DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Andes SCD S.A.

Versión 2.8
2018

Introducción....6
1. Presentación del documento....6
1.1. Nombre del documento e Identificación....6
1.2. Identificación de la Entidad de Certificación Digital....6
1.3. Alcance....7
1.4. Referencias....7
1.5. Definiciones....7
1.6. Lista de acrónimos y abreviaturas....8
1.7. Participantes de PKI o modelo de confianza....8
1.7.1. Autoridad de Certificación (CA)....8
1.7.2. Autoridad de Registro (RA)....11
1.7.3. Suscriptor....12
1.7.4. Solicitante....12
1.7.5. Usuario o tercero aceptante....12
1.8. Ámbito de aplicación....12
1.8.1. Usos del certificado....12
1.8.2. Límites de uso de los certificados....12
1.8.3. Prohibiciones Generales....13
1.8.4. Prohibiciones de uso de los certificados....13
1.9. Catálogo de servicios de certificación....14
1.9.1. Certificados para Entidad Final....14
1.10. Administración de la Política....15
1.10.1. Organización que administra este documento....15
1.10.2. Persona de contacto....15
1.10.3. Procedimientos de aprobación de la política....16
1.10.4. Publicación del documento....16
2. Publicación y registro de certificados....16
2.1. Directorio de certificados....16
2.2. Medios de publicación....16
2.3. Frecuencia de publicación....18
2.4. Control de acceso al directorio de certificados....18
3. Identificación y autenticación....19
3.1. Nombres....19
3.1.1. Tipos de nombres....19
3.1.2. Necesidad para los nombres de ser significativos....19
3.1.3. Anónimos y pseudónimos en los nombres....19
3.1.4. Reglas para interpretar los formatos de nombre....19
3.1.5. Singularidad de los nombres....19
3.1.6. Reconocimiento, autenticación y función de las marcas registradas....19
3.2. Aprobación de la identidad....20
3.2.1. Método para demostrar la posesión de la llave privada....20
3.2.2. Autenticación de la identidad....22
3.2.3. Información no verificada sobre el solicitante....23
3.2.4. Criterio para interoperación....23

3.2.5. Identificación y autenticación para solicitar revocación 23
4. Ciclo de vida del certificado y procedimientos de operación 24
4.1. Emisión de certificados 24
4.1.1. Quién puede solicitar la emisión de un certificado 24
4.1.2. Procedimiento para solicitar emisión de certificado 24
4.1.3. Publicación del certificado por ANDES SCD 24
4.1.4. Par de llaves y uso del certificado 24
4.1.4.1. Por parte del suscriptor 24
4.1.4.2. Por parte de usuarios que confían 24
4.2. Renovación de certificados 24
4.3. Modificación de certificados 25
4.4. Revocación de certificados 25
4.4.1. Circunstancias de revocación 25
4.4.2. Quién puede solicitar la revocación certificados 26
4.4.3. Medios para revocar certificados 26
4.4.4. Procedimiento para revocar certificados 27
4.4.5. Tiempo para procesar la solicitud de revocación 28
4.4.6. Requisitos de verificación de las revocaciones por los usuarios que confían 29
4.4.7. Publicación de certificados revocados 29
4.5. Servicios de información del estado de certificado 29
4.5.1. Características operacionales 29
4.5.2. Disponibilidad del servicio 29
4.5.3. Fin de suscripción 30
4.6. Reposición de certificados 30
4.7. Vigencia de los certificados 30
5. Controles de seguridad 30
5.1. Condiciones exigidas a proveedores críticos 30
5.2. Controles de seguridad física 30
5.2.1. Ubicación y seguridad ambiental 30
5.2.2. Gestión del sistema de acceso 32
5.2.3. Seguridad de los servidores 32
5.3. Controles procedimentales 33
5.3.1. Roles de confianza 33
5.3.2. Número de personas requeridas por tarea 36
5.3.3. Identificación y autenticación de cada rol 36
5.3.4. Roles que requieren separación de deberes 36
5.3.5. Relación entre ANDES SCD y las Autoridades de Registro 36
5.4. Controles de seguridad personal 37
5.4.1. Calificaciones, experiencia y requisitos 37
5.4.2. Procedimientos de comprobación de antecedentes 37
5.4.3. Requisitos de entrenamiento 37
5.4.4. Frecuencia de adiestramiento y requisitos 37
5.4.5. Frecuencia de rotación de trabajo 37
5.4.6. Sanciones por acciones desautorizadas 38

5.4.7. Requisitos de la contratación de personal 38
5.4.8. Documentación suministrada al personal 38
5.5. Controles de Auditoría 38
5.5.1. Tipos de eventos auditados 38
5.5.2. Frecuencia de procesamiento de los registros de auditoría 39
5.5.3. Periodo de resguardo de los registros de auditoría 39
5.5.4. Protección de los registros de auditoría 39
5.5.5. Procedimientos de respaldo de los registros de auditoría 39
5.5.6. Sistemas de recolección de información de auditoría 40
5.5.7. Sistemas de revisión de eventos 40
5.5.8. Análisis de vulnerabilidades 40
5.6. Controles de almacenamiento y archivo de la información 40
5.6.1. Tipo de información a resguardar 40
5.6.2. Periodo de resguardo de la información 40
5.6.3. Protección de la información 40
5.6.4. Procedimiento de respaldo de la información 41
5.6.5. Sistemas de almacenamiento internos y externos 41
5.6.6. Procedimiento para obtener y verificar la información archivada 41
5.7. Cambio de llave 41
5.8. Compromiso y recuperación de desastre 41
5.8.1. Procedimientos para administrar incidentes 42
5.8.2. Recursos informáticos, software y datos corruptos 42
5.8.3. Procedimientos ante compromiso de la llave privada 42
5.8.4. Capacidades de continuidad del negocio ante un desastre 43
5.8.5. Medidas para corrección de vulnerabilidades detectadas 43
5.9. Terminación de CA o RA 43
6. Controles de seguridad técnica 44
6.1. Generación de llaves e instalación 44
6.1.1. Generación del par de llaves 44
6.1.2. Entrega de la llave privada al suscriptor 46
6.1.3. Entrega de la llave pública al emisor del certificado 46
6.1.4. Distribución de la llave pública del suscriptor 47
6.1.5. Distribución de la llave pública de ANDES SCD a los usuarios 47
6.1.6. Periodo de utilización de la llave privada 47
6.1.7. Tamaño de las llaves 47
6.1.8. Parámetros de generación de llave pública y comprobación de calidad 47
6.2. Controles de protección de la llave privada 48
6.2.1. Controles y estándares de módulos criptográficos 48
6.2.2. Control sobre la llaves privada (Multi-persona) 48
6.2.3. Respaldo de la llave privada 48
6.2.4. Almacenamiento de la llave privada 48
6.2.5. Transferencia de la llave privada a partir o a un módulo criptográfico 49
6.2.6. Almacenamiento de la llave privada a un módulo criptográfico 49
6.2.7. Método de activación de la llave privada 50

6.2.8. Método de desactivación de la llave privada 50
6.2.9. Método de destrucción de la llave privada 50
6.2.10. Clasificación de los modulo criptográfico 51
6.3. Otros aspectos de administración del par de llaves 51
6.3.1. Archivo de la llave pública 51
6.3.2. Periodos operacionales del certificado y periodos de uso del par de llaves 51
6.4. Datos de activación 51
6.4.1. Generación e instalación de los datos de activación 51
6.4.2. Protección de datos de activación 52
6.5. Controles de seguridad informática 53
6.5.1. Requisitos específicos de seguridad técnica 53
6.5.2. Nivel de seguridad informática 53
6.6. Controles técnicos del ciclo de vida 53
6.6.1. Controles en el desarrollo de sistema 53
6.6.2. Controles de gestión de la seguridad 53
6.6.3. Controles de seguridad en el ciclo de vida 53
6.7. Controles de seguridad en la red 54
7. Perfiles de certificado, CRL y OCSP 54
7.1. Perfiles de certificado 54
7.1.1. Número de versión 54
7.1.2. Extensiones del certificado 54
7.1.3. Identificadores objeto del algoritmo 55
7.1.4. Formatos de nombres 55
7.1.5. Restricciones de nombre 55
7.1.6. Objeto identificador de la política de certificación 55
7.1.7. Sintaxis y semántica de los calificadores de la política 55
7.1.8. Perfil de la CRL 56
7.1.8.1. Numero de versión 56
7.1.8.2. CRL y extensiones 56
7.2. Perfil OCSP 58
7.2.1. Numero de versión 58
7.2.2. Extensiones OCSP 58
8. Auditoria y otras valoraciones 59
8.1. Frecuencia o circunstancias de valoración 59
8.2. Identidad y calificaciones del asesor 59
8.3. Relación entre el asesor y la entidad evaluada 59
8.4. Temas cubiertos en la valoración 59
8.5. Acciones tomadas como resultado de No Conformidades 59
8.6. Comunicación de resultados 59
9. Negocio y materias legales 60
9.1. Tarifas 60
9.1.1. Tarifas por emisión de certificados 60
9.1.2. Tarifas por acceso a certificados 60
9.1.3. Tarifas por información del estado de un certificado o certificados revocados 60

9.1.4. Política de reembolso....60
9.2. Responsabilidad financiera....60
9.3. Confidencialidad de información comercial....61
9.3.1. Alcance de la información confidencial....61
9.3.2. Información no considerada confidencial....61
9.3.3. Responsabilidades para proteger la información confidencial....61
9.4. Confidencialidad de la información personal....61
9.4.1. Plan de privacidad....61
9.4.2. Información considerada confidencial....62
9.4.3. Información no considerada confidencial....62
9.4.4. Responsabilidad de proteger la información....62
9.4.5. Notificación y consentimiento para usar la información confidencial....62
9.4.6. Acceso a la información a partir de proceso judicial o administrativo....62
9.5. Derechos de propiedad intelectual....62
9.6. Obligaciones y garantías....63
9.6.1. Obligaciones y garantías ANDES SCD....63
9.6.2. Obligaciones y garantías RA....64
9.6.3. Obligaciones y garantías del solicitante....64
9.6.4. Obligaciones y garantías suscriptores....64
9.6.5. Obligaciones y garantías de las partes que confían....65
9.7. Limitaciones de responsabilidad....65
9.7.1. Responsabilidad por la veracidad de la información del Suscriptor....65
9.7.2. Responsabilidad por disponibilidad del servicio....66
9.7.3. Responsabilidad por la funcionalidad del servicio en la infraestructura del Suscriptor....66
9.7.4. Responsabilidad frente delitos informáticos....66
9.8. Protección de datos personales:....67
9.9. Indemnizaciones....67
9.10. Término y terminación....67
9.10.1. Terminación de disposiciones....67
9.10.2. Efecto de terminación y supervivencia....68
9.11. Notificación individual y comunicación con los participantes....68
9.12. Procedimiento de cambio en las DPC y PC....68
9.12.1. Procedimiento de cambio....68
9.12.2. Mecanismo y periodo de notificación....68
9.12.3. Circunstancias bajo las cuales la OID debe cambiarse....69
9.13. Prevención y Resolución de disputas....69
9.14. Ley aplicable....69
9.15. Cumplimiento con la ley aplicable....69

Introducción

ANDES SCD es una entidad de certificación Abierta acreditada ante el Organismo Nacional de Acreditación de Colombia ONAC para prestar sus servicios de certificación digital en el territorio Colombiano y de conformidad con la normatividad Colombiana vigente.

El certificado de acreditación **16-ECD-004** otorgado a ANDES SCD está disponible en el directorio oficial de acreditaciones -Ent.Certificación digital: http://www.onac.org.co/modulos/contenido/default.asp?idmodulo=599

1. Presentación del documento

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

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

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

1.1. Nombre del documento e Identificación

Documento	DECLARACION DE PRÁCTICAS DE CERTIFICACION DE ANDES SCD
Descripción	Este documento presenta las declaraciones de la Autoridad de Certificación ANDES SCD respecto a las operaciones y procedimientos empleados como soporte al servicio de certificación en cumplimiento con la legislación vigente.
Identificador OID	1.3.6.1.4.1.31304.1.1.1.2.8
Versión	V 2.8
Fecha de emisión	22 Junio de 2018
Ubicación	http://www.andesscd.com.co/docs/DPC_ANDESSCD_V2.8.pdf

1.2. Identificación de la Entidad de Certificación Digital

Nombre	Andes Servicio de Certificación Digital S.A.
Razón Social	Andes Servicio de Certificación Digital S.A.
NIT	900.210.800 – 1
Número de Matrícula Cámara de Comercio	01774848 del 15 de febrero de 2008
Certificado de existencia y representación legal	https://www.andesscd.com.co/images/Certificado_de_existencia_y_representacion_legal.pdf
Domicilio Social y Correspondencia	Carrera 27 # 86 – 43 B. El Polo, Bogotá D.C.
Teléfono	(571) 7953430
FAX	(571) 7953430

Dirección correo electrónico	pqrs@andesscd.com.co
Dirección para peticiones, consultas y reclamos	Carrera 27 # 86 – 43 B. El Polo, Bogotá D.C.

La anterior información está disponible en la página web de Andes SCD sección Quiénes somos.

1.3. Alcance

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

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

1.4. Referencias

La presente Declaración de Prácticas de Certificación se emite teniendo en cuenta las recomendaciones de la (Requestforcomments) **RFC 3647**: Internet X.509 Public Key Infraestructure: Certificate Policy and Certification Practices Framework.

