



Andes Servicio de Certificación Digital S.A SIGLA ANDES SCD SA.

POLITICA DE CERTIFICACION

FUNCION PUBLICA

Tabla de Contenido

1. Presentación del documento.....	3
1.1.Nombre del documento e Identificación	3
1.2.Referencias.....	3
1.3.Administración de la política	3
1.3.1. Organización que administra el documento.....	3
1.3.2. Persona de contacto.....	4
1.3.3. Procedimientos de aprobación de la política	4
1.3.4. Publicación del documento	4
1.4.Comunidad de usuarios y aplicabilidad.....	4
1.5.Ámbito de aplicación	5
1.5.1. Usos del certificado	5
1.5.2. Límites de uso de los certificados.....	5
1.5.3. Prohibiciones de uso de los certificados.....	5
2. Publicación y registro de certificados	6
3. Identificación y autenticación	6
3.1.Nombres	6
3.1.1. Tipos de nombres.....	6
3.1.2. Necesidad para los nombres de ser significativos.....	6
3.1.3. Anónimos y pseudónimos en los nombres	6
3.1.4. Reglas para interpretar los formatos de nombre	7
3.1.5. Singularidad de los nombres	7
3.2.Aprobación de la identidad.....	7
3.2.1. Método para demostrar la posesión de la llave privada.....	7
3.2.2. Autenticación de la identidad del solicitante	7
3.2.3. Información no verificada sobre el solicitante	8
3.2.4. Identificación y autenticación para solicitar revocación	8
4. Ciclo de vida del certificado y procedimientos de operación.....	8
4.1.Emisión de certificados	8
4.1.1. Quien pueden solicitar la emisión de un certificado.....	8
4.1.2. Procedimiento para solicitar certificado	8
4.1.3. Publicación del certificado por Andes SCD	8
4.1.4. Par de llaves y uso del certificado	9
4.1.4.1. Por parte del suscriptor.....	9
4.1.4.2. Por parte de usuarios que confían.....	9
4.2.Renovación de certificados.....	9
4.3.Modificación de certificados	9
4.4.Revocación de certificados	9
4.5.Servicios de estado de certificado	9
4.6.Vigencia de los certificados.....	10
5. Controles de seguridad.....	10
6. Controles de seguridad técnica.....	10
6.1.Generación de llaves e instalación	10
6.1.1. Generación del par de llaves.....	10

6.1.2.	<i>Entrega de la llave privada al suscriptor</i>	10
6.1.3.	<i>Entrega de la llave pública al emisor del certificado</i>	10
6.1.4.	<i>Distribución de la llave pública del suscriptor</i>	10
6.1.5.	<i>Distribución de la llave pública de Andes SCD a los usuarios</i>	10
6.1.6.	<i>Periodo de utilización de la llave privada</i>	10
6.1.7.	<i>Tamaño de las llaves</i>	10
6.2.	<i>Controles de protección de la llave privada</i>	10
6.3.	<i>Otros aspectos de administración del par de llaves</i>	11
6.3.1.	Archivo de la llave pública	11
6.3.2.	Periodos operacionales del certificado y periodos de uso del par de llaves	11
6.4.	Datos de activación	12
6.4.1.	Generación de datos de activación e instalación	12
6.4.2.	Protección de datos de activación	12
6.5.	<i>Controles de seguridad informática</i>	12
7.	Perfiles de certificado, CRL y OCSP	13
7.1.	Contenido del certificado	13
7.2.	Perfiles de certificado	14
7.2.1.	Número de versión	14
7.2.2.	Extensiones del certificado	14
7.2.3.	Identificadores de objeto de los algoritmos	15
7.2.4.	Formatos de nombres	15
7.2.5.	Restricciones de nombre	15
7.2.6.	Objeto identificador de la política de certificación	15
7.2.7.	Sintaxis y semántica de los calificadores de la política	15
7.3.	Perfil de la CRL	16
7.3.1.	Numero de versión	16
7.3.2.	CRL y extensiones	16
7.4.	Perfil OCSP	16
7.4.1.	Numero de versión	16
7.4.2.	Extensiones OCSP	16
8.	Auditoria y otras valoraciones	16
9.	Negocio y materias legales	17
9.1.	Tarifas	17
9.2.	Responsabilidad financiera	17
9.3.	Confidencialidad de la información	17
9.4.	Derechos de propiedad intelectual	17
9.5.	Obligaciones y garantías	17
9.6.	Limitaciones de responsabilidad	17
9.7.	Indemnizaciones	17
9.8.	Término y terminación	17
9.9.	Procedimiento de cambio en las especificaciones	17
9.10.	Prevención de disputas	17
9.11.	Ley aplicable y cumplimiento con la ley aplicable	17

