andes
Servicio de Certificación Digital

POLITICA DE CERTIFICACION PERTENENCIA A EMPRESA

2025

Andes SCD S.A.

Tabla de Contenido

Introducción 6

1. Presentación del documento 6

1.1. Nombre del documento e Identificación 6

1.2. Referencias 7

1.3. Administración de la política 7

1.3.1. Organización que administra el documento 7

1.3.2. Persona de contacto 7

1.3.3. Procedimientos de aprobación de la política 7

1.3.4. Publicación del documento 8

1.4. Comunidad de usuarios y aplicabilidad 8

1.5. Ámbito de aplicación 9

1.5.1. Usos del certificado 9

1.5.2. Límites de uso de los certificados 10

1.5.2.1. Límite de uso de los certificados en sistemas operativos 10

1.5.3. Prohibiciones de uso de los certificados 11

1.5.4. Minutas y contratos 12

2. Publicación y registro de certificados 12

3. Identificación y autenticación 13

3.1. Nombres 13

3.1.1. Tipos de nombres 13

3.1.2. Necesidad para los nombres de ser significativos 14

3.1.3. Anónimos y pseudónimos en los nombres 14

3.1.4. Reglas para interpretar los formatos de nombre 14

3.1.5. Singularidad de los nombres 14
3.2. Aprobación de la identidad 14
3.2.1. Método para demostrar la posesión de la llave privada 14
3.2.2. Autenticación de la identidad del solicitante 15
3.2.3. Información no verificada sobre el solicitante 18
3.2.4. Tiempos de Respuesta 18
3.2.4.1. Identificación y autenticación para solicitar revocación 18
4. Ciclo de vida del certificado y procedimientos de operación 19
4.1. Solicitud de certificados 19
4.1.1. Quien pueden solicitar la emisión de un certificado 19
4.1.2. Procedimiento para solicitar certificado 19
4.1.3 Aceptación del certificado. 20
4.1.4. Publicación del certificado por Andes SCD 20
4.1.5. Par de llaves y uso del certificado 20
4.1.5.1. Por parte del suscriptor 20
4.1.5.2. Por parte de usuarios que confían 21
4.2. Renovación de certificados- Par de Llaves 21
4.2.1 Renovación de llaves del certificado 21
4.3. Modificación de certificados 21
4.4 Suspensión de Certificados 21
4.5. Declinación de la Solicitud 22
4.6. Revocación de certificados 22
4.7. Reposición de certificados 23
4.8. Servicios de estado de certificado 23
4.9. Vigencia de los certificados 23

5. Controles de seguridad 24
6. Controles de seguridad técnica 24
6.1. Generación de llaves e instalación 24
6.1.1. Generación del par de llaves 24
6.1.2. Entrega de la llave privada al suscriptor 24
6.1.3. Entrega de la llave pública al emisor del certificado 25
6.1.4. Distribución de la llave pública del suscriptor 25
6.1.5. Distribución de la llave pública de Andes SCD a los usuarios 25
6.1.6. Periodo de utilización de la llave privada 25
6.1.7. Tamaño de las llaves 26
6.2. Controles de protección de la llave privada 26
6.3. Dispositivos Criptográficos admitidos 27
6.3.1. Riesgos asociados 28
6.4. Otros aspectos de administración del par de llaves 29
6.4.1. Archivo de la llave pública 29
6.4.2. Periodos operacionales del certificado y periodos de uso del par de llaves 29
6.5. Datos de activación 29
6.5.1. Generación de datos de activación e instalación 29
6.5.2. Protección de datos de activación 29
6.6. Controles de seguridad informática 30
6.7 Cesación de actividades de la ECD 30
7. Perfiles de certificado, CRL y OCSP 30
7.1. Contenido del certificado 30
7.2. Perfiles de certificado 32
7.2.1. Número de versión 32

