# DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN


**AUTORIDAD CERTIFICADORA ANDES SCD**

**Versión 1.4** **NOVIEMBRE 2011**

## Índice de contenido

**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 conformidad con la normatividad Colombiana vigente. Está facultada para emitir y gestionar certificados digitales dirigidos a personas que en su propio nombre ó en representación de una entidad soliciten la emisión de un certificado digital que acredite su identidad en las comunicaciones electrónicas.

## 1. Presentación del documento

Este documento reúne la Declaración de Prácticas de Certificación (DPC) que rige el funcionamiento y operación de la infraestructura de clave pública PKI de Andes SCD, en general explica las normas y prácticas de la Autoridad de Certificación para prestar el servicio, reúne las medidas técnicas y organizativas para garantizar los niveles de seguridad de PKI, establece los requisitos técnicos y legales para aprobar, emitir, administrar, usar y revocar certificados dentro de la jerarquía de certificación.

Las Prácticas de Certificación son un mecanismo para evaluar el grado de confianza que se puede depositar en un certificado digital por lo tanto deben ser conocidas y aplicadas por los miembros de la Autoridad Certificadora, los miembros de la Autoridad de Registro, Suscriptores, Solicitantes y Usuarios que confían en los certificados emitidos por Andes SCD.

Esta DPC asume que el lector conoce los conceptos básicos de un sistema de infraestructura de clave pública (PKI), certificados digitales y firma digital; en caso contrario se le recomienda al lector que se forme en el conocimiento de los dichos conceptos antes de continuar con la lectura del presente documento.

### 1.1. Nombre del documento e Identificación

| | |
|---|---|
| **Nombre del documento** | DECLARACION DE PRÁCTICAS DE CERTIFICACION DE ANDES SCD |
| **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 certificación en cumplimiento con la legislación vigente. |
| **Identificador OID** | 1.3.6.1.4.1.31304.1.1.1.1.4 |
| **Versión** | V 1.4 |
| **Fecha de emisión** | Noviembre 02 de 2011 |
| **Ubicación documento** | http://www.andesscd.com.co/docs/DPC_AndesSCD_V1.4.pdf |

### 1.2. Alcance

Este documento establece las normas y reglas a seguir por la Autoridad Certificadora Andes SCD en la prestación de sus servicios de certificación, estipula los procedimientos relativos al ciclo de vida del certificado y el régimen jurídico aplicado a los integrantes del modelo de confianza.

Como complemento a este documento existen otros documentos adicionales denominados Políticas de Certificación (PC), cada Política de certificación está dirigida a un tipo de certificado en particular y da a conocer las condiciones, procedimientos y usos particulares para el tipo de certificado.

### 1.3. Referencias

La presente 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.

También, para el desarrollo de su contenido, se ha tenido en cuenta los siguientes estándares:

- **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.

### 1.4. Definiciones

- **Auditoria**: Un procedimiento utilizado para validar que los controles están en funcionamiento y son adecuados para sus propósitos. Incluye el registro y análisis de actividades para detectar intrusiones o abusos en un sistema de información. Los defectos hallados en una auditoría deben ser notificados al personal gestor adecuado para que sean tratados y solucionados.

- **Clave pública y clave privada**: La clave pública se incluye en el certificado digital y la clave privada es conocida únicamente por el titular del certificado. Todo lo que sea cifrado con una de las claves solo se puede descifrar con la otra y viceversa.

- **Centro de datos (Data Center)**: Un Data Center es un edificio o porción de un edificio cuya función primaria es alojar una sala de cómputo y sus áreas de soporte. Los centros de cómputo son el cerebro de los sistemas de información de las empresas, operando 7x24x365 con requerimientos de altísima confiabilidad.

- **Componente informático**: Cualquier dispositivo hardware o software susceptible de utilizar certificados digitales para su propio uso, con el fin de identificarse o intercambiar datos firmados o cifrados.

- **HSM (Hardware Secure Module)**: Componente que ofrece una mayor seguridad para la generación y almacenamiento de claves.

- **Infraestructura de claves públicas (PKI):** Es el conjunto de personas, políticas, procedimientos y sistemas informáticos necesarios para proporcionar los servicios de autenticación, cifrado, integridad y no repudio mediante criptografía de claves públicas y privadas y de certificados digitales.

- **Jerarquía de confianza**: Conjunto de Autoridades de Certificación que mantienen relaciones de confianza por las cuales una CA de nivel superior garantiza la confiabilidad de una o varias de nivel inferior. En el caso de Andes SCD la jerarquía tiene 2 niveles, la CA raíz en el nivel superior garantiza la confianza de sus CA subordinadas que emiten certificados de uso interno y de entidad final.

- **Listas de revocación (CRL: Certificate Revocation List):** Lista de acceso restringido donde figuran exclusivamente las relaciones de certificados revocados.

- **OCSP (Online Certificate Status Protocol):** Protocolo informático que permite comprobar de forma rápida y sencilla la vigencia de un certificado electrónico.

- **PKCS#10**: Estándar de criptografía de clave pública No 10 que define la estructura para una solicitud de firma de certificado.

- **PKCS#12**: Define un formato de fichero usado comúnmente para almacenar claves privadas con su certificado de clave pública protegido mediante clave simétrica.

- **Política de Certificación (PC):** Es un conjunto de disposiciones que indican la aplicabilidad de un certificado para una comunidad, incluyendo requerimientos exigibles a los miembros de dicha comunidad. Además indican la conveniencia de un certificado a un tipo de aplicación con requerimientos comunes de seguridad.

- **X.509**: Estándar desarrollado por la ITU para las Infraestructuras de clave pública y los llamados “Certificados de atributos”.

## 1.5. Lista de acrónimos y abreviaturas

| Abreviatura | Descripción |
|---|---|
| **CA** | Autoridad Certificadora (Certification Authority) |
| **CRL** | Lista de certificados revocados (Certificate Revocation List) |
| **DPC** | Declaración de prácticas de certificación |
| **FIPS** | Normativa federal de proceso de información (Federal Information Processing Standard) |
| **RA** | Autoridad de Registro (Registration Authority) |
| **OID** | Identificador digital de objetos (Object Identifier Digital) |
| **PIN** | Número de Identificación Personal (Personal Identification Number) |
| **PKCS** | Estándares de criptografía de Clave Pública (Public Key Cryptography Standards) |
| **PKI** | Infraestructura de Clave Pública (Public Key Infrastructure) |

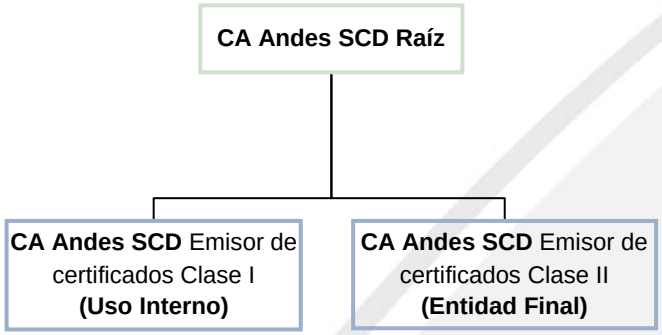
## 1.6. Participantes de PKI ó modelo de confianza

Las entidades y personas que intervienen en el modelo de confianza Andes son:

### *1.6.1. Autoridad de Certificación (CA)*

Es una entidad de confianza que presta servicios de certificación, está facultada para emitir y gestionar certificados digitales actuando como tercera parte de confianza entre el suscriptor y el usuario en las transacciones on-line.

La jerarquía de certificación de Andes SCD está compuesta por las siguientes Autoridades Certificadoras (CA's)




**CA Andes SCD Raíz**: Es la Autoridad Certificadora de primer nivel que emite certificados para sí misma y para sus Autoridades Certificadoras (CA) Subordinadas: CA Andes SCD Emisor de certificados Clase I (uso interno) y CA Andes SCD Emisor de certificados Clase II (Entidad Final).

Los datos de la CA Raíz son los siguientes:

| | | |
|---|---|---|
| **Nombre distintivo** | CN | ROOT CA ANDES SCD S.A. |
| | O | Andes SCD |
| | OU | Division de certificacion |
| | C | CO |
| | L | Bogota D.C. |
| | E | info@andesscd.com.co |
| **Número de serie** | 2d 13 9d 4e 72 a8 a2 12 | |
| **Nombre distintivo del emisor** | CN | ROOT CA ANDES SCD S.A. |
| | O | Andes SCD |
| | OU | Division de certificacion |
| | C | CO |
| | L | Bogota D.C. |
| | E | info@andesscd.com.co |
| **Periodo de validez** | Desde jueves, 08 de julio de 2010 11:36:49 AM<br>Hasta lunes, 09 de julio de 2035 11:36:49 AM | |
| **Usos de la clave** | Firma digital, Firma de certificados, Firma CRL | |
| **Huella digital (SHA-1)** | e8 45 6b ec e2 0d c9 ce 3d 02 0b cd 92 27 b5 f7 1b a5 e7 97 | |

**CA Andes SCD Emisor de certificados de clase I**: Es la Autoridad Certificadora subordinada de la CA Andes SCD Raíz, su función es la de emitir certificados de uso

interno para personal y componentes informáticos de la Autoridad Certificadora y Autoridades de Registro que son necesarios para el funcionamiento interno y operativo.

Los datos de la CA emisora de certificados de clase I son los siguientes:

| | | |
|---|---|---|
| **Nombre distintivo** | CN | CA ANDES SCD S.A. Clase I |
| | O | Andes SCD |
| | OU | Division de certificacion uso interno |
| | C | CO |
| | L | Bogota D.C. |
| | E | info@andesscd.com.co |
| **Número de serie** | 7a af e1 77 99 af c7 cf | |
| **Nombre distintivo del emisor** | CN | ROOT CA ANDES SCD S.A. |
| | O | Andes SCD |
| | OU | Division de certificacion |
| | C | CO |
| | L | Bogota D.C. |
| | E | info@andesscd.com.co |
| **Periodo de validez** | Desde lunes, 12 de julio de 2010 4:54:50PM<br>Hasta jueves, 09 de julio de 2020 4:54:50 PM | |
| **Uso de la clave** | Firma digital, Firma de certificados, Firma CRL | |
| **Huella digital (SHA-1)** | c4 1e d6 2c 60 57 9e f4 bf 16 1f 5e 6e 78 3e 8d 8e 7f fd b9 | |

**CA Andes SCD Emisor de certificados de clase II**: Es la Autoridad Certificadora subordinada de la CA Andes SCD Raíz, su función es la de emitir certificados de entidad final.

Los datos de la CA emisora de certificados de clase II son los siguientes:

| | | |
|---|---|---|
| **Nombre distintivo** | CN | CA ANDES SCD S.A. Clase II |
| | O | Andes SCD. |
| | OU | Division de certificación entidad final |
| | C | CO |
| | L | Bogota D.C. |
| | E | info@andesscd.com.co |
| **Número de serie** | 6e 71 fb 8e c5 17 09 cb | |
| **Nombre distintivo del emisor** | CN | ROOT CA ANDES SCD S.A. |
| | O | Andes SCD |
| | OU | Division de certificacion |
| | C | CO |
| | L | Bogota D.C. |
| | E | info@andesscd.com.co |
| **Periodo de validez** | Desde Viernes, 12 de Agosto de 2011 09:05:38 AM<br>Hasta Lunes, 09 de Agosto de 2021 09:05:38 AM | |
| **Uso de la clave** | Firma digital, Firma de certificados, Firma CRL | |
| **Huella digital (SHA-1)** | 60 62 53 5e 73 b3 99 e6 c6 d8 c7 3a 03 f4 1a a4 d8 b5 3d 10 | |

### *1.6.2. Autoridad de Registro (RA)*

Las Autoridades de Registro son entidades del modelo de confianza que representan el punto de contacto entre el usuario y la Autoridad de Certificación, realiza funciones de validación de identidad, aprueba o rechaza solicitudes de emisión y revocación de certificados digitales.

En el modelo de confianza de Andes SCD un punto de Autoridad de Registro está conformada por:

- ✓ Una parte hardware autorizada para conectarse remotamente a la CA
- ✓ Una parte software que se ejecuta en el hardware autorizado y que corre un programa de administración RA proporcionado por la CA con el cual se gestionan los procedimientos autorizados a ser ejecutados por parte de la RA.
- ✓ Un operador autorizado que utiliza el software de administración de la RA.

Andes SCD emite certificados de uso interno para identificar el hardware y el personal de la RA autorizado. Los certificados emitidos al hardware de la RA son utilizados para establecer un canal seguro de comunicación entre la RA y la CA mediante la creación de una VPN (Red Privada Virtual) que garantiza la confidencialidad e integridad de la información intercambiada. La VPN es el único mecanismo de comunicación entre la CA y RA.

Los certificados de uso interno emitidos al personal de las RA son utilizados para permitir realizar las solicitudes de certificados mediante un software administrador proporcionado por Andes SCD que gestiona la conexión con la CA usando el canal seguro creado por la VPN. Durante la solicitud de conexión un primer mensaje firmado digitalmente por la clave privada del operador RA es enviado a la CA quien verifica la identidad y autorización del personal.

De ser aprobada la conexión por parte de la CA en adelante todos los datos que viajen desde la RA a la CA serán firmados digitalmente por el operador RA, incluidas las solicitudes de generación y revocación.

### *1.6.3. Suscriptor*

Es el titular de un certificado digital a cuya identidad se vinculan unos datos de creación de firma y verificación de firma. En la jerarquía de certificación de Andes SCD existen 2 clases de suscriptores para los certificados emitidos:

| Entorno de certificación | Suscriptores |
|---|---|
| **Certificados de clase I ó de uso interno** | Personal de Andes SCD<br>Personal de Autoridades de Registro<br>Componentes informáticos de Andes SCD<br>Componentes informáticos de RA |
| **Certificados de clase II ó de entidad final** | Personas naturales<br>Personas jurídicas |

### *1.6.4. Solicitante*

Es la persona que ha solicitado la emisión de un certificado digital a Andes SCD

#### *1.6.5. Usuario o tercero aceptante*

Es cualquier usuario que deposita su confianza en los certificados emitidos por la Autoridad Certificadora Andes SCD.

## 1.7. Ámbito de aplicación

La Autoridad Certificadora Andes SCD se encuentra estructurada para proveer servicios de certificación a una amplia variedad de clientes externos y ofrece servicios de certificación al personal interno, componentes informáticos y otros agentes integrados al modelo de confianza como las Autoridades de Registro.

Esta DPC se aplica a todos los certificados emitidos por la CA. Las practicas descritas en la DPC se aplican a la publicación y uso de certificados, listas de revocación y publicadores OCSP para usuarios dentro del dominio de la CA

#### *1.7.1. Usos del certificado*

Las políticas de certificación (PC) correspondientes a cada tipo de certificado son las que determinan los usos apropiados que deben darse a cada certificado. No es objetivo de esta DPC la especificación de dichos usos.

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

Los certificados deben emplearse de acuerdo a la finalidad y funciones definidas en su respectiva política de certificación (PC), sin que puedan utilizarse para otros usos o fines no contemplados en aquella.

Las políticas de certificación correspondientes a cada tipo de certificado determinan las limitaciones y restricciones adicionales en el uso de los certificados. No es objetivo de esta DPC la determinación de dichas limitaciones y restricciones.

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

Debe interpretarse como prohibiciones de uso de los certificados todos aquellos usos que no se encuentren expresamente definidos en la sección usos del certificado de cada Política de Certificado.

Serán consideradas como aplicaciones prohibidas todas aquellas que contravengan las disposiciones, obligaciones y requisitos de la presente Declaración de Prácticas de Certificación.

Las Políticas de Certificación correspondientes a cada tipo de certificado determinan las prohibiciones de uso adicionales.

#### *1.7.4. Limites financieros para el uso de los certificados*

Los certificados emitidos bajo las políticas de certificación de Andes SCD pueden ser usados en conexión con transacciones que tengan un valor inferior de 10.000 dólares

## 1.8. Catálogo de servicios de certificación

### *1.8.1. Certificados de CLASE I – Para Uso interno*

Los certificados de clase I constituyen un elemento técnico necesario para la ejecución de las tareas del personal de la Autoridad Certificadora y de las Autoridades de Registro; el uso de los certificados clase I es estrictamente interno.

Las Políticas de certificación para los certificados Clase I son de carácter confidencial de Andes SCD por lo tanto no se encuentran disponibles en la página web.

### *1.8.2. Certificados de CLASE II – Para Entidad Final*

Andes SCD emite 7 tipos de certificados a las entidades finales del servicio de certificación, A continuación se hace referencia a cada tipo de certificado.

***Certificados personales***

Son certificados emitidos a personas naturales que acreditan la identidad del titular en la firma de documentos garantizando la autenticidad del emisor de la comunicación, el no repudio del origen y la integridad del contenido. El poseedor de un certificado personal actúa en su propio nombre e interés. Para obtener información más detallada consulte la siguiente política de certificación.

| Nombre de política | OID |
|---|---|
| **CERTIFICADOS PERSONALES** | 1.3.6.1.4.1.31304.1.2.1.1.1 |

***Certificados de miembro de comunidad académica***

Son certificados emitidos a personas naturales que acreditan la identidad y su condición como miembro de una comunidad académica, garantizando la autenticidad del emisor de la comunicación, el no repudio del origen y la integridad del contenido. El poseedor de este tipo de certificado actúa en su propio nombre e interés. Para obtener información más detallada consulte la siguiente política de certificación.

| Nombre de política | OID |
|---|---|
| **CERTIFICADOS MIEMBRO DE COMUNIDAD ACADEMICA** | 1.3.6.1.4.1.31304.1.2.2.1.1 |

***Certificados de profesional titulado***

Son certificados emitidos a personas naturales que acreditan la identidad y su título profesional en la firma de documentos garantizando la autenticidad del emisor de la comunicación, el no repudio del origen y la integridad del contenido. El poseedor de un certificado de profesional titulado actúa en su propio nombre e interés. Para obtener información más detallada consulte la siguiente política de certificación.

| Nombre de política | OID |
|---|---|
| **CERTIFICADOS DE PROFESIONAL TITULADO** | 1.3.6.1.4.1.31304.1.2.3.1.1 |

***Certificados de representante legal***

Son certificados que acreditan la identidad del titular y su condición como representante legal de una empresa, identifican tanto al suscriptor como a la empresa y son usados para garantizar la autenticidad del emisor, el no repudio del origen y la integridad del contenido. El titular del certificado puede obrar en nombre de la empresa que representa. Para obtener información más detallada consulte la siguiente política de certificación.

| Nombre de política | OID |
|---|---|
| **CERTIFICADOS DE REPRESENTANTE LEGAL** | 1.3.6.1.4.1.31304.1.2.4.1.1 |

***Certificados de pertenencia a empresa***

Son certificados que acreditan la identidad del titular y su pertenencia, función o cargo desempeñado en una empresa, identifican tanto al suscriptor como a la empresa y son usados para garantizar la autenticidad del emisor, el no repudio del origen y la integridad del contenido. Para obtener información más detallada consulte la siguiente política de certificación.

| Nombre de política | OID |
|---|---|
| **CERTIFICADOS DE PERTENENCIA A EMPRESA** | 1.3.6.1.4.1.31304.1.2.5.1.1 |

***Certificados de Función Pública***

Son certificados emitidos a personas naturales que acreditan la identidad del titular y su condición como funcionario público de una entidad del estado en la firma de documentos, garantizando la autenticidad del emisor de la comunicación, el no repudio del origen y la integridad del contenido. El poseedor de este tipo de certificado actúa en su propio nombre y para el cumplimiento de las funciones de su cargo como servidor público. Para obtener información más detallada consulte la siguiente política de certificación.

| Nombre de política | OID |
|---|---|
| **CERTIFICADOS DE FUNCION PUBLICA** | 1.3.6.1.4.1.31304.1.2.8.1.1 |

***Certificados de Persona Jurídica***

Son certificados emitidos a empresas que acreditan la identidad del titular en la firma de documentos, garantizando la autenticidad del emisor de la comunicación, el no repudio del origen y la integridad del contenido. El poseedor de este tipo de certificado actúa en nombre de la empresa. Para obtener información más detallada consulte la siguiente política de certificación.

| Nombre de política | OID |
|---|---|
| **CERTIFICADOS DE PERSONA JURIDICA** | 1.3.6.1.4.1.31304.1.2.9.1.1 |

## 1.9. Administración de la Política

El contenido de esta Declaración de Prácticas de Certificación es administrado por el comité de Políticas y Seguridad encargado de la elaboración, registro, mantenimiento y actualización de la DPC y las PC de Clase I (uso interno) y de Clase II (entidad final). 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.

