constar la relación con el solicitante** (Documento legible con fecha de expedición menor *a 30 días*) | Presentar Fotocopia documento | Se requiere documento escaneado |

Adicionalmente el solicitante debe suministrar la siguiente información que permitirá a Andes SCD contactarlo cuando sea necesario:

| Requisito | Información adicional |
|---|---|
| 1 | País, departamento y ciudad donde reside |
| 2 | Dirección y número teléfono fijo y celular |
| 3 | Correo electrónico personal |
| 4 | Correo electrónico institucional |

La información suministrada en la solicitud de emisión de certificado de Comunidad académica es estudiada por el supervisor quien se encarga de verificar que la información sea original, suficiente y adecuada de acuerdo a los procedimientos internos definidos por Andes SCD.

En caso de que el suscriptor reclame la modificación de los datos personales respecto a los contenidos en el documento de identificación presentado, deberá enseñar el correspondiente certificado de registro civil donde figura la variación.

#### *3.2.3. Información no verificada sobre el solicitante*

La autoridad de registro verifica toda la información del solicitante que se encuentre respaldada con documentos o evidencias digitales como soporte. No se verifica dirección de residencia y correo electrónico presumiendo la buena fe de la información aportada por el solicitante.

#### *3.2.4. Identificación* y autenticación para solicitar revocación

Se permite solicitar la revocación de un certificado a las siguientes personas:

- Al propio suscriptor, en cuyo caso debe usar el código de revocación que se le entrego en el momento de adquirir el certificado.
- Los operadores autorizados de Andes SCD o de la jerarquía de certificación pueden revocar cualquier certificado en aquellos casos en que se incurra a las circunstancias establecidas en apartado 4.4.1 de la Declaración de Prácticas de Certificación.

## 4. Ciclo de vida del certificado y procedimientos de operación

Los certificados de Comunidad académica emitidos por Andes SCD tienen un periodo de vigencia explícito en los atributos "*válido desde"* y "*válido hasta"* del propio certificado El tiempo de vigencia del certificado no podrá ser mayor a 730 días calendario.

Al finalizar el periodo de vigencia se produce la invalidez del certificado cesando permanentemente su operatividad y se da por terminada la prestación del servicio de certificación entre Andes SCD y el suscriptor.

### *4.1. Emisión de certificados*

La Autoridad de Certificación Andes SCD se asegura de que los suscriptores han sido plenamente identificados y que la petición de certificado es completa.

#### *4.1.1.* Quien pueden solicitar la emisión de un certificado

La solicitud de un certificado digital puede realizarla cualquier persona vinculada a una institución educativa una institución educativa y que este en plena capacidad de asumir las obligaciones y responsabilidades inherentes a la posesión y uso del certificado.

#### *4.1.2. Procedimiento para solicitar certificado*

El procedimiento que debe realizar el solicitante para adquirir un certificado digital se encuentra descrito en la Declaración de Prácticas de Certificación DPC. Ver sección 4.1.2 “Procedimiento para solicitar la emisión de certificado” en la DPC.

#### *4.1.3.* Publicación del certificado por Andes SCD

Una vez emitido el certificado por Andes SCD se procede a la publicación en el directorio de certificados.

#### *4.1.4.* Par de llaves y uso del certificado

##### 4.1.4.1. Por parte del suscriptor

El suscriptor posee una llave pública y una llave privada legalmente validas durante el periodo de vigencia del certificado de Comunidad académica que las legitima. La llave privada es de uso exclusivo del suscriptor para los fines estipulados en esta Política de Certificación y debe ser protegida para impedir el uso no autorizado por parte de terceros.

El suscriptor solo puede usar el certificado y el par de llaves tras aceptar las condiciones de uso establecidas en la DPC y en la presente PC y solo para lo que estas establezcan.

Una vez el certificado haya expirado o este revocado el suscriptor está en la obligación de no volver a usar la llave privada.

##### 4.1.4.2. Por parte de usuarios que confían

Los usuarios que confían en el servicio de certificación de Andes SCD deben verificar los usos establecidos en el campo ‘Key usage’ del certificado o en la presente Política de Certificación para conocer el ámbito de aplicación del certificado Comunidad académica.

Los usuarios que confían en el servicio de certificación de Andes SCD deben asumir la responsabilidad de verificar el estado del certificado antes de depositar su confianza.

### *4.2. Renovación de certificados*

Andes SCD no tiene contemplado el proceso de renovación de certificados, si el suscriptor desea obtener un nuevo certificado debe solicitar la emisión de certificado cuando su certificado original haya caducado

### *4.3. Modificación de certificados*

Los certificados digitales emitidos por Andes SCD no pueden ser modificados.