7.2.2. Extensiones del certificado 32
7.2.3. Identificadores de objeto de los algoritmos 33
7.2.4. Formatos de nombres 33
7.2.5. Restricciones de nombre 33
7.2.6. Objeto identificador de la política de certificación 34
7.2.7. Sintaxis y semántica de los calificadores de la política 34
7.3. Perfil de la CRL 34
7.3.1. Número de versión 34
7.3.2. CRL y extensiones 34
7.4. Perfil OCSP 35
7.4.1. Número de versión 35
7.4.2. Extensiones OCSP 35
8. Auditoria y otras valoraciones 35
9. Negocio y materias legales 36
9.1. Tarifas 36
9.2. Responsabilidad financiera 36
9.3. Confidencialidad de la información 36
9.4. Derechos de propiedad intelectual 36
9.5. Derechos y deberes 37
9.5.1. Derechos y deberes de ANDES SCD 37
9.5.2. Derechos y deberes del solicitante 37
9.5.3. Derechos y deberes del suscriptor. 37
9.5.4. Prohibiciones para el suscriptor: 37
9.6. Principio de Imparcialidad y No Discriminación 38
9.7. Limitaciones de responsabilidad 38

9.8. Indemnizaciones 38

9.9. Término y terminación 38

9.10. Procedimiento de cambio en las especificaciones 38

9.11. Prevención de disputas 38

9.12. Ley aplicable y cumplimiento con la ley aplicable 38

10. Control de Cambios 39

andes Servicio de Certificación Digital	**POLÍTICA DE CERTIFICACIÓN PERTENENCIA A EMPRESA**	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Fecha de vigencia:	24/01/2025
		Versión:	12
		Clasificación de la información:	Público
		Elaboró:	Director de Operaciones
		Revisó:	Comité Políticas y Seguridad
		Aprobó:	Gerente General

Introducción

La presente Política para Certificados de Pertenencia a empresa 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 de Pertenencia a empresa 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 Pertenencia a empresa o hacer uso de este 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 PERTENENCIA A EMPRESA
Descripción	El certificado de pertenencia a empresa acredita la identidad del suscriptor y su condición de pertenencia, función o empleo en una entidad o persona jurídica, y le permite al suscriptor firmar documentos digitalmente en la calidad que acredita su certificado.
Identificador OID	1.3.6.1.4.1.31304.1.2.5.12
Versión	V 12
Fecha de emisión	24 de Enero de 2025
Ubicación	https://www.andesscd.com.co/docs/pc_pertenenciaempresa.pdf

1.2. Referencias

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

- ETSI 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.

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 2415539

1.3.2. Persona de contacto

Razón social : Andes Servicio de Certificación Digital S.A SIGLA ANDES SCD SA.
Nombre : Sandra Cecilia Restrepo Martínez – Gerente General
Dirección : Calle 26 #69c-03 Torre B oficina 701.
Email : info@andesscd.com.co
Teléfono : PBX 601 2415539

1.3.3. Procedimientos de aprobación de la política

La Política de Certificación de Pertenencia a empresa 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 Pertenencia a empresa 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 Pertenencia a Empresa son emitidos a personas Físicas, acreditan la identidad del titular y su condición de pertenencia, función o empleo en una entidad o persona jurídica 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 Pertenencia a empresa actúa en la calidad que acredita su certificado.

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 Pertenencia a empresa conforme a la presente Política de Certificación. En la Declaración de Prácticas de Certificación se detalla la jerarquía de las Autoridades Certificadoras que conforman Andes SCD.

Autoridad de registro (RA)

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

Suscriptores

El suscriptor es aquella persona física que ha adquirido un certificado de Pertenencia a Empresa emitido por la Autoridad de Certificación Andes SCD para obrar en el entorno electrónico a nombre del cargo o función que desempeña en la entidad 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 Pertenencia a Empresa emitido por Andes SCD.

Bajo ninguna circunstancia se aceptan solicitudes de este tipo de certificados a nombre de personas que no demuestren su vinculación laboral a la entidad o persona jurídica.

Usuarios

El usuario es cualquier persona que voluntariamente deposita su confianza en los certificados de Pertenencia a empresa 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 Pertenencia a empresa 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 miembro de una entidad o persona jurídica en el ámbito de su actividad.

Firma digital

Las firmas digitales realizadas con Certificados de Pertenencia a empresa ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio.

- **Autenticidad del origen**: En una comunicación electrónica el suscriptor puede acreditar válidamente su identidad ante otra persona demostrando la posesión de la llave privada asociada con la respectiva llave pública contenida en el certificado
- **Integridad del documento**: Existe la garantía de que el documento no fue alterado o modificado después de firmado por el suscriptor puesto

que el resumen del documento es cifrado con la llave privada del emisor el cual es el único que está en posesión de esta.