### *1.9.1.* Organización que administra este documento

**Nombre** : Comité de Políticas y Seguridad
**Dirección** : Av. Carrera 45 # 103 - 34 Oficina 205
**Email** : comite.politicas.seguridad@andesscd.com.co
**Teléfono** : PBX 571 6001778

### *1.9.2.* Persona de contacto

**Razón social** : Andes Servicio de Certificación Digital S.A SIGLA ANDES SCD SA.
**Nombre** : Juan David Castillo García –Gerente General
**Dirección** : Av. Carrera 45 # 103 - 34 Oficina 205
**Email** : juandavid.castillo@andesscd.com.co
**Teléfono** : PBX 571 6001778

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

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

### *1.9.4.* Publicación del documento

Andes SCD divulga en el sitio WEB de forma inmediata cualquier modificación en la Declaración de Prácticas de Certificación DPC y en las Políticas de Certificación para certificados de entidad final, manteniendo un histórico de versiones. Las políticas de certificación para certificados de uso interno no están disponibles en el sitio WEB y son suministradas al personal en el momento de recibir el certificado de uso interno.

## 2. Publicación y registro de certificados

### *2.1.1. Directorio de certificados*

El directorio de certificados es un directorio WEB de consulta disponible las 24 horas de los 7 días de la semana, donde se hallan todos los certificados de Clase II emitidos por Andes SCD que se encuentran vigentes.

En la página WEB de Andes SCD también se encuentran la CRL de ROOT CA ANDES SCD S.A y CRL de CA ANDES SCD S.A. Clase II o listas de certificados revocados donde se especifica el motivo de revocación, la fecha y hora desde la cual el certificado no tiene validez. Los certificados revocados permanecen de forma indefinida en la CRL de la CA que los emitió.

Un servicio de consulta de certificados se mantiene disponible mediante el protocolo en línea (OCSP) y es accesible de manera permanente por cualquier persona para consultar certificados de clase II ó de entidad final. El directorio de certificados de clase I y las CRL de certificados clase I son de uso interno y solo pueden ser accedidas desde la red interna de Andes SCD

Para garantizar un servicio continuo de verificación de certificados se cuenta con un servidor duplicado y balanceado, de tal forma que en caso de fallas o caída del servidor, el segundo directorio ofrecerá la disponibilidad inmediata del servicio.

### *2.1.2. Medios de publicación*

**Certificados de la CA raíz y CAs subordinadas**

Andes SCD distribuye la clave pública de la CA Raíz y CA emisora de certificados Clase II a través de sus certificados, los cuales están disponibles en las siguientes direcciones:

| Tipo de certificado | Medio de publicación |
|---|---|
| Certificado CA Andes SCD Raíz: | http://www.andesscd.com.co/includes/getCert.php?raiz=1 |
| Certificado CA Andes SCD Clase I – Uso interno | Web: Uso restringido |
| Certificado CA Andes SCD Clase II – Entidad Final | http://www.andesscd.com.co/includes/getCert.php |

**Repositorios de certificados LDAP**

| Repositorios | Medio de publicación |
|---|---|
| CERTIFICADOS Clase I – Uso interno | Solo acceso interno |
| CERTIFICADOS Clase II – Entidad Final | Acceso a LDAP a través de www.andesscd.com.co sección directorio de certificados. |

**Listas de revocación (CRL)**

Las listas de revocación estarán firmadas electrónicamente por la CA de Andes SCD que las emita y en la página de Andes SCD sección histórico de CRL permanecerán publicadas de forma indefinida las CRL de ROOT CA y las CRL de CA Clase II.

| CRL's | Medio de publicación |
|---|---|
| **CRL de ROOT CA ANDES SCD S.A** | http://www.andesscd.com.co/includes/getCert.php?crl=2 |
| **CRL de CA ANDES SCD S.A. Clase I** | Solo acceso interno |
| **CRL de CA ANDES SCD S.A. Clase II** | http://www.andesscd.com.co/includes/getCert.php?crl=1 |

**Protocolo de estado de certificados en línea (OCSP)**

| OCSP | Medio de publicación |
|---|---|
| **CERTIFICADOS De ROOT CA** | http://ocsp.andesscd.com.co |
| **CERTIFICADOS Clase I – Uso interno** | http://ocsp.andesscd.com.co |
| **CERTIFICADOS Clase II – Entidad Final** | http://ocsp.andesscd.com.co |

**Documentación DPC y PC**

Disponible en la dirección http://www.andesscd.com.co/ sección Documentación

### *2.1.3. Frecuencia de publicación*

a) Se publica en la página web de Andes SCD la declaración de prácticas de certificación y las políticas de certificación para entidad final cada vez que hayan cambios de acuerdo al procedimiento estipulado en este documento sección 9.11. Procedimiento de cambio en las DPC y PC.
b) El directorio de certificados se actualiza de forma permanente para reflejar los certificados que se encuentran vigentes.
c) Andes SCD incluye los certificados revocados a la CRL de la CA que emitió el certificado dentro del periodo estipulado en el punto 4.4.7 Publicación de certificados revocados.

### *2.1.4. Control de acceso al directorio de certificados*

El acceso a consulta del directorio de certificados no tiene ninguna restricción, sin embargo para proteger la integridad y autenticidad de la información publicada se cuenta con controles que impiden a personas no autorizadas alterar la información del directorio (al incluir, actualizar o eliminar datos).

La descarga de los certificados y claves públicas de la Autoridad Certificadora Andes SCD se realiza mediante el protocolo seguro de http.

# 3. Identificación y autenticación

A continuación se describen los procedimientos y criterios aplicados por las Autoridades de Registro y Autoridad Certificadora Andes SCD en el momento de autenticar la identidad del solicitante y aprobar la emisión de un certificado.

## 3.1. Nombres

### *3.1.1. Tipos de nombres*

Todos los certificados tienen una sección denominada Asunto cuyo objetivo es permitir identificar al 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.

En la política de certificación (PC) de cada tipo de certificado se especifican los atributos que conforman el DN ó Distinguished name.

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

Todo certificado 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*

No se admiten anónimos ni seudónimos para identificar el nombre de una persona natural o jurídica.

En el caso de una persona jurídica el nombre debe ser exactamente igual a la razón social, no se admiten nombres abreviados.

En el caso de una persona natural el nombre debe estar conformado por nombres y apellidos tal como figura en el documento de identificación reconocido.

### *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

Los nombres distinguidos de los certificados emitidos por Andes SCD serán únicos para cada suscriptor, en cada una de las políticas de certificación se establece la garantía de unicidad.

### *3.1.6.* Reconocimiento, autenticación y función de las marcas registradas

Andes SCD no admite deliberadamente el uso de un nombre de marca registrada cuyo derecho de uso no sea propiedad del suscriptor. Sin embargo la Autoridad Certificadora no está obligada a buscar evidencias de la posesión de marcas registradas antes de la emisión de los certificados.

Andes SCD no asume compromisos en la emisión de certificados respecto al uso por parte de los suscriptores de una marca comercial.

A continuación se describe el procedimiento definido por Andes SCD para la solución de disputas por uso de nombres ó uso de marcas.

Para el caso de personas naturales es irrelevante la existencia de homonimia, toda vez que el elemento diferenciador es el número de documento de identificación.

En el caso de personas jurídicas no es posible el registro de dos usuarios con idéntico nombre. En este sentido el primero en el tiempo en completar la información necesaria para la solicitud del certificado tendrá el derecho al nombre respectivo. Igualmente se seguirán las siguientes reglas:

- Las expresiones y abreviaturas que identifican el tipo de sociedad (Ltda., S.A., S. en C., etc.) no forman parte del nombre y, por lo tanto, no sirven de diferenciador.
- La sola igualdad fonética no es criterio suficiente para considerar que dos nombres son idénticos.
- La adición de números es suficiente para considerar que dos nombres no son idénticos.
- Dos nombres integrados por las mismas palabras pero en distinto orden, no son idénticos.
- Los diminutivos son diferenciadores.
- En nombres conformados con palabras como Bancos, Corporaciones y Cooperativas se aplican las normas pertinentes (D. 1997/88 y L. 78/79). Si hay duda debe consultarse a la Superintendencia Financiera, respecto de los nombres que pueden indicar intermediación, tal como lo señala el decreto mencionado.
- Todo carácter numérico, alfabético, alfanumérico se considera un diferenciador para efectos de la verificación de homonimia, por lo tanto cualquier razón social que tenga un número, una letra, un punto, un guión, un espacio, una apostrofe, un símbolo arroba, hace diferente un nombre o razón social de otra.

## 3.2. Aprobación de la identidad

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

Andes SCD dispone de 2 mecanismos para la emisión de certificados de Entidad Final donde el procedimiento para gestionar la clave privada se maneja de forma diferente de acuerdo a acuerdos establecidos con el suscriptor respecto a la forma de entrega del certificado:

1. El par de claves del suscriptor es generado por el propio suscriptor si el método de entrega del certificado es en dispositivo Token.
2. El par de claves del suscriptor es generado por Andes SCD si el método de entrega del certificado es un archivo con formato PKCS12.

A continuación se describe el método para demostrar la posesión de la clave privada para cada uno de los mecanismos de emisión de certificados de entidad final:

Cuando el par de claves es generado por el propio suscriptor

El futuro suscriptor es la única persona autorizada para crear su propio par de claves (clave privada y clave pública), la clave privada permanece exclusivamente en posesión del suscriptor y en ningún momento es conocida por Andes SCD, mientras que la clave pública si es conocida por Andes SCD porque dicha clave debe ir contenida en el certificado a emitir.

El método utilizado por Andes SCD para comprobar que el solicitante posee la clave privada correspondiente a la clave pública para la que se solicita el certificado queda comprobado de la siguiente forma:

1. En el momento de realizar la solicitud de certificado ante una Autoridad de registro se le entrega un dispositivo Token al solicitante para que proceda a generar y almacenar de forma segura su par de claves.

2. El solicitante inicializa el dispositivo Token suministrando el PIN asignado por el fabricante, este PIN inicial debe ser cambiado por el solicitante quien debe asegurarse de que el PIN solo es conocido por él.

3. El operador de la RA diligencia los datos de la solicitud de certificado en el aplicativo software suministrado por Andes SCD y pide al solicitante generar el par de claves para proseguir con la petición de certificado.

4. Desde el aplicativo software el solicitante ingresa el PIN del Token y debe dar la orden de generar el par de claves. El par de claves generado constituye la identificación digital del solicitante.

   Internamente el aplicativo software de la RA genera la petición de certificado en formato PKCS10. Este formato contiene los datos de la solicitud y la clave pública que acaba de generar el solicitante FIRMADOS implícitamente mediante la clave privada asociada.

5. La petición de certificado en formato PKCS10 es enviada electrónicamente por el aplicativo software de la RA a Andes SCD.

6. Andes SCD comprueba que la clave privada está en posesión del suscriptor al verificar la FIRMA usando la clave pública que se envía en la petición de certificado.

Cuando el par de claves es generado por Andes SCD

Andes SCD se reserva el derecho a la generación del par de claves de los suscriptores con quienes se haya pactado la entrega del certificado en un archivo con formato PKCS12 y mientras el suscriptor este de acuerdo con el procedimiento definido por Andes SCD para la generación de claves y entrega del certificado:

El método utilizado por Andes SCD para comprobar que el solicitante posee la clave privada correspondiente a la clave pública para la que se solicita el certificado queda comprobado de la siguiente forma:

1. El solicitante diligencia en la página web de Andes SCD el formulario de solicitud de certificado enviando los soportes digitales conforme a la PC aplicable y el soporte de pago del certificado digital.

   **Nota**: En la página WEB de Andes aparece publicado los tipos de certificado para los cuales se ofrece la entrega en archivo con formato PKCS12.

2. Las solicitudes de certificado registradas desde la página WEB de Andes SCD son estudiadas por el supervisor quien verifica la información y determina si es aprobada o rechazada.

   a. En caso de rechazar la solicitud se envía un correo electrónico al solicitante indicando los motivos por los cuales se rechazó la solicitud.

   b. En caso de aprobar la solicitud se envía un correo electrónico al solicitante donde se le informa un ENLACE con el cual puede realizar seguimiento de la solicitud de certificado.

3. Andes SCD genera el par de claves y el certificado digital mientras la solicitud haya sido aprobada por el supervisor y se procede a enviar un correo electrónico al solicitante con el enlace a la página web donde puede descargar el certificado en archivo con formato PKCS12 y el pin para la instalación.

   **Nota**: La descarga del certificado en archivo con formato PKCS12 es de un solo uso.

4. Andes SCD comprueba que la clave privada está en posesión del suscriptor al producirse la descarga del archivo PKCS12

### *3.2.2. Autenticación de la identidad*

***Autenticación de identidad de Autoridades de Registro***

Las Autoridades de Registro vinculadas al modelo de confianza Andes SCD cumplen el siguiente protocolo:

a) La Autoridad de Registro cuenta con la infraestructura tecnológica requerida para realizar las funciones delegadas por Andes SCD.

b) Existe un contrato en vigor entre Andes SCD y la Autoridad de Registro donde se concretan los aspectos de la delegación y las responsabilidades.

c) La identidad de los operadores de la Autoridad de Registro está correctamente comprobada y validada

d) Los operadores de la Autoridad de Registro han recibido la información necesaria para el correcto desempeño en sus funciones.

e) La Autoridad de Registro ha sido auditada por un organismo aprobado por Andes SCD.

f) La Autoridad de Registro asume todas las obligaciones y responsabilidades relativas al desempeño de sus funciones

g) La comunicación entre la Autoridad de Registro y Andes SCD se realiza de forma segura mediante el uso de certificados digitales.

***Autenticación de identidad de Miembros de Autoridad de Registro***

Para identificar a un operador o a un administrador de la Autoridad de Registro se exige la presentación personal ante un administrador o persona autorizada por Andes SCD y además debe aportar su cédula de ciudadanía o documento que legalmente identifique a la persona y una carta emitida por la Autoridad de Registro donde acredite la autorización del individuo para actuar como administrador u operador de la misma.

***Autenticación de identidad de Solicitantes y Suscriptores***

**Descripción del Proceso Regular**

Para emitir un certificado de entidad final se exige la presentación personal del solicitante ante una Autoridad de Registro (RA), la presentación personal es obligatoria inclusive si el solicitante es suscriptor del servicio de certificación.

Dentro del proceso de autenticación de la identidad se captura la fotografía y huella dactilar del solicitante, esta información es almacenada electrónicamente de tal forma que la siguiente vez que el suscriptor se presente a solicitar ó revocar un certificado será identificado a partir de su huella dactilar.

En todos los casos la Autoridad de Registro recibe la información presentada por el solicitante revisando si cumple con los documentos exigidos en la respectiva política de certificación y verificando si la información es original, suficiente y adecuada.

En cada política de certificación se establece la información a proporcionar por el solicitante determinándose los tipos de documentos de identidad válidos para la identificación, el procedimiento de identificación del individuo por parte de la CA ó la RA y la forma de acreditar la pertenencia a determinada empresa u organización.

**Descripción del Proceso Especial**

En los casos en que el solicitante y Andes SCD hayan acordado la emisión de certificados en archivo con formato PKCS12 no se requiere la presentación personal del solicitante ante una Autoridad de Registro, la información del solicitante es suministrada desde la página WEB junto con los soportes requeridos para el tipo de certificado. El solicitante debe suministrar a Andes SCD información original, suficiente y adecuada respecto a los requisitos exigidos en la PC aplicable.

***Autenticación de identidad de Personas Jurídicas***

Se realiza mediante la presentación de los documentos originales que acrediten la constitución como empresa y se exige la presentación personal de quien figurara como suscriptor en el certificado.

En cada política de certificación (PC) se establece la información a presentar por el solicitante para acreditar la identidad de una persona jurídica, siempre y cuando sea aplicable para el tipo de certificado

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

En el proceso de solicitud del certificado el solicitante debe suministrar diversos datos que lo identifican plenamente, toda la información solicitada es verificada por la Autoridad

de Registro y por el supervisor aún si no hace parte de la información incluida en el certificado digital.

### *3.2.4. Criterio para interoperación*

La interactividad entre Autoridades Certificadoras externas puede llevarse a cabo mediante la certificación cruzada

Antes de establecer las relaciones de interactividad con Autoridades Certificadoras externas, el Comité de Aprobación de Políticas de Andes SCD debe realizar un estudio del modelo de certificación cruzada a implementar y determinar los criterios mínimos que deben satisfacer las CA externas para el cumplimiento de ciertos requisitos técnicos y procedimentales que permitan interactuar con Andes SCD.

a) La CA externa debe proporcionar un nivel de seguridad en la gestión de los certificados a lo largo de su ciclo de vida, como mínimo igual al de Andes SCD.

b) Debe aportar el informe de auditoría de una autoridad externa de reconocido prestigio relativa a sus operaciones como medio de verificación del nivel de seguridad existente.

c) Establecer un convenio de colaboración en el que se fijen los compromisos adquiridos en materia de seguridad para los certificados incluidos en la interacción.

