



POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA

Andes SCD S.A.

2022



| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

Tabla de Contenido

| | | |
|----------|---|----|
| 1. | Presentación del documento..... | 5 |
| 1.1. | Nombre del documento e Identificación | 5 |
| 1.2. | Referencias | 5 |
| 1.3. | Administración de la política..... | 5 |
| 1.3.1. | Organización que administra el documento | 6 |
| 1.3.2. | Persona de contacto | 6 |
| 1.3.3. | Procedimientos de aprobación de la política | 6 |
| 1.3.4. | Publicación del documento | 6 |
| 1.4. | Comunidad de usuarios y aplicabilidad | 6 |
| 1.5. | Ámbito de aplicación | 7 |
| 1.5.1. | Usos del certificado | 7 |
| 1.5.2. | Límites de uso de los certificados | 8 |
| 1.5.2.1. | Límite de uso de los certificados en sistemas operativos..... | 8 |
| 1.5.3. | Prohibiciones de uso de los certificados | 8 |
| 1.5.4. | Minutas y contratos | 9 |
| 2. | Publicación y registro de certificados | 10 |
| 3. | Identificación y autenticación..... | 10 |
| 3.1. | Nombres..... | 10 |
| 3.1.1. | Tipos de nombres..... | 10 |
| 3.1.2. | Necesidad para los nombres de ser significativos | 10 |
| 3.1.3. | Anónimos y pseudónimos en los nombres..... | 11 |
| 3.1.4. | Reglas para interpretar los formatos de nombre | 11 |
| 3.1.5. | Singularidad de los nombres | 11 |
| 3.2. | Aprobación de la identidad | 11 |
| 3.2.1. | Método para demostrar la posesión de la llave privada | 11 |
| 3.2.2. | Autenticación de la identidad del solicitante | 11 |

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

| | |
|---|----|
| 3.2.3. Información no verificada sobre el solicitante..... | 13 |
| 3.2.4. Tiempos de Respuesta | 13 |
| 3.2.5. Identificación y autenticación para solicitar revocación | 14 |
| 4. Ciclo de vida del certificado y procedimientos de operación | 14 |
| 4.1. Solicitud de certificados..... | 14 |
| 4.1.1. Quien pueden solicitar la emisión de un certificado | 14 |
| 4.1.2. Procedimiento para solicitar certificado..... | 14 |
| 4.1.4. Publicación del certificado por Andes SCD | 15 |
| 4.1.5. Par de llaves y uso del certificado | 15 |
| 4.1.5.1. Por parte del suscriptor | 15 |
| 4.1.5.2. Por parte de usuarios que confían | 16 |
| 4.2. Renovación de certificados-Par de llaves | 16 |
| 4.2.1 Renovación de llaves del certificado..... | 16 |
| 4.3. Modificación de certificados | 16 |
| 4.4 Suspensión de Certificado | 16 |
| 4.5. Revocación de certificados..... | 16 |
| 4.6. Reposición de certificados | 17 |
| 4.7. Servicios de estado de certificado..... | 17 |
| 4.8. Vigencia de los certificados..... | 18 |
| 5. Controles de seguridad | 18 |
| 6. Controles de seguridad técnica | 18 |
| 6.1. Generación de llaves e instalación | 18 |
| 6.1.1. Generación del par de llaves..... | 18 |
| 6.1.2. Entrega de la llave privada al suscriptor..... | 18 |
| 6.1.3. Entrega de la llave pública al emisor del certificado..... | 19 |
| 6.1.4. Distribución de la llave pública del suscriptor..... | 19 |
| 6.1.5. Distribución de la llave pública de Andes SCD a los usuarios | 19 |

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

| | |
|---|----|
| 6.1.6. Periodo de utilización de la llave privada | 19 |
| 6.1.7. Tamaño de las llaves | 19 |
| 6.2. Controles de protección de la llave privada..... | 19 |
| 6.3. Dispositivos Criptográficos admitidos..... | 21 |
| 6.3.1. Riesgos asociados | 21 |
| 6.4. Otros aspectos de administración del par de llaves | 22 |
| 6.4.1. Archivo de la llave pública | 22 |
| 6.4.2. Periodos operacionales del certificado y periodos de uso del par de llaves | 22 |
| 6.5. Datos de activación | 22 |
| 6.5.1. Generación de datos de activación e instalación | 22 |
| 6.5.2. Protección de datos de activación..... | 22 |
| 6.6. Controles de seguridad informática..... | 22 |
| 6.7 Terminación de CA o RA | 22 |
| 7. Perfiles de certificado, CRL y OCSP | 23 |
| 7.1. Contenido del certificado | 23 |
| 7.2. Perfiles de certificado..... | 24 |
| 7.2.1. Número de versión | 24 |
| 7.2.2. Extensiones del certificado..... | 24 |
| 7.2.3. Identificadores de objeto de los algoritmos | 25 |
| 7.2.4. Formatos de nombres | 25 |
| 7.2.5. Restricciones de nombre..... | 25 |
| 7.2.6. Objeto identificador de la política de certificación | 25 |
| 7.2.7. Sintaxis y semántica de los calificadores de la política | 26 |
| 7.3. Perfil de la CRL | 26 |
| 7.3.1. Número de versión..... | 26 |
| 7.3.2. CRL y extensiones | 26 |
| 7.4. Perfil OCSP | 27 |