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

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

1.5. Definiciones

Termino	Descripción
Auditoria	Procedimiento utilizado para validar que los controles están en funcionamiento y son adecuados para sus propósitos. Incluye el registro y análisis de actividades para detectar intrusiones o abusos en un sistema de información. Los defectos hallados en una auditoría deben ser notificados al personal gestor adecuado para que sean tratados y solucionados
Llave pública y Llave privada	La llave pública se incluye en el certificado digital y la llave privada es utilizada únicamente por el titular del certificado. Todo lo que sea cifrado con una de las llaves solo se puede descifrar con la otra y viceversa.
Centro de datos (Data Center	Un Data Center es un edificio o porción de un edificio cuya función primaria es alojar una sala de cómputo y sus áreas de soporte. Los centros de cómputo son el cerebro de los sistemas de información de las empresas, operando 7x24x365 con requerimientos de altísima confiabilidad.
Componente informático	Cualquier dispositivo hardware o software susceptible de utilizar certificados digitales para su propio uso, con el fin de identificarse o intercambiar datos firmados o cifrados.
HSM	Hardware Secure Module. Componente que ofrece una mayor seguridad para la generación y almacenamiento de Llaves
Infraestructura de llaves públicas (PKI	Es el conjunto de personas, políticas, procedimientos y sistemas informáticos necesarios para proporcionar los servicios de autenticación, cifrado, integridad y no repudio mediante criptografía de llaves públicas y privadas y de certificados digitales.
Jerarquía de confianza	Conjunto de Autoridades de Certificación que mantienen relaciones de confianza por las cuales una CA de nivel superior garantiza la confiabilidad de una o varias de nivel inferior. En el caso de ANDES SCD la jerarquía tiene 3 niveles, la CA raíz en el nivel superior garantiza la confianza

Termino	Descripción
	de sus CA subordinadas Clase I, Clase II y Clase III. Y en el tercer nivel se encuentran las CA subordinadas de la CA Clase III convenios.
Listas de revocación	(CRL: CertificateRevocationList):Lista de acceso restringido donde figuran exclusivamente los certificados revocados.
OCSP	OCSP (Online Certificate Status Protocol): Protocolo informático que permite comprobar de forma rápida y sencilla la vigencia de un certificado electrónico
PKCS10	Estándar de criptografía de llave pública No 10 que define la estructura para una solicitud de firma de certificado.
Política de Certificación (PC)	Es un conjunto de disposiciones que indican la aplicabilidad de un certificado para una comunidad, incluyendo requerimientos exigibles a los miembros de dicha comunidad. Además indican la conveniencia de un certificado a un tipo de aplicación con requerimientos comunes de seguridad.
X.509	Estándar desarrollado por la ITU para las Infraestructuras de llave pública y los llamados "Certificados de atributos

1.6. Lista de acrónimos y abreviaturas

Abrev.	Descripción
CA	Autoridad Certificadora (CertificationAuthority)
CRL	Lista de certificados revocados (CertificateRevocationList)
DPC	Declaración de prácticas de certificación
FIPS	Normativa federal de proceso de información (Federal InformationProcessing Standard)
RA	Autoridad de Registro (RegistrationAuthority)
OID	Identificador digital de objetos (ObjectIdentifier Digital)
PIN	Número de Identificación Personal (Personal IdentificationNumber)
PKCS	Estándares de criptografía de llave Pública (Public Key CryptographyStandards)
PKI	Infraestructura de llave Pública (Public Key Infrastructure)

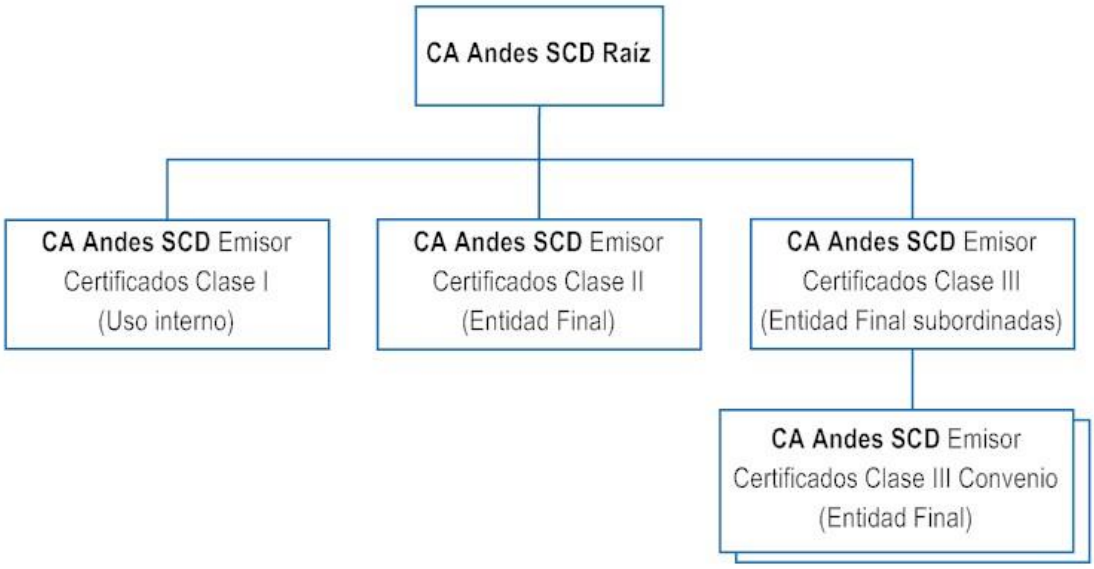
1.7. Participantes de PKI o modelo de confianza

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

1.7.1. Autoridad de Certificación (CA)

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

La jerarquía de certificación de ANDES SCD está compuesta por las siguientes Autoridades Certificadoras (CA)



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

DATOS DEL CERTIFICADO DE LA CA RAIZ		
Nombre distintivo	CN	ROOT CA ANDES SCD S.A.
	O	ANDES SCD
	OU	Division de certificacion
	C	CO
	L	Bogota D.C.
	E	info@andesscd.com.co
Número de serie	2c 31 02 20 35 d1 91 b2	
Nombre distintivo del emisor	CN	ROOT CA ANDES SCD S.A.
	O	ANDES SCD
	OU	Division de certificacion
	C	CO
	L	Bogota D.C.
	E	info@andesscd.com.co
Periodo de validez	Desde sábado, 24 de septiembre de 2016 11:50:57 AM Hasta lunes, 09 de julio de 2035 11:36:59 AM	
Usos de la llave	Firma digital, Firma de certificados, Firma CRL	
Huella digital (SHA-1)	39 77 88 4d a7 b8 3a 00 6a ed 15 8d 50 6a ac 86 1b ca 1a 4f	

CA ANDES SCD Emisor de certificados de clase I: Es la Autoridad Certificadora de segundo nivel subordinada de la CA ANDES SCD Raíz, su función es la de emitir certificados de uso interno para personal y componentes informáticos de la Autoridad Certificadora y Autoridades de Registro.

DATOS DEL CERTIFICADO DE LA CA CLASE I		
Nombre distintivo	CN	CA ANDES SCD S.A. Clase I
	O	ANDES SCD
	OU	Division de certificacion uso interno
	C	CO
	L	Bogota D.C.
	E	info@andesscd.com.co
Número de serie	75 4d 22 a1 3e f3 29 88	
Nombre distintivo del emisor	CN	ROOT CA ANDES SCD S.A.
	O	ANDES SCD
	OU	Division de certificacion
	C	CO
	L	Bogota D.C.
	E	info@andesscd.com.co
Periodo de validez	Desde Sábado, 24 de septiembre de 2016 11:56:01 AM. Hasta jueves, 09 de julio de 2020 4:54:50 PM	
Uso de la llave	Firma digital, Firma de certificados, Firma CRL	
Huella digital (SHA-1)	b0 50 07 ac 9b 5a 13 f2 e3 da 72 67 38 47 01 d9 45 93 58 cc	

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

DATOS DEL CERTIFICADO DE LA CA CLASE II		
Nombre distintivo	CN	CA ANDES SCD S.A. Clase II
	O	ANDES SCD.
	OU	Division de certificación entidad final
	C	CO
	L	Bogota D.C.
	E	info@andesscd.com.co
Número de serie	70 eb f5 b9 17 ba f2 88	
Nombre distintivo del emisor	CN	ROOT CA ANDES SCD S.A.
	O	ANDES SCD
	OU	Division de certificacion
	C	CO
	L	Bogota D.C.
	E	info@andesscd.com.co
Periodo de validez	Desde sábado, 24 de septiembre de 2016 11:59:26 AM Hasta Lunes, 09 de Agosto de 2021 09:05:38 AM	
Uso de la llave	Firma digital, Firma de certificados, Firma CRL	
Huella digital (SHA-1)	c9 d0 6b 90 35 22 e0 e2 f0 a4 32 40 0a db 4e f0 f4 ae 1d d1	

CA ANDES SCD Emisor de certificados de clase III: Es la Autoridad Certificadora de segundo nivel subordinada de la CA ANDES SCD Raíz, su función es la de emitir certificados para CA de entidad final (convenios) subordinadas.

DATOS DEL CERTIFICADO DE LA CA CLASE III		
Nombre distintivo	CN	CA ANDES SCD S.A. Clase III
	O	ANDES SCD.
	OU	Division de certificación entidad final subordinada
	C	CO
	L	Bogota D.C.
	E	info@andesscd.com.co
Número de serie	62 8f b0 4f f1 62 ff c2	
Nombre distintivo del emisor	CN	ROOT CA ANDES SCD S.A.
	O	ANDES SCD
	OU	Division de certificacion
	C	CO
	L	Bogota D.C.
	E	info@andesscd.com.co
Periodo de validez	Desde Sábado, 18 de Julio de 2017 10:24:48 a.m. Hasta Sábado, 15 de Noviembre de 2025 12:34:30 M	
Uso de la llave	Firma digital, Firma de certificados, Firma CRL	
Huella digital (SHA-1)	46 00 c4 d8 3a 1d 97 55 b8 8a 91 5d ae 97 cc 40 83 28 b9 66	

CA ANDES SCD Emisor de certificados de clase III convenios: Las CA de tercer nivel subordinadas de la CA ANDES SCD Clase III emiten certificados de entidad final para personas que interactúan con plataformas de entidades con convenio.

En los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios se especifican los datos del certificado de la CA emisora de los certificados.

1.7.2. Autoridad de Registro (RA)

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

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

a. Software de administración RA proporcionado por la CA con el cual se gestionan los procedimientos autorizados a ser ejecutados por parte de la RA.
b. Operador autorizado utiliza el software de administración de la RA. El control de acceso del operador al software de administración RA es realizado mediante certificados de firma digital emitidos y administrados por ANDES SCD.

1.7.3. Suscriptor

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

Entorno de certificación	Suscriptores
Certificados clase II (Entidad final)	Personas Naturales Personas Jurídicas
Certificados clase III (Entidad final Convenios)	Personas Naturales Personas Jurídicas

1.7.4. Solicitante

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

1.7.5. Usuario o tercero aceptante

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

1.8. Ámbito de aplicación

La Autoridad Certificadora ANDES SCD se encuentra estructurada para proveer servicios de certificación al público en general y para proveer servicios de certificación a nivel interno para personal y componentes informáticos de la Autoridad Certificadora y Autoridades de Registro

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

1.8.1. Usos del certificado

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

1.8.2. Límites de uso de los certificados

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

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

1.8.3. Prohibiciones Generales

Además de la prohibición frente al uso del certificado digital, el suscriptor tendrá las siguientes prohibiciones en el uso del servicio de certificación:

- No interferirá con la capacidad de otros suscriptores para acceder o utilizar el Servicio;
- No interferirá o interrumpirá el Servicio de certificación digital de ANDES, sus servidores o redes conectadas al mismo, o desobedecerá cualquier requisito, procedimiento, política o normativa de las redes conectadas al Servicio;
- No reproducirá, duplicará, copiará, utilizará, distribuirá, venderá, revenderá o explotará de cualquier otra forma, con fines comerciales, cualquier porción del Servicio;
- No realizará acciones como copiar, reproducir, publicar, distribuir, modificar, crear obras derivadas de alquilar, vender, transferir, exhibir, transmitir, compilar o recopilar en una base de datos o explotar comercialmente cualquier parte del Servicio, Contenido, en su totalidad o en parte;
- No “reflejará” el Servicio prestado por Andes SCD, u otro contenido de su propiedad en cualquier otro servidor.

1.8.4. Prohibiciones de uso de los certificados

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

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

La realización de operaciones no autorizadas, 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 para violar cualquier normatividad o regulación, así como transgredir los procedimientos reglados por la Entidad de certificación que otorga el certificado digital.
- No se permite el uso del certificado con el fin de infringir cualquier derecho intelectual o de propiedad de ANDES SCD o de terceros, incluyendo, por ejemplo, software, código, derechos de autor, marcas registradas, marcas de servicio y patentes.
- Andes SCD no responderá por el uso indebido del certificado, ocasionado por la negligencia del suscriptor en el manejo de su llave privada, como permitir el manejo de la misma por parte terceros, o faltando al deber de confidencialidad necesario para salvaguardar la llave privada, de acceso no autorizado o fraudulento.

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

1.9. Catálogo de servicios de certificación

1.9.1. Certificados para Entidad Final

ANDES SCD emite 6 tipos de certificados a las entidades finales del servicio de certificación, A continuación, se hace referencia a cada tipo de certificado y a la política de certificación donde puede obtener información detallada.

Certificados personales

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

Nombre de política	OID
CERTIFICADO PERSONA NATURAL	1.3.6.1.4.1.31304.1.2.1.2.6

Certificados de profesional titulado

El certificado de Profesional Titulado acredita la identidad del suscriptor y su título profesional, y le permite al suscriptor firmar documentos digitalmente en su propio nombre e interés.

Nombre de política	OID
CERTIFICADO PROFESIONAL TITULADO	1.3.6.1.4.1.31304.1.2.3.2.5

Certificados de representante legal

El certificado de representante legal acredita la identidad del suscriptor y su condición como representante legal de una entidad o persona jurídica. Le permite al suscriptor firmar documentos digitalmente en nombre de la entidad o persona jurídica que representa.

Nombre de política	OID
CERTIFICADO REPRESENTANTE LEGAL	1.3.6.1.4.1.31304.1.2.4.2.5

Certificados de pertenencia a empresa

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.

Nombre de política	OID
CERTIFICADO PERTENENCIA A EMPRESA	1.3.6.1.4.1.31304.1.2.5.2.7

Certificados de Función Pública

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.

Nombre de política	OID
CERTIFICADO FUNCION PUBLICA	1.3.6.1.4.1.31304.1.2.8.2.5

Certificados de Persona Jurídica

El certificado de Persona Jurídica acredita la identidad del suscriptor y su condición como empresa o persona jurídica, y le permite al suscriptor firmar documentos digitalmente en la calidad que acredita su certificado.

Nombre de política	OID
CERTIFICADO PERSONA JURIDICA	1.3.6.1.4.1.31304.1.2.9.2.7

Certificados de Comunidad Académica

El certificado de Comunidad Académica acredita la identidad del suscriptor y su calidad como docente, estudiante o miembro de una comunidad académica, y le permite al suscriptor firmar documentos digitalmente en su propio nombre e interés.

Nombre de política	OID
CERTIFICADO COMUNIDAD ACADEMICA	1.3.6.1.4.1.31304.1.2.2.2.4

Certificados Emisor de Factura Electrónica

El certificado para emisor de factura electrónica acredita la identidad del suscriptor y su condición como facturador electrónico, y le permite al suscriptor firmar documentos digitalmente en la calidad que acredita su certificado.

Nombre de política	OID
CERTIFICADO DE FACTURACIÓN ELECTRÓNICA	1.3.6.1.4.1.31304.1.2.6.1.0

1.10. Administración de la Política

El contenido de esta Declaración de Prácticas de Certificación es administrado por el comité de Políticas y Seguridad encargado de la elaboración, registro, mantenimiento y actualización de la DPC, las PC de uso interno y las PC de entidad final. A continuación, se detallan los datos del comité de políticas y seguridad y de una persona de contacto disponibles para responder preguntas respecto a este documento.