### *4.4. Revocación de certificados*

La revocación consiste en la pérdida de fiabilidad del certificado y el cese permanente de su operatividad impidiendo el uso por parte del suscriptor; una vez revocado el certificado la Autoridad Certificadora lo incluye en la CRL con el fin de notificar a terceros que un certificado ha sido revocado en el momento en que se solicite la verificación del mismo.

Los certificados que sean revocados no podrán por ninguna circunstancia volver al estado activo, siendo esta una acción definitiva.

Puede solicitar la revocación de un certificado de Comunidad académica el propio suscriptor titular del certificado a partir de los medios de revocación que ofrece Andes SCD en la sección 4.4.3 de la DPC y siguiendo el procedimiento de revocación especificado en la sección 4.4.4 de la DPC. Adicionalmente, Andes SCD o cualquiera de las autoridades que la componen puede solicitar la revocación de un certificado de Comunidad académica si tuviera conocimiento o sospecha del compromiso de la llave privada del suscriptor o cualquier otro hecho determinante que requiera proceder a revocar el certificado

En la Declaración de Prácticas de Certificación se detallan las circunstancias por las cuales se recurre a la revocación de un certificado digital, los medios disponibles para efectuar la revocación, el procedimiento para revocar un certificado, el tiempo que tarda Andes SCD en procesar la solicitud de revocación y en publicar los certificados revocados en la CRL.

### *4.5. Reposición de certificados*

La reposición de un certificado es el procedimiento donde se sustituye un certificado de firma digital a petición de la entidad/suscriptor que lo ha adquirido por alguna de las siguientes razones:

- Cambio de titular del certificado de firma digital
- Cambio de la información del titular de la firma digital

Andes SCD ha establecido las siguientes condiciones para realizar la reposición de un certificado:

- El certificado debe tener una vigencia inicial igual o superior a 1 año
- El certificado debe tener una vigencia restante mayor a 6 meses
- No haber realizado la reposición del certificado previamente
- Comunicar el motivo de la reposición
- La reposición aplica para solicitar el mismo tipo de certificado adquirido inicialmente

### *4.6. Servicios de estado de certificado*

En la Declaración de Prácticas de Certificación se proporciona información sobre los medios para publicar el estado de los certificados emitidos, la disponibilidad del servicio y el fin de suscripción al servicio de certificación.

### *4.7. Vigencia de los certificados*

El periodo de vigencia de los certificados digitales de Comunidad académica esta explícito en el propio certificado en los atributos *"Valido desde"* y *"Valido Hasta"* y no será mayor a 730 días calendario
El par de llaves tiene el mismo periodo de vigencia del certificado digital que las avala.

## 5. Controles 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.

## 6. Controles de seguridad técnica

### *6.1. Generación de llaves e instalación*

#### *6.1.1. Generación del par de llaves*

Las llaves pública y privada de titulares de Certificados de Comunidad académica son generadas de acuerdo a los procesos estipulados en la DPC Numeral 6.1.1 sección Llaves del suscriptor. El método de generación del par de llaves del suscriptor varía de acuerdo a la forma de entrega del certificado elegido por el suscriptor o según convenio.

#### *6.1.2. Entrega de la llave privada al suscriptor*

Cuando las llaves privadas de los certificados de Comunidad Académica sean generadas por ANDES SCD solo podrán ser almacenadas en dispositivos criptográficos que cumplan con el estándar FIPS 140-2 Nivel 3.

Cuando el formato de entrega es PKCS10 el par de llaves es generado por el propio suscriptor, la llave privada en ningún momento es conocida por ANDES SCD

El mecanismo de entrega de la llave privada a titulares de Certificados de Comunidad Académica se describe en la DPC Numeral 6.1.2.

#### *6.1.3. Entrega de la llave pública al emisor del certificado*

El mecanismo de entrega de la llave pública a titulares de Certificados de Comunidad académica se describe en la DPC Numeral 6.1.3.

#### *6.1.4. Distribución de la llave pública del suscriptor*

La llave pública de cualquier suscriptor de Certificados de Comunidad académica está permanentemente disponible para descarga en el directorio de certificados de Andes SCD mientras el certificado no este revocado.

#### *6.1.5. Distribución de la llave pública de Andes SCD a los usuarios*

La llave pública de la CA Andes raíz, de la CA emisora de certificados Clase II o de entidad final y de las CA emisoras de certificados Clase III o de entidad final convenios están permanentemente disponibles para descarga en la página WEB de Andes SCD.