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

| | |
|---|----|
| 7.4.1. Número de versión | 27 |
| 7.4.2. Extensiones OCSP | 27 |
| 8. Auditoría y otras valoraciones | 27 |
| 9. Negocio y materias legales | 27 |
| 9.1. Tarifas | 27 |
| 9.2. Responsabilidad financiera | 27 |
| 9.3. Confidencialidad de la información | 27 |
| 9.4. Derechos de propiedad intelectual | 28 |
| 9.5. Derechos y deberes | 28 |
| 9.5.1. Derechos y deberes de ANDES SCD | 28 |
| 9.5.2. Derechos y deberes del solicitante | 28 |
| 9.5.3. Derechos y deberes del suscriptor | 28 |
| 9.5.4. Prohibiciones para el suscriptor: | 28 |
| 9.6. Principio de Imparcialidad | 28 |
| 9.7. Limitaciones de responsabilidad | 29 |
| 9.8. Indemnizaciones | 29 |
| 9.9. Término y terminación | 29 |
| 9.10. Procedimiento de cambio en las especificaciones | 29 |
| 9.11. Prevención de disputas | 29 |
| 9.12. Ley aplicable y cumplimiento con la ley aplicable | 29 |
| 10. Control de Cambios | 30 |

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

Introducción

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

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

1. Presentación del documento

1.1. Nombre del documento e Identificación

| | |
|-------------------|---|
| Documento | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA |
| Descripción | El certificado de Comunidad Académica acredita la identidad del suscriptor y su calidad como docente, estudiante, egresado, administrativo, asociado, padre de familia o miembro de una comunidad académica, y le permite al suscriptor firmar documentos digitalmente en su propio nombre e interés. |
| Identificador OID | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| Versión | V 6.0 |
| Fecha de emisión | 05 de Diciembre de 2022 |
| Ubicación | https://www.andesscd.com.co/docs/pc_comunidadacademica.pdf |

1.2. Referencias

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

- ETSI EN 319 411-2: Policy Requirements for certification authorities issuing qualified certificates.
- ETSI EN 319 411-1: Policy Requirements for certification authorities issuing public key certificates.

1.3. Administración de la política

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

1.3.1. Organización que administra el documento

Nombre : Comité de Políticas y Seguridad
Dirección : Calle 26 # 69c-03 Torre B oficina 701.
Email : comite.politicas.seguridad@andesscd.com.co
Teléfono : PBX 601 745 6884

1.3.2. Persona de contacto

Razón social : Andes Servicio de Certificación Digital S.A SIGLA ANDES SCD SA.
Nombre : Sandra Cecilia Restrepo Martinez – Gerente General
Dirección : Calle 26 # 69c-03 Torre B oficina 701.
Email : info@andesscd.com.co
Teléfono : PBX 601 7456884

1.3.3. Procedimientos de aprobación de la política

La Política de Certificación de Comunidad Académica de ANDES SCD es administrada por el Comité de Políticas y Seguridad y es aprobada por la Gerencia General de ANDES SCD, siguiendo el procedimiento de información documentada.

1.3.4. Publicación del documento

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

1.4. Comunidad de usuarios y aplicabilidad

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

Autoridad de certificación (CA)

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

Autoridad de registro (RA)

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

Suscriptores

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

Solicitantes

El solicitante es aquella persona física que desea acceder a los servicios de certificación digital al adquirir un certificado de Comunidad Académica emitido por Andes SCD. En ninguna circunstancia se aceptan solicitudes de este tipo de certificados a nombre de personas que no demuestren estar vinculadas como docente, estudiante, egresado, administrativo, asociado, padre de familia o miembro de una comunidad académica.

Usuarios

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

1.5. Ámbito de aplicación

1.5.1. Usos del certificado

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

Autenticación de identidad

El certificado puede utilizarse para identificar a una persona física como docente, estudiante, egresado, administrativo, asociado, padre de familia o miembro de una comunidad académica en el ámbito de su actividad.

Firma digital

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

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

Cifrado de información

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

1.5.2. Límites de uso de los certificados

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

1.5.2.1. Límite de uso de los certificados en sistemas operativos

Para el uso del certificado tenga en cuenta las siguientes formas de entrega:

- Token Virtual:

Para el uso del token virtual es indispensable contar con el sistema operativo Windows XP service pack 2 y en adelante; para el sistema operativo MacOs es requerido utilizar el servicio de firma en línea suministrado por Andes SCD a través de nuestra página web.

- Token Físico:

Para el uso del token físico es indispensable contar con el sistema operativo Windows seven service pack 2 en adelante; para sistema operativo MacOs se debe contar con la versión Monterrey 12.0.1 y en adelante, así como procesador Intel, para garantizar su funcionamiento.