1.10.1. Organización que administra este 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

1.10.2. 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 : martin.vargas@andesscd.com.co
Teléfono : PBX 571 795 3430

1.10.3. Procedimientos de aprobación de la política

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

1.10.4. Publicación del documento

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

2. Publicación y registro de certificados

2.1. Directorio de certificados

El directorio de certificados es un directorio WEB de consulta disponible las 24 horas de los 7 días de la semana, donde se hallan todos los certificados de entidad final emitidos por ANDES SCD que no se encuentren revocados.

En la página WEB de ANDES SCD también se encuentra la lista de certificados revocados donde se especifica el motivo de revocación, la fecha y hora desde la cual el certificado no tiene validez. Los certificados revocados permanecen de forma indefinida en la CRL de la CA que los emitió. Ver sección 2.2 Medios de comunicación – Listas de revocación (CRL)

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

Para garantizar un servicio continuo de directorio de certificados y OCSP se cuenta con servidor de respaldo, de tal forma que, en caso de fallas o caída del servidor principal, el servidor de respaldo ofrecerá la disponibilidad del servicio.

2.2. Medios de publicación

Certificados de la CA raíz y CA subordinadas

Tipo de certificado	Medio de publicación
CA ANDES SCD Raíz:	http://certs.andesscd.com.co/Raiz.crt
CA ANDES SCD Clase II – Entidad Final	http://certs.andesscd.com.co/ClaseII.crt
CA ANDES SCD Clase III – Entidad Final subordinadas	http://certs.andesscd.com.co/ClaseIII.crt
CA ANDES SCD Clase III Convenios – Entidad Final	En los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios se especifica la URL de descarga del certificado de la CA emisora de los certificados

Repositorios de certificados LDAP

Repositorio certificados	Medio de publicación
Clase I – Uso interno	Solo acceso interno
Clase II – Entidad Final Clase III Convenios – Entidad Final	Acceso a LDAP a través de sección directorio de certificados.

Listas de revocación (CRL)

Las listas de revocación estarán firmadas electrónicamente por la CA de ANDES SCD que las emita

CRL	Medio de publicación
ROOT CA ANDES SCD S.A	http://crl.andesscd.com.co/Raiz.crl
CA ANDES SCD S.A. Clase I	Solo acceso interno
CA ANDES SCD S.A. Clase II	http://crl.andesscd.com.co/ClaseII.crl
CA ANDES SCD S.A. Clase III	http://crl.andesscd.com.co/ClaseIII.crl
CA ANDES SCD Clase III Convenios – Entidad Final	En los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios se especifica la URL de descarga de la CRL para CA emisora de los certificados

Protocolo de estado de certificados en línea (OCSP)

OCSP	Medio de publicación
CERTIFICADOS DE ROOT CA	http://ocsp.andesscd.com.co
CERTIFICADOS Clase I – Uso interno	
CERTIFICADOS Clase II – Entidad Final	
CERTIFICADOS Clase III – Entidad Final subordinadas	
CERTIFICADOS Clase III Convenios – Entidad Final	

Documentación DPC y PC

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

2.3. Frecuencia de publicación

Se publica en la página web de ANDES SCD la declaración de prácticas de certificación y las políticas de certificación para entidad final cada vez que haya cambios de acuerdo al procedimiento estipulado en este documento sección 9.11. Procedimiento de cambio en las DPC y PC.

El directorio de certificados se actualiza de forma permanente para reflejar los certificados que no se encuentran revocados.

ANDES SCD incluye los certificados revocados a la CRL de la CA que emitió el certificado dentro del periodo estipulado en el punto 4.4.7 Publicación de certificados revocados.

2.4. Control de acceso al directorio de certificados

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

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

3. Identificación y autenticación

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

3.1. Nombres

3.1.1. Tipos de nombres

Todos los certificados tienen una sección denominada Asunto cuyo objetivo es permitir identificar al suscriptor del certificado, esta sección contiene un DN o DistinguishedName caracterizado por un conjunto de atributos que conforman un nombre inequívoco y único para cada suscriptor de los certificados emitidos por ANDES SCD.

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

3.1.2. Necesidad para los nombres de ser significativos

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

3.1.3. Anónimos y pseudónimos en los nombres

No se admiten anónimos ni seudónimos para identificar el nombre de una persona natural o jurídica.
En el caso de una entidad o persona jurídica el nombre debe ser exactamente igual a la razón social, no se admiten nombres abreviados.
En el caso de una persona natural el nombre debe estar conformado por nombres y apellidos tal como figura en el documento de identificación reconocido.

3.1.4. Reglas para interpretar los formatos de nombre

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

3.1.5. Singularidad de los nombres

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

3.1.6. Reconocimiento, autenticación y función de las marcas registradas

ANDES SCD no admite deliberadamente el uso de un nombre de marca registrada cuyo derecho de uso no sea propiedad del suscriptor. Sin embargo la Autoridad Certificadora no está obligada a buscar evidencias de la posesión de marcas registradas antes de la emisión de los certificados.
ANDES SCD no asume compromisos en la emisión de certificados respecto al uso por parte de los suscriptores de una marca comercial.
A continuación se describe el procedimiento definido por ANDES SCD para la solución de disputas por uso de nombres o uso de marcas:

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

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

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

3.2. Aprobación de la identidad

3.2.1. Método para demostrar la posesión de la llave privada

ANDES SCD dispone de 2 mecanismos para la emisión de certificados de Entidad Final donde varía el procedimiento para gestionar la llave privada.

1. **Mecanismo 1** - El par de llaves es generado por el propio suscriptor
   Cuando el suscriptor genera su par de llaves, tramita su solicitud desde la página web, elige forma de entrega del certificado "PKCS10" y asocia el CSR que contiene la llave pública y está firmado implícitamente por la llave privada asociada
2. **Mecanismo 2** - El par de llaves es generado por ANDES SCD
   ANDES SCD se reserva el derecho a la generación del par de llaves cuando el suscriptor así lo determine o en función del formato de entrega del certificado.

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

Mecanismo 1 - El par de llaves es generado por el propio suscriptor

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

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

Cuando la forma de entrega del certificado es PKCS10

	Actividad	Detalle	Responsable
1	Generar el par de llaves	Generar el par de llaves y obtener el CSR que contiene la llave pública y está firmado implícitamente por la llave privada asociada	Solicitante
2	Tramitar solicitud desde página web	Ingresar a la página web de Andes SCD opción Solicitar Certificado y realizar lo siguiente: 1. Seleccionar el tipo de certificado que desea adquirir 2. Adjuntar la documentación requerida según PC aplicable al tipo de certificado 3. Diligenciar los datos de la solicitud 4. Seleccionar la fecha de inicio de vigencia del certificado y periodo de vigencia, 5. Seleccionar en forma de entrega del certificado “PKCS10” e informar CSR que contiene la llave pública y está firmado implícitamente por la llave privada asociada 6. Diligenciar los datos de forma de pago del servicio y facturación 7. Aceptar términos y condiciones 8. Registrar la solicitud y recibe correo electrónico con indicaciones	Solicitante
3	Confirmar correo electrónico	Revisar la solicitud y si la información es conforme debe realizar el paso de confirmar correo electrónico, de esta forma ANDES SCD conocerá que el solicitante está conforme con los datos y dará tramite a la solicitud	Solicitante
4	Estudiar solicitud	Verificar la información de la solicitud y determinar si es aprobada o rechazada. • En caso de rechazar la solicitud se envía un correo electrónico al solicitante indicando los motivos por los cuales se rechazó la solicitud y finaliza el proceso • En caso de aprobar la solicitud continua con el siguiente paso de este procedimiento	Andes SCD Supervisor RA
5	Emitir el certificado	Verificar la solicitud de emisión de certificado aprobada y dar la orden de generar el certificado • ANDES SCD comprueba que la llave privada está en posesión del suscriptor al verificar la FIRMA usando la llave pública que se envía en la petición de certificado PKCS10 • Generar el certificado digital • Enviar correo electrónico al solicitante para acceder a la zona segura de suscriptores	Andes SCD Operador
6	Descargar el certificado	Acceder a la zona segura de suscriptores y seguir instrucciones para descargar el certificado	Solicitante (Ahora Suscriptor)

Mecanismo 2 - El par de llaves es generado por ANDES SCD

ANDES SCD se reserva el derecho a la generación del par de llaves cuando el suscriptor así lo determine o en función del formato de entrega del certificado.

El método utilizado por ANDES SCD para comprobar que el solicitante posee la llave privada correspondiente a la llave pública para la que se solicita el certificado puede variar según la entidad con la cual Andes SCD tenga convenio de emisión de certificados. Esta información se especifica en los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios.

3.2.2. Autenticación de la identidad

Autenticación de identidad de Autoridades de Registro

Las RA vinculadas al modelo de confianza ANDES SCD cumplen el siguiente protocolo:

1. La Autoridad de Registro cuenta con la infraestructura tecnológica requerida para realizar las funciones delegadas por ANDES SCD.
2. Existe un contrato en vigor entre ANDES SCD y la Autoridad de Registro donde se concretan los aspectos de la delegación y las responsabilidades.
3. La identidad de los operadores de la Autoridad de Registro está comprobada y validada
4. Los operadores de la Autoridad de Registro han recibido la información necesaria para el correcto desempeño en sus funciones.
5. El procedimiento de autenticación de la autoridad de registro ha sido validado por ANDES SCD.
6. La Autoridad de Registro asume todas las obligaciones y responsabilidades relativas al desempeño de sus funciones
7. La comunicación entre la Autoridad de Registro y ANDES SCD se realiza de forma segura mediante el uso de certificados digitales.

Autenticación de identidad de Solicitantes y Suscriptores

Solicitud emisión de certificado tramitada desde página web

La información del solicitante es suministrada desde la página WEB junto con los soportes requeridos para el tipo de certificado. El solicitante debe suministrar a ANDES SCD información original, suficiente y adecuada respecto a los requisitos exigidos en la PC aplicable.

Solicitud emisión de certificado tramitada por convenios

El mecanismo de autenticación de identidad de solicitantes y suscriptores puede variar según la entidad con la cual Andes SCD tenga convenio de emisión de certificados. Esta información se especifica en los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios.

Autenticación de identidad de Personas Jurídicas

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

3.2.3. Información no verificada sobre el solicitante

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. Criterio para interoperación

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

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

1. La CA externa debe proporcionar un nivel de seguridad en la gestión de los certificados a lo largo de su ciclo de vida, como mínimo igual al de ANDES SCD.
2. La CA externa debe cumplir con los criterios específicos de acreditación de entidades de certificación digital establecidos en el documento CEA-4 1-10 emitido por ONAC.
3. Debe aportar el informe de auditoría de una autoridad externa de reconocido prestigio relativa a sus operaciones como medio de verificación del nivel de seguridad existente.
4. Establecer un convenio de colaboración en el que se fijen los compromisos adquiridos en materia de seguridad para los certificados incluidos en la interacción.

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

3.2.5. Identificación y autenticación para solicitar revocación

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

4. Ciclo de vida del certificado y procedimientos de operación

4.1. Emisión de certificados

4.1.1. Quién puede solicitar la emisión de un certificado

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

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

4.1.2. Procedimiento para solicitar emisión de certificado

Se describe en el documento de uso público Procedimiento para solicitar emisión de certificado identificado con el OID 1.3.6.1.4.1.31304.50.3.8.2.0 que se encuentra publicado en la página web de ANDES SCD.

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

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

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

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 PC correspondiente para conocer el ámbito de aplicación del certificado.

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

4.2. Renovación de certificados

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

4.3. Modificación de certificados

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

4.4. Revocación de certificados

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

4.4.1. Circunstancias de revocación

Un certificado digital emitido por la Autoridad Certificadora ANDES SCD es revocado en los siguientes eventos:

Eventos que afectan la información propia del certificado

1. Cuando hay posterior modificación de los antecedentes del suscriptor. (Ej. El suscriptor cambio de nombre o la entidad cambio de razón social).
2. Cuando se presenta la liquidación de una persona jurídica que se encuentra vinculada en un certificado.
3. Cuando hay falsificación de los antecedentes del suscriptor. (Ej. Después de emitido el certificado se descubre que se presentaron documentos falsos)
4. Cuando se comprueba que alguno de los datos del certificado es incorrecto o que no se cumple algún requisito.

Eventos que afectan la seguridad del modelo de confianza

1. Cuando el suscriptor, RA o ANDES SCD ha quebrantado una obligación, declaración o responsabilidad establecida en los términos y condiciones del servicio o da uso irregular del certificado.
2. Cuando el suscriptor informa que la llave privada del certificado ha sido comprometida o ha perdido su confidencialidad.
3. Cuando se ha cometido una infracción por parte de la RA o ANDES SCD en cuanto a los requisitos y procedimientos establecidos para la gestión de certificados.
4. Cuando el certificado emitido no cumple los procedimientos requeridos por la Declaración de Prácticas de Certificación (DPC) o cuando un requisito no fue satisfecho.

Eventos que afectan directamente al suscriptor

a) Cuando el suscriptor ha fallecido.
b) Cuando el suscriptor ha sido secuestrado.
c) Pérdida de su capacidad o inhabilitación del suscriptor.

Otros eventos:

a) Cuando es la voluntad del suscriptor revocar su certificado.
b) Cuando sea autorizado revocar el certificado por orden judicial o administrativa.

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

4.4.2. Quién puede solicitar la revocación certificados

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

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

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

4.4.3. Medios para revocar certificados

Los certificados digitales de Entidad Final pueden ser revocados a través de los siguientes medios:

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

2. **TELEFONICAMENTE**: El suscriptor puede solicitar la revocación de su certificado digital comunicándose telefónicamente con un operador de call center ANDES SCD durante el horario de atención al público.
   Este servicio está disponible de lunes a viernes en el horario de 8:00 am a 5:30 pm jornada continua.

3. **PRESENCIAL**: El suscriptor puede presentarse personalmente en las instalaciones de Andes SCD durante el horario de atención al público, solicitar el servicio de revocación, informar sus datos personales y el motivo de la revocación.
   Este servicio está disponible de lunes a viernes en el horario de 8:00 am a 5:30 pm jornada continua.

4. **CORREO ELECTRONICO**: A esta forma se recurre en última instancia cuando el suscriptor no tiene el código de revocación o cuando un tercero gestiona la solicitud de revocación de certificado de tipo Pertenencia a Empresa, Representante legal o Función pública para notificar que el suscriptor no se encuentra vinculado a la entidad tal como lo acredita el certificado.

5. **CONVENIOS**: Las entidades con convenios pueden solicitar la revocación de certificados tramitados bajo el convenio haciendo uso de servicios web proporcionados por ANDES SCD.

Los mecanismos anteriores para gestionar las solicitudes de revocación son inmediatos excepto el de correo electrónico que implica verificación por parte de Supervisor en las siguientes 24 horas después de la recepción de la solicitud.
Los medios para revocar certificados digitales de uso interno se especifican en la Política de Certificación correspondiente.