- **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 Pertenencia a empresa 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 10 y superior en versiones 64 y 32 bits; 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.

- Centralizado:

La entrega de certificados bajo el modelo de firma centralizada está condicionada al desarrollo para el consumo de los servicios web expuestos por Andes SCD, para permitir las operaciones de firmado haciendo uso de los certificados custodiados en su infraestructura PKI.

1.5.3. Prohibiciones de uso de los certificados

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

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

1.5.4. Minutas y contratos

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

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

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

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

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 Pertenencia a empresa.

3.1. Nombres

3.1.1. Tipos de nombres

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

Abrev	Nombre	Descripción
CN	Nombre	Nombres y apellidos completos del suscriptor
S	Serial	Número identificación suscriptor
E	Email	Correo electrónico del cargo del suscriptor
C	País	Abreviatura del país donde está ubicada la entidad
ST	Departamento	Nombre del departamento donde está ubicada la entidad
L	Ciudad	Nombre del municipio donde está ubicada la entidad
STREET	Dirección	Dirección donde está ubicada la entidad
T	Titulo	Cargo del suscriptor en la entidad
1.3.6.1.4.1.4710.1.3.2		Número documento + dv de la entidad
O	Organización	Razón social de la entidad o persona jurídica
OU	Unidad Organizacional	Unidad organizacional de la entidad a la cual pertenece el suscriptor. Ej. Operativa, Financiera, Administrativa, etc.
OU	Unidad Organizacional	Pertenencia Empresa 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 Pertenencia a empresa emitido por Andes SCD tiene como característica principal la plena identificación del suscriptor y la asignación de un nombre significativo a su certificado.

3.1.3. Anónimos y pseudónimos en los nombres

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

El nombre de la persona jurídica debe ser la razón social que figura en el RUT, certificado de cámara de comercio, personería jurídica o documento equivalente, no se aceptan siglas o nombres abreviados.
El nombre de la persona natural debe estar conformado por los nombres y apellidos tal y como figura en la cedula de ciudadanía o documento de identificación 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 Pertenencia a empresa 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 Pertenencia a empresa.

3.2.2. Autenticación de la identidad del solicitante

El solicitante puede tramitar su solicitud de emisión de certificado de Pertenencia a empresa de las siguientes formas:

1. **Presencial**: El solicitante realiza la solicitud personalmente en las instalaciones 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.

En todas las solicitudes de certificado de firma digital, la ECD realizará la validación de identidad utilizando los mecanismos con los que dispone para tal fin.

A continuación, se describen los requisitos documentales:

Requisito	Solicitud presencial	Solicitud remota o convenio
Cedula de ciudadanía o documento que acredite la identidad (legible)	Presentar original y Fotocopia documento	Se requiere documento digital en PDF
Documento(s) que acrediten la vinculación de la persona a la entidad (Documento legible que cumpla con los requisitos especificados en el item 3.2.2.1)).	Presentar Fotocopia Documento	Se requiere documento digital en PDF

La documentación indicada en el cuadro anterior se utilizará como soporte adicional. No obstante, nuestras fuentes externas que aseguran y validan la

veracidad de la información, serán nuestra referencia principal y la base para la toma de decisiones en el proceso de estudio y emisión del certificado. En caso de que se detecte alguna novedad o inconsistencia en la información proveniente de estas fuentes, la autoridad de registro podrá solicitar al usuario documentación adicional que respalde y argumente la condición que se desea validar.

3.2.2.1. Información requerida en el documento que acredita vinculación del solicitante a una 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 90 días	La fecha de emisión del documento no debe superar los 90 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, área, correo electrónico o teléfono y firma de quien emite el documento	Debe incluir el nombre, correo electrónico o teléfono, área a la que pertenece y firma digital o manuscrita de la persona que autoriza la emisión del certificado por parte de la empresa.

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

En caso de solicitudes tramitadas por convenio se podrán aceptar otros documentos o evidencias digitales que permitan verificar la relación con la entidad o empresa.