1.5.3. Prohibiciones de uso de los certificados

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

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

1.5.4. Minutas y contratos

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

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

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

- a) Tipo de certificado
- b) Referencia PC OID
- c) Serial del certificado
- d) Inicio de vigencia
- e) Fin de vigencia
- f) Titular del certificado
- g) Entidad
- h) Forma entrega certificado

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

i) Código de Revocación

2. Publicación y registro de certificados

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

3. Identificación y autenticación

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

3.1. Nombres

3.1.1. Tipos de nombres

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

| Abrev | Nombre | Descripción |
|------------------------|------------------------------|---|
| CN | <u>Nombre</u> | Nombres y apellidos completos del suscriptor |
| S | <u>Serial</u> | Número documento identificación |
| E | <u>Email</u> | Correo electrónico del suscriptor |
| C | <u>País</u> | Abreviatura del país donde reside el suscriptor |
| ST | <u>Departamento</u> | Nombre departamento donde reside el suscriptor |
| L | <u>Ciudad</u> | Nombre municipio donde reside el suscriptor |
| STREET | <u>Dirección</u> | Dirección donde reside el suscriptor |
| T | <u>Título</u> | Indica el tipo de vinculación del suscriptor con la comunidad académica |
| 1.3.6.1.4.1.4710.1.3.2 | | Número documento + dv de la entidad |
| O | <u>Organización</u> | Razón social de la entidad o Comunidad Académica. |
| OU | <u>Unidad Organizacional</u> | Comunidad Académica Emitido por Andes SCD Calle 26 #69c-03 Torre B oficina 701. |

3.1.2. Necesidad para los nombres de ser significativos

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

3.1.3. Anónimos y pseudónimos en los nombres

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

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

3.1.4. Reglas para interpretar los formatos de nombre

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

3.1.5. Singularidad de los nombres

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

3.2. Aprobación de la identidad

3.2.1. Método para demostrar la posesión de la llave privada

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

3.2.2. Autenticación de la identidad del solicitante

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

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

| Requisito | Solicitud presencial | Solicitud remota o convenio |
|--|---|---|
| Cédula de ciudadanía o documento que acredite la identidad (Ampliada a 150% y legible) | Presentar original y Fotocopia documento | Se requiere documento escaneado |
| RUT o documento equivalente que acredite identificación de la entidad (Documento completo y legible, es opcional si presenta cámara de comercio - Fecha de expedición menor a 90 días) | Presentar original y Fotocopia documento | Se requiere documento digital en PDF |
| Documento o evidencia digital emitido por la institución educativa donde haga constar la relación con el solicitante (documento legible con requisitos de la siguiente tabla) | Presentar Fotocopia documento | Se requiere documento digital en PDF |
| Validación de Identidad (realizar el proceso de enrolamiento y autenticación satisfactoriamente) ó Solicitud notariada de certificado de firma digital (Documento autenticado (presentación personal ante notaria) donde se solicita la emisión del certificado de Comunidad académica y se informa: nombre completo, dirección – ciudad de residencia, teléfono y correo electrónico personal- Fecha de expedición menor a 90 días) | Se requiere resultado de Validación de identidad mayor a 70% ó documento digital en PDF | Se requiere resultado de Validación de identidad mayor a 70% ó documento digital en PDF |

Requisitos mínimos del documento que acredita vinculación de la persona a la entidad

| Requisito | Observación |
|---|--|
| Documento con membrete | Encabezado y/o pie de página con nombre de la entidad, imagen corporativa, dirección, teléfono de contacto |
| Fecha no superior a 30 días | La fecha de emisión del documento no debe superar los 30 días calendario |
| Acreditación de la identidad de la persona que pertenece a la entidad | Debe incluir nombre completo, tipo y número de identificación e indicar de forma explícita el cargo que desempeña la persona en la entidad. |
| Nombre completo, área y firma de quien emite el documento | Debe incluir el nombre completo, área a la que pertenece y firma digital o manuscrita de la persona que autoriza la emisión del certificado por parte de la empresa. |

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

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

Las solicitudes presenciales serán registradas a través de la página web de Andes SCD por el área de Servicio al Cliente.

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

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

3.2.3. Información no verificada sobre el solicitante

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

3.2.4. Tiempos de Respuesta

El plazo para procesar una solicitud por parte de la RA de ANDES SCD, es de uno a dos días hábiles desde el momento de recibir la documentación e información completa. En caso de presentarse inconsistencias con la documentación suministrada o validación de identidad, los agentes de la RA enviarán un email con un enlace para que el solicitante actualice la información o documentación requerida, si transcurridos 3 días hábiles desde el envío de la notificación no se ha generado la actualización y ante la imposibilidad de contactar al solicitante, la solicitud podrá ser rechazada y el solicitante deberá registrar una nueva solicitud adjuntando la documentación correspondiente.

Cuando el formato de entrega sea token físico, el tiempo de entrega del certificado digital posterior a la emisión, depende del lugar de destino, para ciudades principales el tiempo de entrega será de 1 a 2 días

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

hábiles, para los demás destinos nacionales el tiempo de entrega será de 2 a 3 días hábiles, para destinos especiales o ante la imposibilidad de contactar al suscriptor el tiempo de entrega podrá tomar hasta 5 días hábiles.