El Comité de Administración de Políticas de Andes SCD se reserva el derecho de aceptar la solicitud de interactividad aún si la CA externa cumple con los requisitos.

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

El proceso de identificación y autenticación para solicitar la revocación se define en la política de certificación aplicable a cada tipo de certificado.

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

## *4.1. Emisión de certificados*

### *4.1.1.* Quién puede solicitar la emisión de un certificado

La solicitud de un certificado digital puede realizarla cualquier persona mayor de edad en plena capacidad de asumir las obligaciones y responsabilidades inherentes a la posesión y uso del certificado.

En cada política de certificación se concreta quien puede solicitar un certificado y la información que se debe suministrar en la solicitud.

**Caso de excepción para el proceso especial**

La solicitud de un certificado digital puede realizarla cualquier persona mayor de edad en plena capacidad de asumir las obligaciones y responsabilidades inherentes a la posesión y uso del certificado y que esté de acuerdo con el procedimiento definido por Andes SCD para la generación de claves y entrega del certificado en archivo con formato PKCS12.

En la página WEB de Andes SCD se indican los tipos de certificados para los cuales aplica la entrega en archivo con formato PKCS12.

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

**Descripción del proceso Regular**

El siguiente procedimiento aplica para la solicitud de certificados de Clase II (Entidad final). El procedimiento para emisión de certificados de Clase I (Uso interno) está definido en la correspondiente política de certificación.

***Presentar solicitud de emisión de certificado digital***

El solicitante debe presentarse personalmente ante cualquier RA vinculada al modelo de confianza Andes SCD para solicitar el servicio de certificación digital. La Autoridad de Registro informa al solicitante las responsabilidades y obligaciones que debe cumplir al convertirse en suscriptor del servicio de certificación y si el solicitante está de acuerdo con las condiciones se procede a acreditar su identidad.

***Acreditar identidad del solicitante***

La identidad del solicitante es verificada minuciosamente por el operador RA usando los métodos tradicionales y aplicando sistemas biométricos para identificar al solicitante a partir de la captura de su huella dactilar y la comparación de está contra las demás huellas dactilares recopiladas por Andes SCD en la prestación del servicio de certificación.
Una vez acreditada su identidad, el solicitante debe suministrar la documentación necesaria siguiendo las indicaciones exigidas en la política de certificación que aplica para el tipo de certificado que desea adquirir.

De acuerdo al resultado de la acreditación de identidad y la documentación entregada, la Autoridad de Registro determina si aprueba o rechaza la solicitud.

***Recaudar el costo del certificado***

En caso de ser aprobada la petición de certificado, el solicitante debe cancelar en la RA el valor del certificado digital.

***Formalizar y enviar la solicitud a Andes SCD***

El operador RA diligencia el formato de solicitud de certificado con toda la información requerida para la emisión del mismo. Se aclara que no toda la información solicitada aparece en el certificado y que esta es conservada de manera confidencial por la Autoridad de Certificación Andes SCD.

El operador RA entrega al solicitante el dispositivo TOKEN, el cual debe ser inicializado por el solicitante ante el operador de la Autoridad de Registro a fin de generar los datos de activación del dispositivo y de acceso a la clave privada que contendrá. El solicitante crea el par de claves que conformarán su identidad digital mediante el dispositivo TOKEN.

Aunque Andes SCD no proporciona ningún servicio de generación de claves a los suscriptores, las RA pueden asesorar al solicitante en el proceso de generación de claves directamente en el dispositivo criptográfico sin entenderse este procedimiento como un servicio prestado por la RA

La clave pública generada por el solicitante se incluye en la solicitud de certificado y se genera la petición de certificado en formato PKCS10. La información del formato de solicitud se imprime y se presenta al solicitante con el fin de corroborar que los datos estén correctos, en tal caso el solicitante debe firmar de forma autógrafa la solicitud.

El operador RA firma digitalmente la petición con su certificado de operador RA y envía la solicitud a la Autoridad Certificadora Andes SCD a través de un canal seguro.

> ***Nota**: La clave privada del solicitante en ningún momento es almacenada ni copiada en elementos ajenos al solicitante.*

***Estudiar solicitud del certificado***

El supervisor recibe y revisa las solicitudes de certificados que han sido enviadas por RA activas en el modelo de confianza, verifica que el solicitante no este inhabilitado para adquirir un certificado digital y además realiza un seguimiento de su historial como suscriptor.

El supervisor de Andes SCD está en capacidad de aprobar o rechazar la emisión de certificado

***Emitir el certificado digital***

El certificado es emitido si la petición recibida cumple con las siguientes condiciones:

- No contiene errores técnicos en el formato o contenido de la misma
- La solicitud fue aprobada por el supervisor de Andes SCD
- La Autoridad de Registro Solicita descargar el certificado y el contrato de suscripción.

El proceso de emisión se realiza de forma segura protegiendo la información del solicitante y la clave pública certificada en un sistema que utiliza protección contra falsificación y que mantiene la confidencialidad de los datos intercambiados.

Una vez emitido el certificado digital la Autoridad de Registro que envió la solicitud es responsable de entregar el certificado personalmente al nuevo suscriptor.

Andes SCD hace público certificado en su página WEB para ponerlo a disposición de los usuarios ó terceros que confían.

***Entrega del certificado digital***

El operador RA explica al suscriptor las cláusulas del contrato, hace entrega del TOKEN que contiene el certificado digital y solicita al suscriptor firmar digitalmente el contrato que formaliza la suscripción al servicio de certificación.

El operador RA envía al correo electrónico del suscriptor el contrato firmado digitalmente por el supervisor de Andes SCD y por el suscriptor. En el contrato hay una clave que le permite al suscriptor revocar su certificado digital cuando lo requiera.

La firma del suscriptor en el contrato implica la aceptación del certificado. A partir de la aceptación del certificado y su publicación por parte de Andes SCD el suscriptor dispone de 7 días para revisar y determinar si el contenido del certificado corresponde a la realidad. Transcurrido este periodo si no hay comunicación por parte del suscriptor, se asume que el suscriptor acepta el contenido del certificado y asume cumplir con las obligaciones

En caso de existir alguna diferencia entre los datos suministrados por el solicitante y el contenido del certificado, debe notificarse de inmediato para proceder a revocar el certificado. Si el suscriptor informa que hay inconsistencias en su certificado dentro del periodo de aceptación, se generara un nuevo certificado sin costo alguno para el suscriptor siempre y cuando la diferencia entre los datos sea causada por un error no imputable al suscriptor.

> ***Nota**: Las inconsistencias en los certificados que sean producidos por errores de la RA deben ser asumidos por la misma.*

***Enviar contrato y soporte digital a Andes SCD***

El operador RA debe enviar a Andes SCD el contrato digital firmado, los documentos soporte de la solicitud en formato digital + la imagen escaneada del formulario de solicitud firmado de forma autógrafa por el solicitante.

La Autoridad de Registro tiene un plazo de 2 días hábiles contados a partir de la emisión del certificado para enviar a Andes SCD el contrato digital de suscripción y soportes digitales. Si esta información no es recibida el certificado es revocado.

**Descripción del Proceso Especial**

El siguiente procedimiento aplica para la solicitud de certificados de Clase II (Entidad final) donde el solicitante está de acuerdo con el procedimiento definido por Andes SCD para la generación de claves y entrega del certificado en archivo con formato PKCS12

***Presentar solicitud de emisión de certificado digital***

La solicitud de emisión de certificado digital es presentada por la entidad que ha realizado un convenio con Andes SCD para la emisión masiva de certificados y para la entrega de los certificados en archivo con formato PKCS12.

***Acreditar identidad del solicitante***

Es obligación de la entidad acreditar la identidad de cada una de las personas relacionadas en el convenio para quienes solicita la emisión de certificado.

Es responsabilidad de la entidad suministrar a Andes SCD información original, suficiente y adecuada de cada uno de los solicitantes relacionados en el convenio y entregar los soportes digitales requeridos para el tipo de certificado. La información debe ser suministrada en un archivo estructurado definido por Andes SCD que varía según el tipo de certificado a adquirir.

***Recaudar el costo del certificado***

El recaudo del costo de los certificados es definido a nivel de contrato por Andes SCD y la entidad con la cual se tiene el convenio.

De acuerdo al resultado de la acreditación de identidad y la documentación entregada, la Autoridad de Registro determina si aprueba o rechaza la solicitud.

***Estudiar solicitud del certificado***

Andes SCD carga en el sistema la información del archivo suministrado por la entidad donde se encuentran los datos de los solicitantes relacionados en el convenio y los soportes digitales requeridos para adquirir el tipo de certificado.

El supervisor verifica la información de cada uno de los solicitantes vinculados en el convenio a partir de los soportes digitales suministrados por la entidad, verifica que el solicitante no este inhabilitado para adquirir un certificado digital y además realiza un seguimiento de su historial como suscriptor.

El supervisor de Andes SCD está en capacidad de aprobar o rechazar la emisión de certificado

***Emitir el certificado digital***

Andes SCD procede a generar el par de claves si la solicitud de emisión de certificado es aprobada por el supervisor.
El certificado es emitido si la petición recibida cumple con las siguientes condiciones:

- No contiene errores técnicos en el formato o contenido de la misma
- La solicitud fue aprobada por el supervisor de Andes SCD
- El suscriptor solicita descargar el certificado y el contrato de suscripción.

El proceso de emisión se realiza de forma segura protegiendo la información del solicitante y la clave pública certificada en un sistema que utiliza protección contra falsificación y que mantiene la confidencialidad de los datos intercambiados.

***Entrega del certificado digital***

Andes SCD informa al suscriptor el link a la página web donde tiene la opción de descargar el certificado en archivo con formato PKCS12 una única vez y por seguridad el pin para la instalación de las claves y el certificado en entregado por un medio distinto para la entrega del PKCS12 (Entrega personal, Teléfono, Mensaje de texto).

El contrato de suscripción es enviado por Andes SCD al correo electrónico del suscriptor quien debe descargar el contrato, firmarlo digitalmente y enviarlo por correo electrónico a Andes SCD para formalizar la suscripción al servicio de certificación.

En el contrato de suscripción hay una clave que le permite al suscriptor revocar su certificado digital cuando lo requiera.

La firma del suscriptor en el contrato implica la aceptación del certificado. A partir de la aceptación del certificado y su publicación por parte de Andes SCD el suscriptor dispone de 7 días para revisar y determinar si el contenido del certificado corresponde a la realidad. Transcurrido este periodo si no hay comunicación por parte del suscriptor, se asume que el suscriptor acepta el contenido del certificado y asume cumplir con las obligaciones

En caso de existir alguna diferencia entre los datos suministrados por el solicitante y el contenido del certificado, debe notificarse de inmediato para proceder a revocar el certificado. Si el suscriptor informa que hay inconsistencias en su certificado dentro del periodo de aceptación, se generara un nuevo certificado para el suscriptor siempre y cuando la diferencia entre los datos sea causada por un error no imputable a la entidad que suministro la información.

El costo en que deba incurrirse por inconsistencias o errores en la emisión de un certificado que no sean atribuibles a ANDES SCD, los asumirá la entidad contratante del servicio.

> ***Nota**: Las inconsistencias en los certificados que sean producidos por errores de la entidad que suministro la información deben ser asumidas por la misma.*

***Enviar contrato y soporte digital a Andes SCD***

El suscriptor tiene un plazo de 2 días hábiles contados a partir de la emisión del certificado para enviar a Andes SCD el contrato digital de suscripción. Si esta información no es recibida el certificado es revocado.

### *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 claves y uso del certificado

##### 4.1.4.1. Por parte del suscriptor

Las responsabilidades y limitaciones de uso del par de claves y del certificado se encuentran especificadas en la correspondiente Política de Certificación.

El suscriptor solo puede utilizar la clave privada y el certificado para los usos autorizados en la PC y de acuerdo con lo establecido en los campos 'Key Usage' y 'Extended Key Usage' del certificado.

El suscriptor solo puede usar el certificado y el par de claves tras aceptar las condiciones de uso establecidas en la DPC y 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 clave 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 ó en la PC correspondiente para conocer el ámbito de aplicación del certificado.

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 publica la lista de revocación con el fin de notificar a terceros que un certificado ha sido revocado, en el momento en que se solicite la verificación del mismo.

#### *4.4.1. Circunstancias de revocación*

Un certificado digital emitido por la Autoridad Certificadora Andes SCD es revocado automáticamente por el sistema cuando su periodo de vigencia ha concluido y puede ser revocado previamente al término de validez mediante intervención humana en los siguientes eventos:

*Eventos que afectan la información propia del certificado*

a) Cuando hay posterior modificación de los antecedentes del suscriptor. (Ej. El suscriptor cambio de nombre ó el suscriptor ya no es el representante legal de la empresa).

b) Cuando se presenta la liquidación de una persona jurídica que se encuentra vinculada en un certificado.

c) Cuando hay falsificación de los antecedentes del suscriptor. (Ej. Después de emitido el certificado se descubre que se presentaron documentos falsos)

d) Cuando se comprueba que alguno de los datos del certificado es incorrecto o que no se cumple algún requisito. (Ej. Se detecta que la RA no exigió un documento indispensable para la emisión del certificado ó hay que revocar el certificado porque un dato esta errado).

*Eventos que afectan la seguridad del modelo de confianza*

a) Cuando el suscriptor, RA o Andes SCD ha quebrantado una obligación, declaración o responsabilidad establecida en el contrato de suscripción o da uso irregular del certificado.

b) Cuando el suscriptor informa que la clave privada del certificado ha sido comprometida o ha perdido su confidencialidad.

c) Cuando se ha cometido una infracción por parte de la RA o Andes SCD en cuanto a los requisitos y procedimientos establecidos para la gestión de certificados.

d) Cuando el certificado emitido no cumple los procedimientos requeridos por la Declaración de Prácticas de Certificación (DPC) o cuando un requisito no fue satisfecho. (Ej. Andes SCD no ha recibido el contrato del suscriptor y se ha vencido el plazo estipulado en DPC).

*Eventos que afectan directamente al suscriptor*

a) Cuando el suscriptor ha fallecido.

b) Cuando el suscriptor ha sido secuestrado.

c) Pérdida de su capacidad o inhabilitación del suscriptor.

*Otros eventos:*

a) Cuando es la voluntad del suscriptor revocar su certificado.

b) Cuando sea autorizado revocar el certificado por orden judicial o administrativa.

c) Cuando se informa que el suscriptor ha realizado fraudes con su certificado digital.

### *4.4.2. Quién puede solicitar la revocación certificados*

Andes SCD o cualquiera de las autoridades que la componen puede solicitar la revocación de un certificado si tuviera conocimiento o sospecha del compromiso de la clave privada del suscriptor o cualquier otro hecho determinante que requiera proceder a revocar el certificado.

El suscriptor de certificado o sus responsables, en el caso de certificados de componente, también puede solicitar la revocación de los certificados de acuerdo a las condiciones estipuladas en la sección 4.4.4 de la presente DPC.

En las distintas Políticas de Certificación se define de forma más rigurosa quienes pueden solicitar la revocación de certificados.

### *4.4.3. Medios para revocar certificados*

Los certificados digitales de clase II (Entidad Final) pueden ser revocados a través de los siguientes medios:

1. **INTERNET**: El servicio web ANDES SCD ofrece una sección donde el suscriptor tiene la posibilidad de revocar su certificado digital a partir del número de cedula + Correo electrónico + el código de revocación suministrado en el momento en que se le entrego el certificado.
   *Este servicio está disponible 24 horas / 7 días a la semana.*
   *Para realizar la revocación por internet ingrese a la página http://www.andesscd.com.co y haga clic en la sección Revocación de Certificados.*

2. **TELEFONICAMENTE**: El suscriptor puede solicitar la revocación de su certificado digital comunicándose telefónicamente con un operador de servicio al cliente Andes SCD durante el horario de atención al público.
   *Este servicio está disponible de lunes a viernes en el horario de 8:00 am a 12:00 m y 2:00 pm a 6:00 pm.*

3. **PERSONALMENTE**: El suscriptor puede solicitar la revocación de su certificado digital presentándose personalmente durante el horario de atención al público en cualquier Autoridad de Registro vinculada al modelo de confianza ANDES, allí debe identificarse, informar las causas de revocación y se captura su información biométrica (huella y fotografía). A esta forma se recurre en última instancia cuando el suscriptor no tiene el código de revocación.
   *Este servicio está disponible de lunes a viernes en el horario de 8:00 am a 12:00 m y 2:00 pm a 6:00 pm.*

Los mecanismos anteriores para gestionar las solicitudes de revocación son inmediatos mientras la petición la realice el propio suscriptor personalmente o con su código de revocación. Si la petición de revocación corresponde a un caso especial o es realizada por un tercero, debe ser comunicada al soporte de Andes SCD para que sea tramitada y aprobada por el supervisor según el procedimiento definido.

Los medios para revocar certificados digitales de clase I (uso interno) se especifican en la Política de Certificación correspondiente.

### *4.4.4.* Procedimiento *para* revocar certificados

Los siguientes procedimientos para revocar un certificado aplican únicamente para certificados de clase II ó de Entidad Final. Los procedimientos para revocar certificados de clase I ó de uso interno se definen en la respectiva Política de Certificación.

***Procedimiento de revocación presencial***

- El suscriptor debe presentarse personalmente ante cualquier Autoridad de Registro y manifestar por escrito su deseo de revocar el certificado digital. (Para el caso de los certificados donde el suscriptor es una empresa, la revocación presencial debe solicitarla el representante legal).
- El operador RA procede a gestionar la revocación del certificado a partir del aplicativo informático suministrado por Andes SCD, donde se identifica al suscriptor a partir de su huella dactilar y se ingresa el motivo de la revocación.
- El operador RA envía la petición de revocación a Andes SCD a través de una comunicación segura
- La petición de revocación es recibida en Andes SCD y el certificado es revocado de inmediato
- El sistema automáticamente envía un correo electrónico al suscriptor informando que el certificado ha sido revocado
- El certificado es publicado en la próxima CRL de CA ANDES SCD S.A. Clase II.

***Procedimiento de revocación en línea***

- El suscriptor puede revocar en cualquier momento su certificado ingresando a la sección revocación de la página WEB de Andes SCD, suministra los datos de su certificado digital, el respectivo código de revocación, ingresa el motivo de la revocación y acepta explícitamente la tramitación de la solicitud y las consecuencias de esta.
- La petición de revocación es atendida de inmediato
- El sistema automáticamente envía un correo electrónico al suscriptor confirmando que el certificado ha sido revocado, la hora de revocación y la causa de la misma.
- El certificado es publicado en la próxima CRL de CA ANDES SCD S.A. Clase II.

***Procedimiento de revocación telefónico***

El suscriptor puede solicitar la revocación de su certificado digital realizando una llamada telefónica al número que se encuentra en la página http://www.andesscd.com.co en la sección revocaciones, dicho número se encuentra habilitado de forma específica para atender solicitudes de revocación de certificados.

