Elaboró	Revisó	Aprobó

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)

AC CAMERFIRMA COLOMBIA

AC CITISEG

AC CAMERFIRMA S.A.

VERSION 5

Identificación de Certificados (OID)

La forma de identificar distintos tipos de certificados digitales es a través de identificadores de objeto (OID's). Un OID concreto permite a las aplicaciones distinguir claramente el certificado que se presenta.

El identificador está compuesto por una serie de números separados entre sí por puntos y con un significado concreto de cada uno de ellos.

El siguiente cuadro muestra las diferentes variables respecto a los certificados emitidos:

NOMBRE ABREVIADO	OID (1)				DESCRIPCIÓN
	CA	Personal	Personal	Soporte	
CAM-COL-CA-HW-KUSU	20	1	1	2	Certificado de Comunidad Academica, claves en hardware y generadas por el titular
CAM-COL-FP-HW-KUSU	20	1	2	2	Certificado de Función Pública, claves en hardware y generadas por el titular
CAM-COL-PJ-HW-KUSU	20	1	3	2	Certificado de Persona Jurídica, claves en hardware y generadas por el titular
CAM-COL-PN-HW-KUSU	20	1	4	2	Certificado de Persona Natural, claves en hardware y generadas por el titular
CAM-COL-PE-HW-KUSU	20	1	5	2	Certificado de Pertenencia a Empresa, claves en hardware y generadas por el titular
CAM-COL-PT-HW-KUSU	20	1	6	2	Certificado de Profesional Titulado, claves en hardware y generadas por el titular
CAM-COL-RE-HW-KUSU	20	1	7	2	Certificado de Representante de Empresa, claves en hardware y generadas por el titular
CAM-PC-CSIGN-SW-KUSU	10	12	2		Certificados de firma de código
CAM-PC-TS-HW-KPSC	10	13	1	3	Certificado de Sello de Tiempo, claves en hardware y generadas por el PSC
CAM-PC-SSL-SW-KUSU	10	11	2	1	Certificado de Servidor Seguro OV – SSL, generadas por el titular (Certificado fuera del alcance de la acreditación)

(1) Los OID parten de la base común 1.3.6.1.4.1.17326.

ÍNDICE DE CONTENIDO

1 INTRODUCCIÓN

1.1 Consideración Inicial

Por no haber una definición taxativa de los conceptos de Declaración de Practicas de Certificación y Políticas de Certificación y debido a algunas confusiones formadas, se entiende que es necesario aclarar estos conceptos.

Política de Certificación (PC) es el conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y utilización comunes, es decir, en general una Política de Certificación debe definir la aplicabilidad de tipos de certificado para determinadas aplicaciones que exigen los mismos requisitos de seguridad y formas de usos.

La Declaración de Practicas de Certificación (DPC) es definida como un conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados. En general contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, además de sobre la relación de confianza entre el Firmante/Suscriptor o Tercero que confía y la Autoridad de Certificación. Deben ser documentos comprensibles y sólidos, que proporcionan una descripción exacta de los servicios ofertados, procedimientos detallados de la gestión del ciclo de vida de los certificados, etc.

Estos conceptos de Políticas de Certificación y Declaración de Practicas de Certificación son distintos, pero aun así es muy importante su interrelación.

En resumen, una Política define "qué" requerimientos de seguridad son necesarios para la emisión de los certificados. La Declaración de Prácticas de Certificación nos dice "cómo" se cumplen los requerimientos de seguridad impuestos por la Política.

Con el fin de simplificar la documentación y facilitar la comprensión, las Políticas de Certificación están integradas en esta Declaración de Prácticas de Certificación.

La entidad CITISEG S.A.S y su correspondiente jerarquía de certificación asociada será referida a lo lago de este documento de DPC con el término de "SubCA" y deberá seguir lo indicado en estas DPC. En aquellos aspectos en los que la CITISEG S.A.S. emplee un proveedor de servicios de certificación, se entenderán las obligaciones de la SubCA son aplicables a dicho proveedor a través del acuerdo contractual suscrito entre ambas partes.