Para el caso de personas vinculadas a empresas por contratos de prestación de servicio o a través de empresas temporales intermediarias aplican las siguientes reglas para el documento que acredita el cargo:

a. Quienes se encuentren vinculados a una empresa como contratistas en virtud de un contrato de prestación de servicios profesionales, deberán aportar una certificación en tal sentido expedida por la organización a la que pertenecen, indicando el cargo y su función principal, solicitando la expedición del respectivo certificado para el contratista interesado.
b. Por su parte, para quienes se encuentren vinculados a la organización, a través de una empresa temporal, deberán aportar una carta elaborada y suscrita por la Empresa de Servicios Temporales, indicando que el trabajador ha sido asignado, en misión o como trabajador temporal, a la empresa relacionada en el certificado a expedir, como el cargo que ocupa.

Sera responsabilidad de las organizaciones relacionadas en el certificado expedido de pertenencia a empresa, el sensibilizar a los contratistas como a los trabajadores en misión, sobre el uso del certificado digital, indicándoles los límites existentes en el uso de este, y las consecuencias a nivel jurídico y administrativo de estampar la firma digital, en documentos que no tengan relación alguna con la organización o con el ejercicio de las funciones asignadas a su cargo.
Adicionalmente el solicitante debe suministrar la siguiente información que permitirá a Andes SCD contactarlo cuando sea necesario:

Requisito	Información adicional
1	País, departamento y ciudad donde reside
2	Dirección y número teléfono fijo y celular
3	Correo electrónico personal
4	Correo electrónico de su cargo

La información suministrada en la solicitud de emisión de certificado de Pertenencia a empresa es estudiada por el agente de RA 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

La RA de ANDES SCD procesa las solicitudes de uno a dos días hábiles posteriores al registro de la solicitud junto con la documentación e información completa y un resultado exitoso en la validación de identidad, así como la confirmación por parte de la entidad. 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 trascurridos 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 su emisión dependerá del lugar de destino. Para obtener más información consultar nuestra política de entrega de certificados en nuestra página web.

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 entrego en el momento de adquirir el certificado.
- A representante autorizado de la entidad 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 Pertenencia a empresa 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 Pertenencia a empresa 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 mayor de edad que demuestre estar vinculada laboralmente a una entidad o persona jurídica, que se encuentre autorizada para obrar en nombre de la empresa en función del cargo que representa 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. en la sección "Procedimiento para solicitar la emisión de certificado"

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 Pertenencia a Empresa que las legitima. La llave privada es de uso exclusivo del suscriptor para los fines estipulados en esta Política de Certificación y debe ser protegida para impedir el uso no autorizado por parte de terceros.
El suscriptor solo puede usar el certificado y el par de llaves tras aceptar las condiciones de uso establecidas en la DPC y en la presente PC y solo para lo que estas establezcan.
Una vez el certificado haya expirado o este revocado el suscriptor está en la obligación de no volver a usar la llave privada.

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

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

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 Pertenencia a Empresa.

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 Certificados

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. Declinación de la Solicitud

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD en la sección declinación de la solicitud.

4.6. 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 de este.

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.

Puede solicitar la revocación de un certificado de Pertenencia a empresa 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 Pertenencia a empresa si tuviera conocimiento o sospecha del compromiso de la llave privada del suscriptor o cualquier otro hecho determinante que requiera 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.

4.7. 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
- Cambios de la información del titular del certificado, siempre y cuando pertenezca a la misma empresa.

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

- Para realizar la solicitud de reposición, el certificado a sustituir debe estar vigente.
- El certificado a sustituir debe tener una vigencia inicial igual o superior a 6 meses
- El certificado a sustituir debe tener una vigencia restante mayor a 60 días
- Comunicar el motivo de la cancelación del certificado a sustituir
- La reposición aplica para solicitar el mismo tipo de certificado adquirido inicialmente

Las condiciones de reposición pueden variar según los acuerdos específicos con usuarios gestionados a través de un coordinador o mediante convenios.

4.8. Servicios de estado de certificado

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

4.9. Vigencia de los certificados

El periodo de vigencia de los certificados digitales de Pertenencia a empresa 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 alterno 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 Pertenencia a empresa son generadas de acuerdo con los procesos estipulados en la DPC en la sección Generación del par de Llaves del suscriptor. 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 pertenencia a empresa sean generadas por ANDES SCD solo podrán ser almacenadas en dispositivos

criptográficos seguros "Token o HSM" que cumplan con el estándar FIPS 140-2 Nivel 3. La entrega de la Llave privada se hace directamente al suscriptor o responsable o persona autorizada por el mismo.