Introducción

La presente Política para Certificados de Función Pública 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 Función Pública 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 Función Pública o hacer uso del mismo para comprobación de firmas electrónicas con el fin de conocer el ámbito de aplicación y los efectos legales asociados al uso de este tipo de certificado

1. Presentación del documento

1.1. Nombre del documento e Identificación

Documento	POLITICA DE CERTIFICACION FUNCIÓN PÚBLICA
Descripción	Los certificados de Función Pública son emitidos a nombre de personas naturales; acreditan la identidad del titular y su carácter de funcionario público o de particular en ejercicio de una función pública, ya sea por designación o como resultado de la suscripción de un contrato que lo habilite como tal, 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 titular de un certificado de Función Pública actúa en la calidad acreditada en él.
Identificador OID	1.3.6.1.4.1.31304.1.2.8.2.1
Versión	V 2.1
Fecha de emisión	Noviembre 24 de 2015
Ubicación	http://www.andesscd.com.co/docs/PC2.0/pc_funcionpublica_v2.1.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 TS 101 456: Policy Requirements for certification authorities issuing qualified certificates.
- ETSI TS 102 042: Policy Requirements for certification authorities issuing public key certificates.

1.3. Administración de la política

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

1.3.1. Organización que administra el documento

Nombre : Comité de Políticas y Seguridad
Dirección : Carrera 27 No 86 - 43
Email : comite.politicas.seguridad@andesscd.com.co
Teléfono : PBX 571 795 3430

1.3.2. Persona de contacto

Razón social : Andes Servicio de Certificación Digital S.A SIGLA ANDES SCD SA.
Nombre : Martín Vargas Linares – Gerente General
Dirección : Carrera 27 No 86 - 43
Email : gerencia@andesscd.com.co
Teléfono : PBX 571 795 3430

1.3.3. Procedimientos de aprobación de la política

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

1.3.4. Publicación del documento

Las Políticas de Certificación de Función Pública 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 Función Pública son emitidos a nombre de personas naturales; acreditan la identidad del titular y su carácter de funcionario público o de particular en ejercicio de una función pública, ya sea por designación o como resultado de la suscripción de un contrato que lo habilite como tal, 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 titular de un certificado de Función Pública actúa en la calidad acreditada en él

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 Función pública 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 tipo presencial, 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 Función Pública emitido por la Autoridad de Certificación Andes SCD para obrar en el entorno electrónico acreditando su identidad y condición como funcionario público o ejercicio de una función pública. 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 Función Pública emitido por Andes SCD. Bajo ninguna circunstancia se aceptan solicitudes de este tipo de certificados a nombre de personas que no demuestren su vinculación como funcionario público o particular que ejerce función pública.

	POLITICA DE CERTIFICACION FUNCION PUBLICA	
	Identificador OID	1.3.6.1.4.1.31304.1.2.8.2.1
	Clasificación	Documento Público
		Versión 2.1
		24 Noviembre 2015

Usuarios

El usuario es cualquier persona que voluntariamente deposita su confianza en los certificados de Función Pública 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 Función Pública 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 funcionario público o particular que ejerce una función pública en el ámbito de su actividad.

Firma digital

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

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

Cifrado de información

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

1.5.2. Límites de uso de los certificados

Los certificados de Función pública 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.

1.5.3. 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 Función Pública 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.