4.4.4. Procedimiento para revocar certificados

Los siguientes procedimientos para revocar un certificado aplican únicamente para certificados de Entidad Final.

Procedimiento en línea

1. Ingresar a la página web de Andes SCD https://www.andesscd.com.co
2. Hacer clic en la sección Revocar Certificado
3. Ingresar el número de cedula, correo electrónico, serial del certificado en hexadecimal y código de revocación del certificado que desea revocar. El serial del certificado en hexadecimal y el código de revocación se encuentran en la notificación de emisión de certificado.
4. Hacer clic en el botón BUSCAR
5. Se presenta la información del suscriptor y se permite visualizar el certificado
6. Seleccionar de la lista el motivo de la revocación (Cese de Operación, Reemplazado, Compromiso de la llave, Cancelación de privilegios)
7. Escribir en observaciones la razón por la cual desea revocar.
8. Hacer clic en el botón REVOCARy el certificado es revocado de inmediato
9. El sistema automáticamente envía un correo electrónico al suscriptor confirmando que el certificado ha sido revocado.
10. El certificado es publicado en la próxima CRL de la CA que emitió el certificado.

Procedimiento telefónico

1. Realizar llamada telefónica al número que se encuentra publicado en la página web de Andes SCD https://www.andesscd.com.co
2. Solicitar el servicio de revocación telefónica
3. Suministrar al operador del Call Center la siguiente información del certificado que desea revocar:
   - Número de cedula
   - Correo electrónico
   - Serial del certificado en hexadecimal
   - Código de revocación
   - Motivo de revocación
4. El operador del Call Center gestiona la solicitud de revocación
5. El sistema automáticamente envía un correo electrónico al suscriptor confirmando que el certificado ha sido revocado.
6. El certificado es publicado en la próxima CRL de la CA que emitió el certificado.

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

Procedimiento presencial

1. El suscriptor debe presentarse personalmente en las instalaciones de Andes SCD durante el horario de atención al público (Lunes a viernes en el horario de 7:30 am a 5:30 pm)
2. Solicitar el servicio de revocación, informar sus datos personales y motivo de la revocación por escrito.
3. La petición de revocación es recibida por el Supervisor RA y el certificado es revocado de inmediato
4. El sistema automáticamente envía un correo electrónico al suscriptor informando que el certificado ha sido revocado
5. El certificado es publicado en la próxima CRL de la CA que emitió el certificado.

Procedimiento correo electrónico

1. El solicitante debe elaborar una carta de solicitud de revocación que debe contener la siguiente información
    a. Fecha de solicitud de la revocación
    b. Serial del certificado a revocar
    c. Tipo de certificado
    d. Titular del certificado (Nombre completo e identificación)
    e. Motivo de revocación
    f. Nombre completo, identificación y teléfono de contacto (si el solicitante no es el suscriptor)
    g. Firma del solicitante
2. El solicitante debe enviar al correo mailra@andesscd.com.co mensaje con asunto "Solicitud de Revocación de Certificado" adjuntando carta donde se solicite formalmente la revocación del certificado.
3. Las solicitudes de revocación recibidas en el correo mailra@andesscd.com.co son registradas automáticamente en el sistema de Tickets OTRS y son atendidas por el Supervisor RA en las siguientes 24 horas a la recepción de la solicitud.
4. El Supervisor RA realiza la verificación correspondiente de los datos suministrados en la carta de solicitud de revocación y ejecuta el proceso de revocación en caso de conformidad.
5. El sistema automáticamente envía un correo electrónico al suscriptor informando que el certificado ha sido revocado
6. El certificado es publicado en la próxima CRL de la CA que emitió el certificado

Procedimiento convenios

En los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios se especifica el procedimiento a seguir por la entidad con convenio para revocar certificados.

4.4.5. Tiempo para procesar la solicitud de revocación

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

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

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

La verificación de las revocaciones es obligatoria para el uso por parte de terceros, esta verificación se realiza mediante la consulta directa de CRL de la CA que emitió el certificado o mediante consulta OCSP. Es de carácter obligatorio la comprobación de las CRL por parte de los usuarios para ver el estado de los certificados en los cuales van a confiar, debe descargarse la última CRL de la página web de ANDES SCD y comprobar la validez de la CRL previamente a cada uso.

4.4.7. Publicación de certificados revocados

La información relativa a la revocación de un certificado se difunde mediante la publicación periódica de las siguientes listas de revocación:

CRL	Periodicidad de publicación
CRL de CA ANDES SCD S.A. Clase II	48 horas
CRL de CA ANDES SCD S.A. Clase III	30 días
CRL de CA ANDES SCD S.A. Clase III Convenios	48 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.
La CRL de CA ANDES SCD S.A. Clase I se genera cada 15 días y no son publicadas porque son de uso interno de ANDES SCD.

Nota: La CRL de ROOT CA se genera cuando se necesite activando momentáneamente la CA Raíz (la CA Raíz permanece offline).

4.5. Servicios de información del estado de certificado

4.5.1. Características operacionales

Se dispone de 2 servicios que proporcionan información del estado de los certificados emitidos:

1. Publicación de CRL: El acceso a las CRL se realiza vía HTTP/HTTPS
2. Servicio de validación en línea OCSP: Mediante el uso de este protocolo que cumple con la RFC 2560, 5019 y 6960 se determina el estado actual de cualquier certificado sin requerir las CRL.

4.5.2. Disponibilidad del servicio

El servicio on-line de comprobación de revocaciones está disponible las 24 horas del día de los 7 días de la semana. ANDES SCD realiza los esfuerzos necesarios para que el servicio no se encuentre suspendido de forma continua por más de 24 horas.

4.5.3. Fin de suscripción

El fin de suscripción se produce cuando expira el periodo de vigencia del certificado o se revoca el certificado por alguna de las causas descritas en la sección 4.4.1 Circunstancias de revocación.

4.6. Reposición de certificados

En las políticas de certificación se especifica el proceso de reposición de certificados.

4.7. Vigencia de los certificados

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

5. Controles de seguridad

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

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

SECCION	OID DOCUMENTO
Política de seguridad de la información	1.3.6.1.4.1.31304.100.2.2
Manual de seguridad de la información	1.3.6.1.4.1.31304.100.6.51
Procedimiento de gestión de incidentes de seguridad de la información	1.3.6.1.4.1.31304.100.2.12
Procedimiento de gestión de inventario de activos tecnológicos	1.3.6.1.4.1.31304.100.3.2
Metodología de Gestión de riesgos	1.3.6.1.4.1.31304.100.6.49
Manual de procedimientos en protección de datos personales	1.3.6.1.4.1.31304.100.6.45

5.1. Condiciones exigidas a proveedores críticos

Para Andes SCD, es un deber la prestación de un excelente servicio, por esta razón, los proveedores han de ser la primera línea para poder sustentar nuestro compromiso de servicio y con la calidad de este, así bien nuestros proveedores son evaluados de forma anual para validar el cumplimento de los niveles de servicio definidos contractualmente.

El centro de datos principal debe cumplir con una disponibilidad de sitio del 99,9% para la prestación de los servicios de certificación digital, además debe cumplir con los demás requisitos tanto administrativos como técnicos definidos contractualmente.

5.2. Controles de seguridad física

5.2.1. Ubicación y seguridad ambiental

Los sistemas y equipamientos empleados por ANDES SCD para ofrecer el servicio de certificación se encuentran ubicados físicamente en el Data Center Triara, un centro de datos de clase mundial ubicado en la Sabana de Bogotá en un lugar estratégico de gran desarrollo empresarial.

El Data Center Triara es un sitio que ha sido diseñado con especificaciones TIA/EIA 942 – TierIV [1], cumple con estrictas normas de construcción y seguimiento a rigurosos estándares de operación para garantizar que los equipos e información allí alojados cuenten con el máximo nivel de seguridad.

Sus instalaciones están localizadas en una zona nula de actividad sísmica y se encuentran dentro de un bunker de concreto armado y acero, las edificaciones son resistentes a inundaciones, vendavales, descargas eléctricas y precipitaciones atmosféricas y están dotadas con un subsistema arquitectónico, un subsistema de telecomunicaciones, un subsistema eléctrico, un subsistema mecánico y un sistema de seguridad física articulado por metodologías de administración de riesgo y seguridad.

Los servicios de seguridad que ofrece el Data Center Triara han sido integrados a las políticas y procedimientos de seguridad de ANDES SCD describiendo cada uno de los controles implementados para evitar el riesgo, alteración, sustracción, daño o pérdida de los activos involucrados en la prestación del servicio de certificación digital.

Perímetro de seguridad física

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

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

Protección contra amenazas externas y ambientales

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

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

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

5.2.2. Gestión del sistema de acceso

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

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

1. Autenticación ante aplicaciones críticas mediante Certificados Digitales combinado con nombre de usuario y contraseña.
2. Controles basados en cortafuegos de alta disponibilidad
3. Lista actualizada de usuarios autorizados a ingresar al sistema especificando el nivel de acceso y privilegios que tiene cada usuario.
4. Monitorización para detectar accesos no autorizados de forma inmediata

5.2.3. Seguridad de los servidores

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

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

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

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

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

5.3. Controles procedimentales

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

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

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

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

5.3.1. Roles de confianza

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

a. Operador CA: Es el responsable de revisar las solicitudes de emisión de certificado aprobadas por el Supervisor RA y dar la orden de generar el certificado.

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

c. Administradores de HSM: Es el responsable de administrar el dispositivo criptográfico que crea y almacena las llaves privadas de la CA raíz y las CA subordinadas, es responsable del funcionamiento de los componentes de la PKI, del hardware y del software. Está autorizado para

realizar cambios en la configuración del sistema y supervisar el correcto funcionamiento del servicio de certificación.

- Recuperación de la funcionalidad del HSM en caso de fallo.
- Recuperación de las llaves en caso de borrado accidental.
- Ampliación del número de HSM integrados a la infraestructura
- Administración de cuentas de usuarios del HSM (Administradores u operadores).
- -Ceremonia de generación de llaves para las CA
- Activación de llaves privadas de CA para su utilización.
- Gestionar los controles de acceso de los usuarios a los equipos, aplicativos y componentes de la infraestructura tecnológica de ANDES SCD
- Realizar las tareas relacionadas con la administración de la CA, como gestionar el ciclo de vida de los certificados, crear nuevos perfiles de certificados y mantener los controles de seguridad convenidos.
- Realizar Instalación y configuración de sistemas operativos, productos software en los servidores de ANDES SCD
- Realizar mantenimiento a los servidores y sistemas y se encargara de cubrir los requerimientos de seguridad establecidos para la operación, administración y comunicación de los sistemas y recursos tecnológicos de ANDES SCD.
- Monitorizar y verificar el correcto servicio de CRL, OCSP.
- Establecer y documentar procesos de monitorización de sistemas, aplicaciones y servicios
- Supervisar la ejecución de políticas de protección de datos y sistemas de respaldo.
- Supervisar que el directorio de certificados se mantenga actualizado.
- Supervisar el correcto funcionamiento de los servidores y componentes del sistema de certificación.
- Supervisar el correcto funcionamiento del servicio de certificación y administración del ciclo de vida de los certificados.

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

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

Funciones del Comité de Políticas y Seguridad:

- Revisar por lo menos una vez al año las Políticas de Seguridad de la Información (PSI) y si hay modificaciones proponerlas ante la dirección para su aprobación.
- Implementar metodologías para comunicar los riesgos e incidentes de seguridad presentados en los diferentes componentes del modelo de confianza (ANDES SCD, RA, entidades finales).

- Establecer y apoyar los planes de capacitación que permitan actualizar a los empleados en aspectos de seguridad.
- Definir las directrices básicas de seguridad para los requerimientos en la adquisición de hardware y software.
- Asignar responsabilidades a cada área para incrementar la seguridad de la información y vigilar que estas sean cumplidas.
- Vigilar que las excepciones de la política de seguridad estén autorizadas únicamente por la dirección de ANDES SCD y que se deje constancia de los riesgos que en forma consciente se están asumiendo y el periodo de vigencia de la excepción.
- Investigar las violaciones de seguridad y presentar informes al área directiva.
- Realizar seguimiento a las acciones disciplinarias y legales asociadas con las violaciones de seguridad investigadas.
- Preparar y mantener el plan de contingencia y recuperación de desastres ante alguna emergencia.
- Liderar las pruebas periódicas sobre el plan de contingencia y recuperación de desastres

f. Coordinador de seguridad: Debe velar por el diseño, implantación y cumplimiento de los procedimientos y prácticas de seguridad en las instalaciones y los procedimientos y prácticas de seguridad para proteger la información gestionada en el perímetro físico de seguridad de ANDES SCD.
   - Desarrollar métodos y técnicas para monitorear efectivamente los sistemas de seguridad de la información y reportar periódicamente su funcionamiento a la alta dirección.
   - Hacer un seguimiento y documentación de los riesgos e incidentes que afectan los recursos y la información y crear controles específicos.
   - Cerciorarse de que los sistemas están correctamente documentados.
   - Resuelve las incidencias relacionadas con vulnerabilidades a la seguridad
   - Mantener actualizadas las Políticas de Seguridad de acuerdo a las disposiciones vigentes.

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

h. Operadores call center ANDES SCD: Son las personas encargadas de atender las inquietudes de usuarios, solicitantes y suscriptores
   - Atención al cliente vía chat, email o telefónicamente
   - Brindan información de carácter no confidencial
   - Realizan el registro de incidencias y gestión de soportes

5.3.2. Número de personas requeridas por tarea

Se garantiza que se dispone por lo menos 2 personas para realizar las tareas que requieren control multipersona como:

- La generación de llaves de las CA
- La recuperación y respaldo de la llave privada de las CA
- La emisión de certificados de las CA
- Activación de la llave privada de las CA

5.3.3. Identificación y autenticación de cada rol

El acceso a recursos se realiza dependiendo del activo mediante certificados digitales y usuario y contraseña.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

Las personas asignadas para cada rol son identificadas por el auditor interno quien verifica que cada persona realiza las operaciones para las que está asignado.

5.3.4. Roles que requieren separación de deberes

La asignación del personal garantiza que se cumplen las siguientes condiciones

- Un administrador de HSM no puede ser administrador RA
- Un supervisor RA no puede ser operador de la CA.
- Un coordinador de seguridad no puede ser administrador RA.
- Un auditor interno no puede ser administrador HSM.