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 Pertenencia a empresa 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 Pertenencia a empresa se describe en la DPC en la 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 Pertenencia a empresa está permanentemente disponible para descarga en el directorio de certificados de Andes SCD mientras el certificado no esté 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 Pertenencia a empresa 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 las CA subordinadas emisoras de certificados de entidad final

6.1.7. Tamaño de las llaves

El tamaño mínimo de las llaves de certificados de Pertenencia a empresa es de 2048 bits basadas en el algoritmo RSA.

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

6.2. Controles de protección de la llave privada

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

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

Control de protección	Llave privada generada por suscriptor desde Dispositivo TOKEN y CSR
Respaldo de la llave privada	Andes SCD no realiza respaldo sobre las llaves privadas de los suscriptores generadas desde dispositivo TOKEN o cuando el certificado se genera a partir de CSR. Andes SCD nunca está en posesión de dichas llaves y solo permanecen bajo custodia del propio suscriptor
Almacenamiento de la llave privada	Las llaves privadas de los suscriptores generadas desde dispositivo TOKEN NUNCA son almacenadas por Andes SCD. Igualmente sucede cuando el certificado es generado a partir de CSR entregado por el suscriptor. 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 envidad a Andes SCD.
Activación de la llave privada	La activación del dispositivo TOKEN que contiene la llave privada del suscriptor se realiza a través de un PIN que debe ser personalizado por el propio suscriptor en el momento de generar el par de llaves. La protección de los datos de activación es responsabilidad del suscriptor
Desactivación de la llave privada	El método para desactivar la llave privada del suscriptor es retirar el dispositivo TOKEN del equipo, inmediatamente cualquier contenido asociado queda deshabilitado incluyendo la llave privada
Destrucción de llave privada	La destrucción de la llave privada puede realizarla el propio suscriptor utilizando las funciones que provee el dispositivo TOKEN, teniendo cuidado de no afectar otras llaves privadas almacenadas en el dispositivo. La destrucción de la llave privada del suscriptor puede realizarla el propio suscriptor eliminando la llave privada correspondiente al CSR enviado a Andes SCD.

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, DES, 3DES, MD5 y SHA-256 implementados por hardware.
- Hardware generador de números aleatorios.
- Hardware generador de firma digital.
- Espacio mínimo disponible de 64 Kb.
- Certificación FIPS 140-2 Nivel 3
- Certificación CE y FCC.
- Soporte completo para aplicaciones PKI.
- Compatible con interfaces CAPI y PKCS#11.
- Soporte para el almacenamiento de múltiples llaves.
- Soporte para X.509 V3 formato estándar de certificado.

6.3.1. Riesgos asociados

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

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

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

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

6.4. Otros aspectos de administración del par de llaves

6.4.1. Archivo de la llave pública

Andes SCD mantiene archivados todos los certificados digitales de Pertenencia a empresa, los cuales incluyen la llave pública durante el periodo estipulado en la sección "archivo de la llave publica "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 Pertenencia a empresa está regido por la validez de este 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 Pertenencia a empresa 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 Cesación de actividades de la ECD

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

7. Perfiles de certificado, CRL y OCSP

7.1. Contenido del certificado

Formato de certificados de Pertenencia a empresa		
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	Documento de identificación de suscriptor
	E	Correo electrónico del cargo del suscriptor

	C	Abreviatura país donde está la entidad
	ST	Nombre departamento donde está la entidad
	L	Nombre del municipio donde está la entidad
	STREET	Dirección de la entidad
	T	Cargo del suscriptor en la entidad
	1.3.6.1.4.1.4710.1.3.2	Documento identificación + DV de la entidad.
	O	Razón social de la entidad
	OU	Unidad organizacional del cargo en la entidad
	OU	Pertenencia Empresa Emitido por Andes SCD Calle 26 #69c-03 Torre B oficina 701.
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.
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 Pertenencia a empresa 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 Pertenencia a empresa 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 Pertenencia a empresa.