2. Publicación y registro de certificados

En la Declaración de Prácticas de Certificación (DPC) de Andes SCD se detalla información del directorio de certificados, los medios de publicación, la frecuencia de publicación y el control de acceso al directorio de certificados.

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 Función Pública

3.1. Nombres

3.1.1. Tipos de nombres

Los certificados de Función Pública 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 identificación suscriptor
E	<u>Email</u>	Correo electrónico del cargo del suscriptor
C	<u>País</u>	Abreviatura del país donde está ubicada la entidad
ST	<u>Departamento</u>	Nombre del departamento donde está ubicada la entidad
L	<u>Ciudad</u>	Nombre del municipio donde está ubicada la entidad
STREET	<u>Dirección</u>	Dirección donde está ubicada la entidad
T	<u>Título</u>	Cargo del suscriptor en la entidad
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
OU	<u>Unidad Organizacional</u>	Nombre de la unidad organizacional de la entidad a la cual está vinculado el suscriptor.
OU	<u>Unidad Organizacional</u>	Funcion Publica Emitido por Andes SCD Cra 27 86 43

3.1.2. Necesidad para los nombres de ser significativos

Todo certificado de Función Pública 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 Persona Jurídica.

El nombre de la persona jurídica debe ser la razón social que figura en el RUT, 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 Función Pública 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 Función Pública.

3.2.2. Autenticación de la identidad del solicitante


El solicitante puede tramitar su solicitud de emisión de certificado de Función Pública de las siguientes formas:

- Presencial:** El solicitante realiza la solicitud personalmente ante una Autoridad de Registro de Andes SCD.
- Remota :** El solicitante realiza la solicitud desde la página WEB de Andes SCD.
- Convenios:** Las solicitudes de emisión de certificados por convenios son tramitadas por un coordinador externo de la entidad con convenio o del personal autorizado de Andes de acuerdo a los procedimientos internos definidos por Andes SCD.

Requisito	Solicitud presencial	Solicitud remota o convenio
Cedula 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 legible)	Presentar Fotocopia documento	Se requiere documento escaneado
Documentos que acrediten la vinculación de la persona como funcionario público o particular que ejerce función pública y donde se especifique el cargo que desempeña (Documento legible y reciente)	Presentar Fotocopia documento	Se requiere documento escaneado

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

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

 Andes SCD <small>Servicio de Certificación Digital</small>	POLITICA DE CERTIFICACION FUNCION PUBLICA	
	Identificador OID	1.3.6.1.4.1.31304.1.2.8.2.1
	Clasificación	Documento Público
		Versión 2.1
		24 Noviembre 2015

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

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

3.2.3. Información no verificada sobre el solicitante

Andes SCD verifica toda la información del solicitante que se encuentre respaldada con documentos soporte. No se verifica dirección de residencia y correo electrónico presumiendo la buena fe de la información aportada por el solicitante.

3.2.4. Identificación y autenticación para solicitar revocación

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

- Al propio suscriptor, en cuyo caso debe usar la clave de revocación que se le entregó en el momento de adquirir el certificado o debe presentarse personalmente ante una Autoridad de Registro donde será identificado a partir de su huella dactilar.
- A representante autorizado de la entidad donde el suscriptor realiza la función pública, en cuyo caso debe notificar formalmente por escrito a Andes SCD el motivo por el cual se solicita la revocación del certificado de función pública 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 apartado 4.4.1 de la Declaración de Prácticas de Certificación.

4. Ciclo de vida del certificado y procedimientos de operación

Los certificados de Función Pública emitidos por Andes SCD tienen un periodo de vigencia explícito en los atributos "válido desde" y "válido hasta" del propio certificado. En el contrato de suscripción se indica el tiempo de vigencia en días.

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

4.1. Emisión de certificados

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

4.1.1. Quien pueden solicitar la emisión de un certificado

La solicitud de emisión de un certificado digital puede realizarla cualquier persona mayor de edad que demuestre ser un funcionario público o un particular en ejercicio de una función pública y que este en plena capacidad de asumir las obligaciones y responsabilidades inherentes a la posesión y uso del certificado.