5.3.5. Relación entre ANDES SCD y las Autoridades de Registro

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

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

5.4. Controles de seguridad personal

5.4.1. Calificaciones, experiencia y requisitos

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

1. Conceptos básicos de PKI
2. Responsabilidades del cargo
3. Uso y operación del software y hardware utilizado
4. Copias de seguridad y medidas de seguridad a tener en cuenta cuando se abandona momentáneamente el equipo de trabajo.
5. Políticas y procesamientos de seguridad y operación de ANDES SCD
6. Elaboración de reportes para notificar los incidentes o anomalías que pudieran afectar la seguridad de los datos o accesos a plataformas informáticas. Por incidencia se entienden las siguientes circunstancias
   - Cambios no autorizados en la información
   - Intentos de acceso o accesos a información confidencial por personas no autorizadas
   - Errores en el aplicativo informático
   - Cualquier otro tipo de problema que pueda afecte la prestación y calidad del servicio.

5.4.2. Procedimientos de comprobación de antecedentes

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

5.4.3. Requisitos de entrenamiento

El personal de ANDES SCD involucrado en el ciclo de vida de los certificados debe conocer la documentación sobre Políticas de Seguridad y aplicarlas para realizar de forma competente sus funciones.

El personal debe formarse en los siguientes aspectos:

- Declaración de Prácticas de Certificación.
- Políticas de Certificación
- Concienciación seguridad de la información.
- CEA 4.1-10

5.4.4. Frecuencia de adiestramiento y requisitos

El personal de ANDES SCD involucrado en el ciclo de vida de los certificados debe estar actualizado respecto a procedimientos y las últimas versiones de las Políticas y Prácticas de Certificación a fin de asegurar la correcta realización de sus funciones.

5.4.5. Frecuencia de rotación de trabajo

La rotación de trabajo entre el personal de ANDES SCD está contemplada para garantizar la continuidad de la prestación del servicio en caso de ausencia de alguno de los empleados. La rotación de trabajo

entre los roles de confianza se realiza únicamente con personal calificado para realizar las funciones del cargo.

5.4.6. Sanciones por acciones desautorizadas

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

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

- Prohibición de compartir llaves, contraseñas o datos para acceder a sistemas y aplicaciones de ANDES SCD incluso dentro de la misma organización. El usuario es el único responsable de lo que se haga con su llave por lo tanto debe protegerla.
- Prohibición de cualquier ataque contra elementos o sistemas de seguridad (Ej. Borrado de programas, archivos e informaciones vitales para ANDES SCD)
- Prohibición de instalación de software que no cuente con licencia de uso y desinstalación de software requerido para realizar sus actividades.
- Prohibición de uso de activos de la infraestructura para fines que no le han sido encomendados.
- Prohibición de actividades ilícitas o ilegales que atenten contra la moral y derechos de terceros
- Prohibición de disponer de información sensible o confidencial para usos ajenos a su actividad dentro del modelo de confianza. (Ej. Extraer clandestinamente información confidencial de las instalaciones de ANDES SCD o de RA y revelarla ante terceros)
- Compromiso de confidencialidad respecto a las informaciones que accede en el desempeño de sus funciones incluso después de terminar la vinculación con ANDES SCD.

5.4.7. Requisitos de la contratación de personal

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

5.4.8. Documentación suministrada al personal

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

5.5. Controles de Auditoría

5.5.1. Tipos de eventos auditados

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

1. Encendido y apagado de los servidores
2. Intentos exitosos y fallidos de cambiar parámetros de seguridad del sistema operativo de los servidores.
3. Inicio y fin de sesión en los servidores
4. Intentos de accesos no autorizados al sistema a través de la red al sistema de certificación.
5. Registros realizados desde las aplicaciones de la Autoridad de Certificación

6. Cambio de contraseña
7. Cambios en la creación de perfiles de certificados
8. Intentos exitosos y fallidos de generar, firmar, emitir o revocar certificados
9. Intentos exitosos y fallidos de generar, firmar o emitir una CRL
10. Administración y ciclo de vida de los certificados digitales
    - Actualización de información relacionada con el suscriptor
    - Registro de solicitud de emisión de certificado
    - Revocación de certificado
    - Resultado del estudio de la solicitud de emisión de certificado
    - Generación de certificado
    - Descarga de certificado

Los eventos del syslog detallan la fecha y hora, la severidad del evento, el servidor donde ocurrió el evento, cual aplicación generó el evento y descripción del evento.
La severidad del evento se clasifica en las siguientes categorías:

- Info : Mensaje de tipo informativo
- Debug : Mensaje de depuración de bajo nivel
- Notice : Mensaje de evento inusual pero que no constituye condición de error
- Warning: Mensaje que indica que un error puede ocurrir si una acción no es tomada.
- Error : Mensaje de condición de error

Los eventos auditados por aplicaciones de ANDES SCD detallan, la fecha y hora, usuario responsable, tipo de evento auditado y descripción de la acción realizada

5.5.2. Frecuencia de procesamiento de los registros de auditoría

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

5.5.3. Periodo de resguardo de los registros de auditoría

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

5.5.4. Protección de los registros de auditoría

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

5.5.5. Procedimientos de respaldo de los registros de auditoría

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

5.5.6. Sistemas de recolección de información de auditoría

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

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

Los sistemas de recolección de información tienen las siguientes características:

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

5.5.7. Sistemas de revisión de eventos

Se dispone de herramientas para consultar los eventos auditados a partir de múltiples parámetros de búsqueda que facilitan la detección de eventos según categoría de severidad

5.5.8. Análisis de vulnerabilidades

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

5.6. Controles de almacenamiento y archivo de la información

5.6.1. Tipo de información a resguardar

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

- Todos los eventos de la auditoría del syslog
- Todos los datos relativos a los certificados emitidos
- Solicitudes de emisión y revocación de certificados.
- Versiones de documentación (Prácticas y Políticas de Certificación, Políticas de Seguridad, manuales técnicos y operativos)

5.6.2. Periodo de resguardo de la información

Todos los datos del sistema relativos al ciclo de vida de los certificados se conservan de forma digital durante el periodo que establezca la legislación vigente cuando sea aplicable. Los certificados vigentes y caducados se conservan publicados en LDAP de acuerdo con el RFC 4523.
La información relativa a la identificación y autenticación del suscriptor se conservan durante al menos 15 años.

5.6.3. Protección de la información

ANDES SCD asegura la correcta protección de la información mediante la asignación de personal calificado para su tratamiento y sistemas de alta disponibilidad.

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

5.6.4. Procedimiento de respaldo de la información

La información y el aplicativo software utilizados por ANDES SCD en los servidores catalogados como críticos son sincronizados por un mecanismo automático y en línea a servidores de respaldo

5.6.5. Sistemas de almacenamiento internos y externos

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

5.6.6. Procedimiento para obtener y verificar la información archivada

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

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

5.7. Cambio de llave

Los cambios de llave de las CA de ANDES SCD se realizan al cumplirse su periodo de vigencia y siguiendo el protocolo de cambio de llaves de la CA.

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

Cuando se emita un nuevo certificado para cada una de las CA de la jerarquía de certificación de ANDES SCD se creará un nuevo par de llaves para cada CA.

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

- La nueva llave pública firmada por la llave privada antigua.
- La antigua llave pública firmada con la llave privada nueva.

En el documento de uso interno **Administración de la llave privada de la CA** identificado con el OID 1.3.6.1.4.1.31304.100.1.4 detalla el proceso de cambio de llaves de la CA raíz de las CA subordinadas.

El cambio de llaves de suscriptores de certificados de uso interno y de entidad final varía según el tipo de certificado y se encuentra definido en cada Política de Certificación (PC)

5.8. Compromiso y recuperación de desastre

ANDES SCD ha desarrollado un plan de contingencia y continuidad del negocio establecido y probado para garantizar la prestación de los servicios de acuerdo a las normas aplicables.

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

5.8.1. Procedimientos para administrar incidentes

ANDES SCD dispone del siguiente procedimiento para gestionar incidentes o eventos que puedan afectar la confidencialidad, integridad y disponibilidad de la información y los servicios:

1. **Detección y reporte del incidente**: Conocimiento del incidente a través de sistemas de monitorización, sistemas de detección de intrusos, registros del sistema, aviso por parte del personal o por parte de los clientes.
2. **Análisis y evaluación del incidente**: Una vez detectado el incidente se determina el procedimiento de respuesta y se contacta con las personas responsables para evaluar y documentar las acciones a tomar según la gravedad de la incidencia. Se efectúa una investigación para determinar cuál fue el alcance del incidente, es decir averiguar hasta donde llego el ataque y la máxima información posible de la incidencia.
3. **Control de daños ocasionados por incidente**: Reaccionar rápidamente para contener la incidencia y evitar que se propague tomando medidas como bloquear accesos al sistema.
4. **Investigación y recopilación de evidencias**: Revisar registros de auditoría para realizar un seguimiento de lo ocurrido.
5. **Recuperación y medidas contra incidencia**: Restaurar el sistema a su correcto funcionamiento y documentar el procedimiento y formas de evitar que vuelva a presentarse la incidencia.
6. **Análisis posterior de la incidencia para mejorar el procedimiento**: Realizar un análisis de todo lo ocurrido, detectar la causa de la incidencia, corregir la causa para el futuro, analizar la respuesta y corregir errores en la respuesta.

ANDES SCD tiene establecido un Plan de Contingencias que especifica las acciones a ejecutar, componentes o recursos a utilizar y como debe reaccionar el personal en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación.

5.8.2. Recursos informáticos, software y datos corruptos

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

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

5.8.3. Procedimientos ante compromiso de la llave privada

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

ANDES SCD con el fin de continuar verificando los certificados emitidos durante su periodo de funcionamiento.

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

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

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

5.8.4. Capacidades de continuidad del negocio ante un desastre

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

- La redundancia de los componentes más críticos
- El chequeo periódico de los servicios
- Habilitación de los servicios en centro de datos alterno.

5.8.5. Medidas para corrección de vulnerabilidades detectadas

ANDES SCD contempla en el documento Plan de continuidad del negocio con el OID 1.3.6.1.4.1.31304.100.6.64.4.0 los procedimientos de seguridad para el manejo de eventos que puedan afectar la prestación del servicio de certificación

5.9. Terminación de CA o RA

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

- La Autoridad Certificadora ANDES SCD notificará con un tiempo 30 días de anticipación a la Superintendencia de Industria y Comercio y al Organismo Nacional de Acreditación la intención de cesar sus actividades como prestador de servicios de certificación.
- Una vez se haya recibido autorización por parte de la Superintendencia de Industria y Comercio y del Organismo Nacional de Acreditación para el cese de las actividades se hará en la forma y siguiendo el cronograma presentado por la ECD al ente de vigilancia y control y que éste apruebe y se recurrirá a los medios de comunicación para notificar a los usuarios del sistema de certificación el cese de la actividad como Prestador de Servicios de Certificación.
- La comunicación del cese de actividades a los usuarios del servicio de certificación se realiza mediante 2 avisos publicados en diarios de amplia circulación nacional, con un intervalo de 15 días, informando sobre la terminación de las actividades, la fecha precisa de la cesación, las

consecuencias jurídicas de la cesación respecto a los certificados expedidos, La posibilidad de que un suscriptor obtenga el reembolso equivalente al valor del tiempo de vigencia restante del certificado y la autorización emitida por la Superintendencia de Industria y Comercio para que la ECD pueda cesar el servicio, y si es el caso, se seguirán publicando las CRL hasta cuando expire el último de los certificados emitidos.

- Transmitir todas las responsabilidades, obligaciones y derechos dentro del sistema de certificación a otra Autoridad Certificadora que esté dispuesta a continuar con el servicio. En caso de no encontrar otra Autoridad Certificadora que acepte la transferencia de derechos y obligaciones, se procede a la revocación de todos los certificados que estén sin expirar en el momento del cese definitivo de la Autoridad de Certificación.
- ANDES SCD realizará un esfuerzo para asegurar que la interrupción del servicio de certificación cause las menores molestias a los suscriptores y a las personas que necesitan verificar firmas digitales.
- Pagar una compensación a los suscriptores que lo soliciten por revocar sus certificados antes de la fecha de expiración por motivo de cese de la Autoridad de Certificación, esta compensación no excede la tarifa de compra del certificado y es proporcional de acuerdo al tiempo transcurrido desde el inicio de vigencia del certificado y la fecha de revocación, si lo solicitan dentro de los dos (2) meses siguientes a la segunda publicación.
- Revocar toda autorización a entidades subcontratadas para actuar en nombre de ANDES SCD en el procedimiento de emisión de certificados.
- La ECD debe cumplir los planes anteriores, mantener la documentación y registros de pruebas anuales en su sede principal y accesible a ONAC.
- Cumplir las obligaciones impuestas por la ley Colombiana.

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

6. Controles de seguridad técnica

6.1. Generación de llaves e instalación

6.1.1. Generación del par de llaves

Llaves de la CA

ANDES SCD cuenta con una jerarquía de confianza de 3 niveles conformada por la CA de nivel superior o CA Raíz que garantiza la confiabilidad de sus 3 CA subordinadas de segundo nivel que han sido creadas para diferentes propósitos:

- CA Emisora de certificados Clase I: Emite certificados de uso interno para personal y componentes informáticos que son indispensables para el funcionamiento interno y operativo de la Autoridad Certificadora y Autoridades de Registro.
- CA Emisora de certificados Clase II o de entidad final: Emite certificados a personas que en su propio nombre, representando una entidad o acreditando un cargo ha solicitado la emisión de un certificado digital a ANDES SCD.
- CA Emisora de certificados Clase III o de entidad final subordinadas: Emite certificados a CA subordinadas de entidad final convenios.

- CA Emisora de certificados Clase III Convenios: Existen diferentes CA de tercer nivel subordinadas de la CA Clase III. Cada CA de tercer nivel emite certificados a personas para interactuar con plataforma de la entidad con convenio que tramito la solicitud.

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

Llaves del suscriptor

1. **Mecanismo 1** - El par de llaves generado por el propio suscriptor
   Aplica cuando el suscriptor ha elegido forma de entrega del certificado PKCS10.
   El par de llaves (llave pública y llave privada) es creado por el propio suscriptor, la llave privada permanece exclusivamente en posesión del suscriptor y en ningún momento es conocida por Andes SCD, mientras que la llave pública es enviada por el suscriptor a Andes SCD en el CSR para la emisión del certificado.

2. **Mecanismo 2** - El par de llaves generado por ANDES SCD
   Aplica cuando a solicitud de emisión de certificado se ha realizado mediante convenios o cuando el suscriptor ha delegado a ANDES SCD la generación del par de llaves.

Mecanismo 1 - **El par de llaves es generado por el propio suscriptor**
Las llaves pública y privada de titulares de certificados Entidad final son generadas por el propio suscriptor de forma segura utilizando TOKEN, HSM o por software

A continuación se describe las características de los TOKEN utilizados
El TOKEN es un dispositivo criptográfico de custodia de la llave privada aportan un nivel de seguridad igual o superior a lo establecido para los dispositivos de creación de datos de firma ofreciendo lo siguiente:

- 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 disponible de 64 Kb
- Certificación CE y FCC
- Certificación FIPS 140-2 Nivel 3.
- 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

El dispositivo criptográfico posee una clave de activación (PIN) para hacer uso de las llaves privadas, esta clave de activación debe ser de uso exclusivo del suscriptor para garantizar que los datos de creación de firma están protegidos contra la utilización de terceros.