1.2 Vista General

En este documento se especifica la Declaración de Prácticas de Certificación (en adelante DPC) y las Políticas de Certificación que la SubCA de Nivel 1 "AC CAMERFIRMA COLOMBIA – 2016" y la SubCA de Nivel 2 "AC CITISEG – 2016", han establecido para la emisión de certificados y se basa en la especificación de los siguientes estándares:

- RCF 3647 – Internet X.509 Public Key Infrastructure Certificate Policy, de IETF,
- RFC 3739 - Internet X.509 Public Key Infrastructure: Qualified Certificates Profile, de IETF.
- RFC 5280 - Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL), de IETF.
- TS 101 456 VI.2.1 Policy requirements for certification authorities issuing qualified certificate, de ETSI

- TS 102 042 VI. 1.1 Policy requirements for certification authorities issuing public key certificate, de ETSI.
- TS 102 023 VI.2.1 Policy requirements for time-stamping authorities, de ETSIEquivalente técnicamente al RFC 3628 de IETF.

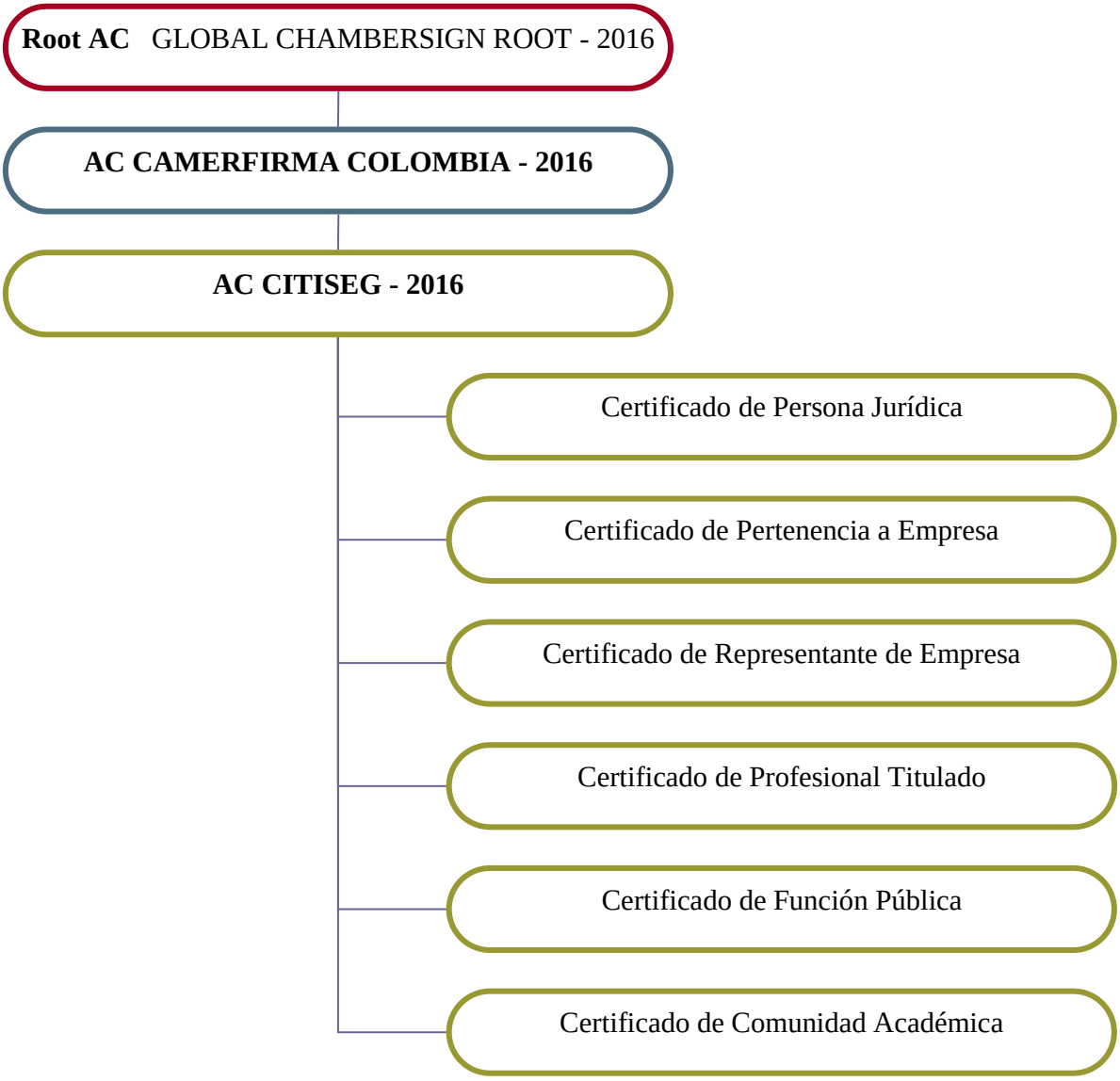
Se ha tenido también en cuenta las recomendaciones del documento técnico Security CWA 14167-1 Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.