4.1.2. Procedimiento para solicitar certificado

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

4.1.3. Publicación del certificado por Andes SCD

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

4.1.4. Par de llaves y uso del certificado

4.1.4.1. Por parte del suscriptor

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

El suscriptor solo puede usar el certificado y el par de llaves tras aceptar las condiciones de uso establecidas en la DPC y en la presente PC y solo para lo que estas establezcan. Una vez el certificado haya expirado o este revocado el suscriptor está en la obligación de no volver a usar la llave privada.

4.1.4.2. Por parte de usuarios que confían

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

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

4.2. Renovación de certificados

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

4.3. Modificación de certificados

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

4.4. Revocación de certificados

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

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

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

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

4.5. 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.

4.6. Vigencia de los certificados

El periodo de vigencia de los certificados digitales de Función Pública esta explícito en el propio certificado en los atributos “Valido desde” y “Valido Hasta”.

El par de llaves tiene el mismo periodo de vigencia del certificado digital que las avala.

5. Controles de seguridad

Los controles procedimentales, de seguridad física, de seguridad personal y de auditoría definidos para trabajar bajo un ambiente seguro y las capacidades de recuperación ante desastres establecidos para garantizar la operación de los servicios de certificación se encuentran especificados en la Declaración de Prácticas de Certificación de Andes SCD.

6. Controles de seguridad técnica

6.1. Generación de llaves e instalación

6.1.1. Generación del par de llaves

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

6.1.2. Entrega de la llave privada al suscriptor

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

6.1.3. Entrega de la llave pública al emisor del certificado

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

6.1.4. Distribución de la llave pública del suscriptor

La llave pública de cualquier suscriptor de Certificados de Función Pública cuyo certificado fue emitido por Andes SCD 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 y de la CA emisora de certificados Clase II o de entidad final está permanentemente disponible 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 Función Pública 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 de las llaves de certificados de Función Pública es de 2048 bits basadas en el algoritmo RSA.

El tamaño de las llaves certificadas de la CA Clase II emisora de los certificados de Función Pública 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	Llave privada generada por Andes SCD y almacenada en Archivo PKCS12
<u>Respaldo de la llave privada</u>	Andes SCD no realiza respaldo sobre las llaves privadas de los suscriptores generadas desde dispositivo TOKEN. Andes SCD nunca está en posesión de dichas llaves y solo permanecen bajo custodia del propio suscriptor	Andes SCD no realiza respaldo sobre las llaves privadas de los suscriptores contenidas en archivos PKCS12. Andes SCD genera el par de llaves del suscriptor y permanecen almacenados en Andes SCD hasta que el suscriptor realice la descarga y elimine el archivo PKCS12 del repositorio de Andes SCD.
<u>Almacenamiento de la llave privada</u>	Las llaves privadas de los suscriptores generadas desde dispositivo TOKEN NUNCA son almacenadas por Andes SCD. 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	Las llaves privadas de los suscriptores contenidas en archivos PKCS12 son almacenadas por Andes SCD mientras el suscriptor realiza la descarga y da la orden explícita de eliminar el PKCS12 del repositorio de Andes SCD. El Suscriptor debe asegurarse de descargar el archivo PKCS12 y dar la orden de eliminarlo del repositorio de Andes SCD. El archivo PKCS12 debe ser almacenado y conservado por el propio suscriptor.
<u>Transferencia de la llave privada</u>	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 de los suscriptores se encuentra dentro del archivo PKCS12, el cual es descargado por el suscriptor desde la zona segura que utiliza el protocolo HTTPS. El archivo PKCS12 protege el uso de la llave privada a través de un PIN que es custodiado por el suscriptor.
<u>Activación de la llave privada</u>	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	La activación del archivo PKCS12 que contiene la llave privada del suscriptor se realiza a través de un PIN asignado de forma automática y aleatoria por Andes SCD y entregado al suscriptor. La protección de los datos de activación es responsabilidad exclusiva del suscriptor
<u>Desactivación de la llave privada</u>	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	El método para desactivar la llave privada del suscriptor que ha importado su certificado a partir de un PKCS12 es retirar el certificado del almacén de certificados que lo contenga, inmediatamente cualquier contenido asociado queda deshabilitado incluyendo la llave privada
<u>Destrucción de llave privada</u>	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 el archivo PKCS12

6.3. Otros aspectos de administración del par de llaves

6.3.1. Archivo de la llave pública

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

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

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

El par de llaves tiene vigencia mientras exista un certificado de Función Pública 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.