#### *6.1.6. Periodo de utilización de la llave privada*

El periodo de utilización de la llave privada es el mismo tiempo de la vigencia del certificado de Comunidad académica o menos si el certificado es revocado antes de caducar.
En la DPC de Andes SCD se detalla el periodo de utilización de la llave privada de la CA raíz y de la CA emisora de certificados de Clase II o de Entidad Final.

### *6.1.7. Tamaño de las llaves*

El tamaño mínimo de las llaves de certificados de Comunidad académica es de 2048 bits basadas en el algoritmo RSA.

El tamaño de las llaves certificadas de la CA emisora de los certificados de Comunidad académica tiene una longitud de 4096 bits basadas en el algoritmo RSA.

## *6.2. Controles de protección de la llave privada*

En la Declaración de Prácticas de Certificación de Andes SCD se especifican los controles y estándares de los módulos criptográficos, el control, respaldo, almacenamiento, activación, desactivación y destrucción de las llaves privadas de la Autoridad de Certificación.

A continuación se especifican los controles de protección de la llave privada del suscriptor

| Control de protección | Llave privada generada por suscriptor desde Dispositivo TOKEN y CSR |
|---|---|
| Respaldo de la llave privada | Andes SCD no realiza respaldo sobre las llaves privadas de los suscriptores generadas desde dispositivo TOKEN o cuando el certificado se genera a partir de CSR. Andes SCD nunca está en posesión de dichas llaves y solo permanecen bajo custodia del propio suscriptor |
| Almacenamiento de la llave privada | Las llaves privadas de los suscriptores generadas desde dispositivo TOKEN NUNCA son almacenadas por Andes SCD. Igualmente sucede cuando el certificado es generado a partir de CSR entregado por el suscriptor.<br>La llave privada debe ser almacenada por el propio suscriptor mediante la conservación del dispositivo TOKEN u otros métodos, debido a que pueden ser necesarias para descifrar la información histórica cifrada con la llave pública |
| Transferencia de la llave privada | La llave privada de los suscriptores generada desde el TOKEN nunca sale del dispositivo.<br>Con el dispositivo TOKEN se genera el par de llaves y se protege su uso a través de un PIN que solo conoce el suscriptor.<br>La llave privada generada por el usuario que entrega CSR para generación de certificado es custodiada por el suscriptor y nunca es envidad a Andes SCD. |
| Activación de la llave privada | La activación del dispositivo TOKEN que contiene la llave privada del suscriptor se realiza a través de un PIN que debe ser personalizado por el propio suscriptor en el momento de generar el par de llaves. La protección de los datos de activación es responsabilidad del suscriptor |
| Desactivación de la llave privada | El método para desactivar la llave privada del suscriptor es retirar el dispositivo TOKEN del equipo, inmediatamente cualquier contenido asociado queda deshabilitado incluyendo la llave privada |
| Destrucción de llave privada | La destrucción de la llave privada puede realizarla el propio suscriptor utilizando las funciones que provee el dispositivo TOKEN, teniendo cuidado de no afectar otras llaves privadas almacenadas en el dispositivo.<br><br>La destrucción de la llave privada del suscriptor puede realizarla el propio suscriptor eliminando la llave privada correspondiente al CSR enviado a Andes SCD. |

Certificados tramitados por convenios

En los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 se especifican los controles de protección de la llave privada cuando el certificado ha sido tramitado mediante convenio

## 6.3. Dispositivos Criptográficos admitidos

Los dispositivos criptográficos admitidos por ANDES SCD deben cumplir con las siguientes características:

- Genera pares de llaves RSA hasta de 2048 bits.
- Algoritmos para la generación RSA y SHA-256 implementados por hardware.
- Hardware generador de números aleatorios.
- Hardware generador de firma digital.
- Espacio mínimo disponible de 64 Kb.
- Certificación FIPS 140-2 Nivel 3
- Certificación CE y FCC.
- Soporte completo para aplicaciones PKI.
- Compatible con interfaces CAPI y PKCS#11.
- Soporte para el almacenamiento de múltiples llaves.
- Soporte para X.509 V3 formato estándar de certificado.

### *6.3.1.* Riesgos asociados

Los dispositivos criptográficos admitidos por ANDES SCD pueden presentar riesgos como:

- Perdida del dispositivo
- Compromiso de la llave
- Daño por manipulación inadecuada o condiciones ambientales.
- Daño por variaciones en el voltaje.

Para mitigar los riesgos asociados deben tenerse en cuenta unas normas de seguridad:

- El PIN es confidencial, personal e intransferible.
- Se recomienda cambiar el PIN periódicamente.
- Los dispositivos criptográficos deben mantenerse en condiciones ambientales adecuadas lejos de la humedad.
- En caso de compromiso o pérdida de la llave privada debe solicitarse la revocación del certificado.