De igual modo, se han incorporado en este documento las prácticas de certificación y políticas de certificados para los certificados de Sello Electrónico, Servidor Seguro-SSL, Firma de Código y Sello de Tiempo emitidos desde la jerarquía Chambers of Commerce Root gestionada por AC Camerfirma SA.

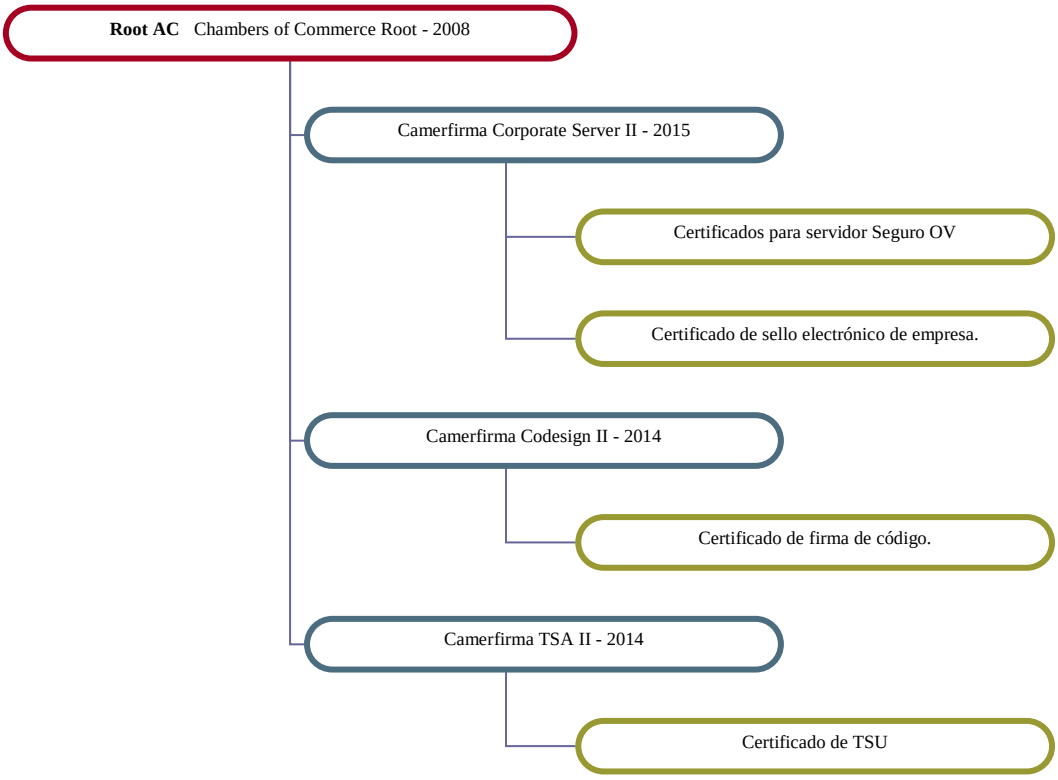
Esta DPC se encuentra en conformidad con las Políticas de Certificación de los diferentes certificados emitidos por la SubCA que vienen indicados en el apartado siguiente, así como con las leyes que regulan la emisión de la firma electrónica en España y en Colombia.

1.2.1 Jerarquía

En este apartado presentaremos la jerarquía que gestiona las Autoridades de Certificación Subordinadas que se encuentran regidas por esta DPC. Ambas ACs Subordinadas forman parte de la jerarquía de certificación de la Autoridad de Certificación española AC Camerfirma SA, que está compuesta por diversas Autoridades de Certificación (en inglés AC o Certification Authority).



De igual forma, se adjunta la jerarquía de los certificados emitidos por la jerarquía Chambers of Commerce Root.