El operador del centro de servicios de Andes SCD que atiende la llamada telefónica solicita al suscriptor información del certificado a revocar, el motivo de la revocación y el código de revocación. Si el código de revocación suministrado por el suscriptor es correcto se revoca el certificado y se envía un correo electrónico al suscriptor informándole la revocación y el motivo.

***Nota**:* El suscriptor debe abstenerse de comunicar a terceros su código de revocación si no está seguro de revocar su certificado. La responsabilidad de custodia del código de revocación es exclusiva del propio suscriptor

***Nota**:* El supervisor de Andes SCD puede revocar certificados cuando se de alguno de los eventos especificados en la sección 4.4.1.

### *4.4.5.* Tiempo para procesar la solicitud de revocación

La solicitud de revocación presentada por el suscriptor es ejecutada de inmediato siempre y cuando se realice presencialmente por el suscriptor ó se realice vía web ó telefónicamente suministrando el código de revocación.

El servicio de gestión de revocaciones está disponible vía web los 7 días de la semana y las 24 horas del día. En caso de un fallo en el sistema ó cualquier otro factor que no esté bajo control de Andes SCD, se realizarán los mayores esfuerzos para asegurar que el servicio de revocación no se encuentre suspendido durante más tiempo que el periodo máximo de 24 horas.

### *4.4.6.* Requisitos de verificación de las revocaciones por los usuarios que confían

La verificación de las revocaciones es obligatoria para el uso por parte de terceros, esta verificación se realiza mediante la consulta directa de la CRL de CA ANDES SCD S.A. Clase II o mediante consulta OCSP.

Es de carácter obligatorio la comprobación de las CRL de ROOT CA ANDES SCD S.A y CRL de CA ANDES SCD S.A. Clase II por parte de los usuarios para ver el estado de los certificados en los cuales van a confiar, debe descargarse la última CRL de la página web de Andes SCD y comprobar la validez de la CRL previamente a cada uso.

### *4.4.7.* Publicación de certificados revocados

La información relativa a la revocación de un certificado se difunde mediante la publicación periódica de la CRL de ROOT CA ANDES SCD S.A y la CRL de CA ANDES SCD S.A. Clase II.

Las listas de revocación de certificados CRL de ROOT CA ANDES SCD S.A se genera y se publica cada 30 días y la CRL de CA ANDES SCD S.A. Clase II se genera y se publica cada 48 horas y permanecen publicadas por un periodo de tiempo. El usuario puede encontrar a la vez varias CRL de CA ANDES SCD S.A. Clase II, por esta razón se recomienda revisar la fecha de la CRL para comprobar que es la emitida recientemente.

Las CRL de CA ANDES SCD S.A. Clase I se generan cada 15 días y no son publicadas porque son solo de uso interno de Andes SCD.

### *4.5. Servicios de información del estado de certificado*

#### *4.5.1. Características operacionales*

Andes SCD dispone como mínimo de 2 servicios que proporcionan información sobre el estado de los certificados emitidos:

- Publicación de CRL: El acceso a las CRL de ROOT CA ANDES SCD S.A y CRL de CA ANDES SCD S.A. Clase II se puede hacer vía HTTP disponible para todos los usuarios ó puede hacerse vía LDAP disponible solo para usuarios de la red interna.
- Servicio de validación en línea OCSP: Mediante el uso de este protocolo que cumple con la RFC 2560 se determina el estado actual de cualquier certificado sin requerir las CRL's.

#### *4.5.2. Disponibilidad del servicio*

Andes SCD presta un servicio on-line de comprobación de revocaciones que está disponible las 24 horas del día de los 7 días de la semana y además realiza todos los esfuerzos necesarios para que el servicio nunca se encuentre suspendido de forma continua por más de 24 horas.

#### *4.5.3. Fin de suscripción*

El contrato de suscripción al servicio de certificación digital finaliza cuando expira el periodo de vigencia del certificado ó se revoca el certificado por alguna de las causas descritas en la sección 4.4.1 Circunstancias de revocación.

### *4.6. Vigencia de los certificados*

En las políticas de certificación se especifica el periodo de vigencia del respectivo certificado y adicionalmente el periodo de vigencia del par de claves.

## 5. Controles de seguridad

Los aspectos referentes a medidas técnicas y procedimentales que garantizan la seguridad de los servicios e información de Andes SCD se encuentran especificados en detalle en las Políticas de Seguridad de la Información (PSI). Estas políticas contemplan las responsabilidades de las distintas áreas del modelo de confianza pertenecientes en Andes SCD, notificando a cada persona los procedimientos y controles que le incumben dentro de la organización.

La Declaración de Políticas de Seguridad de Andes SCD está compuesta por las siguientes secciones o documentos de uso interno.

| SECCION | OID DOCUMENTO |
|---|---|
| Políticas administración de Seguridad de la Información | 1.3.6.1.4.1.31304.100.2.2 |
| Políticas Clasificación y Administración de Activos | 1.3.6.1.4.1.31304.100.2.3 |
| Políticas Seguridad de los Recursos Humanos | 1.3.6.1.4.1.31304.100.2.4 |
| Políticas Seguridad Física y Ambiental | 1.3.6.1.4.1.31304.100.2.5 |
| Políticas Gestión de Comunicaciones y Operaciones | 1.3.6.1.4.1.31304.100.2.6 |
| Políticas Control de Acceso al Sistema | 1.3.6.1.4.1.31304.100.2.7 |
| Políticas Prevención de Virus Informáticos | 1.3.6.1.4.1.31304.100.2.8 |
| Políticas Desarrollo y Mantenimiento de Sistemas | 1.3.6.1.4.1.31304.100.2.9 |
| Políticas para la administración de backups y ejecución del plan de contingencias | 1.3.6.1.4.1.31304.100.2.10 |
| Políticas Monitoreo y cumplimiento | 1.3.6.1.4.1.31304.100.2.11 |
| Gestión de incidentes de la seguridad de la información | 1.3.6.1.4.1.31304.100.2.12 |

En el presente documento se mencionarán las medidas de seguridad más relevantes

### 5.1. *Controles de seguridad física*

#### *5.1.1. Ubicación y seguridad ambiental*

Los sistemas y equipamientos empleados por Andes SCD para ofrecer el servicio de certificación residen en el Data Center Telmex, un centro de datos de clase mundial ubicado en la Sabana de Bogotá en un lugar estratégico de gran desarrollo empresarial.

El Data Center Telmex 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 Telmex 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.

Perímetro de seguridad física

El perímetro físico de seguridad de Andes SCD comprende el área donde se generan los certificados digitales y donde se almacena el conjunto de servidores requeridos para prestar el servicio de certificación digital, este perímetro de seguridad reside en el Data Center Telmex y está protegido mediante los siguientes mecanismos:

a. Las instalaciones cuentan con 3 anillos de seguridad permanente: Acceso al centro empresarial, acceso a las instalaciones de Telmex y acceso al Centro de datos.
b. El centro de datos cuenta con un único punto de acceso protegido por personal de seguridad las 7x24x365.
c. Sistemas de acceso mediante autorización en listas de acceso y verificación del documento de identidad.
d. Acceso al edificio y zonas seguras del personal de administración mediante dispositivos de autenticación que incluye biometría y tarjetas de proximidad.
e. Acceso de visitantes con cita previa y con acompañamiento si se dirige a zonas seguras.
f. Sistemas de seguridad física certificada con circuito cerrado de televisión y sistemas de cámaras de seguridad al interior y exterior del centro de datos.
g. Monitoreo de cámaras desde la cabina de control
h. Zonas de carga y descarga aisladas del centro de datos, donde se controla todo lo que ingresa y sale de las instalaciones.

Protección contra amenazas externas y ambientales

El lugar donde se ubican los servidores y dispositivos críticos para la operación de Andes SCD cuenta con protecciones físicas de tal forma que se minimice el riesgo a Robo, Incendios, Inundación y condiciones ambientales que puedan afectar la operación de las instalaciones de procesamiento de información

[1] "The Uptime Institute" ha definido un sistema de calificación y certificación de los centros de datos basado en 4 niveles (TIERS), conforme más alto sea el nivel de "Tier" mayor es la confiabilidad del centro de datos. Tier IV es el diseño Tolerante a Fallas, proporciona la seguridad de no presentar interrupciones brindando una disponibilidad del 99.995%.

a. Sistemas de aire acondicionado redundantes diseñados para permitir que los equipos obtengan siempre condiciones ambientales optimas en cuanto a temperatura y humedad para su buen desempeño.
b. Sistemas Antiincedios Inergen (Agente limpio acorde con el protocolo de Kiotol), que consiste en un sistema de extinción vía gas que no crea neblina al ser expulsado para no disminuir la visibilidad de las salidas de emergencia y no dejar residuos que afecten los equipos de cómputo.
c. Sistemas de ventilación y enfriamiento certificados
d. Alimentación redundante de energía de 34,5 KV proveniente de subestaciones diferentes y acometidas independientes.
e. La infraestructura asegura la continuidad de sus operaciones en caso de fallas en el suministro, mediante la utilización de sistemas de alimentación ininterrumpida de alta capacidad que proveen energía a las instalaciones críticas.
f. Sistema perimetral de detección de intrusos que incluye monitoreo permanente al mismo.
g. Control de entradas y salidas de información, aplicaciones o equipamientos llevando un inventario del material existente y de las entradas y salidas que se han producido.

### *5.1.2.Gestión del sistema de acceso*

El sistema de control de acceso físico es garantizado por los servicios de seguridad que brinda Data Center Telmex mediante los mecanismos descritos en la sección anterior denominada “Perímetro de seguridad física” y “Protección contra amenazas externas y ambientales”.

El sistema de control de acceso lógico a las aplicaciones críticas de Andes SCD se realiza aplicando los siguientes mecanismos:

a. Autenticación ante aplicaciones críticas mediante Certificados Digitales de uso interno (Clase I) combinado con nombre de usuario y contraseña.
b. Controles basados en cortafuegos de alta disponibilidad
c. Lista actualizada de usuarios autorizados a ingresar al sistema especificando el nivel de acceso y privilegios que tiene cada usuario.
d. Monitorización para detectar accesos no autorizados de forma inmediata

### *5.1.3.Seguridad de los servidores*

Cada servidor de Andes SCD cuenta con un servidor de respaldo que se mantiene sincronizado respecto al servidor principal y que entra en funcionamiento para reemplazar al servidor principal cuando este falle.

En los servidores se dispone de un procedimiento de detección y registro de los intentos de acceso no autorizados de tal forma que se pueda conocer la procedencia, la fecha y hora, las áreas que se han intentado acceder y las manipulaciones realizadas.

Los servidores expuestos a Internet tienen configurado un cortafuego a nivel de aplicación para proteger la red privada de intrusos y a la vez permitir el acceso autorizado desde y hacia el exterior.

El servidor CA que realiza la gestión de certificados no está expuesto a internet y tiene configurado un cortafuegos que rechaza todas las entradas, el servidor CA rastrea periódicamente las solicitudes de certificados encontradas en el servidor RA, las procesa y genera los respectivos certificados digitales.

Realización de monitoreo de los sistemas operativos de servidores, control de acceso, ciclo de vida de los certificados y aspectos que indiquen el uso no autorizado del sistema y que puedan reducir al mínimo el riesgo de interrupciones en los procesos del negocio.

## *5.2. Controles procedimentales*

Los controles procedimentales se encargan de garantizar una distribución de las funciones realizando un control en diferentes jerarquías del modelo de confianza a fin de limitar el fraude interno y evitar que una sola persona se encargue de principio a fin de todo el proceso. Para cada área se definen los siguientes aspectos:

- Habilidades requeridas
- Formación y concientización
- Deberes y responsabilidades del cargo o Manual de funciones
- Medidas de seguridad a las que está sometido
- Niveles de acceso a información y sistemas
- Monitorización y auditoria de la función

Los controles procedimentales se consideran información confidencial de Andes SCD y se describen en detalle en los manuales de funciones y en la Declaración de Políticas de Seguridad PSI.

A través de auditorías internas realizadas periódicamente se procura que toda la gestión de procedimientos operacionales y la administración de los procedimientos se lleva a cabo de forma segura.

### *5.2.1.* Roles de confianza

El modelo de confianza cuenta con una jerarquía que garantiza la segregación de funciones, reparte el control y evita el fraude interno, evitando que una sola persona controle de principio a fin todas las funciones de certificación.

a. *Operador RA*: Es el responsable de recibir las peticiones de emisión y revocación de certificados, verificar el pago del certificado por parte del solicitante, comprobar la identidad, aprobar o rechazar la solicitud y enviar a Andes SCD la documentación suministrada por el solicitante.

b. *Administrador RA*: Es el responsable de gestionar la seguridad en la RA, realizar la instalación y actualización de las herramientas tecnológicas proporcionadas por Andes SCD y dar soporte a los operadores RA en el uso de los aplicativos utilizados para el servicio de certificación digital.

c. Representante RA: Es responsable de verificar y garantizar que en la RA se da cumplimiento a las Políticas y Prácticas de Certificación.

d. *Supervisor Andes SCD*: Es el responsable de la seguridad procedimental, inspecciona las solicitudes de emisión y revocación de certificados y mantiene la responsabilidad de verificar la calidad y cumplimiento de las Políticas y Prácticas de Certificación.

e. *Administradores de HSM*: Es el responsable de administrar el dispositivo criptográfico que crea y almacena las claves privadas de la CA raíz, CA emisora de certificados clase I ó de uso interno y la CA emisora de certificados de clase II ó de entidad final.

Los administradores del HSM se encargan de realizar las siguientes operaciones:

- Recuperación de la funcionalidad del HSM en caso de fallo.
- Recuperación de las claves en caso de borrado accidental.
- Ampliación del número de HSM integrados a la infraestructura
- Administración de cuentas de usuarios del HSM (Administradores ú operadores).

f. *Operadores del HSM*: Los operadores del HSM son responsables de las siguientes actividades

- Ceremonia de generación de claves para las CA's
- Activación de claves privadas de CA's para su utilización.

g. *Administrador del sistema*: Es responsable del funcionamiento de los componentes de la PKI, del hardware y del software. Está autorizado para realizar cambios en la configuración del sistema y supervisar el correcto funcionamiento del servicio de certificación.

- Gestionar los controles de acceso de los usuarios a los equipos, aplicativos y componentes de la infraestructura tecnológica de Andes SCD
- Realizar las tareas relacionadas con la administración de la CA, como gestionar el ciclo de vida de los certificados, crear nuevos perfiles de certificados y mantener los controles de seguridad convenidos.
- Realizar Instalación y configuración de sistemas operativos, productos software en los servidores de Andes SCD
- Realizar mantenimiento a los servidores y sistemas y se encargara de cubrir los requerimientos de seguridad establecidos para la operación, administración y comunicación de los sistemas y recursos tecnológicos de Andes SCD.
- Monitorizar y verificar el correcto servicio de CRL's, OCSP.
- Establecer y documentar procesos de monitorización de sistemas, aplicaciones y servicios
- Supervisar la ejecución de políticas de protección de datos, sistemas de respaldo y copias de seguridad.
- Supervisar que el directorio de certificados se mantenga actualizado.
- Supervisar el correcto funcionamiento de los servidores y componentes del sistema de certificación.
- Supervisar el correcto funcionamiento del servicio de certificación y administración del ciclo de vida de los certificados.

h. *Auditor interno*: Es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, informando sobre el cumplimiento de las especificaciones y medidas de seguridad establecidas en la PSI y por las normas, procedimientos y prácticas que de ella surjan.

i. *Comité de Políticas y Seguridad:* El Comité de Políticas y Seguridad tiene a cargo la administración de las DPC, PC, PSI y plan de continuidad del Negocio y el seguimiento en cada área de las actividades relativas a la seguridad de la información (análisis de riesgo, monitoreo de incidentes, investigación, implementación de controles, administración de la continuidad, etc.). El Comité de Políticas y Seguridad tiene la facultad de proponer la asignación de funciones.

   Funciones del Comité de Políticas y Seguridad:
   - Revisar por lo menos una vez al año las Políticas de Seguridad de la Información (PSI) y si hay modificaciones proponerlas ante la dirección para su aprobación.
   - Implementar metodologías para comunicar los riesgos e incidentes de seguridad presentados en los diferentes componentes del modelo de confianza (Andes SCD, RA's, entidades finales).
   - Establecer y apoyar los planes de capacitación que permitan actualizar a los empleados en aspectos de seguridad.
   - Definir las directrices básicas de seguridad para los requerimientos en la adquisición de hardware y software. (Ej. Dispositivos criptográficos Token)
   - Asignar responsabilidades a cada área para incrementar la seguridad de la información y vigilar que estas sean cumplidas.
   - Vigilar que las excepciones de la política de seguridad estén autorizadas únicamente por la dirección de Andes SCD y que se deje constancia de los riesgos que en forma consciente se están asumiendo y el periodo de vigencia de la excepción.
   - Investigar las violaciones de seguridad y presentar informes al área directiva.
   - Realizar seguimiento a las acciones disciplinarias y legales asociadas con las violaciones de seguridad investigadas.
   - Preparar y mantener el plan de contingencia y recuperación de desastres ante alguna emergencia.
   - Liderar las pruebas periódicas sobre el plan de contingencia y recuperación de desastres

j. *Coordinador de seguridad:* Debe velar por el diseño, implantación y cumplimiento de los procedimientos y prácticas de seguridad en las instalaciones de producción, desarrollo y operación de Andes SCD y los procedimientos y prácticas de seguridad para proteger la información residente en el perímetro físico de seguridad de Andes SCD.
   - Desarrollar métodos y técnicas para monitorear efectivamente los sistemas de seguridad de la información y reportar periódicamente su funcionamiento a la alta dirección.

- Hacer un seguimiento y documentación de los riesgos e incidentes que afectan los recursos y la información y crear controles específicos.
- Cerciorarse de que los sistemas están correctamente documentados.
- Resuelve las incidencias relacionadas con vulnerabilidades a la seguridad
- Mantener actualizadas las Políticas de Seguridad de acuerdo a las disposiciones vigentes.

k. *Asesor del Área Legal:* El asesor legal tiene como responsabilidad verificar el cumplimiento de las Políticas de Seguridad (PSI) en la gestión de todos los contratos, acuerdos u otra documentación de Andes SCD con sus empleados y con terceros. Asimismo, asesora en materia legal a Andes SCD, en lo que se refiere a la seguridad de la información. Redacta el compromiso de confidencialidad en los contratos con Empleados, Autoridades de Registro y Suscriptores y asesora sobre sanciones aplicadas por el incumplimiento de la Política de Seguridad.

l. *Operadores del centro de servicios Andes SCD*: Son las personas encargadas de atender las inquietudes de usuarios, solicitantes y suscriptores
- Atención al cliente vía chat, email o telefónicamente
- Brindan información de carácter no confidencial
- Realizan el registro de incidencias y gestión de soportes
- Revocan certificados a solicitud del suscriptor si este suministra el código de revocación.