Mecanismo 2 - **El par de llaves es generado por Andes SCD**
Las llaves pública y privada de titulares de certificados de Entidad final son generadas por ANDES SCD mientras la solicitud sea de convenios o cuando el suscriptor así lo determine.

En las solicitudes de emisión de certificados tramitada por convenios el proceso puede variar según la entidad con la cual Andes SCD tenga convenio de emisión de certificados. Esta información se especifica en los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios.

Garantía de la seguridad que ofrecen las llaves
ANDES SCD basa en el algoritmo RSA la generación de todas las llaves públicas y privadas para sus CA y suscriptores del servicio de certificación.

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

ANDES SCD utiliza llaves de longitud 2048 bits para certificados de uso interno y entidad final

6.1.2. Entrega de la llave privada al suscriptor
De acuerdo al mecanismo de generación de llaves varia la entrega de la llave privada del suscriptor

Mecanismo 1 - **El par de llaves es generado por el propio suscriptor**
No procede porque la llave privada en ningún momento es conocida por ANDES SCD. La llave privada es generada por el propio suscriptor.

Mecanismo 2 - **El par de llaves es generado por Andes SCD**
El método de entrega de la llave privada al suscriptor puede variar según la entidad con la cual Andes SCD tenga convenio de emisión de certificados o en función del formato de entrega. Esta información se especifica en los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios.

6.1.3. Entrega de la llave pública al emisor del certificado
De acuerdo al mecanismo de generación de llaves varia la entrega de la llave pública del suscriptor a ANDES SCD.

Mecanismo 1 - El par de llaves es generado por el propio suscriptor
La entrega de la llave pública del suscriptor a ANDES SCD se realiza de forma segura en formato PKCS10, el cual es generado al registrar desde la página web la solicitud de emisión de certificado con forma de entrega “PKCS10” y contiene la llave publica generada por el propio suscriptor

Mecanismo 2 - **El par de llaves es generado por Andes SCD**

No procede porque para este caso ANDES SCD tiene la llave pública del suscriptor

6.1.4. Distribución de la llave pública del suscriptor

La llave pública de cualquier suscriptor de Certificados de Entidad Final cuyo certificado fue emitido por ANDES SCD está permanentemente disponible para descarga en el directorio de certificados de la página web.

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

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

La llave pública de CA ANDES Raíz y las CA Subordinadas se encuentran permanentemente disponibles para descarga en la página WEB de ANDES SCD.

6.1.6. Periodo de utilización de la llave privada

Llave privada de la CA

El periodo de uso de la llave privada de la CA ANDES Raíz es de 25 años, la fecha de inicio y fin esta explicita en el certificado y en la sección 1.7.1 de este documento.

El periodo de uso de la llave de la CA emisora de Certificados Clase I, la CA emisora de Certificados Clase II y la CA emisora de Certificados Clase III es de 10 años. La fecha de inicio y fin de cada uno de estos certificados esta explicita en el respectivo certificado y en la sección 1.7.1 de este documento.

El periodo de uso de la llave de las CA de tercer nivel subordinadas de la CA Clase III es de 5 años. La fecha de inicio y fin de cada uno de este certificado esta explicita en el respectivo certificado y en los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios

Llave privada de suscriptores

El periodo de utilización de la llave privada de Certificados de uso interno y Certificados de entidad final está definido en la Política de Certificación aplicable. Para algunos tipos de certificados el periodo de utilización de la llave privada es el mismo que el periodo de la vigencia del certificado.

6.1.7. Tamaño de las llaves

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

6.1.8. Parámetros de generación de llave pública y comprobación de calidad

La llave pública de la CA Raíz y de las CA subordinadas están codificadas de acuerdo con PKCS#1. El algoritmo de generación de llaves es el RSA.

Los parámetros de generación de las llaves y los medios de comprobación de la calidad de los parámetros de generación de llaves para Certificados de entidad final se encuentran definidos en la Política de Certificación aplicable.

6.2. Controles de protección de la llave privada

6.2.1. Controles y estándares de módulos criptográficos

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

6.2.2. Control sobre la llaves privada (Multi-persona)

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

6.2.3. Respaldo de la llave privada

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

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

Las copias de respaldo de las llaves privadas de firma de las CA están almacenadas de forma segura. Este procedimiento se describe en detalle en las Políticas de Seguridad de ANDES SCD

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

6.2.4. Almacenamiento de la llave privada

Llave privada de la CA

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

Las fracciones de las llaves privadas de la CA son custodiadas por la firma CSA, entidad líder el manejo, administración y depósito de documentos físicos, y tienen el tratamiento de seguridad propio de la custodia fiduciaria de títulos valores. La firma CSA tiene sede en varias ciudades del país, cuenta con certificación ISO 9001:2000 y su objeto principal consiste en prestar los Servicios de Organización, Administración y Conservación Documental de Fondos Acumulados, Archivo Central y de Gestión, Elaboración y Ajuste de Tablas de Retención y Valoración Documental, así como los servicios de reprografía (microfilmación y digitalización). La Detección automática de incendios, instalación eléctrica

montada en tubo de acero para evitar cortocircuitos, edificios aislados para eludir percances generados en edificios ajenos a CSA Ltda, sistemas de seguridad internos y externos, y garantía de suministro eléctrico permanente.

Llave privada de los suscriptores

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

Mecanismo 1 - El par de llaves es generado por el propio suscriptor

Las llaves privadas generadas por el propio suscriptor NUNCA son almacenadas por ANDES SCD, deben ser almacenadas por ellos mismos, mediante la conservación del dispositivo de creación de firma u otros métodos, debido a que pueden ser necesarias para descifrar la información histórica cifrada con la llave pública, siempre que el dispositivo de custodia permita la operación.

Mecanismo 2 - El par de llaves es generado por Andes SCD

El almacenamiento de la llave privada del suscriptor generada por ANDES SCD puede variar según convenio de emisión de certificados o en función del formato de entrega. Esta información se especifica en los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios.

6.2.5. Transferencia de la llave privada a partir o a un módulo criptográfico

Llave privada de CA

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

Llave privada de suscriptores

Mecanismo 1 - El par de llaves es generado por el propio suscriptor

En el caso de los suscriptores que realizan solicitud con forma de entrega de certificado PKCS10 deben generar su propio par de llaves y proteger el uso y custodia de su llave privada.

Mecanismo 2 - El par de llaves es generado por Andes SCD

La transferencia de la llave privada del suscriptor generada por ANDES SCD puede variar según la entidad con la cual Andes SCD tenga convenio de emisión de certificados o en función del formato de entrega. Esta información se especifica en los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios.

6.2.6. Almacenamiento de la llave privada a un módulo criptográfico

La llave privada de la CA Raíz y las CA Subordinadas son creadas y almacenadas de forma cifrada en un módulo criptográfico HSM.

6.2.7. Método de activación de la llave privada

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

Activación de llaves CA

La activación de las llaves privadas de ANDES SCD se realiza de manera automática una vez se inicia el HSM.

Activación de llaves suscriptor

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. La protección de los datos de activación es responsabilidad exclusiva del suscriptor.

La activación de la llave privada del suscriptor generada por ANDES SCD puede variar según convenio de emisión de certificados. Esta información se especifica en los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios.

6.2.8. Método de desactivación de la llave privada

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

Desactivación de llave privada CA

La llave privada de la CA queda inactiva una vez se apaga el HSM.

Desactivación de llave privada suscriptores

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.

La desactivación de la llave privada del suscriptor generada por ANDES SCD puede variar según convenio de emisión de certificados. Esta información se especifica en los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios.

6.2.9. Método de destrucción de la llave privada

Destrucción de llave privada CA

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

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

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

Destrucción de llave privada de suscriptores

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

La destrucción de la llave privada del suscriptor generada por ANDES SCD puede variar según convenio de emisión de certificados. Esta información se especifica en los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios.

6.2.10. Clasificación de los modulo criptográfico

El módulo criptográfico utilizado para generar las llaves privadas de las CA de ANDES SCD cumple con el estándar FIPS 140-2 nivel 3.

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 durante un periodo de 15 años, cada uno de estos certificados incluyen la llave pública correspondiente. Estos archivos están protegidos por los controles de acceso a los demás componentes de la infraestructura.

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

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

El par de llaves tiene vigencia mientras exista un certificado 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

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

6.4.1. Generación e instalación de los datos de activación

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

Datos activación de dispositivo HSM

El administrador del HSM dispone de una clave de administración y de opciones que le permite generar y administra las cuentas de usuario para los operadores que activaran las llaves privadas de ANDES

SCD. Cada uno de los operadores del HSM a su vez dispone de una clave que deben custodiar bajo su responsabilidad de modo que ningún operador conozca más de una clave y se garantice que nadie tiene un control individual de las actividades críticas del HSM como activar y usar la llave privada de las CA raíz y subordinadas.

Datos activación de dispositivo TOKEN

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

Datos activación para acceder a llave privada del suscriptor generada por Andes SCD

El mecanismo de activación puede variar según convenio de emisión de certificados. Esta información se especifica en los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios.

6.4.2. Protección de datos de activación

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

Protección de datos de activación del HSM

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

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

Protección de datos de activación del TOKEN

El PIN o dato de activación del TOKEN debe ser personalizado por el suscriptor.
El suscriptor debe proceder a cambiar el PIN de su TOKEN si existe la sospecha de que un tercero conoce este dato. Para cambiar el PIN es necesario descargar el aplicativo software que ofrece el fabricante del TOKEN y que se encuentra disponible en la página web de ANDES SCD.
La protección de los datos de activación es responsabilidad exclusiva del suscriptor.

Protección de datos de activación para acceder a llave privada del suscriptor generada por Andes SCD

El mecanismo de protección puede variar según convenio de emisión de certificados. Esta información se especifica en los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios.

6.5. Controles de seguridad informática

6.5.1. Requisitos específicos de seguridad técnica

Cada servidor de la CA incluye las siguientes funcionalidades:

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

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

6.5.2. Nivel de seguridad informática

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

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles en el desarrollo de sistema

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

6.6.2. Controles de gestión de la seguridad

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

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

6.6.3. Controles de seguridad en el ciclo de vida

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

- Controles para la gestión de las llaves de la CA indicando como se genera, como se almacena y como se protegen las llaves privadas de la CA raíz y las CA subordinadas.
- Controles para distribuir de manera segura la llave pública de la CA a los suscriptores y terceros de confianza.

- Controles de seguridad en la emisión de certificados desde el momento en que se recibe la solicitud de emisión de certificado hasta que se entrega el certificado al suscriptor.
- Controles de seguridad para la revocación de certificados (mecanismos rápidos y seguros para revocar, controles para revocar certificados presencialmente, on-line o telefónicamente, acuse de recibido proporcionado por la CA para indicar que recibió la solicitud de revocación, actualización de la CRL, envío de email informando al suscriptor que su certificado fue revocado)
- Controles de seguridad en la publicación de certificados: (la CA mantiene controles para proporcionar la seguridad de que en el momento de la emisión el certificado está disponible para suscriptores y partes que confían, administración del repositorio solo está a cargo de personal autorizado, integridad de la información del repositorio)

6.7. Controles de seguridad en la red

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

- Los componentes de red se encuentran localizados en instalaciones seguras con monitoreo permanente.
- La red interna de ANDES SCD es protegida por cortafuegos configurados con políticas de acceso y sistemas de alertas para evitar el acceso no autorizado.
- La comunicación de información sensible entre ANDES SCD y las Autoridades de Registro es realizada mediante protocolo SSL que garantiza la confidencialidad e integridad de la información intercambiada.
- Se implementan cortafuegos y controles para proteger la red interna de accesos externos.
- Existen procedimientos y disposiciones respecto al uso de las redes y servicios de red.

7. Perfiles de certificado, CRL y OCSP

7.1. Perfiles de certificado

7.1.1. Número de versión

Todos los certificados emitidos por ANDES SCD están de conformidad con el estándar X.509 V3 y de conformidad con el RFC 5280 para perfiles de certificados y CRL.

7.1.2. Extensiones del certificado

Las extensiones utilizadas de forma genérica en los certificados son:

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

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

7.1.3. Identificadores objeto del algoritmo

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

7.1.4. Formatos de nombres

Los certificados digitales emitidos por ANDES SCD están restringidos a 'Distinguishedname' (DN) X.500 que son únicos y no ambiguos, los certificados contienen el DN del emisor y del suscriptor del certificado en los campos issuername y subjectname respectivamente. En cada Política de Certificación se describen los DN usados para el suscriptor.

7.1.5. Restricciones de nombre

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

7.1.6. Objeto identificador de la política de certificación

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

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

De esta forma ANDES SCD asigna jerárquicamente un OID a cada uno de sus documentos a partir de la raíz: **1.3.6.1.4.1.31304.**
El OID asignado a la presente declaración de prácticas de certificación (DPC) es **1.3.6.1.4.1.31304.1.1.1** adicionalmente se le añade una extensión con formato Y.Z que especifica la versión. Entonces la OID **1.3.6.1.4.1.31304.1.1.1.Y.Z** es interpretada como la DPC publicación Z de la versión Y
Cada Política de Certificación tiene asignado un OID dentro del rango privado de numeración, todas las PC comienzan con el prefijo **1.3.6.1.4.1.31304.1.2**

7.1.7. Sintaxis y semántica de los calificadores de la política

La extensión de los certificados referente a los calificadores de la política de certificación contiene la siguiente información:

- **Policyidentifier:** Contiene el identificador de la PC que aplica al tipo de certificado
- **CPS**: Indica la URL donde están publicadas las Practicas de Certificación (DPC) para ser consultadas por los usuarios
- **UserNotice:** La utilización de este certificado está sujeta a las Políticas de Certificado (PC) y Prácticas de Certificación (DPC) establecidas por ANDES SCD.