1.2.1.1 Autoridad de Certificación Raíz

Se denomina Autoridad de Certificación Raíz (o AC Root) a la entidad dentro de la jerarquía que emite certificados a otras Autoridades de Certificación, y cuyo certificado de clave pública ha sido autofirmado. Su función es firmar el certificado de las otras AC pertenecientes a la Jerarquía de Certificación. En el caso que nos ocupa, los datos de identificación del Certificado Raíz actual de AC Camerfirma SA son:

- CN: *GLOBAL CHAMBERSIGN ROOT - 2016*
- Identificador de la clave: *1139 A49E 8484 AAF2 D90D 985E C474 1A65 DD5D 94E2*
- Válido desde: *14 de Abril de 2.016*
- Válido hasta: *8 de Abril de 2.040*
- Longitud de clave RSA: *4.096 bits*

Esta Jerarquía está creada por AC Camerfirma SA para la emisión de certificados bajo proyectos concretos a nivel internacional, con una/s determinada/s Entidad/es entre las que se encuentra la SubCA.

De igual modo, los datos de identificación del Certificado Raíz actual de AC Camerfirma SA empleado para los certificados de Sello Electrónico, Servidor Seguro-SSL, Firma de Código y Sello de Tiempo son:

- CN: *Chambers of Commerce Root - 2008*
- Identificador de la clave: *F924 AC0F B2B5 F879 C0FA 6088 1BC4 D94D 029E 1719*
- Válido desde: *1 de Agosto de 2.008*
- Válido hasta: *31 de Julio de 2.038*
- Longitud de clave RSA: *4.096 bits*

1.2.1.2 Autoridad de Certificación Intermedia de Nivel 1

Se llama Intermedia de Nivel 1 o Autoridad de Certificación Subordinada a la entidad de certificación dentro de la jerarquía que emite los Certificados Intermedios de Nivel 2 y su certificado de clave pública ha sido firmado digitalmente por la Autoridad de Certificación Raíz *GLOBAL CHAMBERSIGN ROOT - 2016*.

En el presente caso, los datos de identificación del actual Certificado Intermedio de Nivel 1, generado y gestionado por AC Camerfirma SA a través del cual emite los Certificados Intermedios de Nivel 2, se detallan a continuación:

- CN: *AC CAMERFIRMA COLOMBIA - 2016*
- Identificador de la clave: *394E 613C 7852 7BF4 FF42 3195 9FC4 7ECC 9762 E6E4*
- Válido desde: *14 de Abril de 2.016*
- Válido hasta: *9 de Marzo de 2.040*
- Longitud de clave RSA: *4.096 bits*

El OID de AC CAMERFIRMA COLOMBIA – 2016 es: 2.5.29.32.0 (Any Policy)

Adicionalmente, se presentan los certificados Intermedia de Nivel 1 que emiten los certificados de Sello Electrónico, Servidor Seguro-SSL, Firma de Código y Sello de Tiempo bajo la jerarquía Chambers of Commerce Root.

- CN: *Camerfirma Corporate Server II - 2015*
- Identificador de la clave: *63E9 F0F0 5600 6865 B021 6C0E 5CD7 1908 9D08 3465*

- Válido desde: *Jueves 15 de Enero de 2.015*
- Válido hasta: *Martes 15 de Diciembre de 2.037*
- Longitud de clave RSA: *4.096 bits*

- CN: *Camerfirma Codesign II - 2014*
- Identificador de la clave: *3E11 6F6A 15E7 7F9B 4A2F 126D 595B FEB5 5F8C C365*
- Válido desde: *Lunes 16 de Marzo de 2.009*
- Válido hasta: *Jueves 14 de Marzo de 2.019*
- Longitud de clave RSA: *4.096 bits*

- CN: *Camerfirma TSA II - 2014*
- Identificador de la clave: *0E31 4D5D E9E1 C25C 5BBC F52B 05BA AF47 0D16 ABDC*
- Válido desde: *Lunes 16 de Marzo de 2.009*
- Válido hasta: *Jueves 14 de Marzo de 2.019*
- Longitud de clave RSA: *4.096 bits*

1.2.1.3 Autoridad de Certificación Intermedia de Nivel 2

Se llama Intermedia de Nivel 2 o Autoridad de Certificación Subordinada a la entidad de certificación dentro de la jerarquía que emite los certificados de entidad de los usuarios finales, y su certificado de clave pública ha sido firmado digitalmente por la Autoridad de Certificación Intermedia de Nivel 1 *AC CAMERFIRMA COLOMBIA - 2016*.