### *5.2.2.* Número de personas requeridas por tarea

Se garantiza que se dispone por lo menos 2 personas para realizar las tareas que requieren control multipersona como:
- La generación de claves de las CA's
- La recuperación y respaldo de la clave privada de las CA's
- La emisión de certificados de las CA's
- Activación de la clave privada de las CA's

### *5.2.3.* Identificación y autenticación de cada rol

El acceso a recursos se realiza dependiendo del activo mediante login/password y certificados digitales de clase I ó de uso interno.
Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.
Las personas asignadas para cada rol son identificadas por el auditor interno quien verifica que cada persona realiza las operaciones para las que está asignado.

### *5.2.4.* Roles que requieren separación de deberes

La asignación del personal garantiza que se cumplen las siguientes condiciones
- Un administrador de HSM no puede ser Auditor interno
- Un administrador de sistemas no puede ser coordinador de seguridad ni Auditor interno
- Un coordinador de seguridad no puede ser administrador de sistemas, ni auditor interno.
- Un auditor interno no puede ser administrador de sistemas ni coordinador de seguridad.

#### *5.2.5. Relación entre Andes SCD y las Autoridades de Registro*

En la relación del modelo de confianza se tienen en cuenta los siguientes aspectos:

- El contrato estipulado entre Andes SCD y RA detalla los aspectos de delegación y responsabilidades del personal y debe cumplirse a cabalidad por las partes.
- Los operadores de la RA deben ser capacitados y evaluados periódicamente para asegurar el correcto desempeño de sus funciones.
- La RA asume todas las obligaciones y responsabilidades relativas al desempeño de sus funciones
- La identidad de la RA y de los operadores vinculados a la RA es comprobada y validada por personal autorizado de Andes SCD.
- La comunicación entre Andes SCD y RA se realiza de forma segura mediante el uso de certificados digitales, de esta forma a cada uno de los operadores RA se le expide un certificado digital de uso interno que lo identifica y que es fundamental para la realización de sus actividades, el uso es personal e intransferible, siendo el operador RA el único responsable de las consecuencias que puedan derivarse por el mal uso, divulgación o pérdida de los mismos.
- En el contrato entre Andes SCD y la RA se incluyen cláusulas de indemnización en caso de infracción de sus obligaciones legales o contractuales.

### *5.3. Controles de seguridad personal*

#### *5.3.1. Calificaciones, experiencia y requisitos*

Todo el personal de Andes SCD y cada RA es instruido para realizar las actividades asignadas, se les realiza un seguimiento y evaluación para determinar si están calificado para realizar las funciones encomendadas. Los programas de capacitación involucran los siguientes puntos

a. Conceptos básicos de PKI
b. Responsabilidades del cargo
c. Uso y operación del software y hardware utilizado
d. Copias de seguridad y medidas de seguridad a tener en cuenta cuando se abandona momentáneamente el equipo de trabajo.
e. Políticas y procesamientos de seguridad y operación de Andes SCD
f. Elaboración de reportes para notificar los incidentes o anomalías que pudieran afectar la seguridad de los datos o accesos a plataformas informáticas. Por incidencia se entienden las siguientes circunstancias
    - Cambios no autorizados en la información
    - Intentos de acceso o accesos a información confidencial por personas no autorizadas
    - Inconvenientes en la realización de copias de seguridad y/o sistemas de respaldo
    - Errores en el aplicativo informático
    - Problemas de conexión VPN
    - Reportar incidentes que afecten la seguridad de la infraestructura al responsable de seguridad
    - Cualquier otro tipo de problema que pueda afecte la calidad del servicio.
    - Procedimientos de recuperación ante desastres para garantizar la continuidad del servicio.

### *5.3.2. Procedimientos de comprobación de antecedentes*

Andes SCD realiza las investigaciones pertinentes antes de la contratación de cualquier persona, nunca se asignan tareas confiables en las operaciones de la Autoridad Certificadora a personal con antigüedad inferior a 6 meses. Las Autoridades de Registro pueden establecer criterios siendo responsable por el desempeño de las personas que autoricen.

### *5.3.3. Requisitos de entrenamiento*

El personal de Andes SCD y RA debe conocer la documentación sobre Políticas de Seguridad y aplicarlas para realizar de forma competente sus funciones.

El personal debe formarse en los siguientes aspectos:

- Declaración de Prácticas de Certificación.
- Concienciación sobre la seguridad física, lógica y técnica
- Operación del software y hardware para cada papel específico.
- Procedimientos de seguridad para cada rol específico.
- Procedimientos de operación y administración para cada rol específico.
- Procedimientos para la recuperación de la operación de la PKI en caso de desastres.

### *5.3.4. Frecuencia de adiestramiento y requisitos*

El personal de Andes SCD y de cada RA debe estar actualizado respecto a procedimientos y las últimas versiones de las Políticas y Prácticas de Certificación a fin de asegurar la correcta realización de sus funciones.

### *5.3.5. Frecuencia de rotación de trabajo*

La rotación de trabajo entre el personal de Andes SCD está contemplada para garantizar la continuidad de la prestación del servicio en caso de ausencia de alguno de los empleados. La rotación de trabajo entre los roles de confianza se realiza únicamente con personal calificado para realizar las funciones del cargo.

### *5.3.6. Sanciones por acciones desautorizadas*

Si algún miembro de la RA o Andes SCD comete alguna infracción o hecho delictivo que afecte el modelo de confianza se procede a aplicar un proceso disciplinario y según la gravedad del asunto será retirado de sus funciones por Andes SCD.

La desobediencia de alguna de las siguientes prohibiciones genera un proceso disciplinario:

- Prohibición de compartir claves, contraseñas o datos para acceder a sistemas y aplicaciones de Andes SCD incluso dentro de la misma organización. El usuario es el único responsable de lo que se haga con su clave por lo tanto debe protegerla.
- Prohibición de cualquier ataque contra elementos o sistemas de seguridad (Ej. Borrado de programas, archivos e informaciones vitales para Andes SCD)
- Prohibición de instalación de software que no cuente con licencia de uso y desinstalación de software requerido para realizar sus actividades.
- Prohibición de uso de activos de la infraestructura para fines que no le han sido encomendados.
- Prohibición de actividades ilícitas ó ilegales que atenten contra la moral y derechos de terceros

- Prohibición de disponer de información sensible o confidencial para usos ajenos a su actividad dentro del modelo de confianza. (Ej. Extraer clandestinamente información confidencial de las instalaciones de Andes SCD o de RA y revelarla ante terceros)
- Compromiso de confidencialidad respecto a las informaciones que accede en el desempeño de sus funciones incluso después de terminar la vinculación con Andes SCD.

#### *5.3.7. Requisitos de la contratación de personal*

En el momento de realizar la contratación del personal de Andes SCD deben darse a conocer las cláusulas de confidencialidad y requerimientos operacionales, la RA debe realizar este mismo procedimiento a su interior con los operadores RA y administrador RA.

#### *5.3.8. Documentación suministrada al personal*

Andes SCD pone a disposición de todo el personal la documentación donde se detallan las funciones encomendadas, las Políticas y Prácticas de Certificación, las Políticas de Seguridad aplicables al rol y manuales de uso del sistema de certificación digital con el fin de que pueda desarrollar de forma competente sus funciones.

### *5.4. Controles de Auditoría*

#### *5.4.1.* Tipos de eventos auditados

Los eventos auditables se clasifican en categorías según la importancia del evento en:

- *Informativo*: Los eventos que contienen información de operaciones realizadas con éxito.
- *Advertencia*: Indica que se ha detectado un hecho inusual durante la operación.
- *Error*: indica el fallo de una operación debido a un error predecible.
- *Error fatal*: indica que ha ocurrido una circunstancia excepcional durante una operación.

Cada evento auditado detalla la fecha y hora en que ocurrió el evento, el usuario que genero el evento, el tipo de evento, la acción que generó el evento y observaciones cuando aplica.

Se registra la auditoría sobre los siguientes eventos referentes al sistema de seguridad de Andes SCD

a. Encendido y apagado de los servidores
b. Intentos exitosos y fallidos de cambiar parámetros de seguridad del sistema operativo de los servidores.
c. Inicio y fin de sesión en los servidores
d. Intentos de accesos no autorizados al sistema a través de la red al sistema de certificación.
e. Registros realizados desde las aplicaciones de la Autoridad de Certificación
f. Cambio de contraseña
g. Cambios en la creación de perfiles de certificados
h. Intentos exitosos y fallidos de generar, firmar, emitir o revocar certificados
i. Intentos exitosos y fallidos de generar, firmar o emitir una CRL
j. Intentos exitosos y fallidos de verificación de huella dactilar.

k. Intentos exitosos y fallidos de alterar la información de suscriptores
l. Administración del ciclo de vida de la clave de las CA's de Andes SCD
   - Resguardo y almacenamiento de la clave de Andes SCD
   - Recuperación de la clave de Andes SCD
   - Destrucción de la clave en caso de compromiso o vulnerabilidad

m. Administración y ciclo de vida de los certificados digitales
   - Actualización de información relacionada con el suscriptor o información substancial del certificado.
   - Recepción de solicitudes de emisión y revocación de certificados
   - Emisión de certificados
   - Descarga de los certificados por parte de la Autoridad de Registro.
   - Envío de contrato de suscripción y soportes por parte de la Autoridad de Registro.

### *5.4.2.* Frecuencia de procesamiento de los registros de auditoría

Los registros de auditoría se revisan por lo menos 1 vez por semana en busca de actividades sospechosas

### *5.4.3.* Periodo de resguardo de los registros de auditoría

Las copias de seguridad de los registros de auditoría se almacenaran por al menos 5 años.

### *5.4.4. Protección de los registros de auditoría*

Se almacenan registros de forma automática que contienen información de seguimiento a eventos relacionados con las actividades del servicio ofrecido por Andes SCD.

### *5.4.5. Procedimientos de respaldo de los registros de auditoría*

Se dispone de un procedimiento de respaldo de los registros de auditoría que consisten en recopilar en una base de datos centralizada los registros de auditoria de los servidores que ofrece el servicio de certificación. La recopilación de los registros de auditoria se realiza en tiempo real.

### *5.4.6. Sistemas de recolección de información de auditoría*

La recopilación de la información de auditoría de Andes SCD se realiza mediante procesos automáticos y manuales ejecutados desde las aplicaciones PKI. Los registros de las auditorías de los sistemas de la Autoridad Certificadora y las Autoridades de Registro se almacenan en los sistemas internos de Andes SCD.

La auditoría de los eventos sensibles que tienen que ver con el ciclo de vida de los certificados se almacena a nivel de base de datos.

Los sistemas de recolección de información tienen las siguientes características:

a. Permiten verificar la integridad de la base de datos, es decir, detecta una posible manipulación fraudulenta de los datos.
b. Asegura el no repudio por parte de los autores de las operaciones realizadas sobre los datos.
c. Almacena versiones sucesivas de auditoría conservando permanentemente un histórico de las operaciones realizadas.

#### *5.4.7. Sistemas de revisión de eventos*

Se dispone de 3 herramientas para consultar los eventos auditados a partir de múltiples parámetros de búsqueda que facilitan al auditor la detección de eventos de tipo informativo, advertencias ó errores.

#### *5.4.8. Análisis de vulnerabilidades*

Andes SCD realiza periódicamente una revisión de discrepancias en la información de los registros de auditoría y actividades sospechosas, de acuerdo al procedimiento interno establecido al efecto en las políticas de seguridad.

### *5.5. Controles de almacenamiento y archivo de la información*

#### *5.5.1. Tipo de información a resguardar*

Se conservan los eventos que se registren durante el ciclo de vida de cada certificado digital emitido por Andes SCD.

- Todos los eventos de la auditoría
- Todos los datos relativos a los certificados (datos personales del suscriptor, expediente digitalizado de solicitud, contrato de suscripción, información del certificado).
- Solicitudes de emisión y revocación de certificados.
- Todos los certificados emitidos ó publicados
- Todas las CRL emitidas y registros del estado de los certificados generados
- Versiones de documentación (Prácticas y Políticas de Certificación, Políticas de Seguridad, manuales técnicos y operativos)

#### *5.5.2.* **Periodo de resguardo de la información**

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 se conservan publicados en el repositorio durante 2 años desde su expiración. Los contratos con los suscriptores y cualquier información relativa a la identificación y autenticación del suscriptor se conservan durante al menos 15 años.

#### *5.5.3.* **Protección de la información**

Andes SCD asegura la correcta protección de la información mediante la asignación de personal calificado para su tratamiento, sistemas de alta disponibilidad y el resguardo de copias de seguridad.

Se dispone de documentación técnica y de configuración donde se detallan todas las acciones tomadas para garantizar la protección de los archivos.

#### *5.5.4.* **Procedimiento de respaldo de la información**

La información y los aplicativos software utilizados por Andes SCD son respaldados por copias de seguridad incrementales, progresivas ó completas que se realizan periódicamente según la criticidad de la información.

Las copias de seguridad catalogadas como completas abarcan todos los aplicativos e información crítica, las copias de seguridad progresivas contienen la información que ha cambiado y las copias de seguridad incremental salva los archivos e información modificada desde la última copia de seguridad completa.

La periodicidad, contenido crítico y controles de seguridad de las copias de seguridad es información confidencial de Andes SCD y se encuentra definido en la Declaración de Políticas de Seguridad (PSI).

#### *5.5.5.* Sistemas de almacenamiento internos y externos

La información almacenada electrónicamente es protegida contra cambios, borrado o alteración no autorizada mediante la implementación de controles de acceso lógicos y físicos estipulados en la Declaración de Políticas de Seguridad de Andes SCD.

#### *5.5.6.* Procedimiento para obtener y verificar la información archivada

Andes SCD no almacena en papel ningún tipo de documento producto de la prestación del servicio de certificación, todos los soportes necesarios para la prestación del servicio se almacenan en medios electrónicos que se protegen mediante controles de acceso físico y lógico de tal forma que solo el personal de confianza autorizado puede tener acceso

Los datos almacenados digitalmente son firmados para garantizar la integridad y autenticidad de la información. El procedimiento de verificación de la información del archivo es de carácter confidencial y es aplicado únicamente por personal autorizado.

### *5.6. Cambio de clave*

Los cambios de claves de las CA's de Andes SCD se realizan al cumplirse su periodo de vigencia y siguiendo el protocolo de cambio de claves de la CA.

La clave privada antigua solo se usa para la firma de CRL's mientras existan certificados activos emitidos por la clave antigua.

Cuando se emita un nuevo certificado para cada una de las CA's de la jerarquía de certificación de Andes SCD se creará un nuevo par de claves para cada CA.

Los siguientes certificados se pondrán a disposición pública en el Registro de Certificados:

- La nueva Clave pública firmada por la clave privada antigua.
- La antigua Clave pública firmada con la clave privada nueva.

En el documento de uso interno **Administración de la clave privada de la CA** identificado con el OID 1.3.6.1.4.1.31304.100.1.4 detalla el proceso de cambio de claves de la CA raíz de las CA's subordinadas.

El cambio de claves de suscriptores de certificados Clase I y Clase II varía según el tipo de certificado y se encuentra definido en cada Política de Certificación (PC)

### *5.7. Compromiso y recuperación de desastre*

Andes SCD ha desarrollado un plan de contingencias para recuperar todos los sistemas en menos de 48 horas, aunque se asegura que los servicios críticos como la revocación y publicación de información del estado de los certificados estarán disponibles en menos de 24 horas.
Cualquier fallo en la consecución de las metas marcadas por este plan de contingencias, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la CA para implementar dichos procesos.

Los mecanismos técnicos implementados por Andes SCD para dar soporte a la recuperación tras incidentes se encuentran detallados en el Documento de Infraestructura Tecnológica de Andes SCD

### *5.7.1. Procedimientos para administrar incidentes*

Dentro de la Declaración de Políticas de Seguridad (PSI) de Andes SCD se definen los procedimientos de gestión y respuesta a incidentes y su respectiva documentación para prevenir o dar una respuesta rápida en caso de que se presente de nuevo el incidente. A continuación se describen los aspectos más relevantes del procedimiento:

- **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.
- **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 llego el ataque y la máxima información posible de la incidencia.
- **Control de daños ocasionados por incidente**: Reaccionar rápidamente para contener la incidencia y evitar que se propague tomando medidas como bloquear accesos al sistema.
- **Investigación y recopilación de evidencias**: Revisar registros de auditoría para realizar un seguimiento de lo ocurrido.
- **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.
- **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 tiene establecido un Plan de Contingencias que especifica las acciones a ejecutar, componentes ó 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.

### *5.7.2. Recursos informáticos, software y datos corruptos*

Si alguno de los recursos informáticos, software ó información críticos para la prestación del servicio de certificación llegara a fallar o fuera alterado se seguirá el procedimiento de recuperación establecido en el Plan de Continuidad del Negocio según el caso.

Paralelamente se realiza una auditoria para determinar el origen del problema y se toman las medidas pertinentes para evitar que se vuelva a presentar.

### *5.7.3. Procedimientos ante compromiso de la clave privada*

Si la clave privada de una CA de Andes SCD se ve comprometida se procederá a revocar el certificado, se publica la revocación en la respectiva CRL y se notifica a todos los participantes del modelo de confianza afectados. El certificado revocado de la CA

permanecerá accesible en el repositorio de Andes SCD con el fin de continuar verificando los certificados emitidos durante su periodo de funcionamiento.

Inmediatamente se gestionara el trámite para adquirir un nuevo certificado y par de claves para la CA conservando la misma denominación. En caso de que la clave privada comprometida sea la de CA Andes Raíz se emitirá un nuevo certificado para las CA subordinadas firmado por la nueva clave privada de la CA raíz. Las CA's subordinadas no emitirán certificados hasta que les sea emitido el nuevo certificado.

Se emitirá un nuevo certificado a cada uno de los suscriptores a quienes se les revoco el certificado por motivo del compromiso de la clave privada de Andes SCD. Todos los procedimientos están completamente documentados en el plan de continuidad del negocio:

- Como revocar la clave privada de Andes SCD
- Como generar la nueva clave y distribuirla entre los usuarios
- Como revocar y remitir los certificados de los suscriptores

### *5.7.4. Capacidades de continuidad del negocio ante un desastre*

Para garantizar la continuidad del negocio ante un desastre se contemplan los siguientes aspectos

- La redundancia de los componentes más críticos
- El chequeo periódico de los servicios de copia de respaldo

### *5.7.5.* Medidas para corrección de vulnerabilidades detectadas

Andes SCD contempla en el documento Políticas para la Administración de Backups y Ejecución del Plan de Contingencias identificado con el OID 1.3.6.1.4.1.31304.100.2.10 los procedimientos de seguridad para el manejo de eventos que puedan afectar la prestación del servicio de certificación. Los eventos considerados son los siguientes:

- Compromiso de clave privada de alguna de las CA´s 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.