7.1.8. Perfil de la CRL

7.1.8.1. Numero de versión

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

7.1.8.2. CRL y extensiones

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

CRL de ROOT CA ANDES SCD S.A

Perfil de CRL según estándar X.509V2 – CRL CA Raíz		
Nombre	**Descripción**	**Valor**
Versión	Versión de la CRL	V2
Numero CRL	Número único de la CRL	Identificador de la CRL
Emisor	CN	ROOT CA ANDES SCD S.A.
	O	ANDES SCD
	OU	Division de certificacion
	C	CO
	L	Bogota D.C.
	E	info@andesscd.com.co
Algoritmo firma	Algoritmo de firma de la CRL	SHA256withRSA
Fecha efectiva de emisión	Periodo de validez de la CRL	Fecha de emisión de la CRL en tiempo UTC
Siguiente actualización	Fecha emisión próxima CRL	Fecha emisión próxima CRL en tiempo UTC
URL distribución	URL donde se publica la CRL	http://crl.andesscd.com.co/Raiz.crl
Certificados revocados	Lista de certificados revocados especificando el número de serie, fecha de revocación y motivo de la revocación	

CRL de CA ANDES SCD S.A. Clase I

Perfil de CRL según estándar X.509V2 – CRL Clase I		
Nombre	**Descripción**	**Valor**
Versión	Versión de la CRL	V2
Numero CRL	Número único de la CRL	Identificado de la CRL
Emisor	CN	CA ANDES SCD S.A. Clase I
	O	ANDES SCD
	OU	Division de certificacion uso interno
	C	CO
	L	Bogota D.C.
	E	info@andesscd.com.co
Algoritmo de firma	Algoritmo de firma de la CRL	SHA256withRSA
Fecha efectiva de emisión	Periodo de validez de la CRL	Fecha de emisión de la CRL en tiempo UTC
Siguiente actualización	Fecha emisión próxima CRL	Fecha emisión próxima CRL en tiempo UTC
URL distribución	URL donde se publica la CRL	USO INTERNO

Certificados revocados	Lista de certificados revocados especificando número serie, fecha de revocación y motivo revocación

CRL de CA ANDES SCD S.A. Clase II

Perfil de CRL según estándar X.509V2 – CRL Clase II		
Nombre	**Descripción**	**Valor**
Versión	Versión de la CRL	V2
Numero 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 de firma de la CRL	SHA256withRSA
Fecha efectiva de emisión	Periodo de validez de la CRL	Fecha de emisión de la CRL en tiempo UTC
Siguiente actualización	Fecha emisión próxima CRL	Fecha emisión próxima CRL en tiempo UTC
URL distribución	URL donde se publica la CRL	http://crl.andesscd.com.co/ClaseII.crl
Certificados revocados	Lista de certificados revocados especificando número serie, fecha de revocación y motivo revocación	

CRL de CA ANDES SCD S.A. Clase III

Perfil de CRL según estándar X.509V2 – CRL Clase III		
Nombre	**Descripción**	**Valor**
Versión	Versión de la CRL	V2
Numero CRL	Número único de la CRL	Identificado de la CRL
Emisor	CN	CA ANDES SCD S.A. Clase III
	O	ANDES SCD
	OU	Division de certificación entidad final subordinada
	C	CO
	L	Bogota D.C.
	E	info@andesscd.com.co
Algoritmo de firma	Algoritmo de firma de la CRL	SHA256withRSA
Fecha efectiva de emisión	Periodo de validez de la CRL	Fecha emisión de la CRL en tiempo UTC
Siguiente actualización	Fecha emisión próxima CRL	Fecha emisión próxima CRL en tiempo UTC
URL distribución	URL donde se publica la CRL	http://crl.andesscd.com.co/ClaseIII.crl

Certificados revocados	Lista de certificados revocados especificando número serie, fecha de revocación y motivo revocación

CRL de CA ANDES SCD S.A. Clase III Convenios

En los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5 correspondiente a convenios se especifica el perfil de la CRL de la CA emisora de los certificados

7.2. Perfil OCSP

En el documento interno Administración de OCSP identificado con el OID 1.3.6.1.4.1.31304.100.1.13 se describe como se utiliza el protocolo OCSP según lo especificado en la RFC 2560,5019 y 6960.

7.2.1. Numero de versión

El certificado OCSP se emite de acuerdo al estándar X509 V3

7.2.2. Extensiones OCSP

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

8. Auditoria y otras valoraciones

8.1. Frecuencia o circunstancias de valoración

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

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

8.2. Identidad y calificaciones del asesor

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

8.3. Relación entre el asesor y la entidad evaluada

El auditor interno no debe tener relación funcional con las áreas objeto de la auditoría.
Al margen de la función de auditoría, el auditor externo y la parte auditada no deberán tener relación alguna que pueda derivar en un conflicto de intereses.

8.4. Temas cubiertos en la valoración

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

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

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

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

8.5. Acciones tomadas como resultado de No Conformidades

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

8.6. Comunicación de resultados

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

9. Negocio y materias legales

9.1. Tarifas

9.1.1. Tarifas por emisión de certificados

La tarifa por el servicio de emisión de certificados digitales está disponible en la PC de cada uno de los servicios.

9.1.2. Tarifas por acceso a certificados

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

9.1.3. Tarifas por información del estado de un certificado o certificados revocados

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

9.1.4. Política de reembolso

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

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

9.2. Responsabilidad financiera

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

Se aclara que ANDES SCD no asumirá responsabilidad alguna por la no ejecución o retraso en la prestación de los servicios de certificación, si esta falla o retraso es consecuencia de casos fortuitos, casos de fuerza mayor, culpa exclusiva de la víctima, hecho de un tercero en general, de cualquier circunstancia que este fuera de control de ANDES SCD y en particular de las situaciones declaradas en la sección 9.7 de esta DPC “Limitaciones de responsabilidad”.

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

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

Información de la póliza de responsabilidad civil

Entidad aseguradora : AIG SEGUROS COLOMBIA S.A.
Tomador : ANDES Servicio de Certificación Digital S.A SIGLA ANDES SCD S.A.
Asegurado : ANDES SCD S.A.
Beneficiario : Terceros afectados de buena fe.
Valor : 5.859.315.000 Pesos.

9.3. Confidencialidad de información comercial

9.3.1. Alcance de la información confidencial

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

Se cataloga como confidencial la siguiente información:

1. Llaves privadas de la CA Raíz y CA subordinadas de ANDES SCD
2. Información personal de suscriptores que no está contenida en el certificado digital
3. Información de parámetros de seguridad, control y procedimiento de auditoría
4. Documentación de infraestructura técnica, Declaración de Políticas de Seguridad, Documento guía de Ceremonia de generación de llaves y Plan de Contingencias.

9.3.2. Información no considerada confidencial

Se cataloga como pública la siguiente información

1. Declaración de Prácticas de Certificación (DPC) y Políticas de Certificación de certificados de Entidad Final.
2. Los certificados emitidos por ANDES SCD
3. Listas de Certificados Revocados (CRL)

9.3.3. Responsabilidades para proteger la información confidencial

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

9.4. Confidencialidad de la información personal

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

9.4.1. Plan de privacidad

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

9.4.2. Información considerada confidencial

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

9.4.3. Información no considerada confidencial

A continuación, se hace referencia a la información considerada no confidencial

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

9.4.4. Responsabilidad de proteger la información

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

9.4.5. Notificación y consentimiento para usar la información confidencial

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

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

ANDES SCD no entregará información de sus Suscriptores a terceros sin autorización por escrito, previa, expresa e informada por parte del suscriptor titular de la información, salvo en los casos en que dicha información sea solicitada por una autoridad judicial en ejercicio de sus funciones legales y constitucionales, caso en el cual ANDES SCD procederá a la entrega de la información e informará al suscriptor de la solicitud realizada por la autoridad, para que este pueda tomar las acciones pertinentes encaminadas a proteger la confidencialidad de sus datos personales.

9.5. Derechos de propiedad intelectual

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

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

El Suscriptor reconoce que, en la utilización del certificado de firma digital asignado, cualquier tecnología subyacente utilizada y todo el contenido disponible en el Servicio son propiedad de ANDES y de sus proveedores, está protegido por leyes nacionales y tratados internacionales que cubren los derechos de propiedad intelectual, incluidos los derechos morales y patrimoniales de autor.

9.6. Obligaciones y garantías

9.6.1. Obligaciones y garantías ANDES SCD

Infraestructura:

a) Contar con los elementos tecnológicos, económicos, humanos e instalaciones requeridas para ofrecer los servicios de certificación, así como los controles de seguridad física, de procedimientos y estrategias necesarias para garantizar la confianza y operación de los servicios.
b) Garantizar el cumplimiento de los requisitos impuestos por la legislación vigente.

Técnicos

c) Proteger las llaves privadas de la Autoridad Certificadora ANDES SCD
d) No copiar ni almacenar las llaves privadas correspondientes a los certificados emitidos a Entidad Final y tampoco de certificados de uso interno emitidos con el propósito de utilizarse para firma electrónica, cuando estos sean generados sobre los dispositivos criptográficos de la Entidad Final. Para el caso de convenios se seguirán las disposiciones establecidas con la entidad con la cual Andes SCD tiene convenio. Esta información se especifica en los documentos referenciados con la rama de OID 1.3.6.1.4.1.31304.100.5. correspondiente a convenios.
e) Emitir Certificados conformes con el estándar X.509 V3 y de acuerdo a lo solicitado por el suscriptor.
f) Garantizar que se puede determinar la fecha y hora en la que se expidió un certificado o se revocó.
g) Utilizar sistemas fiables para almacenar los certificados e impedir que personas no autorizadas modifiquen los datos y detectar cualquier indicio que afecte la seguridad.
h) Mantener actualizado el directorio de certificados indicando los certificados emitidos y si están vigentes o revocados.
i) Almacenar en la infraestructura PKI de forma indefinida las CRL y los certificados digitales vigentes, vencidos y revocados.
j) Publicar de manera oportuna en la página WEB los certificados que se encuentran vigentes y las CRL de la CA Raíz y las CA subordinadas
k) Informar a los suscriptores la proximidad del vencimiento de su certificado enviando un correo electrónico 30, 15, 7 y 1 días antes del vencimiento.

Organizacionales

l) Cumplir lo dispuesto en las Políticas y Prácticas de Certificación.
m) Disponer de personal calificado, con el conocimiento y experiencia necesaria para la prestación del servicio de certificación ofrecido por ANDES SCD.
n) Aprobar o denegar las solicitudes de emisión de certificados enviadas por la Autoridad de Registro
o) Proporcionar al solicitante en la página web de ANDES SCD la siguiente información de manera gratuita:
   - Las Políticas y Prácticas de certificación y todas sus actualizaciones.

- Obligaciones del firmante y la forma en que han de custodiarse los datos
- Procedimiento para solicitar emisión de certificado.
- El procedimiento de revocación de su certificado.
- Mecanismos para garantizar la fiabilidad de la firma electrónica a lo largo del tiempo
- Las condiciones y límites del uso del certificado

p) Informar a los suscriptores de la revocación de sus certificados inmediatamente a que se produzca dicho evento.
q) Informar a Superintendencia de Industria y Comercio y al Organismo Nacional de Acreditación de Colombia ONAC sobre los eventos que puedan comprometer la prestación del servicio de ANDES SCD.
r) Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor.
s) Tomar medidas contra la falsificación de certificados y garantizar su confidencialidad durante el proceso de generación y su entrega al suscriptor mediante un procedimiento seguro.

9.6.2. Obligaciones y garantías RA

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

9.6.3. Obligaciones y garantías del solicitante

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

9.6.4. Obligaciones y garantías suscriptores

a) Garantizar la veracidad de las declaraciones que realizó en el momento de solicitar el certificado digital y la información que contiene el certificado

b) La llave privada es personal e intransferible por esta razón se debe custodiar de forma diligente para evitar que otras personas puedan suplantar su identidad y firmar documentos en su nombre o acceder a mensajes confidenciales. La utilización de la llave privada por otras personas es responsabilidad y riesgo del titular, pues si no se toman las medidas necesarias carecería de sentido el sistema de seguridad que se pretende instaurar.
c) Conservar confidencialmente el código de revocación suministrado en el momento de la entrega del certificado, se recomienda guardarlo en un lugar diferente al certificado.
d) Usar el certificado según lo dispuesto en las Políticas y Prácticas de Certificación aplicables para el tipo de certificado
e) Respetar las disposiciones de los términos y condiciones y las limitaciones de uso del certificado
f) Utilizar la llave privada únicamente con dispositivos criptográficos acordes a los niveles de seguridad exigidos por ANDES SCD.
g) Informar a la mayor brevedad posible la existencia de alguna causa de revocación.
h) Informar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
i) No utilizar la llave privada y el certificado desde el momento en que se solicita revocación y tampoco cuando el certificado que avala el par de llaves no sea válido.
j) Verificar que la información contenida en el certificado es verdadera y exacta, en caso de existir algún dato incompleto o incorrecto notificar de inmediato a ANDES SCD.
k) Respetar los derechos de terceras personas y responsabilizarse frente a las mismas por los perjuicios que la mala utilización del certificado de firma digital asignado pueda causar, así como salir en defensa de ANDES, si es demandada por cualquier circunstancia relacionada con la mala utilización del mismo.
l) Realizar y conservar por sus propios medios los archivos de respaldo o copias de seguridad de la información relacionada con las facturas firmadas digitalmente con el certificado asignado.

9.6.5. Obligaciones y garantías de las partes que confían

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

9.7. Limitaciones de responsabilidad

9.7.1. Responsabilidad por la veracidad de la información del Suscriptor

El Suscriptor asume todos los riesgos por perjuicios que pudieran derivarse de conductas como otorgar información falsa, suplantar la identidad de terceros, validar documentos o información incompleta o desactualizada.

9.7.2. Responsabilidad por disponibilidad del servicio

El Suscriptor reconoce y acepta que ni ANDES ni ningún representante, ni trabajador o socio suyo será responsable por la no disponibilidad que en algún momento pueda tener el servicio en eventos de fuerza mayor, caso fortuito o hechos de un tercero, no obstante se compromete a obrar diligentemente para reducir al mínimo las posibilidades de fallas o interrupciones en el mismo.

Las fallas ocasionadas por la incapacidad o insuficiencia de los equipos del Suscriptor, o por su falta de conocimientos frente al uso del servicio, no serán en ningún caso imputables a ANDES y no se podrá exigir de su parte el saneamiento de ningún perjuicio.

9.7.3. Responsabilidad por la funcionalidad del servicio en la infraestructura del Suscriptor

El Suscriptor será el único responsable de la provisión y el pago de los costos necesarios para asegurar la compatibilidad del servicio (certificado de firma digital), frente a sus equipos, incluyendo todo el hardware, software, componentes eléctricos y otros componentes físicos o lógicos requeridos para acceder y usar el mismo, incluyendo de forma enunciativa pero no limitativa servicios de telecomunicaciones, acceso y conexión a Internet, links, navegadores, u otros programas, equipos y servicios requeridos para acceder y usar el servicio.

9.7.4. Responsabilidad frente delitos informáticos

En el evento en que el Suscriptor sea víctima de alguna de las conductas tipificadas como delito, por la Ley 1273 de 2009 (Ley de delitos Informáticos), en sus sistemas de información, en sus aplicaciones e infraestructura tecnológica, en la ejecución transacciones electrónicas, o en el acceso y uso del servicio, ataques de phishing, suplantaciones de identidad, por negligencia en el manejo y confidencialidad del certificado digital, este será el único responsable y saneará los perjuicios a que haya lugar, toda vez que es su obligación adoptar las medidas de seguridad, políticas, campañas culturales, instrumentos legales y demás mecanismos para salvaguardar la confidencialidad y el buen uso de su certificado digital.