## *6.4. Otros aspectos de administración del par de llaves*

### *6.4.1.* Archivo de la llave pública

Andes SCD mantiene archivados todos los certificados digitales de Comunidad académica, los cuales incluyen la llave pública durante el periodo estipulado en el apartado 6.3.1 de la DPC.

### *6.4.2.* Periodos operacionales del certificado y periodos de uso del par de llaves

El tiempo de vida del certificado de Comunidad académica está regido por la validez del mismo o mientras no se manifieste de forma explícita su revocación en una CRL o en el sistemas de verificación en línea. Si alguno de estos eventos sucede se da por terminada la validez del certificado y este solo podrá usarse para fines de comprobación histórica.

El par de llaves tiene vigencia mientras exista un certificado de Comunidad académica válido que las sustente. Una vez el certificado deje de ser válido las llaves pierden toda validez legal y su uso se limita a fines exclusivamente personales.

## 6.5. Datos de activación

### *6.5.1.* Generación de datos de activación e instalación

El suscriptor debe generar los datos de activación de su TOKEN cambiando el PIN inicial que trae por defecto el dispositivo.
El PIN debe ser custodiado por el suscriptor de modo que no sea conocido por nadie más y se garantice el control exclusivo del TOKEN.

En los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 se indica el mecanismo de generación de datos de activación cuando el certificado ha sido tramitado mediante convenio.

### *6.5.2.* Protección de datos de activación

El PIN o dato de activación del TOKEN debe ser personalizado por el solicitante antes de generar su par de llaves o si existe la sospecha de que un tercero conoce este dato.
Para cambiar el PIN es necesario descargar el aplicativo software que ofrece el fabricante del TOKEN y que se encuentra disponible en la página web de Andes SCD

En los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 se indica la protección de datos de activación cuando el certificado ha sido tramitado mediante convenio.

## *6.6. Controles de seguridad informática*

En la Declaración de Prácticas de Certificación se describen los controles de Andes SCD para lograr un adecuado resguardo de los recursos informáticos.

## 7. Perfiles de certificado, CRL y OCSP

### *7.1.* Contenido *del certificado*

| Formato de certificados de Comunidad académica | | |
|---|---|---|
| **Campo** | **Descripción** | **Valor** |
| Versión | Versión del certificado | V3 |
| Serial number | Número que identifica al certificado | Número de serie del certificado del suscriptor |
| 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 (issuer) | Datos de la CA subordinada de entidad final que emitió el certificado. | Ver en el certificado los datos de la CA Clase II o la CA Subordinada de la CA Clase III |
| Valido desde | Fecha y hora UTC inicio validez | Fecha de inicio de la validez del certificado |
| Válido hasta | Fecha y hora UTC fin validez | Fecha final de la validez del certificado |
| Asunto | CN | Nombre completo del suscriptor |
| | Serial Number | Número documento identificación del suscriptor |
| | E | Correo electrónico del suscriptor |
| | C | Abreviatura del país donde reside el suscriptor |
| | ST | Nombre departamento donde reside suscriptor |
| | L | Nombre municipio donde reside el suscriptor |
| | STREET | Dirección donde reside el suscriptor |
| | T | Indica el tipo de vinculación del suscriptor con la comunidad académica. |
| | O | Nombre de la universidad o Comunidad Académica. |
| | OU | Nombre de facultad y carrera a la que se encuentra vinculado |
| | OU | Comunidad académica Emitido por Andes SCD Cra 27 86 43 |
| Llave pública | Llave pública del titular del certificado | RSA (2048 Bits) |
| Extensiones | Extensiones utilizadas en los certificados | Ver apartado 7.2.2 de este documento para más detalles. |
| 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<br>No repudio<br>Cifrado de información |

## 7.2. Perfiles de certificado

### 7.2.1. Número de versión

Los certificados de Comunidad académica emitidos bajo esta política están de conformidad con el estándar X.509 V3 y de conformidad con el RFC 5280 para perfiles de certificados y CRL.