## *5.8. Terminación de CA o RA*

En el caso de cesar las actividades de Andes SCD como prestador de servicios de certificación se tomarán las siguientes medidas a fin de causar el menor daño posible a suscriptores y usuarios del sistema de certificación:

- La Autoridad Certificadora Andes SCD notificará con un tiempo 30 días de anticipación a la Superintendencia de Industria y Comercio la intención de cesar sus actividades como prestador de servicios de certificación.

- Una vez se haya recibido autorización por parte de la Superintendencia de Industria y Comercio para el cese de las actividades se recurrirá a los medios de comunicación para notificar a los usuarios del sistema de certificación el cese de la actividad como Prestador de Servicios de Certificación.
  La comunicación del cese de actividades a los usuarios del servicio de certificación 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, la fecha precisa de la cesación y las consecuencias jurídicas de la cesación respecto a los certificados expedidos.

- Transmitir todas las responsabilidades, obligaciones y derechos dentro del sistema de certificación a otra Autoridad Certificadora que esté dispuesta a continuar con el servicio. En caso de no encontrar otra Autoridad Certificadora que acepte la transferencia de derechos y obligaciones, se procede a la revocación de todos los certificados que estén sin expirar en el momento del cese definitivo de la Autoridad de Certificación.
- Andes SCD realizará un esfuerzo para asegurar que la interrupción del servicio de certificación cause las menores molestias a los suscriptores y a las personas que necesitan verificar firmas digitales.
- Pagar una compensación a los suscriptores que lo soliciten por revocar sus certificados antes de la fecha de expiración por motivo de cese de la Autoridad de Certificación, esta compensación no excede la tarifa de compra del certificado y es proporcional de acuerdo al tiempo transcurrido desde el inicio del contrato de suscripción y la fecha e revocación.
- Revocar toda autorización a entidades subcontratadas para actuar en nombre de Andes SCD en el procedimiento de emisión de certificados.
- Cumplir las obligaciones impuestas por la ley Colombiana.

En caso de que la Autoridad de Registro cese en la realización de sus funciones se anulará toda autorización para obrar como Autoridad de Registro delegada del Servicio de Certificación de Andes SCD y se revocaran los certificados digitales de uso interno emitidos a operarios y componentes de la RA.

# 6. Controles de seguridad técnica

## *6.1. Generación de claves e instalación*

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

***Claves de la CA***

Andes SCD cuenta con una jerarquía de confianza de 2 niveles conformada por 3 CA's, la CA de nivel superior ó *CA Raíz* garantiza la confiabilidad de sus CA's subordinadas de nivel inferior que han sido creadas para diferentes propósitos:

- *CA Emisora de certificados Clase I*: Emite certificados de uso interno para personal y componentes informáticos que son indispensables para el funcionamiento interno y operativo de la Autoridad Certificadora y Autoridades de Registro.

- *CA Emisora de certificados Clase II* ó de entidad final: Emite certificados a personas que en su propio nombre, representando una empresa o responsable de un componente informático ha solicitado la emisión de un certificado digital a Andes SCD.

El par de claves de cada una de las anteriores CA's ha sido generado de acuerdo con el procedimiento de Ceremonias de Generación de claves identificado con el OID 1.3.6.1.4.1.31304.100.1.9.1.1, el proceso de generación de claves fue realizado por personal autorizado según los roles de confianza usando un Módulo de hardware criptográfico (HSM) con certificación de seguridad FIPS 140-2 nivel 3 y el cual usa el estándar AIS 20 para la generación de números aleatorios.

***Claves del suscriptor***

**Descripción del Proceso Regular**

Las claves pública y privada de titulares de certificados Clase II (Entidad final) son generadas por el propio suscriptor de forma segura utilizando un dispositivo criptográfico TOKEN. Estos dispositivos criptográficos de custodia de la clave privada aportan un nivel de seguridad igual o superior a lo establecido para los dispositivos de creación de datos de firma. Las características de los TOKENS utilizados son las siguientes:

- Genera pares de claves RSA hasta de 2048 bits
- Algoritmos para la generación RSA, DES, 3DES, MD5 y SHA-1 implementados por hardware.
- Hardware generador de números aleatorios
- Hardware generador de firma digital
- Espacio disponible de 64 Kb
- Certificación CE y FCC
- Soporte completo para aplicaciones PKI
- Compatible con interfaces CAPI y PKCS#11
- Soporte para el almacenamiento de múltiples claves
- Soporte para X.509 V3 formato estándar de certificado
- Soporte para Microsoft® Windows®98(Second Edition), Windows®Me, Windows®2000, Windows®XP, Windows®2003, Windows®Vista, Linux MAC OS X.

El dispositivo criptográfico posee una clave de activación (PIN) para hacer uso de las claves privadas, esta clave de activación debe ser de uso exclusivo del suscriptor para

garantizar que los datos de creación de firma están protegidos contra la utilización de terceros.

**Descripción del Proceso Especial**

Las claves pública y privada de titulares de certificados Clase II (Entidad final) son generadas por Andes SCD si el método de entrega del certificado es en archivo con formato PKCS12. El archivo PKCS12 es destruido por Andes SCD después de efectuarse la descarga del archivo por parte del suscriptor.

El archivo con formato PKCS12 requiere una clave de activación (PIN) para hacer uso de la clave privada y el certificado, esta clave de activación debe ser de uso exclusivo del suscriptor para garantizar que los datos de creación de firma están protegidos contra la utilización de terceros.

Los pares de claves de los titulares de certificados Clase I (uso interno) se generan en función de lo estipulado en la Política de Certificación aplicable al tipo de certificado.

***Garantía de la seguridad que ofrecen las claves***

Andes SCD basa en el algoritmo RSA la generación de todas las claves públicas y privadas para sus CA's y suscriptores del servicio de certificación.

El algoritmo RSA sustenta la seguridad de sus claves en la dificultad computacional que implica factorizar números primos muy grandes. Por ejemplo para factorizar un número primo de 232 dígitos que equivale a una clave de 768 bits se usaron alrededor de 670 máquinas con procesador Opteron de 2.2GHz trabajando en paralelo durante 3 años.

Andes SCD utiliza claves de longitud mínima de 1024 bits para los certificados de Clase I que equivalen a números de 309 dígitos lo que supone un esfuerzo computacional superior que el usado para factorizar claves como la del ejemplo anterior. Para los certificados de Clase II la longitud mínima de las claves es de 2048 bits.

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

**Descripción del Proceso Regular**

No procede para certificados Clase II (Entidad final) porque la clave privada en ningún momento es conocida por Andes SCD. Para este tipo de certificados la clave privada es generada por el propio solicitante usando un dispositivo TOKEN que almacena la clave privada y protege su uso mediante un PIN.

Para los Certificados de Clase I el método de entrega de la clave privada a sus titulares depende de cada certificado y es definido en la Política de Certificación aplicable.

**Descripción del Proceso Especial**

Andes SCD informa al suscriptor el enlace a la página web donde tiene la opción de descargar el certificado en archivo con formato PKCS12 una única vez. En el PKCS12 se encuentra contenida la clave privada del suscriptor.

Por seguridad el pin para la instalación de las claves y el certificado es entregado por un medio distinto para la entrega del PKCS12 (Entrega personal, Teléfono, Mensaje de texto).

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

**Descripción del Proceso Regular**

En los certificados de Clase II (entidad final), el par de claves es generado por el futuro suscriptor por lo tanto el suscriptor siempre está en posesión de su propia clave pública.

La entrega de la clave pública del suscriptor a Andes SCD se realiza en el momento de presentar la solicitud de certificado ante la Autoridad de Registro, allí el solicitante suministra los datos indispensables para generar el certificado, entre ellos su clave pública; esta información es procesada por la Autoridad de registro y transmitida de forma segura a Andes SCD en el formato PKCS#10.

**Descripción del Proceso Especial**

Andes SCD informa al suscriptor el enlace a la página web donde tiene la opción de descargar el certificado en archivo con formato PKCS12 una única vez. En el PKCS12 se encuentra contenida la clave pública del suscriptor.

Por seguridad el pin para la instalación de las claves y el certificado en entregado por un medio distinto para la entrega del PKCS12 (Entrega personal, Teléfono, Mensaje de texto).

Para los Certificados de Clase I el método de entrega de la clave pública a sus titulares depende de cada certificado y es definido en la Política de Certificación aplicable.

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

La clave pública de cualquier suscriptor de Certificados Clase II (Entidad Final) cuyo certificado fue emitido por Andes SCD está permanentemente disponible para descarga en el directorio de certificados de Andes SCD.

La clave pública de suscriptores de Certificados Clase I (uso interno) está permanentemente disponible para uso interno de Andes SCD.

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

La clave pública de CA Andes Raíz, CA emisora de certificados Clase I y la CA emisora de certificados Clase II se encuentran permanentemente disponibles para descarga en la página WEB de Andes SCD.

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

*Clave privada de la CA*

El periodo de uso de la clave privada de la CA Andes Raíz es de 25 años, la fecha de inicio y fin esta explicita en el certificado y en la sección 1.6.1 de este documento.

El periodo de uso de la clave privada de la CA emisora de Certificados Clase I (uso interno) y la CA emisora de Certificados Clase II es de 10 años. La fecha de inicio y fin de cada uno de estos certificados esta explicita en el respectivo certificado y en la sección 1.6.1 de este documento.

*Clave privada de suscriptores*

El periodo de utilización de la clave privada de Certificados de Clase I y Certificados de Clase II está definido en la Política de Certificación aplicable. Para algunos tipos de certificados el periodo de utilización de la clave privada es el mismo que el periodo de la vigencia del certificado.

#### *6.1.7. Tamaño de las claves*

El tamaño de las claves certificadas de la CA Raíz y de CA's subordinadas tiene una longitud de 4096 bits basadas en el algoritmo RSA.
El tamaño mínimo de las claves certificadas para uso interno es de 1024 bits basadas en el algoritmo RSA.
El tamaño de las claves certificadas para entidad final es de 2048 bits basadas en el algoritmo RSA.

#### *6.1.8. Parámetros de generación de clave pública y comprobación de calidad*

La clave pública de la CA Raíz y de las CA's subordinadas están codificadas de acuerdo con RFC 3280 y PKCS#1. El algoritmo de generación de claves es el RSA.

Los parámetros de generación de las claves y los medios de comprobación de la calidad de los parámetros de generación de claves para Certificados de Clase I y Certificados de Clase II se encuentran definidos en la Política de Certificación aplicable.

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

#### *6.2.1. Controles y estándares de módulos criptográficos*

El modulo criptográfico usado para generar y custodiar las claves privadas de Andes CA es un módulo HSM que se rige con el estándar FIPS140-2 del NIST cumpliendo con nivel de seguridad 3.

#### *6.2.2. Control sobre la clave privada (Multi-persona)*

El acceso a la clave privada utilizadas por la CA Raíz y las CA´s subordinadas se realiza a través del módulo criptográfico (HSM) mediante la participación de 2 personas de un grupo de 4 posibles, este control multi-persona garantiza que nadie tiene un control individual de las actividades críticas como activar y usar la clave privada de las CA raíz y subordinadas.

#### *6.2.3. Respaldo de la clave privada*

Periódicamente se realiza un test de pruebas para asegurar el correcto funcionamiento del dispositivo HSM que contiene las claves privadas de las CA's raíz y subordinadas.

Existe por lo menos una copia de respaldo de las clave privadas de las CA's que hace posible su recuperación en caso de desastre, deterioro o pérdida de la misma, es almacenada y recuperada sólo por el personal autorizado según los roles de confianza, usando al menos un control dual en un medio físico seguro.

Las copias de respaldo de las claves privadas de firma de las CA's están almacenadas de forma segura. Este procedimiento se describe en detalle en las Políticas de Seguridad de Andes SCD

En el caso de las claves privadas de suscriptores no se realiza ningún tipo de respaldo porque esta clave sólo permanece en custodia del suscriptor y nunca está en posesión de Andes SCD.

### *6.2.4. Almacenamiento de la clave privada*

*Clave privada de la CA*

Cuando las claves privadas de la CA están fuera del módulo criptográfico HSM se mantienen cifradas y la clave con la que se realizó el cifrado se encuentra dividida y resguardada en 2 dispositivos criptográficos, el acceso está restringido a personal autorizado según los roles de confianza.

Las fracciones de las claves privadas de la CA son custodiadas por la firma CSA, entidad líder el manejo, administración y depósito de documentos físicos, y tienen el tratamiento de seguridad propio de la custodia fiduciaria de títulos valores. La firma CSA tiene sede en varias ciudades del país, cuenta con certificación ISO 9001:2000 y su objeto principal consiste en prestar los Servicios de Organización, Administración y Conservación Documental de Fondos Acumulados, Archivo Central y de Gestión, Elaboración y Ajuste de Tablas de Retención y Valoración Documental, así como los servicios de reprografía (microfilmación y digitalización). La Detección automática de incendios, instalación eléctrica montada en tubo de acero para evitar cortocircuitos, edificios aislados para eludir percances generados en edificios ajenos a CSA Ltda, sistemas de seguridad internos y externos, y garantía de suministro eléctrico permanente.

*Clave privada de los suscriptores*

Las claves privadas de los certificados internos que usan los distintos componentes del sistema de la CA para comunicarse entre sí, firmar y cifrar la información son almacenados por Andes SCD por un periodo de al menos 10 años.

**Uso de dispositivo Token**

Las claves privadas de los suscriptores NUNCA son almacenadas por Andes SCD, deben ser almacenadas por ellos mismos, mediante la conservación del dispositivo de creación de firma u otros métodos, debido a que pueden ser necesarias para descifrar la información histórica cifrada con la clave pública, siempre que el dispositivo de custodia permita la operación.

**Uso del archivo con formato PKCS12**

Las claves privadas de los suscriptores son almacenadas por Andes SCD hasta que se produce la descarga del PKCS12 por parte del suscriptor. Una vez el suscriptor realiza la descarga se procede a eliminar el certificado en formato PKCS12 de los sistemas de Andes SCD y de esta forma se borra la clave privada del suscriptor.

### *6.2.5. Transferencia de la clave privada a partir o a un módulo criptográfico*

*Clave privada de CA*

Las claves privadas de las CA´s se generan directamente en el módulo criptográfico HSM siguiendo el procedimiento documentado de Ceremonia de Generación de Claves, la transferencia de las claves privadas a partir del módulo criptográfico se limitan únicamente a la realización de copias de seguridad en conformidad a la sección 6.2.3 de este documento.

*Clave privada de suscriptores*

**Uso de dispositivo Token**

En el caso de los suscriptores la clave privada nunca sale del TOKEN, este se encarga de generar el par de claves y proteger su uso a partir de un PIN.

**Uso del archivo con formato PKCS12**

En el caso de los suscriptores que tienen su clave privada en un PKCS12 deben proteger su uso a partir de un PIN.

### *6.2.6. Almacenamiento de la clave privada a un módulo criptográfico*

Las claves privadas de la CA Raíz, la CA clase I y la CA clase II son creadas y almacenadas de forma cifrada en un módulo criptográfico HSM.

### *6.2.7. Método de activación de la clave privada*

Activar la clave privada consiste en iniciar sesión en el dispositivo que la almacena permitiendo realizar operaciones con la clave privada por un tiempo indefinido hasta que sea desactivada.

*Activación de claves CA*

La activación de las claves privadas de Andes SCD se realiza utilizando mecanismos técnicos remotos y procedimientos que requieren la participación simultánea de 2 operadores de un grupo de 4 posibles para activar las funciones criptográficas del dispositivo HSM, cada uno de estos operadores tiene una clave que debe custodiar bajo su responsabilidad de tal forma que ninguno de los operadores conozca más de una clave de acceso y se garantice el control multipersona.

*Activación de claves suscriptor*

**Uso de dispositivo Token**

La activación del dispositivo TOKEN que contiene la clave 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 claves. La protección de los datos de activación es responsabilidad exclusiva del suscriptor.

**Uso de Archivo PKCS12**

La activación de la clave privada contenida en el archivo PKCS12 es realizada a través de un PIN asignado por Andes SCD en el momento de generar el par de claves y el certificado. La protección de los datos de activación es responsabilidad exclusiva del suscriptor.

### *6.2.8. Método de desactivación de la clave privada*

Desactivar la clave privada consiste en finalizar la sesión en el dispositivo que la almacena evitando que se puedan realizar operaciones con la clave privada. Cualquier operación con la clave privada después de desactivada requiere la activación del dispositivo.

*Desactivación de clave privada CA*

Para la desactivación de la clave privada de la CA se usa el mismo modelo descrito para la activación, un proceso de 2 de 4 personas autorizadas según los roles de confianza.

*Desactivación de clave privada suscriptores*

**Uso de dispositivo Token**

El método para desactivar la clave privada del suscriptor es retirar el dispositivo TOKEN del equipo, inmediatamente cualquier contenido asociado queda deshabilitado incluyendo la clave privada.

**Uso de Archivo en formato PKCS12**

El método para desactivar la clave privada del suscriptor es retirar el certificado del almacén de certificados que lo contenga, inmediatamente cualquier contenido asociado queda deshabilitado incluyendo la clave privada.

### *6.2.9. Método de destrucción de la clave privada*

*Destrucción de clave privada CA*

La destrucción de las claves privadas de las CA's se realiza cuando se haya finalizado su periodo operacional o periodo de validez, cuando haya compromiso de las claves ó cuando se origine el cese de la Autoridad de Certificación.

El proceso de destrucción de claves es efectuada por personal autorizado utilizando las funciones que provee el modulo criptográfico HSM de forma que no resulten afectadas las demás claves privadas que residen en el dispositivo.

En el documento de uso interno **Procedimiento de destrucción de claves de la CA** identificado con el OID 1.3.6.1.4.1.31304.100.1.10 se detalla el proceso de destrucción de claves de la CA.

*Destrucción de clave privada de suscriptores*

**Uso de dispositivo Token**

La destrucción de la clave privada del suscriptor puede realizarla el propio suscriptor utilizando las funciones que provee el dispositivo TOKEN, teniendo en cuenta que si tiene más claves privadas dentro del dispositivo, estas no se vean afectadas.

**Uso del archivo en formato PKCS12**

La destrucción de la clave privada del suscriptor puede realizarla el propio suscriptor eliminando el archivo PKCS12.

### *6.2.10. Clasificación de los modulo criptográfico*

El módulo criptográfico utilizado para generar las claves privadas de las CA's de Andes SCD cumple con el estándar FIPS 140-2 nivel 3.

## *6.3. Otros aspectos de administración del par de claves*

### *6.3.1.* Archivo de la clave pública

Andes SCD mantiene archivados todos los certificados durante un periodo de 15 años, cada uno de estos certificados incluyen la clave pública correspondiente. Estos archivos

están protegidos por los controles de acceso a los demás componentes de la infraestructura.