6.4. Datos de activación

6.4.1. Generación de datos de activación e instalación

En esta sección se indica el mecanismo de generación de los datos de activación del dispositivo TOKEN o Archivo PKCS12 que almacenan el par de llaves y el certificado del suscriptor.

Generación de datos de Activación	
Dispositivo TOKEN	Archivo PKCS12
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.	Andes SCD genera de forma automática y aleatoria el PIN de activación de los archivos PKCS12 que contienen el par de llaves y el certificado del suscriptor. El PIN debe ser custodiado por el suscriptor de modo que no sea conocido por nadie más y garantice el control exclusivo del archivo PKCS12

6.4.2. Protección de datos de activación

La protección de los datos de activación del dispositivo TOKEN o el archivo PKCS12 es responsabilidad exclusiva del suscriptor. A continuación se indican los mecanismos de protección:

Protección de datos de Activación	
Dispositivo TOKEN	Archivo PKCS12
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	El PIN o dato de activación del archivo PKCS12 es asignado por Andes SCD de forma automática y aleatoria y este PIN puede ser cambiado por el suscriptor a través de diferentes mecanismos como el uso de OpenSSL y el almacén de certificados de los navegadores. El suscriptor debe proteger el PIN y el archivo PKCS12.

6.5. Controles de seguridad informática

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

7. Perfiles de certificado, CRL y OCSP

7.1. Contenido del certificado

Formato de certificados de Función Pública		
Campo	Descripción	Valor
Versión	Versión del certificado	V3
Serial number	Número que identifica unívocamente 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)	CN	CA ANDES SCD S.A. Clase II
	O	Andes SCD.
	OU	Division de certificacion entidad final
	C	CO
	L	Bogota, D.C.
	E	info@andesscd.com.co
Valido desde	Fecha y hora UTC inicio validez del certificado	Fecha de inicio de la validez del certificado
Válido hasta	Fecha y hora UTC fin validez del certificado	Fecha final de la validez del certificado
Asunto	CN	Nombre completo del suscriptor
	Serial Number	Número documento identificación suscriptor
	E	Correo electrónico del suscriptor
	C	Abreviatura país donde está la entidad
	ST	Nombre departamento donde está la entidad
	L	Nombre municipio donde está la entidad
	STREET	Dirección donde está ubicada la entidad
	T	Cargo del suscriptor en la entidad
	1.3.6.1.4.1.4710.1.3.2	Número documento + dv de la entidad
	O	Razón social de la entidad
	OU	Unidad organizacional del cargo
	OU	Funcion Publica Emitido por Andes SCD Cra 27 86 43
	Llave pública	Llave pública del titular del certificado
Extensiones	Extensiones utilizadas en los certificados de Función Pública.	Ver apartado 7.2.2 de este documento para más detalles.
Algoritmo de identificación	Algoritmo utilizado para obtener la huella digital del certificado	Sha1
Huella digital	La síntesis o huella digital de los datos del certificado	fingerprint
Uso de la llave	Propósitos para los cuales se debe utilizar el certificado.	Firma Digital No repudio Cifrado de información

7.2. Perfiles de certificado


7.2.1. Número de versión

Los certificados de Función Pública emitidos bajo esta política están de conformidad con el estándar X.509 V3 y de conformidad con el RFC 3280 para perfiles de certificados y CRL.