3.2.5. Identificación y autenticación para solicitar revocación

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

- Al propio suscriptor, en cuyo caso debe usar el código de revocación que se le entregó en el momento de adquirir el certificado.
- Al representante autorizado de la comunidad académica a la cual está vinculado el suscriptor, en cuyo caso debe notificar formalmente por escrito a Andes SCD el motivo por el cual se solicita la revocación del certificado de Comunidad académica emitido para el suscriptor.
- Los operadores autorizados de Andes SCD o de la jerarquía de certificación pueden revocar cualquier certificado en aquellos casos en que se incurra a las circunstancias establecidas en la Declaración de Prácticas de Certificación.

4. Ciclo de vida del certificado y procedimientos de operación

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

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

4.1. Solicitud de certificados

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

4.1.1. Quien pueden solicitar la emisión de un certificado

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

4.1.2. Procedimiento para solicitar certificado

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

4.1.3 Aceptación del certificado.

El procedimiento para la aceptación del certificado se encuentra descrito en la Declaración de Prácticas de Certificación DPC. Ver sección “aceptación del certificado”.

4.1.4. Publicación del certificado por Andes SCD

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

4.1.5. Par de llaves y uso del certificado

4.1.5.1. Por parte del suscriptor

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

El suscriptor solo puede utilizar la llave 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 par de llaves asociado a los certificados de entidad final emitidos por Andes SCD tienen habilitados los siguientes usos:

- Firma Digital
- No repudio
- Cifrado de información

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

El par de llaves asociado a los certificados de las CA subordinadas de Andes SCD tienen habilitados los siguientes usos:

- Firma digital
- Firma de certificados
- Firma CRL

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

4.1.5.2. Por parte de usuarios que confían

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

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

4.2. Renovación de certificados-Par de llaves

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

4.2.1 Renovación de llaves del certificado

El suscriptor podrá realizar la renovación del certificado con un nuevo par de llaves, mediante la solicitud de emisión del certificado cuando este haya caducado o haya sido revocado.

4.3. Modificación de certificados

Los certificados digitales emitidos por Andes SCD no pueden ser modificados. Toda modificación sobre el contenido de los certificados implica la revocación y la emisión de un nuevo certificado el cual estará sujeto a proceso de solicitud y verificación, cumpliendo los requisitos establecidos en la presente política de certificación

4.4 Suspensión de Certificado

Los certificados digitales emitidos por ANDES SCD no pueden ser suspendidos. Toda suspensión sobre el estado del certificado implica la revocación y la emisión de un nuevo certificado el cual estará sujeto a proceso de solicitud y verificación cumpliendo los requisitos establecidos en la presente política de certificación

4.5. Revocación de certificados

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

ANDES SCD, publica la CRL cada 24 horas, la última CRL emitida para cada CA contiene todos los certificados emitidos por la respectiva CA que se encuentran revocados a la fecha de generación de la CRL. Se recomienda al usuario revisar la fecha de la CRL para comprobar que es la emitida recientemente.

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

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

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

4.6. Reposición de certificados

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

- Pérdida del dispositivo Token
- Pérdida o exposición del PIN del certificado
- Cambio de la información del titular de la firma digital, excepto el número de identificación

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

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

El procedimiento para solicitar la reposición de un certificado se compone de los siguientes procedimientos.

- Revocación de certificado.
- Solicitud de emisión de certificado.

El suscriptor deberá seguir los dos procedimientos nombrados anteriormente, cumpliendo las condiciones establecidas por Andes SCD e informando el motivo de la reposición formalmente en la solicitud.

4.7. Servicios de estado de certificado

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

4.8. Vigencia de los certificados

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

5. Controles de seguridad

Los sistemas y equipamientos empleados por ANDES SCD para ofrecer el servicio de certificación se encuentran ubicados físicamente en un Data Center diseñado con especificaciones con las más 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 y disponibilidad. En caso de presentarse un incidente con su Data Center principal, ANDES SCD cuenta con un centro de datos alternativo que cuenta con óptimos mecanismos de seguridad para garantizar la continuidad en la prestación de los servicios.

La infraestructura tecnológica que soporta los servicios de certificación que son monitoreados continuamente a través de un NOC/SOC para identificar cualquier tipo de alerta o incidente que pueda comprometer la seguridad o disponibilidad en la prestación de los servicios.

Los demás controles procedimentales, de seguridad física y de seguridad personal, se encuentran especificados en la Declaración de Prácticas de Certificación de Andes SCD.

6. Controles de seguridad técnica

6.1. Generación de llaves e instalación

6.1.1. Generación del par de llaves

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

6.1.2. Entrega de la llave privada al suscriptor

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

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

El mecanismo de entrega de la llave privada a titulares de Certificados de Comunidad Académica se describe en la DPC. En la sección “entrega de la llave privada al suscriptor”.

6.1.3. Entrega de la llave pública al emisor del certificado

El mecanismo de entrega de la llave pública a titulares de Certificados de Comunidad académica se describe en la DPC. Sección “entrega de la llave publica al emisor del certificado”

6.1.4. Distribución de la llave pública del suscriptor

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

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

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

6.1.6. Periodo de utilización de la llave privada

El periodo de utilización de la llave privada es el mismo tiempo de la vigencia del certificado de Comunidad académica o menos si el certificado es revocado antes de caducar.