### 7.2.2. Extensiones del certificado

Los certificados de Comunidad académica emitidos por Andes SCD utilizan una serie de extensiones que pretenden establecer los usos del certificado, referenciar las Políticas de Certificación aplicables y restricciones adicionales. A continuación se detallan las extensiones incluidas en los certificados digitales de Comunidad académica

| Extensiones Certificados Comunidad académica según estándar X.509V3 | |
|---|---|
| Nombre | **Valor** |
| Acceso a la información de la entidad emisora | Método de acceso=Protocolo de estado de certificado en línea<br>Dirección URL=http://ocsp.andesscd.com.co |
| Identificador de la llave del titular | Identificador de llave del titular |
| Identificador de llave entidad emisora | Identificador de la llave de la CA de Andes SCD que emitió el certificado |
| Puntos de distribución de la CRL | URL de publicación de CRL de la CA que emitió el certificado. |
| Uso de la llave | Firma Digital<br>No repudio<br>Cifrado de información |
| Uso mejorado de la llave | Autenticación del cliente<br>Correo Seguro |
| Nombre alternativo del titular | Email del suscriptor<br>RFC 822 Name (e-mail address) |
| Restricciones Básicas | Tipo de asunto=Entidad final<br>Restricción de longitud de ruta=Ninguno |
| Directiva de certificados | [1]Directiva de certificados:<br>Identificador de directiva=1.3.6.1.4.1.31304.1.2.2.2.6<br>[1,1]Información de certificador de directiva:<br>Id. de certificador de directiva=Aviso de usuario<br>Certificador:<br>Texto de aviso=La utilización de este certificado está sujeta a las Políticas de Certificado de Comunidad académica (PC) y Prácticas de Certificación (DPC) establecidas por Andes SCD.<br>[1,2]Información de certificador de directiva:<br>Id. de certificador de directiva=CPS<br>Certificador:<br>URL de DPC vigente |

### *7.2.3. Identificadores de objeto de los algoritmos*

Los certificados digitales de Comunidad académica emitidos bajo esta política utilizan los siguientes algoritmos y sus correspondientes identificadores (OID)

- OID del algoritmo de firma SHA256withRSAEncryption 1.2.840.113549.1.1.11
- OID del algoritmo de la llave pública RSAEncryption 1.2.840.113549.1.1.1

### *7.2.4. Formatos de nombres*

Los Certificados digitales de Comunidad académica emitidos por Andes SCD están restringidos a 'Distinguished names' (DN) X.500 que son únicos y no ambiguos, los certificados contienen el DN del emisor y del suscriptor del certificado en los campos issuer name y subject name respectivamente.

### *7.2.5.* Restricciones de nombre

Los certificados digitales emitidos bajo esta política cuentan con DN conforme a las recomendaciones X.500 que son únicos y no ambiguos.

### *7.2.6.* Objeto identificador de la política de certificación

Las políticas y prácticas de certificación son identificadas mediante un número único denominado OID, el OID asignado a la presente política es 1.3.6.1.4.1.31304.1.2.2.2.6.

En la Declaración de Prácticas de Certificación en el apartado 7.1.6 encuentra más información respecto a este tema.

### *7.2.7.* Sintaxis y semántica de los calificadores de la política

La extensión de los certificados referente a los calificadores de la Política de Certificación contiene la siguiente información:

- **Policy identifier:** Contiene el identificador de la Política de Certificado Comunidad académica
- **CPS**: Indica la URL donde esta publicada la Declaración de la Practicas de Certificación (DPC) para ser consultadas por los usuarios
- **User Notice**: contiene el texto "La utilización de este certificado está sujeta a las Políticas de Certificado de Comunidad académica (PC) y Declaración de Prácticas de Certificación (DPC) establecidas por Andes SCD".

### *7.3. Perfil de la CRL*

#### *7.3.1.* Numero de versión

Las CRL emitidas por Andes SCD corresponden con el estándar X.509 versión 2

#### *7.3.2.* CRL y extensiones

Se emite la lista de revocación CRL según lo estipulado en la RFC 2459

| Perfil de CRL según estándar X.509V2 – CRL | | |
|---|---|---|
| **Nombre** | **Descripción** | **Valor** |
| Versión | Versión de la CRL | V2 |
| Numero de CRL | Número único de la CRL | Identificado de la CRL |
| Emisor | Datos de la CA subordinada de entidad final que emitió la CRL | Ver en la CRL los datos de la CA que emitió la CRL |
| Algoritmo de firma | Algoritmo usado para firma de la CRL | SHA256withRSA |
| Fecha efectiva de emisión | Periodo de validez después de emitida la CRL | Fecha de emisión de la CRL en tiempo UTC |
| Siguiente actualización | Fecha en que se emitirá la siguiente CRL | Fecha de emisión de la próxima CRL en tiempo UTC |
| Emitir puntos de distribución | URL donde se publican las CRL emitidas por Andes SCD | Ver en la CRL la URL de publicación |
| Certificados revocados | Lista de certificados revocados especificando el número de serie, fecha de revocación y motivo revocación | |

### *7.4. Perfil OCSP*

#### *7.4.1.* Numero de versión

El certificado OCSP se emite de acuerdo al estándar X.509 V3

#### *7.4.2.* Extensiones OCSP

| Extensiones OCSP según estándar X.509V3 | |
|---|---|
| **Nombre** | **Valor** |
| Basic Contraints, critical | CA false |
| Key Usage critical | Firma digital |
| Extended Key Usage | OCSPSigner |
| Subject Key Identifier | identificador de llave |

## 8. Auditoria y otras valoraciones

La información sobre la auditoria y otras valoraciones se encuentra especificada en la Declaración de Prácticas de Certificación de Andes SCD.