7.2.2. Extensiones del certificado

Los certificados de Función Pública 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 Función Pública

Extensiones Certificados Función Pública 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	a8 4b b4 f4 0b a7 b6 5b d4 a0 28 85 10 9d 04 13 33 c4 a7 f7
Puntos de distribución de la CRL	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://www.andesscd.com.co/includes/getCert.php?crl=1 Emisor CRL: Dirección del directorio: C=CO L=Bogota D.C. O=Andes SCD. OU=Division de certificacion entidad final CN=CA ANDES SCD S.A. Clase II E=info@andesscd.com.co
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=1.3.6.1.4.1.31304.1.2.8.2.1 [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 Función Pública (PC) y Prácticas de Certificación (DPC) establecidas por Andes SCD. [1,2]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.andesscd.com.co/docs/DPC_AndesSCD_V2.1.pdf

 Andes SCD <small>Servicio de Certificación Digital</small>	POLITICA DE CERTIFICACION FUNCION PUBLICA	
	Identificador OID	1.3.6.1.4.1.31304.1.2.8.2.1
	Clasificación	Documento Público
		Versión 2.1
		24 Noviembre 2015

7.2.3. Identificadores de objeto de los algoritmos

Los certificados digitales de Función Pública 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 Función Pública 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 1.3.6.1.4.1.31304.1.2.8.2.0.

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

7.2.7. Sintaxis y semántica de los calificadores de la política

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

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

 Andes SCD Servicio de Certificación Digital	POLITICA DE CERTIFICACION FUNCION PUBLICA	
	Identificador OID	1.3.6.1.4.1.31304.1.2.8.2.1
	Clasificación	Documento Público
		Versión 2.1
		24 Noviembre 2015

7.3. Perfil de la CRL

7.3.1. Numero de versión

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

7.3.2. CRL y extensiones

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

Perfil de CRL según estándar X.509V2 – CRL Clase II		
Nombre	Descripción	Valor
Versión	Versión de la CRL	V2
Numero de CRL	Número único de la CRL	Identificado de la CRL
Emisor	CN	CA ANDES SCD S.A. Clase II
	O	Andes SCD
	OU	Division de certificación entidad final
	C	CO
	L	Bogota, D.C.
	E	info@andesscd.com.co
Algoritmo de firma	Algoritmo usado para la firma de la CRL	SHA1withRSA
Fecha efectiva de emisión	Periodo de validez después de emitida la CRL	Fecha de emisión de la CRL en tiempo UTC
Siguiente actualización	Fecha en que se emitirá la siguiente CRL	Fecha de emisión de la próxima CRL en tiempo UTC
Emitir puntos de distribución	URL donde se publican las CRL emitidas por Andes SCD	http://www.andesscd.com.co/includes/getCert.php?crl=1
Certificados revocados	Lista de certificados revocados especificando el número de serie, fecha de revocación y motivo de la revocación	

7.4. Perfil OCSP

7.4.1. Numero de versión

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

7.4.2. Extensiones OCSP

Extensiones OCSP según estándar X.509V3	
Nombre	Valor
Basic Constraints, 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

En la Declaración de Prácticas de Certificación se define donde se encuentra el marco tarifario por los servicios de certificación ofrecidos por la Autoridad Certificadora Andes SCD.

9.2. Responsabilidad financiera

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

9.3. Confidencialidad de la información

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

9.4. Derechos de propiedad intelectual

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

9.5. Obligaciones y garantías

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

9.6. Limitaciones de responsabilidad

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

9.7. Indemnizaciones

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

9.8. Término y terminación

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

9.9. Procedimiento de cambio en las especificaciones

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

9.10. Prevención de disputas

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

9.11. Ley aplicable y cumplimiento con la ley aplicable

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

CONTROL DE CAMBIOS	
Descripción del cambio	Sección PC
Se actualizó la versión del documento PC y fecha de emisión	1.1
Se actualizó datos de contacto y organización que administra el documento	1.3
Se actualizó atributo OU del DN a: Funcion publica Emitido por Andes SCD Cra 27 86 43	3.1.1 y 7.1
Se actualizó OID PC y URL DPC en Directiva de certificados	7.2.2