### *6.3.2.* Periodos operacionales del certificado y periodos de uso del par de claves

El tiempo de vida del certificado 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 claves tiene vigencia mientras exista un certificado válido que las sustente.
Una vez el certificado deje de ser válido las claves pierden toda validez legal y su uso se limita a fines exclusivamente personales.

## 6.4. Datos de activación

Los datos de activación son valores requeridos por los dispositivos criptográficos para permitir el acceso a las claves privadas que contienen.

### *6.4.1.* Generación e instalación de los datos de activación

La generación e instalación de los datos de activación consiste en la creación de los datos que permiten la autenticación ante el dispositivo que contiene la clave privada aprobando su uso.

*Datos activación de dispositivo HSM*

El administrador del HSM dispone de una clave de administración y de opciones que le permite generar y administra las cuentas de usuario para los operadores que activaran las claves privadas de Andes SCD. Cada uno de los operadores del HSM a su vez dispone de una clave que deben custodiar bajo su responsabilidad de modo que ningún operador conozca más de una clave y se garantice que nadie tiene un control individual de las actividades críticas del HSM como activar y usar la clave privada de las CA raíz y subordinadas.

*Datos activación de dispositivo TOKEN*

El suscriptor debe generar los datos de activación de su TOKEN cambiando el PIN inicial que trae por defecto el dispositivo, esto debe realizarlo por primera vez en la Autoridad de Registro usando el aplicativo software que suministra el fabricante del TOKEN. 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.

*Datos activación de archivo con formato PKCS12*

Andes SCD generar los datos de activación del archivo con formato PKCS12 a partir de un PIN aleatorio de mínimo 12 caracteres, mínimo 1 carácter en mayúscula, mínimo 2 números y mínimo 2 caracteres no numéricos. El PIN debe ser custodiado por el suscriptor de modo que no sea conocido por nadie más y se garantice el control exclusivo del archivo PKCS12.

### *6.4.2.* Protección de datos de activación

La protección de los datos de activación de los dispositivos criptográficos impide el uso no autorizado de la clave privada.

*Protección de datos de activación del HSM*

Los datos de activación del dispositivo HSM son catalogados información confidencial y cada clave de acceso particular debe ser conocida únicamente por el operador responsable de activar el dispositivo simultáneamente con otro operador. En ningún caso un operador debe conocer más de una clave de Activación.

Los operadores del HSM son responsables de custodiar su clave y no deben revelar su condición de operadores del HSM ni de otros operadores ante ninguna tercera parte.
Las claves de acceso de los operadores del HSM son cambiadas periódicamente para disminuir la posibilidad de compromiso.

*Protección de datos de activación del TOKEN*

El PIN ó dato de activación del TOKEN debe ser personalizado por el solicitante antes de generar su par de claves.
El suscriptor debe proceder a cambiar el PIN de su TOKEN 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.
La protección de los datos de activación es responsabilidad exclusiva del suscriptor.

*Protección de datos de activación de archivo con formato PKCS12*

El PIN o dato de activación del archivo PKCS12 es asignado aleatoriamente por Andes SCD. El PIN no puede ser personalizado por el suscriptor y debe ser custodiado de modo que no sea conocido por nadie más y se garantice el control exclusivo del archivo PKCS12.

## *6.5. Controles de seguridad informática*

### *6.5.1.* Requisitos específicos de seguridad técnica

Cada servidor de la CA incluye las siguientes funcionalidades:

- Control de acceso a los servicios de CA
- Gestión de privilegios para asignar las tareas pertinentes a cada usuario
- Identificación y autenticación de usuarios para las aplicaciones de la CA a partir de certificados digitales de Clase I ó uso interno.
- Auditoría de eventos relativos a la seguridad.
- Mecanismos de recuperación de claves y del sistema de CA.

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

### *6.5.2.* Nivel de seguridad informática

- Configuración de la seguridad del sistema operativo
- Documentación técnica y de configuración de la CA
- Configuración de seguridad de las aplicaciones
- Configuración de usuarios y privilegios
- Plan de administración y mantenimiento del sistema de alta disponibilidad
- plan de contingencia y recuperación a desastres

## 6.6. Controles técnicos del ciclo de vida

### *6.6.1.* Controles en el desarrollo de sistema

Andes SCD ha diseñado una metodología de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que eliminen cualquier vulnerabilidad descubierta.

### *6.6.2.* Controles de gestión de la seguridad

Andes SCD realiza jornadas para la formación y concientización de los empleados en cuanto a la implantación de las políticas de seguridad, usando documentación descriptiva producto de la realimentación y seguimiento de la gestión de la seguridad.

De acuerdo al análisis de riesgos Andes SCD clasifica los activos según sus necesidades de protección y realiza una planeación de capacidad de tal forma que sea posible garantizar la alta disponibilidad y escalabilidad de los servicios.

### *6.6.3.* Controles de seguridad en el ciclo de vida

Andes SCD da cubrimiento a los siguientes controles de seguridad especificando el tratamiento de cada control en la Declaración de Políticas de Seguridad (PSI):

- Controles para la gestión de las claves de la CA indicando como se genera, como se almacena y como se protegen las claves privadas de la CA raíz y las CA's subordinadas.
- Controles para distribuir de manera segura la clave pública de la CA a los suscriptores y terceros de confianza.
- Controles de seguridad en la emisión de certificados desde el momento en que se identifica al solicitante hasta que se entrega el certificado. (verificación de la identidad de la RA, verificación de la identidad del solicitante, verificación de la correspondencia de la clave pública con la clave privada del solicitante, firma digital de la solicitud por el operador RA autorizado, comprobación de errores técnicos u omisiones en la petición de certificado, verificación de singularidad en el nombre distinguido del certificado, detección de claves publicas duplicadas y aceptación de la solicitud por parte del supervisor, envío de email informando al suscriptor la emisión del certificado, publicación del certificado en el directorio de certificados).
- Controles de seguridad para la revocación de certificados (mecanismos rápidos y seguros para revocar, controles para revocar certificados presencialmente, on-line o telefónicamente, acuse de recibido proporcionado por la CA para indicar que recibió la solicitud de revocación, actualización de la CRL, envío de email informando al suscriptor que su certificado fue revocado)
- Controles de seguridad en la publicación de certificados: (la CA mantiene controles para proporcionar la seguridad de que en el momento de la emisión el certificado está disponible para suscriptores y partes que confían, administración del repositorio solo está a cargo de personal autorizado, integridad de la información del repositorio)

### 6.7. Controles de seguridad en la red

El control de acceso a la red está restringido a personal autorizado

- Los componentes de red se encuentran localizados en instalaciones seguras con monitoreo permanente.
- La red interna de Andes SCD es protegida por cortafuegos configurados con políticas de acceso y sistemas de alertas para evitar el acceso no autorizado.
- La comunicación de información sensible entre Andes SCD y las Autoridades de Registro es realizada vía VPN incluyendo el uso de firmas digitales.
- Se implementan cortafuegos y controles para proteger la red interna de accesos externos.
- Existen procedimientos y disposiciones respecto al uso de las redes y servicios de red.

# 7. Perfiles de certificado, CRL y OCSP

## *7.1. Perfiles de certificado*

### *7.1.1. Número de versión*

Todos los certificados emitidos por Andes SCD están de conformidad con el estándar X.509 V3 y de conformidad con el RFC 3280 para perfiles de certificados y CRL's.

### *7.1.2. Extensiones del certificado*

Las extensiones utilizadas de forma genérica en los certificados son:

- BasicConstraints: Calificada como crítica.
- KeyUsage: Calificada como crítica.
- ExtendedKeyUsage: Calificada como crítica
- CertificatePolicies: Calificada como no crítica
- SubjectAlternativeName: Calificada como no crítica
- CRLDistributionPoint: Calificada como no crítica
- OCSPServiceLocator: Calificada como no crítica
- UseCertificatePolicies: Calificada como no crítica

En cada Política de Certificación se establecen las variaciones en el conjunto de extensiones utilizadas por cada tipo de certificado.

### *7.1.3. Identificadores objeto del algoritmo*

OID del algoritmo de firma SHA1withRSAEncryption 1.2.840.113549.1.1.5
OID del algoritmo de la clave pública RSAEncryption 1.2.840.113549.1.1.1

### *7.1.4. Formatos de nombres*

Los certificados digitales 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. En cada Política de Certificación se describen los DN usados para el suscriptor.

### *7.1.5.* Restricciones de nombre

Los certificados digitales emitidos por Andes SCD cuentan con DN conforme a las recomendaciones X.500 que son únicos y no ambiguos.

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

Un OID o identificador de objeto es una secuencia de números única asignada jerárquicamente por alguna de las agencias registradoras existentes como IANA, ANSI o BSI con el fin de permitir identificar objetos en la red. Una vez una organización ha adquirido un OID tiene derecho a asignar libremente esa rama de la jerarquía según sus intereses.

Andes SCD tiene asignado el OID 31304 desde Junio de 2008 registrado ante organización internacional IANA (Internet Assigned Numbers authority), bajo la rama iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 – IANA Registered Private Enterprise). Esto puede consultarlo en la dirección: http://www.iana.org/assignments/enterprise-numbers.

De esta forma Andes SCD asigna jerárquicamente un OID a cada uno de sus documentos a partir de la raíz: **1.3.6.1.4.1.31304.**

El OID asignado a la presente declaración de prácticas de certificación (DPC) es **1.3.6.1.4.1.31304.1.1.1.4** adicionalmente se le añade una extensión con formato Y.Z que especifica la versión. Entonces la OID **1.3.6.1.4.1.31304.1.1.1.Y.Z** es interpretada como la DPC publicación Z de la versión Y

Cada Política de Certificación tiene asignado un OID dentro del rango privado de numeración, todas las PC comienzan con el prefijo **1.3.6.1.4.1.31304.1.2**

### *7.1.7.* 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 que aplica al tipo de certificado
- **CPS**: Indica la URL donde están publicadas las Practicas de Certificación (DPC) para ser consultadas por los usuarios
- **User Notice:** La utilización de este certificado está sujeta a las Políticas de Certificado (PC) y Prácticas de Certificación (DPC) establecidas por Andes SCD.

### *7.1.8. Perfil de la CRL*

### *7.1.9.* Numero de versión

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

### *7.1.10.* CRL y extensiones

Se emite la lista de revocación CRL según lo estipulado en la RFC 2459
A continuación se presenta el formato del perfil de CRL para cada una de las CA

***CRL de ROOT CA ANDES SCD S.A***

| Perfil de CRL según estándar X.509V2 – CRL CA Raíz | | |
|---|---|---|
| **Nombre** | **Descripción** | **Valor** |
| **Versión** | Versión de la CRL | V2 |
| **Numero de CRL** | Número único de la CRL | Identificado de la CRL |
| **Emisor** | CN | ROOT CA ANDES SCD S.A. |
| | O | Andes SCD |
| | OU | Division de certificacion |
| | C | CO |
| | L | Bogota D.C. |
| | E | info@andesscd.com.co |
| **Algoritmo de firma** | Algoritmo usado para la firma de la CRL | SHA1withRSA |
| **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 |
| **URL distribución** | URL donde se publican las CRL emitidas por Andes SCD | http://www.andesscd.com.co/includes/getCert.php?crl=2 |
| **Certificados revocados** | Lista de certificados revocados especificando el número de serie, fecha de revocación y motivo de la revocación | |

***CRL de CA ANDES SCD S.A. Clase I***

| Perfil de CRL según estándar X.509V2 – CRL Clase I | | |
|---|---|---|
| **Nombre** | **Descripción** | **Valor** |
| **Versión** | Versión de la CRL | V2 |
| **Numero de CRL** | Número único de la CRL | Identificado de la CRL |
| **Emisor** | CN | CA ANDES SCD S.A. Clase I |
| | O | Andes SCD |
| | OU | Division de certificacion uso interno |
| | C | CO |
| | L | Bogota D.C. |
| | E | info@andesscd.com.co |
| **Algoritmo de firma** | Algoritmo usado para la firma de la CRL | SHA1withRSA |
| **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 |
| **URL distribución** | URL donde se publican las CRL emitidas por Andes SCD | USO INTERNO |
| **Certificados revocados** | Lista de certificados revocados especificando el número de serie, fecha de revocación y motivo de la revocación | Certificados REVOCADOS de Clase I ó Uso Interno. |

***CRL de CA ANDES SCD S.A. Clase II***

| Perfil de CRL según estándar X.509V2 – CRL Clase II | | |
|---|---|---|
| **Nombre** | **Descripción** | **Valor** |
| **Versión** | Versión de la CRL | V2 |
| **Numero de CRL** | Número único de la CRL | Identificado de la CRL |
| **Emisor** | CN | CA ANDES SCD S.A. Clase II |
| | O | Andes SCD |
| | OU | Division de certificación entidad final |
| | C | CO |
| | L | Bogota D.C. |
| | E | info@andesscd.com.co |
| **Algoritmo de firma** | Algoritmo usado para la firma de la CRL | SHA1withRSA |
| **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 |
| **URL distribución** | URL donde se publican las CRL emitidas por Andes SCD | http://www.andesscd.com.co/includes/getCert.php?crl=1 |
| **Certificados revocados** | Lista de certificados revocados especificando el número de serie, fecha de revocación y motivo de la revocación | Certificados REVOCADOS de Clase II ó Entidad Final. |

## *7.2. Perfil OCSP*

En el documento interno Administración de OCSP identificado con el OID 1.3.6.1.4.1.31304.100.1.13se describe como se utiliza el protocolo OCSP según lo especificado en la RFC 2560.

### *7.2.1.* Numero de versión

El certificado OCSP se emite de acuerdo al estándar x,509 V3

### *7.2.2.* Extensiones OCSP

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

# 8. Auditoria y otras valoraciones

## 8.1. Frecuencia o circunstancias de valoración

Se realizarán periódicamente auditorías internas para garantizar la adecuación del funcionamiento y operación respecto con las estipulaciones incluidas en esta Declaración de Prácticas de Certificación, en las Políticas de Certificado y la Declaración de Políticas de Seguridad.

Se realizará una auditoría externa cada año para verificar el cumplimiento de los principios de Web Trust para autoridades certificadoras.

| No auditoria | Firma auditora | Periodo cubierto |
|---|---|---|
| **1** | Deloitte | Enero 2010 a Diciembre 2010 |

## 8.2. Identidad y calificaciones del asesor

Las auditorías externas son realizadas por empresas de reconocido prestigio en el área de la auditoria.

## 8.3. Relación entre el asesor y la entidad evaluada

El auditor interno no debe tener relación funcional con las áreas objeto de la auditoría.

Al margen de la función de auditoría, el auditor externo y la parte auditada no deberán tener relación alguna que pueda derivar en un conflicto de intereses.

## 8.4. Temas cubiertos en la valoración

La auditoría determina la adecuación de los servicios de Andes SCD con esta DPC y las PC's aplicables y verifica los siguientes aspectos:

***Publicación de la información***: Verificando que se hacen públicas la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificación (PC) y que presta sus servicios de acuerdo a estas declaraciones.

***Integridad de servicio***: Verifica que la Autoridad Certificadora mantiene los controles efectivos para asegurar que la información del suscriptor es autenticada adecuadamente, la integridad de las claves y certificados gestionados y su protección a lo largo de todo su ciclo de vida.

***Controles de seguridad***: Verifica que la Autoridad Certificadora hace uso de controles efectivos para asegurar la confidencialidad de los datos de los suscriptores, la administración y gestión está restringida a personal autorizado, existen planes de continuidad en las operaciones propias del servicio de certificación y ciclo de vida de los certificados y existen Políticas de Seguridad para disminuir las vulnerabilidades y riesgos que pueden presentarse.

## 8.5. Acciones tomadas como resultado de No Conformidades

En caso de que el auditor detecte alguna no conformidad, se tomarán todas las medidas correctivas necesarias para resolverla en el menor tiempo posible.

## 8.6. Comunicación de resultados

El auditor comunica los resultados de la auditoría al Comité de Aprobación de Políticas de Andes SCD encargado de aprobar las Políticas, al área se seguridad y al área donde se detecte la no conformidad. .

# 9. Negocio y materias legales

## 9.1. Tarifas

### *9.1.1.* Tarifas por emisión de certificados

La tarifa por el servicio de emisión de certificados digitales está disponible en la sección Tarifas de la página Web http://www.andesscd.com.co/.

### *9.1.2.* Tarifas por acceso a certificados

El acceso a consulta al directorio de certificados es un servicio gratuito, sin embargo Andes SCD se reserva el derecho de imponer una tarifa para los casos de descarga masiva de certificados ó cualquier otro caso en el que considere deba recaudar una tarifa. Las tarifas están a disposición en la página WEB de Andes SCD.

### *9.1.3.* Tarifas por información del estado de un certificado ó certificados revocados

El acceso a consulta y descarga de las listas de revocación (CRL de ROOT CA ANDES SCD S.A y CRL de CA ANDES SCD S.A. Clase II) es un servicio gratuito, sin embargo Andes SCD se reserva el derecho a imponer alguna tarifa para otros medios de comprobación del estado de los certificados o cualquier otro caso en el que se considere deba recaudar una tarifa.
Las tarifas están a disposición en la página WEB de Andes SCD.

### *9.1.4.* Tarifas por otros servicios

Las tarifas correspondientes a otros servicios ofrecidos por Andes SCD están a disposición en la sección Tarifas de la página Web http://www.andesscd.com.co/.

### *9.1.5.* Política de reembolso

El dinero recibido por los servicios de certificación no es reembolsable bajo ninguna circunstancia porque la tarifa se causa por el solo hecho de recibir la solicitud y acreditar la identidad del solicitante.

Si dentro del periodo de aceptación el suscriptor reclama alguna inconsistencia en su certificado y esta inconsistencia es causada por un error no atribuible al suscriptor no se realizara reembolso de la tarifa, en este caso se procede a revocar el certificado de inmediato y se emite un nuevo certificado sin costo alguno para el suscriptor. Finalizado el periodo de Aceptación si no hay comunicación por parte del suscriptor se concluye que éste está conforme con el contenido de su certificado y que asume sus responsabilidades y obligaciones como suscriptor del servicio de certificación.

## 9.2. Responsabilidad financiera

Para indemnizar los daños y perjuicios que se puedan ocasionar a los usuarios del servicio de certificación digital se dispone de un seguro de responsabilidad civil que cubre los perjuicios contractuales y extracontractuales de los suscriptores y terceros de buena fe exentos de culpa, mientras los daños y perjuicios se deriven de errores, omisiones o actos de mala fe por parte de Andes SCD.