## 9. Negocio y materias legales

### 9.1. Tarifas

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

| Vigencia | 6 meses | 1 año | 2 años |
|---|---|---|---|
| Certificado en Token (clientes nuevos) | $105.000 | $ 160.000 | $ 230.000 |
| Certificado en Token (Renovación) | No aplica | $ 122.000 | $ 218.000 |

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

### 9.2. Responsabilidad financiera

En la Declaración de Prácticas de Certificación de Andes SCD se especifica el valor de la cobertura para indemnizar los daños y perjuicios que pudiera ocasionar el uso de los certificados expedidos por Andes SCD.

### 9.3. Confidencialidad de la información

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD

### 9.4. Derechos de propiedad intelectual

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD

### 9.5. Obligaciones y garantías

En la Declaración de Prácticas de Certificación se listan las obligaciones y garantías por parte de la Autoridad de Certificación Andes SCD, las Autoridades de Registro, los solicitantes, suscriptores y usuarios del servicio de certificación

#### *9.5.1.* Obligaciones y responsabilidad de ANDES SCD.

Las obligaciones y responsabilidad de ANDES SCD como entidad de certificación digital son las siguientes:

1. Contar con los elementos tecnológicos, económicos, humanos e instalaciones requeridas para ofrecer los servicios de certificación, así como los controles de seguridad física, de procedimientos y estrategias necesarias para garantizar la confianza y operación de los servicios.
2. Garantizar el cumplimiento de los requisitos impuestos por la legislación vigente.
3. Proteger las llaves privadas de la Autoridad Certificadora ANDES SCD.
4. No copiar ni almacenar las llaves privadas correspondientes a los certificados emitidos a Entidad Final y tampoco de certificados de uso interno emitidos con el propósito de utilizarse para firma electrónica, cuando estos sean generados sobre los dispositivos criptográficos de la Entidad Final.
5. Emitir Certificados conformes con el estándar X.509 V3 y de acuerdo a lo solicitado por el suscriptor.
6. Garantizar que se puede determinar la fecha y hora en la que se expidió un certificado o se revocó.
7. Utilizar sistemas fiables para almacenar los certificados e impedir que personas no autorizadas modifiquen los datos y detectar cualquier indicio que afecte la seguridad.

8. Mantener actualizado el directorio de certificados indicando los certificados emitidos y si están vigentes o revocados.
9. Almacenar en la infraestructura PKI de forma indefinida las CRL y los certificados digitales vigentes, vencidos y revocados.
10. Publicar de manera oportuna en la página WEB los certificados que se encuentran vigentes y las CRL de la CA Raíz y las CA subordinadas.
11. Informar a los suscriptores la proximidad del vencimiento de su certificado enviando un correo electrónico 30, 15, 7 y 1 días antes del vencimiento.
12. Cumplir lo dispuesto en las Políticas y Prácticas de Certificación.
13. Disponer de personal calificado, con el conocimiento y experiencia necesaria para la prestación del servicio de certificación ofrecido por ANDES SCD.
14. Aprobar o denegar las solicitudes de emisión de certificados enviadas por la Autoridad de Registro.
15. Proporcionar al solicitante en la página web de ANDES SCD la siguiente información de manera gratuita: - Las Políticas y Prácticas de certificación y todas sus actualizaciones. - Obligaciones del firmante y la forma en que han de custodiarse los datos - Procedimiento para solicitar emisión de certificado. - El procedimiento de revocación de su certificado. - Mecanismos para garantizar la fiabilidad de la firma electrónica a lo largo del tiempo - Las condiciones y límites del uso del certificado.
16. Informar a los suscriptores de la revocación de sus certificados inmediatamente a que se produzca dicho evento.
17. Informar Superintendencia de Industria y Comercio sobre los eventos que puedan comprometer la prestación del servicio de ANDES SCD.
18. Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor.
19. Tomar medidas contra la falsificación de certificados y garantizar su confidencialidad durante el proceso de generación y su entrega al suscriptor mediante un procedimiento seguro. Las demás que se encuentran contempladas en su declaración de Prácticas de Certificación, las cuales se entienden incorporadas en el presente documento. Dicho documento se encuentra disponible en la página web.