Además de las situaciones enunciadas anteriormente, frente a las siguientes circunstancias ANDES SCD no se hará responsable

a) Uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente DPC, utilizar un certificado revocado o por depositar confianza en el sin antes verificar el estado del mismo.
b) Por el uso fraudulento de los certificados o CRL (Lista de certificados revocados).
c) Por daños y/o perjuicios producto de la errada interpretación de las Prácticas de Certificación por parte de usuarios y suscriptores en el uso de los servicios.
d) Por el incumplimiento de las obligaciones establecidas para el suscriptor o usuarios en la normativa vigente
e) Por el contenido de los mensajes o documentos firmados o por el contenido de páginas web que posean un certificado
f) Por prácticas no notificadas a ANDES SCD que afecten la llave privada del suscriptor permitiendo su uso por terceros (Ej. robo, perdida o compromiso)
g) Por la no recuperación de documentos cifrados con la llave pública del suscriptor

h) Fraude en la documentación presentada por el solicitante o datos ingresados de forma incorrecta en la solicitud.
i) Por uso del certificado por parte del suscriptor fuera de su periodo de vigencia o cuando ANDES SCD haya informado la revocación del certificado.

Con la aceptación de los términos y condiciones de uso del certificado de firma digital suministrado por ANDES SERVICIOS DE CERTIFICACIÓN DIGITAL S.A, se obliga al suscriptor a indemnizar a ANDES SCD como entidad certificadora por cualquier acto u omisión que provoque daños, pérdidas, deudas y gastos procesales en los que ANDES SCD pudiera incurrir, que sean causados por la utilización y publicación de los certificados y que provenga de:

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

9.8. Protección de datos personales:

ANDES, tratará la información personal de sus suscriptores, de acuerdo a los parámetros legales, y con la debida diligencia, para garantizar su confidencialidad, seguridad y circulación restringida, para esto cuenta con políticas de protección de datos personales, las cuales se encuentran publicadas en su sitio web, en el link https://www.andesscd.com.co/images/Politicas_de_Tratamiento_de_Datos_Personales.pdf, estas políticas pueden ser consultadas por los suscriptores, con el fin de conocer sus derechos derivados de Habeas Data, como conocer, actualizar, rectificar y suprimir los datos personales que se encuentren en poder de Andes SCD, siempre y cuando no haya deber legal o contractual de permanencia de estos datos, en nuestra base de datos.

9.9. Indemnizaciones

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

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

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

9.10. Término y terminación

9.10.1. Terminación de disposiciones

La Declaración de Prácticas de Certificación y cada una de las Políticas de Certificación entran en vigor desde el momento en que se publican en la página web de ANDES SCD, a partir de ese momento la

versión anterior del documento queda derogada y la nueva versión reemplaza íntegramente la versión anterior. ANDES SCD conserva en el repositorio las anteriores versiones de la DPC y de cada PC.

9.10.2. Efecto de terminación y supervivencia

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

9.11. Notificación individual y comunicación con los participantes

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

9.12. Procedimiento de cambio en las DPC y PC

9.12.1. Procedimiento de cambio

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

- El comité de Políticas y Seguridad realiza los cambios que considere pertinentes sobre las DPC y las PC siguiendo protocolo de Análisis y Aprobación de la Política identificado con el OID 1.3.6.1.4.1.31304.100.2.1.
- Los cambios realizados en la DPC o PC son analizados por el área directiva de ANDES SCD para su estudio y aprobación.
- El auditor interno procede a validar los cambios aprobados sobre la DPC y la PC y genera un informe de diagnóstico donde se relacionan las conformidades y no conformidades encontradas en la validación.
- La DPC y PC actualizada es publicada en la página web de ANDES SCD si el informe diagnóstico del auditor interno tiene resultado conforme.

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

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

9.12.2. Mecanismo y periodo de notificación

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

9.12.3. Circunstancias bajo las cuales la OID debe cambiarse

En caso de que los cambios de la DPC y PC no afecten a la aceptabilidad de los certificados se procede al incremento del número menor de versión en el documento y el incremento en el último número del identificador de objeto (OID) que lo representa. No se considera necesario comunicar este tipo de modificaciones a los usuarios de los certificados correspondientes a la PC o DPC modificada.

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

9.13. Prevención y Resolución de disputas

Si desea comunicar a ANDES SCD cualquier petición, queja, reclamo, disputa, sugerencia o felicitación en relación con el contenido del presente documento o en general con la prestación del servicio de certificación, envíe un email al correo electrónico pqrs@andesscd.com.co o en la línea (571) 7953430 Opción 1. Si desea mayor información sobre nuestro procedimiento de peticiones, quejas, reclamos, sugerencias y felicitaciones (OID 1.3.6.1.4.1.31304.100.6.8)

9.14. Ley aplicable

El funcionamiento y las operaciones realizadas por la Autoridad Certificadora ANDES SCD, así como la presente Declaración de Prácticas de Certificación y las Políticas de Certificación aplicables a cada tipo de certificado están sujetas a la normativa que les sea aplicable y en especial a:

a) Ley 527 de 1999, Por medio de la cual se define y reglamente el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
b) Decreto 1747 de 2000, por el cual se reglamenta parcialmente la ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.

9.15. Cumplimiento con la ley aplicable

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

Versión	Fecha	Detalle	Responsable
1.3	24/02/2011	Versión inicial autorizada por la SIC según resolución 14349 de marzo 2011	Comité políticas y seguridad
1.4	02/11/2011	- Introducción: Se modifica introducción para incluir resolución de autorización SIC-	Comité políticas y seguridad

Versión	Fecha	Detalle	Responsable
		- 1.1 - Se actualiza el OID, versión de DPC, fecha de emisión y dirección de publicación de la DPC V 1.4 - 1.4 - Se incluye definición de PKCS#12 - 1.6.1 - Se actualizan los datos del certificado CA Clase II - 1.8.2 - Se incorpora el tipo de certificado Función Pública y Persona Jurídica dentro del catálogo de servicios de Andes SCD - 1.9 - Se actualiza dirección física y teléfono de las instalaciones de Andes SCD - 2.1.2 - Se indican las CRL que se publican en el histórico de CRL y se determina el tiempo de publicación. - 3.2 - Se incluye método para demostrar la posesión de la clave privada cuando se entrega el certificado en archivo PKCS12 y se indica la forma de Autenticación de identidad de Solicitantes y Suscriptores de certificados en archivo PKCS12. - 4.4.7 - Se actualiza periodo de emisión de CRL Clase I y Clase II	
2.0	09/10/2014	- 1.6.2 - Se actualiza la sección autoridad de registro en cuanto a comunicación con Andes SCD - 1.6.3 - Se actualiza tabla de suscriptores de certificados clase I - 1.8.2 - Se actualiza el OID de las políticas de certificado vigentes - 1.9 - Se actualiza datos de contacto y organización que administra el documento - 3.2 - Se actualiza sección aprobación de la identidad - 4.4.1 - Se actualiza sección causales de revocación - 4.4.2 - Se hace referencia a documento adicional que describe procedimiento para solicitar emisión de certificado - 5 - Se cambia el termino Telmex por Triara - 5.2.1 - Se suprime el rol de confianza representante RA y administrador RA - 5.5.4 - Se modifica Procedimiento de respaldo de la información - 6.1.7 - El tamaño de las llaves de certificados clase I – Uso interno es 2048 bits - 9.2 - Se actualiza información de póliza de responsabilidad civil - Todo el documento - Se cambia el termino clave privada y clave pública por llave privada y llave publica	Comité políticas y seguridad
2.1	24/11/2015	- 1.1 - Se actualiza la versión del documento DPC y fecha de emisión - 1.4 - Referencia a CA Clase III en definición de jerarquía de confianza - 1.6 - Se incluye información de la CA Clase III - 1.8 - Se actualizó el OID de las políticas de certificado vigentes - 1.9 - Se actualiza datos de contacto y organización que administra el documento - 2.0 - Se incluye información medios de publicación de certificados y CRL para la jerarquía clase III - 3.2.1, 3.2.2, 6.1.2,6.1.3 y 9.6.1d - Se referencia documento OID que describe procedimientos en convenios. - 4.4.6, 9.4.3 y 9.6 j - Referencia a CRL para la jerarquía clase III	Comité políticas y seguridad

Versión	Fecha	Detalle	Responsable
		- 4.4.7 - Se incluye periodicidad de publicación de CRL para la jerarquía clase III - 6.1.1 - Se incluye información de jerarquía CA Clase III y OID generación llaves CA Clase III - 6.1.5 - Referencia a llave publica para CA de la jerarquía clase III - 6.1.6 - Se incluye periodo de uso de las llaves privadas de la CA jerarquía clase III - 9.2 - Se actualiza información de la póliza de responsabilidad civil	
2.2	26/09/2016	- 1.1 - Se actualiza la versión del documento DPC y fecha de emisión - 1.2 - Se agrega Identificación de la Entidad de Certificación Digital - 1.10.2 - Se actualiza email de la persona de contacto - 1.7.1 – Se actualiza datos de CA Raíz y CA subordinadas renovadas por cambio de algoritmo de firma de sha1 a sha256 - 2.1 y 2.3 - Se precisa que en directorio de certificados se publican certificados que no se encuentren revocados. - 2.2 y 4.4.7 - Se elimina referencia al histórico de CRL - 3.2.1, 6.1.1, 6.1.2 y 6.1.3 - Cambio en el procedimiento para gestionar la llaves según la forma de entrega del certificado elegida por el cliente. Se describe nuevo procedimiento PKCS10 Token. - 4.4.4 – Se actualiza el procedimiento de revocación presencial. - 4.4.7 – se incluye Nota indicando que la CRL de ROOT CA no se publicara periódicamente porque la CA permanece Offline - 4.6 – Se incluye la reposición de certificados. - 5.2.1 - Actualización de roles de confianza - 5.4.1 - Se actualiza los tipos de severidad de los eventos auditados del syslog - 5.8 - Se complementa sección terminación de CA o RA - 7.1.1 - Se actualiza RFC 3280 por 5280 - 7.1.3 – Se actualiza referencia al OID algoritmo de firma sha1 por OID de algoritmo de firma sha256 - Introducción: Se hace referencia al territorio Colombiano	Comité políticas y seguridad
2.3	06/01/2017	- Se actualiza introducción del documento referenciando certificado acreditación ONAC - 1.5 Se elimina referencia al termino PKCS12 - 1.7. Se hace referencia a documento convenios para CA con jerarquía de tercer nivel - 2.2 Se actualiza URL publicación certificados CA y CRL - 3.2.1 Se incluye procedimiento certificados con forma entrega PKCS10 y se elimina forma de entrega PKCS12 - 3.2.4 Se referencia cumplimiento de CEA-4 1-10 como requisito de interoperabilidad. - 4.4.3 horario de atención revocación telefónica y presencial. - 4.4.4 Se referencia a procedimiento de revocación de certificados de convenios	Comité políticas y seguridad

Versión	Fecha	Detalle	Responsable
		- 4.4.6, 4.4.7, 6.1.1, 6.1.2 y 6.1.3 Se incluye referencia a forma de entrega PKCS10 y se elimina forma de entrega PKCS12 - 6.1.5, 6.1.6 Se generaliza CA subordinadas convenios - 6.2.7, 6.2.8 y 6.2.9, 6.4.2, 9.6.1 d) se elimina referencia a PKCS12 - 7.1.8 Se hace referencia a documento convenios para perfil de CRL CA con jerarquía de tercer nivel	
2.4	14/02/2017	- 1.9.1 Se actualiza el OID de la Política de certificado de Pertenencia a empresa y Persona Natural - 4.4.3. Se incluye medio para solicitar revocación de certificado: Correo electrónico - 4.4.4. Se describe procedimiento para solicitar revocación de certificado por medio de correo electrónico y se detallan los demás procedimientos de revocación. - 5 Se actualiza referencia a documentos que conforman la Política de Seguridad	Comité políticas y seguridad
2.5	01/07/2017	- 1.9.1 Se retira el tipo de certificado Comunidad académica - Se reemplazó “contrato suscripción” por “términos y condiciones del servicio” en todo el documento - 9.5 Se actualizo sección Derechos de propiedad intelectual	Comité políticas y seguridad
2.6	26/10/2017	- 1.7.1 se actualizan datos del certificado CA Clase III - 1.8.3 Se agregó sección prohibiciones Generales - 1.8.4 Se incluyen prohibiciones de uso que aplican para todos los certificados emitidos por Andes SCD - 1.9 se aumenta versión de PC persona jurídica y pertenencia a empresa - 3.2.1, 6.1.1, 6.1.2, 6.2.4 y 6.2.5. se incluye en mecanismo 2 el formato de entrega Token - 4.5.1 y 7.2 se hace referencia a RFC OCSP - 9.6.4 Se incluye sección K y l en obligaciones y garantías suscriptores - 9.7 se actualizo sección limitaciones de responsabilidad - 9.8 se agrega sección protección de datos personales	Comité políticas y seguridad
2.7	20/03/2018	- 1.7.3 Se referencian los certificados de personas jurídicas dentro de la Clase III convenios - 1.9.1 Se actualiza OID de las políticas de cada de uno de los certificados. - 3.2.1Se definen los dos mecanismos para la emisión de certificados (cuando la llave privada es generada por el suscriptor y cuando la llave privada es generada por ANDES SCD) - 3.2.3Se referencia a la autoridad de registro como responsable de verificar la información del solicitante. - 5. Se reemplaza metodología de gestión de activos de información por Procedimiento de gestión de inventario de activos tecnológicos y se actualiza su OID - 5.1Se incluye referencia a condiciones exigidas a proveedores críticos	Comité políticas y seguridad

Versión	Fecha	Detalle	Responsable
		- 5.3.1 Se modifica perfil de Administrador HSM describiendo sus funciones. - 5.3.4Se actualiza el apartado segregación de deberes - 5.4.3Se hace referencia a formación de las personas involucradas en el ciclo de vida de los certificados. - 5.4.4Se ajusta frecuencia de adiestramiento para hacer referencia al personal que interviene en el ciclo de vida de los certificados. - 5.6.2 Se hace referencia a la RFC 4523 relacionada con el LDAP. - 7.1.8.2 Se actualiza algoritmo de firma en la CRL Raíz y Clase II - 9.1.1Se referencian tarifas de los servicios a las PC - 9.2Se actualiza valor de la Póliza de responsabilidad civil - 9.4.6Se hace referencia a acceso a la información a partir de proceso judicial o administrativo.	
2.8	26/06/2018	- 1.9.1 Se incluye en catálogo de servicios de certificación el tipo de certificado comunidad académica y emisor de factura electrónica - 1.9.1 Se aumentó versión de PC Persona jurídica	Comité políticas y seguridad