Extensiones Certificados Pertenencia a empresa 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)
Restricciones Básicas	Tipo de asunto=Entidad final Restricción de longitud de ruta=Ninguno
Directiva de certificados	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.31304.1.2.5.12 [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 Pertenencia a empresa (PC) y Prácticas de Certificación (DPC) establecidas por Andes SCD. [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: URL de DPC vigente

7.2.3. Identificadores de objeto de los algoritmos

Los certificados digitales de Pertenencia a empresa 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 Pertenencia a empresa 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 1.3.6.1.4.1.31304.1.2.5.12

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.

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 Pertenencia a empresa
- **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 la PC de Pertenencia a empresa 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 2459

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	Datos de la CA subordinada de entidad final que emitió la CRL	Ver en la CRL los datos de la CA que emitió la CRL
Algoritmo de firma	Algoritmo usado para firma de la CRL	SHA256withRSA
Fecha efectiva de emisión	Periodo de validez después de emitida la CRL	Fecha de emisión de la CRL en tiempo UTC
Siguiente actualización	Fecha en que se emitirá la siguiente CRL	Fecha de emisión de la próxima CRL en tiempo UTC
Emitir puntos de distribución	URL donde se publican las CRL emitidas por Andes SCD	Ver en la CRL la URL de publicación
Certificados revocados	Lista de certificados revocados especificando el número de serie, fecha de revocación y motivo revocación	

7.4. Perfil OCSP

7.4.1. 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 Contraints, critical	CA false
Key Usage critical	Firma digital
Extended Key Usage	OCSPSigner
Subject Key Identifier	identificador de llave

8. Auditoria y otras valoraciones

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

9. Negocio y materias legales

9.1. Tarifas

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

Formato de entrega	1 año	2 años	Valor de Reposición
Token Virtual	$160.380	$234.600	$23.656
Token físico	$160.380	$237.600	$67.640

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

- El valor de reposición aplica por la vigencia restante del certificado a sustituir siempre y cuando se cumplan las condiciones mencionadas en el ítem Reposiciones de esta política de certificación

9.2. Responsabilidad financiera

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

9.3. Confidencialidad de la información

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

9.4. Derechos de propiedad intelectual

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

9.5. 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 y No Discriminación

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 y en la Declaración de prácticas de certificación de ANDES SCD.

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

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	- 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	- 1.3 - Se actualiza dirección y PBX de Andes SCD - 3.1.1 y 7.1 - Se actualiza atributo OU del DN a Certificado Pertenencia empresa Emitido por Andes SCD Av. Calle 72 # 9 - 55 - 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 Pertenencia Empresa Emitido por Andes SCD Av Cll 72 9 55 Of 501	Comité políticas y seguridad
2.1	24/11/2015	- 1.1 - Se actualiza versión del documento PC y fecha de emisión	Comité políticas y seguridad

		- 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: Pertenencia Empresa Emitido por Andes SCD Cra 27 86 43 - 7.2.2 - Se actualiza OID PC y URL DPC Directiva de certificados	
2.2	26/09/2016	- 1.3.2 – Se actualiza email de persona de contacto - 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. - 7.2.1 - Se actualiza RFC 3280 por 5280	Comité políticas y seguridad
2.3	06/01/2017	- 4, 4.7 – Se especifica que la vigencia máxima del certificado son 730 días calendario - 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	14/02/2017	- 3.2.2 Se incluye fragmento respecto a requisitos para emitir certificado de pertenencia a empresa a solicitantes con contrato de prestación de servicios o vinculados a través de empresas temporales.	Comité políticas y seguridad
2.5	01/07/2017	- 3.2.4 se reemplaza termino clave revocación por código revocación	Comité políticas y seguridad

		- 4. Se suprime el termino contrato de suscripción - 4.5 se incluyó condición para reposición de certificados - 7.2 URL y versión DPC 2.5 y PC 2.5	
2.6	26/10/2017	- 3.2.2 Se detalla los requisitos mínimos que debe tener el documento que acredita vinculación del solicitante a la entidad	Comité políticas y seguridad
2.7	20/03/2018	- 1.5.4 Se incluye el apartado minutas y contratos. - 2. Se hace referencia al RFC 4523 relacionado con el LDAP. - 3.2.2 Se incluyen otros mecanismos que permitan validar la identidad del suscriptor. - 3.2.3 Se hace referencia a autoridad de registro encargada de recopilar las evidencias requeridas. - 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. - 6.3.1Se 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 V.2.7 - 9.1 Se incluyen tarifas de los certificados de acuerdo con su vigencia - 9.5.1 Se describen obligaciones y responsabilidades de ANDES SCD. - 9.5.2 Se describen obligaciones del suscriptor.	Comité de políticas y seguridad