La cobertura máxima fijada por Andes SCD para la indemnización de daños y perjuicios es de US$50.000 por cada certificado emitido independientemente de las veces que haya sido

usado y de la cantidad de personas afectadas, es decir, el valor de la indemnización será distribuido proporcionalmente entre las personas afectadas.

Se aclara que Andes SCD no asumirá responsabilidad alguna por la no ejecución ó retraso en la prestación de los servicios de certificación, si esta falla ó retraso es consecuencia de casos fortuitos, casos de fuerza mayor ó, en general, de cualquier circunstancia que este fuera de control de Andes SCD y en particular de las situaciones declaradas en la sección 9.7 de esta DPC "Limitaciones de responsabilidad".

Andes SCD no es responsable de aquellos daños y perjuicios que se deriven de:

a) Incumplimiento o ejecución incorrecta de las obligaciones a cargo del Solicitante, suscriptor y/o Usuario.
b) Incorrecta utilización de los certificados digitales y claves privadas por parte del suscriptor, ó cualquier daño o perjuicio indirecto que pudiera resultar.

**Información de la póliza de responsabilidad civil**

| | |
|---|---|
| Entidad aseguradora | : Chartis Seguros Colombia S.A |
| Tomador | : Andes Servicio de Certificación Digital S.A SIGLA ANDES SCD S.A. |
| Asegurado | : ANDES SCD S.A. |
| Beneficiario | : Terceros afectados de buena fe. |
| Valor | : 7000 SMMLV |

## 9.3. Confidencialidad de información comercial

### *9.3.1.* Alcance de la información confidencial

Toda la información que no sea considerada por Andes SCD como pública es considerada de carácter confidencial.

Se cataloga como confidencial la siguiente información:

a) Claves privadas de la CA Raíz y CA's subordinadas de Andes SCD
b) Información personal de suscriptores que no está contenida en el certificado digital
c) Información de parámetros de seguridad, control y procedimiento de auditoría
d) Documentación de infraestructura técnica, Declaración de Políticas de Seguridad, Políticas de Certificación para certificados Clase I, Documento guía de Ceremonia de generación de claves y Plan de Contingencias.

### *9.3.2.* Información no considerada confidencial

Se cataloga como pública la siguiente información

a) Declaración de Practicas de Certificación (DPC) y Políticas de Certificación de certificados Clase II ó de Entidad Final.
b) Los certificados emitidos por Andes SCD
c) Listas de Certificados Revocados (CRL)

### *9.3.3.* Responsabilidades para proteger la información confidencial

El personal de Andes SCD que participe en cualquier actividad u operación del Servicio de Certificación está sujeto al deber de secreto en el marco de las obligaciones contractuales contraídas con Andes SCD.

## 9.4. Confidencialidad de la información personal

Se considera confidencial toda la información de suscriptores que no sea incluida en el certificado.

### *9.4.1.* Plan de privacidad

El plan de privacidad para proteger la información catalogada confidencial se encuentra definido en la Declaración de Políticas de Seguridad PSI y abarca controles para proteger y asignar cada tipo de información un grado de criticidad.

### *9.4.2.* Información considerada confidencial

Andes SCD considera confidencial toda la información que no esté catalogada expresamente como pública y que no cuente con la aprobación de divulgación por parte del propietario de la información.

### *9.4.3.* Información no considerada confidencial

A continuación se hace referencia a la información considerada no confidencial

- Los certificados emitidos o en trámite de emisión
- La vinculación del suscriptor a un certificado emitido por Andes SCD
- El número de serie del certificado
- El nombre y los apellidos del suscriptor del certificado, en caso de certificados individuales, así como cualquier otra circunstancia o dato personal del titular mientras sea significativa para la finalidad del certificado.
- La dirección de correo electrónico del suscriptor del certificado.
- El periodo de validez del certificado, especificando la fecha de emisión y la fecha de caducidad.
- Los estados o situaciones que afectan al certificado y la fecha de inicio de cada uno, es decir desde que fecha está revocado.
- Las listas de revocación CRL de ROOT CA ANDES SCD S.A y CRL de CA ANDES SCD S.A. Clase II.
- Las políticas y prácticas de certificación
- Cualquier información cuya publicidad sea impuesta normativamente.

### *9.4.4.* Responsabilidad de proteger la información

La información de suscriptores y usuarios está restringida a personal autorizado y protegida de usos no especificados en las prácticas del negocio.

### *9.4.5.* Notificación y consentimiento para usar la información confidencial

No se difunde información declarada como confidencial sin la aprobación o consentimiento expreso por escrito de la entidad u organización dueña de la información, a menos que exista una imposición legal.

### *9.4.6.* Acceso a la información a partir de proceso judicial o administrativo

Los datos personales de los suscriptores de carácter confidencial solo pueden ser comunicados a terceros sin la autorización del afectado mientras sea solicitud de un proceso judicial o administrativo.

## 9.5. Derechos de propiedad intelectual

Los derechos de propiedad intelectual de la presente Declaración de Prácticas de Certificación pertenecen a Andes SCD.

Andes SCD es la única entidad que dispone de los derechos de propiedad intelectual sobre los certificados digitales que emita.

## 9.6. Obligaciones y garantías

### *9.6.1.* Obligaciones y garantías Andes SCD

**Infraestructura**:

a) 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.
b) Garantizar el cumplimiento de los requisitos impuestos por la legislación vigente.

**Técnicos**

c) Proteger las claves privadas de la Autoridad Certificadora Andes SCD
d) No copiar ni almacenar las claves 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. Para los casos de generación del par de llaves por parte de la Autoridad certificadora Andes SCD, ellas serán ubicadas en el dispositivo software hasta que sean entregados a la Entidad Final según el acuerdo establecido por la organización que haya contratado el servicio; acto seguido será eliminado del sistema de forma automática.
e) Emitir Certificados conformes con el estándar X.509 V3 y de acuerdo a lo solicitado por el suscriptor.
f) Garantizar que se puede determinar la fecha y hora en la que se expidió un certificado ó se revocó.
g) Utilizar sistemas fiables para almacenar los certificados e impedir que personas no autorizadas modifiquen los datos y detectar cualquier indicio que afecte la seguridad.
h) Mantener actualizado el directorio de certificados indicando los certificados emitidos y si están vigentes o revocados.
i) Almacenar en la infraestructura PKI de forma indefinida las CRL y los certificados digitales vigentes, vencidos y revocados.
j) Publicar de manera oportuna en la página WEB los certificados que se encuentran vigentes y las CRL de ROOT CA ANDES SCD S.A y CRL de CA ANDES SCD S.A. Clase II.
k) Informar a los suscriptores la proximidad del vencimiento de su certificado enviando un correo electrónico 15, 7 y 3 días antes del vencimiento.

**Organizacionales**

l) Cumplir lo dispuesto en las Políticas y Prácticas de Certificación.
m) Disponer de personal calificado, con el conocimiento y experiencia necesaria para la prestación del servicio de certificación ofrecido por Andes SCD.

n) Aprobar o denegar las solicitudes de emisión de certificados enviadas por la Autoridad de Registro
o) 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
   - 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
p) Informar a los suscriptores de la revocación de sus certificados inmediatamente a que se produzca dicho evento.
q) Informar Superintendencia de Industria y Comercio sobre los eventos que puedan comprometer la prestación del servicio de Andes SCD.
r) Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor.
s) 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.

### *9.6.2.* Obligaciones y garantías RA

a) Respetar y cumplir las disposiciones estipuladas en las Políticas y Prácticas de Certificación, en el contrato firmado con Andes SCD y en el contrato firmado con cada suscriptor.
b) Exigir al solicitante todos los documentos requeridos para el tipo de certificado que desea obtener.
c) Comprobar la identidad de los solicitantes de certificados verificando la exactitud, suficiencia y autenticidad de la información suministrada por el solicitante.
d) Antes de iniciar el trámite de la emisión del certificado verificar que el solicitante ha realizado el pago del certificado digital que desea adquirir.
e) Comunicar a Andes SCD con la debida celeridad las solicitudes que reciba para emisión y revocación del certificado.
f) Proteger los datos de carácter personal suministrados por el solicitante de acuerdo a la política para el manejo de información confidencial.
g) Hacer entrega del certificado al suscriptor
h) Todos los trámites realizados deben ser firmados electrónicamente por los operadores RA que los realizan, asumiendo de esta forma su plena responsabilidad en el proceso.
i) Formalizar los contratos de expedición de certificados con el suscriptor en los términos y condiciones que establezca la Autoridad Certificadora Andes SCD

### *9.6.3.* Obligaciones y garantías del solicitante

a) Suministrar a la RA información veraz y actualizada conforme a los requerimientos estipulados en la Política de Certificado que aplica para el tipo de certificado que desea obtener.
b) Notificar durante el periodo de validez del certificado cualquier cambio en sus antecedentes contenidos en el certificado. Por ejemplo cambio de nombre, email, etc.

### *9.6.4.* Obligaciones y garantías suscriptores

a) Garantizar la veracidad de las declaraciones que realizó en el momento de solicitar el certificado digital y la información que contiene el certificado
b) La clave privada es personal e intransferible por esta razón se debe custodiar de forma diligente para evitar que otras personas puedan suplantar su identidad y firmar documentos en su nombre o acceder a mensajes confidenciales. La utilización de la clave privada por otras personas es responsabilidad y riesgo del titular, pues si no se toman las medidas necesarias carecería de sentido el sistema de seguridad que se pretende instaurar.
c) Conservar confidencialmente el código de revocación suministrado en el momento de la entrega del certificado, se recomienda guardarlo en un lugar diferente al certificado.
d) Usar el certificado según lo dispuesto en las Políticas y Prácticas de Certificación aplicables para el tipo de certificado
e) Respetar las disposiciones del contrato de suscripción y las limitaciones de uso del certificado.
f) Utilizar la clave privada únicamente con dispositivos criptográficos acordes a los niveles de seguridad exigidos por Andes SCD.
g) Informar a la mayor brevedad posible la existencia de alguna causa de revocación.
h) Informar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
i) No utilizar la clave privada y el certificado desde el momento en que se solicita revocación y tampoco cuando el certificado que avala el par de claves no sea válido.
j) Verificar que la información contenida en el certificado es verdadera y exacta, en caso de existir algún dato incompleto o incorrecto notificar de inmediato a Andes SCD.

### *9.6.5.* Obligaciones y garantías de las partes que confían

a) Verificar antes de depositar su confianza en un certificado su validez en el momento de efectuar cualquier acción basada en los mismos y asegurarse de que el certificado es apropiado para el uso que se pretende.
b) Aceptar que los mensajes o documentos firmados con la clave privada del suscriptor tiene el mismo efecto y validez legal que si se hubiera realizado la firma autógrafa.
c) Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados digitales en los que confía.
d) Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerada como causa de revocación.

## 9.7. Limitaciones de responsabilidad

En las siguientes circunstancias Andes SCD no se hará responsable

a) Desastres naturales o cualquier otro caso de fuerza mayor
b) Fallos o problemas en el servicio de Internet
c) Uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente DPC, utilizar un certificado revocado o por depositar confianza en el sin antes verificar el estado del mismo.

d) Por el uso fraudulento de los certificados o CRL's (Lista de certificados revocados).
e) Por daños y/o perjuicios producto de la errada interpretación de las Prácticas de Certificación por parte de usuarios y suscriptores en el uso de los servicios.
f) Por el incumplimiento de las obligaciones establecidas para el suscriptor o usuarios en la normativa vigente
g) Por el contenido de los mensajes o documentos firmados o por el contenido de páginas web que posean un certificado
h) Por prácticas no notificadas a Andes SCD que afecten la clave privada del suscriptor permitiendo su uso por terceros (Ej. robo, perdida ó compromiso)
i) Por la no recuperación de documentos cifrados con la clave pública del suscriptor
j) Fraude en la documentación presentada por el solicitante o datos ingresados de forma incorrecta en la solicitud por el operador de la RA.
k) Por uso del certificado por parte del suscriptor fuera de su periodo de vigencia o cuando Andes SCD haya informado la revocación del certificado.

En el contrato firmado con el suscriptor se obliga al suscriptor a indemnizar a Andes SCD como entidad certificadora por cualquier acto u omisión que provoque daños, pérdidas, deudas y gastos procesales en los que Andes SCD pudiera incurrir, que sean causados por la utilización y publicación de los certificados y que provenga de:

a) Incumplimiento de términos y obligaciones establecidos en la Declaración de Prácticas de Certificación.
b) Falsedad en los datos suministrados por los suscriptores
c) Omisión en hechos fundamentales que afectan la naturaleza del certificado
d) Incumplimiento en las custodia de claves privadas

## 9.8. Indemnizaciones

Andes SCD incluye en los instrumentos jurídicos que le vinculen con el suscriptor las cláusulas de indemnización en caso de infracción de sus obligaciones legales o contractuales.

El suscriptor debe indemnizar a Andes SCD como entidad certificadora por cualquier acto u omisión que provoque daños, pérdidas, deudas y gastos procesales en los que Andes SCD pudiera incurrir, que sean causados por la utilización y publicación de los certificados y que provenga de:

a) Incumplimiento de términos y obligaciones establecidos en la declaración de prácticas de certificación.
b) Falsedad en los datos suministrados por los suscriptores
c) Omisión en hechos fundamentales que afectan la naturaleza del certificado
d) Incumplimiento en las custodia de claves privadas

## 9.9. Término y terminación

### *9.9.1.* Terminación de disposiciones

La Declaración de Prácticas de Certificación y cada una de las Políticas de Certificación entran en vigor desde el momento en que se publican en la página web de Andes SCD, a partir de ese momento la versión anterior del documento queda derogada y la nueva versión reemplaza íntegramente la versión anterior. Andes SCD conserva en el repositorio las anteriores versiones de la DPC y de cada PC.

#### *9.9.2.* Efecto de terminación y supervivencia

Para los certificados digitales que hayan sido emitidos bajo una versión antigua de DPC o PC aplica la nueva versión de la DPC o PC en todo lo que no se oponga a las declaraciones de la versión anterior.

### 9.10. Notificación individual y comunicación con los participantes

Andes SCD notifica los cambios en la presente política de certificación mientras estos cambios sean relevantes que afecten las declaraciones y procedimientos del servicio de certificación digital, en cada notificación se especificara el texto de las secciones que sufrieron cambios. No se procede a notificación cuando los cambios son no relevantes como errores tipográficos, URL, información de contacto y actualización de referencias.

### 9.11. Procedimiento de cambio en las DPC y PC

#### *9.11.1.* Procedimiento de cambio

El procedimiento de cambio de la Declaración de Practicas de Certificación y las Políticas de certificación es el siguiente:

- El comité de Políticas y Seguridad realiza los cambios que considere pertinentes sobre las DPC y las PC siguiendo protocolo de Análisis y Aprobación de la Política identificado con el OID 1.3.6.1.4.1.31304.100.2.1.

- Los cambios realizados en la DPC o PC son analizados por el área directiva de Andes SCD para su estudio y aprobación.

- El auditor interno procede a validar los cambios aprobados sobre la DPC y la PC y genera un informe de diagnóstico donde se relacionan las conformidades y no conformidades encontradas en la validación.

- La DPC y PC actualizada es publicada en la página web de Andes SCD si el informe diagnóstico del auditor interno tiene resultado conforme.

  **Nota**: En la página web de Andes SCD se mantiene un histórico de versiones de la DPC y PC de entidad final a partir de la versión vigente el 23 de Marzo de 2011, fecha en que la Superintendencia de Industria y Comercio autorizo a Andes SCD para operar como Entidad de Certificación mediante la resolución 14349.

- Se comunica a los usuarios de los certificados los correspondientes cambios a la DPC ó PC si los cambios pudieran afectar la aceptabilidad de los certificados.

#### *9.11.2.* Mecanismo y periodo de notificación

En caso de que el Comité de Políticas y Seguridad de Andes SCD considere que los cambios a la DPC ó PC pueden afectar a la aceptabilidad de los certificados para propósitos específicos se comunica a los usuarios de los certificados correspondientes a la PC o DPC modificada que se ha efectuado un cambio y que deben consultar la nueva DPC que está disponible en la página web.

#### *9.11.3.* Circunstancias bajo las cuales la OID debe cambiarse

En caso de que los cambios de la DPC y PC no afecten a la aceptabilidad de los certificados se procede al incremento del número menor de versión en el documento y el incremento en el último número del identificador de objeto (OID) que lo representa. No se

considera necesario comunicar este tipo de modificaciones a los usuarios de los certificados correspondientes a la PC ó DPC modificada.

En caso de que los cambios de la DPC y PC puedan afectar la aceptabilidad de los certificados para propósitos específicos se procede al incremento en el número mayor de versión del documento y la puesta en cero del número menor de la misma. También se modifican los 2 últimos números del identificador de objeto que lo representa. Este tipo de modificaciones se comunicara a los usuarios de los certificados correspondientes a la PC o DPC.

### 9.12. Prevención y Resolución de disputas

Si desea comunicar a Andes SCD cualquier queja, disputa ó reclamación en relación con el contenido del presente documento ó en general con la prestación del servicio de certificación, envíe un email al correo electrónico comite.reclamaciones@andesscd.com.co y detalle los aspectos relativos a la reclamación, esta notificación será estudiada por el área Jurídica de Andes SCD a fin de aclarar la controversia ó lograr una solución para la reclamación.

### 9.13. Ley aplicable

El funcionamiento y las operaciones realizadas por la Autoridad Certificadora Andes SCD, así como la presente Declaración de Prácticas de Certificación y las Políticas de Certificación aplicables a cada tipo de certificado 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.

### 9.14. Cumplimiento con la ley aplicable

Andes SCD manifiesta el cumplimiento de la ley 527 de 1999 y que la Declaración de Practicas de Certificación es satisfactoria de acuerdo a los requisitos establecidos por la Superintendencia de Industria y comercio.

| CONTROL DE CAMBIOS RESPECTO DPC V 1.3 | |
|---|---|
| **Descripción del cambio** | **Sección DPC** |
| Se modifica introducción para incluir resolución de autorización SIC | Introducción |
| Se actualiza el OID, versión de DPC, fecha de emisión y dirección de publicación de la DPC V 1.4 | 1.1 |
| Se incluye definición de PKCS#12 | 1.4 |
| Se actualizan los datos del certificado CA Clase II | 1.6.1 |
| Se incorpora el tipo de certificado Función Pública y Persona Jurídica dentro del catálogo de servicios de Andes SCD | 1.8.2 |
| Se actualizo dirección física y teléfono de las instalaciones de Andes SCD | 1.9 |
| Se indican las CRL que se publican en el histórico de CRL y se determina el tiempo de publicación. | 2.1.2 |
| Se incluye método para demostrar la posesión de la clave privada cuando se entrega el certificado en archivo PKCS12 y se indica la forma de Autenticación de identidad de Solicitantes y Suscriptores de certificados en archivo PKCS12. | 3.2 |
| Se actualizo periodo de emisión de CRL Clase I y Clase II | 4.4.7 |