### *9.5.2.* Obligaciones del suscriptor.

El suscriptor tendrá las siguientes obligaciones:

1. Pagar la remuneración pactada en la cláusula cuarta de los Términos y condiciones del servicio aceptados por el suscriptor en el momento en que lo indique ANDES SCD.
2. Custodiar el Certificado tomando todas las precauciones a su alcance para evitar el acceso de terceras personas a éste.
3. Mantener y garantizar la confidencialidad de la llave privada y del código de uso del Certificado. El suscriptor es el responsable único y directo de la confidencialidad de la llave privada y el PIN para la instalación de la misma.
4. Informar en forma inmediata a ANDES SCD cualquier cambio o alteración en la información que se haya incorporado en el certificado digital, o de cualquier alteración que pueda afectar la prestación del servicio de ANDES SCD.
5. Informar a las personas que confían en el certificado digital de las medidas y precauciones que deben tomarse para poder confiar en un certificado digital de ANDES SCD.
6. Utilizar el certificado digital tan solo para los usos y de acuerdo a las condiciones especificadas en el certificado digital, en la Declaración de Prácticas de Certificación y la Política de Certificación aplicable.

7. Solicitar la revocación del certificado digital cuando ocurra cualquiera de las causales contempladas en la Declaración de Prácticas de Certificación.
8. Respetar los derechos de terceras personas y responsabilizarse frente a las mismas por los perjuicios que la utilización del certificado digital pueda causar, así como salir en defensa de ANDES SCD si ésta es demandada por cualquier circunstancia relacionada con la utilización del certificado digital.
9. Seguir en todo caso las instrucciones que le imparta ANDES SCD para el uso del certificado digital y la ejecución de los Términos y condiciones del servicio aceptados por el suscriptor, y permitir en todo caso la verificación del cumplimiento de las mismas.
10. Contar de manera permanente con toda la infraestructura tecnológica y de seguridad necesaria para la utilización adecuada de los certificados digitales, de acuerdo con los requerimientos que haga ANDES SCD.
11. Contar de manera permanente con personal capacitado para la administración y funcionamiento adecuado de los certificados digitales.
12. El suscriptor persona jurídica deberá velar por la correcta utilización de los certificados digitales de ANDES SCD que se utilicen en su empresa.
13. El suscriptor persona jurídica deberá informar inmediatamente cualquier modificación que ocurra en su sistema de representación legal o en la relación jurídica que tiene con el suscriptor persona natural.
14. Realizar y conservar por sus propios medios los archivos de respaldo o copias de seguridad de la información relacionada con los Términos y condiciones del servicio anteriormente aceptados y la utilización del certificado digital.
15. Cualquier otra que se derive de la Declaración de Prácticas de Certificación, de las Políticas de Certificación específicas del certificado digital aplicable al caso.

### *9.5.3.* Prohibiciones para el suscriptor:

El suscriptor, en el consumo de los servicios de certificación de ANDES, deberá Abstenerse de:

1. Alterar o modificar, en todo o en parte, el certificado digital o el software entregado por ANDES SCD, o permitir que terceras personas lo hagan.
2. Copiar o reproducir en cualquier forma el certificado digital, 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 certificado digital o del software que se relacione con la prestación del servicio de ANDES SCD.
4. Transferir, ceder o negociar los derechos otorgados en virtud de los servicios de ANDES.
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.
6. Darle al certificado digital un uso distinto de aquel que se desprende de la Declaración de Prácticas de Certificación.

## 9.6. Principio de Imparcialidad

En las relaciones con los clientes, cualquiera sea tu naturaleza, tamaño, calidad, así como en la prestación de los servicios de ANDES, se actuará de acuerdo con los principios definidos en la política de Imparcialidad, Integridad E Independencia OID 1.3.6.1.4.1.31304.100.3.80.