En la DPC de Andes SCD se detalla el periodo de utilización de la llave privada de la CA raíz y de la CA emisora de certificados de Clase II o de Entidad Final.

6.1.7. Tamaño de las llaves

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

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

6.2. Controles de protección de la llave privada

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

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

| | |
|---------------------------------|--|
| Destrucción de llave privada | <p>La destrucción de la llave privada puede realizarla el propio suscriptor utilizando las funciones que provee el dispositivo TOKEN, teniendo cuidado de no afectar otras llaves privadas almacenadas en el dispositivo.</p> <p>La destrucción de la llave privada del suscriptor puede realizarla el propio suscriptor eliminando la llave privada correspondiente al CSR enviado a Andes SCD.</p> |
|---------------------------------|--|

6.3. Dispositivos Criptográficos admitidos

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

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

6.3.1. Riesgos asociados

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

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

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

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

6.4. Otros aspectos de administración del par de llaves

6.4.1. Archivo de la llave pública

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

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

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

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

6.5. Datos de activación

6.5.1. Generación de datos de activación e instalación

El suscriptor debe generar los datos de activación de su TOKEN cambiando el PIN inicial que trae por defecto el dispositivo.

El PIN debe ser custodiado por el suscriptor de modo que no sea conocido por nadie más y se garantice el control exclusivo del TOKEN.

6.5.2. Protección de datos de activación

El PIN o dato de activación del TOKEN debe ser personalizado por el solicitante antes de generar su par de llaves o si existe la sospecha de que un tercero conoce este dato.

Para cambiar el PIN es necesario descargar el aplicativo software que ofrece el fabricante del TOKEN y que se encuentra disponible en la página web de Andes SCD.

6.6. Controles de seguridad informática

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

6.7 Terminación de CA o RA

En la Declaración de Prácticas de Certificación se describen los procedimientos para la notificación y terminación de la CA o RA.

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

7. Perfiles de certificado, CRL y OCSP

7.1. Contenido del certificado

| Formato de certificados de Comunidad académica | | |
|--|--|--|
| Campo | Descripción | Valor |
| Versión | Versión del certificado | V3 |
| Serial number | Número que identifica al certificado | Número de serie del certificado del suscriptor |
| Algoritmo de firma | Algoritmo usado por Andes SCD para firmar el certificado | SHA256WithRSA |
| Algoritmo hash de firma | Algoritmo usado para obtener el resumen de los datos | Sha256 |
| Emisor (issuer) | Datos de la CA subordinada de entidad final que emitió el certificado. | Ver en el certificado los datos de la CA Clase II o la CA Subordinada de la CA Clase III |
| Valido desde | Fecha y hora UTC inicio validez | Fecha de inicio de la validez del certificado |
| Válido hasta | Fecha y hora UTC fin validez | Fecha final de la validez del certificado |
| Asunto | CN | Nombre completo del suscriptor |
| | Serial Number | Número documento identificación del suscriptor |
| | E | Correo electrónico del suscriptor |
| | C | Abreviatura del país donde reside el suscriptor |
| | ST | Nombre departamento donde reside suscriptor |
| | L | Nombre municipio donde reside el suscriptor |
| | STREET | Dirección donde reside el suscriptor |
| | T | Indica el tipo de vinculación del suscriptor con la comunidad académica. |
| | O | Nombre de la universidad o Comunidad Académica. |
| | OU | Nombre de facultad y carrera a la que se encuentra vinculado |
| OU | Comunidad académica Emitido por Andes SCD Av. Calle 26 NO 69C-03 | |
| Llave pública | Llave pública del titular del certificado | RSA (2048 Bits) |
| Extensiones | Extensiones utilizadas en los certificados | Ver sección "extensiones del certificado" de este documento para más detalles. |

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

| | | |
|-----------------------------|--|---|
| Algoritmo de identificación | Algoritmo utilizado para obtener la huella digital del certificado | Sha1 |
| Huella digital | La síntesis o huella digital de los datos del certificado | fingerprint |
| Uso de la llave | Propósitos para los cuales se debe utilizar el certificado. | Firma Digital No repudio Cifrado de información |

7.2. Perfiles de certificado

7.2.1. Número de versión

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

7.2.2. Extensiones del certificado

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

| Extensiones Certificados Comunidad académica según estándar X.509V3 | |
|---|---|
| Nombre | Valor |
| Acceso a la información de la entidad emisora | Método de acceso=Protocolo de estado de certificado en línea Dirección URL=http://ocsp.andesscd.com.co |
| Identificador de la llave del titular | Identificador de llave del titular |
| Identificador de llave entidad emisora | Identificador de la llave de la CA de Andes SCD que emitió el certificado |
| Puntos de distribución de la CRL | URL de publicación de CRL de la CA que emitió el certificado. |
| Uso de la llave | Firma Digital No repudio Cifrado de información |
| Uso mejorado de la llave | Autenticación del cliente Correo Seguro |
| Nombre alternativo del titular | Email del suscriptor RFC 822 Name (e-mail address) |