		- 9.5.3 Se describen prohibiciones para el suscriptor. - 9.6 Se hace referencia al principio de imparcialidad.	
2.8	16/07/2018	- 7.2.2 se hace referencia a URL de DPC vigente	Comité de Políticas y seguridad
2.9	14/09/2018	- 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 a PC - 7.2.6 Se actualiza OID	Comité de Políticas y seguridad
3.0	25/11/2019	- 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
3.1	04/11/2020	- 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

3.2	1/02/2021	- 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 de tarifas. - Se actualiza el OID de la PC.	Comité de políticas y seguridad
3.3	28/04/2021	- Se adiciona la fecha de expedición y el registro de las solicitudes presenciales en el apartado 3.2.2. Autenticación de la identidad del solicitante. Se elimina el párrafo referente a los documentos necesarios para las solicitudes tramitadas por convenio. - 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
4	15/06/2022	-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	Comité de Políticas y Seguridad / Analista Senior SGI

		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.	
5	12/10/2022	- 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. - 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. - Se modifica el titulo y el contenido del	Comité de Políticas y Seguridad / Analista Senior SGI

		numeral 9.5.1 Derechos y deberes de Andes SCD.	
6	05/12/2022	- 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). - Se incluye en la sección 3.2.2.1, el correo electronico para realizar confirmacion. - Se modifica vigencia del documento RUT a 90 días.	Comité de Políticas y Seguridad / Analista Senior SGI
7	30/03/2023	- Se actualiza Logo de Andes y fuente de la letra. - Se actualiza colores del formato de acuerdo con el manual de marca 2023. - Se actualiza el OID, Versión y fecha de emisión en la sección Nombre del documento e Identificación - Se modifica el cargo Gerente de Operaciones a Director de Operaciones. - Se actualizan el numeral "Autenticación de la identidad" incluyendo validación de identidad y nota para los requisitos documentales. - Se actualizan los límites de uso de los certificados en el formato de entrega token virtual.	Comité de Políticas y Seguridad / Analista Senior SGI
8	16/11/2023	- Se actualiza el OID y Versión - Se actualiza número de teléfono de ANDES SCD.	Comité de políticas y seguridad / Analista Senior SGI

		- Se modifica título 6.7 de "Terminación de CA o RA" a "Cesación de actividades de la ECD". - Se incluye el termino de declinación de solicitudes. - En el tiempo de respuesta se especifica que se debe contar con la validacion de identidad exitosa. - Se modifican condiciones de reposición de certificados.	
9	19/02/2024	- Se actualiza el OID y Versión - Se actualizan las tarifas y se incluye el valor de reposición de los certificados.	Comité de políticas y seguridad / Profesional SGI
10	07/05/2024	- Se actualiza el OID y Versión - Se actualizan motivos de reposición de acuerdo con el tipo de certificado. - Se actualizan límites de uso de los certificados en sistemas operativos - Se elimina documento RUT como requisito del certificado.	Comité de políticas y seguridad / Profesional SGI
11	06/06/2024	- Se actualiza fecha y OID del documento - Se actualiza el ítem principio de imparcialidad incluyendo el termino No Discriminación. - Se actualizan tarifas del servicio.	Comité de políticas y seguridad / Profesional SGI

12	24/01/2025	- Se actualiza el logo y la portada del documento de acuerdo con el manual de marca corporativa. - Se actualizan el ítem nombre del documento, la identificación, el OID, la versión y la fecha del documento. - Se actualizan las tarifas del servicio. - Se modifica el apartado relacionado con la reposición de certificados. - Se actualiza el numeral "Autenticación de la identidad" para incluir una nota sobre los requisitos documentales. - Se revisa y actualiza el ítem "Tiempos de respuesta", incorporando la política de entrega de certificados de firma digital	Comité de políticas y seguridad / Director de Operaciones/ Coordinador de Operaciones

Firmado por:
Sandra Cecilia Restrepo Martinez
2025/01/24 10:02:36:144

SANDRA CECILIA RESTREPO MARTINEZ
Gerente General