### 9.7. Limitaciones de responsabilidad

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD

### 9.8. Indemnizaciones

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD

### 9.9. Término y terminación

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD

### 9.10. Procedimiento de cambio en las especificaciones

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD

### 9.11. Prevención de disputas

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD

### 9.12. Ley aplicable y cumplimiento con la ley aplicable

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD

## Control de Cambios

| Versión | Fecha | Detalle | Responsable |
|---|---|---|---|
| 1.1 | 24/02/2011 | Versión inicial autorizada por la SIC según resolución 14349 de marzo 2011 | Comité políticas y seguridad |
| 1.2 | 02/11/2011 | - 3.1.1 y 7.1.1 – Se actualiza distinguish name del certificado<br>- 6.1.7 y 7.1.1 – Se aumenta tamaño de las llaves a 2048<br>- 6 – Se hace referencia a la forma de entrega de certificados PKCS12<br>- 4.6 – Se ofrece certificados de diferentes vigencias. La vigencia esta explicita en el propio certificado | Comité políticas y seguridad |
| 2.0 | 09/10/2014 | - 1.3 - Se actualiza dirección y PBX de Andes SCD<br>- 3.1.1 y 7.1 - Se actualiza atributo OU del DN a Certificado Comunidad académica Emitido por Andes SCD Av. Calle 72 # 9 - 55 Oficina 501<br>- 3.2.2 - Se actualiza documentos requeridos para emisión de certificado de firma digital<br>- Todo el documento - Se actualiza término p12 por PKCS12<br>- 6.1.7 - En la sección tamaño de las llaves se elimina el termino mínimo para hacer referencia al tamaño de las llaves generadas por Andes SCD.<br>- 3.1.1 y 7.1 - El 27 enero 2015 se abrevia atributo OU del DN a Comunidad académica Emitido por Andes SCD Av Cll 72 9 55 Of 501 | Comité políticas y seguridad |
| 2.1 | 24/11/2015 | - 1.1 - Se actualiza versión del documento PC y fecha de emisión<br>- 1.3 - Se actualiza datos de contacto y organización que administra el documento<br>- 1.5.2 - Referencia a OID documento con limitaciones de uso certificados de convenios<br>- 3.1.1 y 7.1 - Se actualiza atributo OU del DN a: Comunidad académica | Comité políticas y seguridad |

| | | | |
|---|---|---|---|
| | | Emitido por Andes SCD Cra 27 86 43<br>- 7.2.2 - Se actualiza OID PC y URL DPC Directiva de certificados | |
| 2.2 | 26/09/2016 | - 1.3.2 – Se actualiza email de persona de contacto<br>- 4 – Se limita vigencia máxima del certificado a 730 días.<br>- 4.5 – Se incluye la reposición de certificados.<br>- 4.7 – Se limita vigencia máxima del certificado a 730 días.<br>- 7.2.1 - Se actualiza RFC 3280 por 5280 | Comité políticas y seguridad |
| 2.3 | 06/01/2017 | - 4, 4.7 – Se especifica que la vigencia máxima del certificado son 730 días calendario<br>- 6.1, 6.2, 6.3, 6.4 se elimina forma de entrega PKCS12<br>- 7.2 URL y versión 2.3 de DPC y PC | Comité políticas y seguridad |
| 2.4 | 22/06/2018 | - 1.5.4 Se incluye el apartado minutas y contratos.<br>- 2. Se hace referencia al RFC 4523 relacionado con el LDAP.<br>- 3.2.3 Se hace referencia a autoridad de registro encargada de recopilar las evidencias requeridas.<br>- 3.2.4 se reemplaza termino clave revocación por código revocación<br>- 4. Se suprime el termino contrato de suscripción<br>- 4.5 se incluyó condición para reposición de certificados<br>- 6.1.2 Se hace referencia a los dispositivos criptográficos FIPS 140-2 Nivel 3 para la entrega de la llave privada de los suscriptores.<br>- 6.3 Se hace referencia a los dispositivos criptográficos.<br>- 6.3.1Se hace referencia a riesgos de los dispositivos criptográficos y recomendaciones de seguridad.<br>- 7.2.2 Se actualiza en la directiva de los certificados el enlace a la DPC<br>- 7.3.2 Se actualiza algoritmo de firma SHA256withRSA<br>- 9.1 Se incluyen tarifas de certificados según vigencia<br>- 9.5.1 Se describen obligaciones y responsabilidades de ANDES SCD.<br>- 9.5.2 Se describen obligaciones del suscriptor.<br>- 9.5.3 Se describen prohibiciones para el suscriptor.<br>- 9.6 Se hace referencia al principio de imparcialidad | Comité políticas y seguridad |
| 2.5 | 16/07/2018 | - 7.2.2 se hace referencia a URL de DPC vigente | Comité de Políticas y seguridad |
| 2.6 | 14/09/2018 | - 1.1 Se actualiza fecha de emisión y url descarga de la PC.<br>- 1.3.2 Se actualiza nombre e email del gerente general.<br>- 7.2.2 Se actualiza identificador OID de PC<br>- 7.2.6 Se actualiza identificador OID | Comité de Políticas y seguridad |