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

| | |
|---------------------------|--|
| Restricciones Básicas | Tipo de asunto=Entidad final Restricción de longitud de ruta=Ninguno |
| Directiva de certificados | <p>[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.31304.1.2.2.6.0 [1,1]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=La utilización de este certificado está sujeta a las Políticas de Certificado de Comunidad académica (PC) y Prácticas de Certificación (DPC) establecidas por Andes SCD.</p> <p>[1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: URL de DPC vigente</p> |

7.2.3. Identificadores de objeto de los algoritmos

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

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

7.2.4. Formatos de nombres

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

7.2.5. Restricciones de nombre

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

7.2.6. Objeto identificador de la política de certificación

Las políticas y prácticas de certificación son identificadas mediante un número único denominado OID, el OID asignado a la presente política es 1.3.6.1.4.1.31304.1.2.2.6.0

En la Declaración de Prácticas de Certificación en la sección objeto identificador de la política de certificación se encuentra más información respecto a este tema.

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

7.2.7. Sintaxis y semántica de los calificadores de la política

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

- **Policy identifier:** Contiene el identificador de la Política de Certificado Comunidad académica
- **CPS:** Indica la URL donde esta publicada la Declaración de la Practicas de Certificación (DPC) para ser consultadas por los usuarios
- **User Notice:** contiene el texto “La utilización de este certificado está sujeta a las PC de comunidad academica y a las DPC establecidas por Andes SCD”. Código de Acreditación 16 - ECD-004.

7.3. Perfil de la CRL

7.3.1. Número de versión

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

7.3.2. CRL y extensiones

Se emite la lista de revocación CRL según lo estipulado en la RFC 5280

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

7.4. Perfil OCSP

7.4.1. Número de versión

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

7.4.2. Extensiones OCSP

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

8. Auditoría y otras valoraciones

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

9. Negocio y materias legales

9.1. Tarifas

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

| Formato de entrega | 3 meses | 6 meses | 1 año | 2 años |
|--------------------|-----------|-----------|------------|------------|
| Token Virtual | \$ 57,857 | \$ 92,571 | \$ 135,000 | \$ 200,000 |
| Token Físico | N/A | \$ 96,639 | \$ 150,000 | \$ 220,000 |

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

9.2. Responsabilidad financiera

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

9.3. Confidencialidad de la información

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

9.4. Derechos de propiedad intelectual

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

9.5. Derechos y deberes

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

9.5.1. Derechos y deberes de ANDES SCD.

En la Declaración de Prácticas de Certificación se listan los derechos y deberes por parte de la Autoridad de Certificación Andes SCD.

9.5.2. Derechos y deberes del solicitante

En la Declaración de Prácticas de Certificación se listan los derechos y deberes por parte de los solicitantes

9.5.3. Derechos y deberes del suscriptor

En la Declaración de Prácticas de Certificación se listan los derechos y deberes por parte de los suscriptores.

9.5.4. Prohibiciones para el suscriptor:

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

1. Alterar o modificar, en todo o en parte, el certificado digital o el software entregado por ANDES SCD, o permitir que terceras personas lo hagan.
2. Copiar o reproducir en cualquier forma el certificado digital, o permitir su copia o reproducción.
3. Realizar ingeniería inversa, decodificar, desensamblar o realizar cualquier tipo de acción tendiente a conocer o descifrar el código fuente, el código objeto u otra información relevante respecto del certificado digital o del software que se relacione con la prestación del servicio de ANDES SCD.
4. Transferir, ceder o negociar los derechos otorgados en virtud de los servicios de ANDES.
5. Permitir que terceras personas se beneficien de o utilicen, directa o indirectamente, los derechos que se derivan de la prestación de servicios de certificación digital, bajo las condiciones de este documento.
6. Darle al certificado digital un uso distinto de aquel que se desprende de la Declaración de Prácticas de Certificación.

9.6. Principio de Imparcialidad

En las relaciones con los clientes, cualquiera sea tu naturaleza, tamaño, calidad, así como en la prestación de los servicios de ANDES, se actuará de acuerdo con los principios definidos en [la política de Imparcialidad, Integridad e Independencia](#).

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

9.7. Limitaciones de responsabilidad

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

9.8. Indemnizaciones

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

9.9. Término y terminación

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

9.10. Procedimiento de cambio en las especificaciones

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

9.11. Prevención de disputas

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

9.12. Ley aplicable y cumplimiento con la ley aplicable

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

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

10. Control de Cambios

| Versión | Fecha | Detalle | Responsable |
|---------|------------|--|------------------------------|
| 1.1 | 24/02/2011 | Versión inicial autorizada por la SIC según resolución 14349 de marzo 2011 | Comité políticas y seguridad |
| 1.2 | 02/11/2011 | <ul style="list-style-type: none"> - 3.1.1 y 7.1.1 – Se actualiza distinguish name del certificado - 6.1.7 y 7.1.1 – Se aumenta tamaño de las llaves a 2048 - 6 – Se hace referencia a la forma de entrega de certificados PKCS12 - 4.6 – Se ofrece certificados de diferentes vigencias. La vigencia esta explicita en el propio certificado | Comité políticas y seguridad |
| 2.0 | 09/10/2014 | <ul style="list-style-type: none"> - 1.3 - Se actualiza dirección y PBX de Andes SCD - 3.1.1 y 7.1 - Se actualiza atributo OU del DN a Certificado Comunidad académica Emitido por Andes SCD Av. Calle 72 # 9 - 55 Oficina 501 - 3.2.2 - Se actualiza documentos requeridos para emisión de certificado de firma digital - Todo el documento - Se actualiza término p12 por PKCS12 - 6.1.7 - En la sección tamaño de las llaves se elimina el termino mínimo para hacer referencia al tamaño de las llaves generadas por Andes SCD. - 3.1.1 y 7.1 - El 27 enero 2015 se abrevia atributo OU del DN a Comunidad académica Emitido por Andes SCD Av CII 72 9 55 Of 501 | Comité políticas y seguridad |
| 2.1 | 24/11/2015 | <ul style="list-style-type: none"> - 1.1 - Se actualiza versión del documento PC y fecha de emisión - 1.3 - Se actualiza datos de contacto y organización que administra el documento - 1.5.2 - Referencia a OID documento con limitaciones de uso certificados de convenios - 3.1.1 y 7.1 - Se actualiza atributo OU del DN a: Comunidad académica Emitido por Andes SCD Cra 27 86 43 - 7.2.2 - Se actualiza OID PC y URL DPC Directiva de certificados | Comité políticas y seguridad |
| 2.2 | 26/09/2016 | <ul style="list-style-type: none"> - 1.3.2 – Se actualiza email de persona de contacto - 4 – Se limita vigencia máxima del certificado a 730 días. - 4.5 – Se incluye la reposición de certificados. - 4.7 – Se limita vigencia máxima del certificado a 730 días. | Comité políticas y seguridad |

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

| | | | |
|-----|------------|--|---------------------------------|
| | | - 7.2.1 - Se actualiza RFC 3280 por 5280 | |
| 2.3 | 06/01/2017 | <ul style="list-style-type: none"> - 4, 4.7 – Se especifica que la vigencia máxima del certificado son 730 días calendario - 6.1, 6.2, 6.3, 6.4 se elimina forma de entrega PKCS12 - 7.2 URL y versión 2.3 de DPC y PC | Comité políticas y seguridad |
| 2.4 | 22/06/2018 | <ul style="list-style-type: none"> - 1.5.4 Se incluye el apartado minutas y contratos. - 2. Se hace referencia al RFC 4523 relacionado con el LDAP. - 3.2.3 Se hace referencia a autoridad de registro encargada de recopilar las evidencias requeridas. - 3.2.4 se reemplaza termino clave revocación por código revocación - 4. Se suprime el termino contrato de suscripción - 4.5 se incluyó condición para reposición de certificados - 6.1.2 Se hace referencia a los dispositivos criptográficos FIPS 140-2 Nivel 3 para la entrega de la llave privada de los suscriptores. - 6.3 Se hace referencia a los dispositivos criptográficos. - 6.3.1 Se hace referencia a riesgos de los dispositivos criptográficos y recomendaciones de seguridad. - 7.2.2 Se actualiza en la directiva de los certificados el enlace a la DPC - 7.3.2 Se actualiza algoritmo de firma SHA256withRSA - 9.1 Se incluyen tarifas de certificados según vigencia - 9.5.1 Se describen obligaciones y responsabilidades de ANDES SCD. - 9.5.2 Se describen obligaciones del suscriptor. - 9.5.3 Se describen prohibiciones para el suscriptor. - 9.6 Se hace referencia al principio de imparcialidad | Comité políticas y seguridad |
| 2.5 | 16/07/2018 | - 7.2.2 se hace referencia a URL de DPC vigente | Comité de Políticas y seguridad |
| 2.6 | 14/09/2018 | <ul style="list-style-type: none"> - 1.1 Se actualiza fecha de emisión y url descarga de la PC. - 1.3.2 Se actualiza nombre e email del gerente general. - 7.2.2 Se actualiza identificador OID de PC - 7.2.6 Se actualiza identificador OID | Comité de Políticas y seguridad |

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

| | | | |
|-----|------------|---|---|
| 2.7 | 25/11/2019 | <ul style="list-style-type: none"> - 1.3.1, 1.3.2, 3.1.1 Se actualiza dirección y teléfono de la ECD - 3.2.4 se agrega tiempos de respuesta - 4.4 Se actualiza periodos de publicación de la CRL - 5. Se agrega sitios cubiertos en el alcance de acreditación (Noc, Triara, IFX) - 9.1 Se actualizan Tarifas correspondientes al año 2019 - Se eliminan referencias correspondientes a procedimiento de convenios en el apartado 6 | Comité de políticas y seguridad |
| 2.8 | 04/11/2020 | <ul style="list-style-type: none"> - Nombre del documento e Identificación (1.1): Actualización ubicación y versión - Procedimientos de aprobación de la política (1.3.3): Actualización de responsables de revisión y aprobación - Controles de seguridad (5): Actualización de dirección de datacenter y ubicación infraestructura de monitoreo SOC y NOC | Comité de políticas y seguridad |
| 2.9 | 01/02/2021 | <ul style="list-style-type: none"> - Actualización de las normas ETSI TS 101 456 y ETSI TS 102 042 por ETSI EN 319 411-2 y ETSI EN 319 411-1, respectivamente. - Actualización RFC 2459 por RFC 5280. - Se actualiza el OID de la PC. | Comité de Políticas y Seguridad |
| 3.0 | 28/04/2021 | <ul style="list-style-type: none"> - Se actualiza la descripción del nombre del documento, ampliando los suscriptores del presente certificado. - Se actualiza el apartado 1.4. Comunidad de Usuarios y Aplicabilidad, ampliando los suscriptores del presente certificando. - Se actualiza el apartado 1.5.1. Usos del Certificado, ampliando los suscriptores del presente certificando. - Se actualizan los atributos del DN en el apartado 3.1.1. - Se actualiza el apartado 3.2.2. Autenticación de la identidad del solicitante, la tabla de los requisitos y se añade la tabla de requisitos mínimos del documento que acredita vinculación de la persona a la entidad. - Se actualizan los tiempos de respuesta del apartado 3.2.4. - Se actualiza el OID de la PC. - Se actualiza el nombre del cargo del Director de Proyectos y Operaciones. | Comité de Políticas y Seguridad / Analista Senior SGI |



**POLÍTICA DE CERTIFICACIÓN
COMUNIDAD ACADÉMICA**

| | |
|----------------------------------|------------------------------|
| Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| Fecha de vigencia: | 05/12/2022 |
| Versión: | 6.0 |
| Clasificación de la información: | Público |
| Elaboró: | Gerente de Operaciones |
| Revisó: | Comité Políticas y Seguridad |
| Aprobó: | Gerente General |

| | | | |
|-----|------------|---|--|
| 4.0 | 15/06/2022 | <ul style="list-style-type: none"> - -Se actualiza el OID de la PC. - -Se actualiza el cargo "Director de Proyectos y Operaciones" a "Gerente de Operaciones" responsable de elaborar el documento. - -Actualización información numeral 1.1 de acuerdo con la nueva versión del documento. - -Numeral 4.1 se actualiza la definición "emisión" por "solicitud". - -Se incluye el numeral 4.1.3 Aceptación del certificado. - -Se agrega a la definición del numeral 4.2 "Par de llaves". - -Se incluye el numeral 4.2.1 Renovación de llaves del certificado. - -Se incluye el numeral 4.4 Suspensión de certificados. - -En el numeral 4.6 reposición de certificados se incluye el procedimiento para la reposición de certificados. - -Se incluye el numeral 6.7 "Terminación de la CA y RA". - -Se actualiza la última versión del identificador OID en el numeral 7.2.6. - -Se incluye el código de la extensión del certificado en el numeral 7.2.7 sección User Notice - -Se incluye nota aclaratoria en el numeral 9.1 respecto al costo de revocar certificados. | Comité de Políticas y Seguridad / Analista Senior SGI. |
| 5.0 | 12/10/2022 | <ul style="list-style-type: none"> - Se actualiza el identificador OID, la fecha de emisión versión y fecha del documento. - Se actualiza en el numeral 1.3.2 nombre de representante legal y el correo de contacto - Se incluye el numeral 1.5.2.1 Límite de uso de los certificados en sistemas operativos. - Se incluye en el numeral 4.1.3 ver sección aceptación del certificado - En el numeral 4.1.5 se incluye uso de los certificados. - Se modifica numeral 4.3 modificación del certificado de acuerdo con lo exigido por el CEA. - Se modifica numeral 4.4 suspensión del certificado de acuerdo con lo exigido por el CEA. - Se actualiza ítem 5, controles de seguridad. - Se actualiza el numeral 9.1 Tarifas y se incluyen las tarifas para el token virtual. - Se actualiza el título del numeral 9.5 por derechos y deberes. | Comité de Políticas y Seguridad / Analista Senior SGI. |

| | | | |
|---|--|----------------------------------|------------------------------|
|  | POLÍTICA DE CERTIFICACIÓN COMUNIDAD ACADÉMICA | Identificador OID: | 1.3.6.1.4.1.31304.1.2.2.6.0 |
| | | Fecha de vigencia: | 05/12/2022 |
| | | Versión: | 6.0 |
| | | Clasificación de la información: | Público |
| | | Elaboró: | Gerente de Operaciones |
| | | Revisó: | Comité Políticas y Seguridad |
| | | Aprobó: | Gerente General |

| | | | |
|-----|------------|---|--|
| | | - Se modifica el título y el contenido del numeral 9.5.1 Derechos y deberes de Andes SCD. | |
| 6.0 | 05/12/2022 | <ul style="list-style-type: none"> - Se actualiza el OID, Versión y fecha de emisión del documento. - Se incluye en la sección 3.2.2. los tipos de mecanismo con la descripción de validación de la identidad del solicitante (onboarding o carta notariada). | Comité de Políticas y Seguridad / Analista Senior SGI. |

SANDRA CECILIA RESTREPO MARTINEZ
Gerente General