Este certificado Intermedio de Nivel 2 también ha sido generado por AC Camerfirma SA, pero será gestionado por la SubCA como Entidad de Certificación acreditada en Colombia para emitir los certificados finales a suscriptores. En este caso, AC Camerfirma SA actuará como prestador de servicios de certificación para la SubCA ubicada en Colombia.

La SubCA tiene la siguiente Autoridad de Certificación Intermedia de Nivel 2, cuya información más relevante es:

- CN: *AC CITISEG - 2016*
- SHA1 hash: *BB57 7F9C 3178 5BEA 7A43 51A3 AD72 971F E0D8 667C*
- Válido desde: *14 de Abril de 2.016*
- Válido hasta: *8 de Febrero de 2.040*
- Longitud de clave RSA: *4.096 bits*

El OID de AC CITISEG – 2016 es: 2.5.29.32.0 (Any Policy)

1.2.1.4 Certificados de usuarios finales

La SubCA expide una serie de certificados digitales orientados a satisfacer las necesidades de sus clientes, en función de sus líneas de negocio mediante su Autoridad de Certificación Intermedia de Nivel 2 indicada en el apartado anterior.

Los Certificados Digitales que emite la SubCA son los siguientes:

Certificado de Persona Jurídica. OID: 1.3.6.1.4.1.17326.20.1.3.2

Se trata de un certificado digital emitido a favor de una Entidad jurídica que podrá ser utilizado cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario. El solicitante del certificado deberá tener capacidad para representar a la entidad titular del certificado.

Certificado de Persona Natural. OID: 1.3.6.1.4.1.17326.20.1.4.2

El certificado digital de persona natural, sirve exclusivamente para que una persona natural se identifique como tal y su uso se restringe para realizar todo tipo de trámites como Persona Natural como son firmar mensajes de datos y/o documentos.

Certificado de Pertenencia a Empresa. OID: 1.3.6.1.4.1.17326.20.1.5.2

El certificado digital de pertenencia a entidad garantiza la identidad de la persona física titular del certificado, así como su vinculación a una determinada Entidad en virtud del cargo que ocupa en la misma.

Certificado de Representante de Empresa. OID: 1.3.6.1.4.1.17326.20.1.7.2

El certificado digital de representante es emitido a favor de una persona física representante de una determinada Entidad. El titular del certificado se identifica no únicamente como persona física perteneciente a una empresa, sino que añade su cualificación como representante legal o apoderado general de la misma.

La solicitud de un certificado de representante está limitada únicamente a los representantes legales (administradores) o a quienes ostentan un poder notarial general para actuar en nombre y representación de la Entidad.

Certificado de Profesional Titulado. OID: 1.3.6.1.4.1.17326.20.1.6.2

El certificado digital de Profesional Titulado, es emitido para que una persona natural acredite su calidad como Profesional Titulado y/o matriculado y su uso se restringe para realizar todo tipo de trámites como son firmar mensajes de datos y/o documentos relacionados en su condición de profesional titulado o matriculado.

Certificado de Función Pública. OID: 1.3.6.1.4.1.17326.20.1.2.2

Certificado que tiene por objeto identificar a los empleados públicos, así como su vinculación a una concreta Administración Pública en virtud del cargo que ocupa en la misma.

Certificado de Comunidad Académica. OID: 1.3.6.1.4.1.17326.20.1.1.2

El certificado digital de Comunidad Académica tiene por objeto acreditar su calidad como docente o estudiante como integrante de la comunidad académica

De igual modo, la SubCA expide los siguientes certificados digitales mediante las Autoridades de Certificación Intermedias de Nivel 1 dependientes de la jerarquía Chambers of Commerce Root – 2008.

Certificado de Componente. OID: 1.3.6.1.4.1.17326.10.11.2.1

Este certificado está asociado a una clave custodiada por una máquina o aplicativo. Las operaciones realizadas comúnmente se realizan de forma automática y desasistida. La acción de las claves asociadas al certificado de sello electrónico dota de integridad y autenticidad a los documentos y transacciones sobre los que se aplica. También se puede utilizar como elemento de identificación cliente de maquina en protocolos de comunicación seguros SSL/TLS o HTTPS, así como el cifrado de información.

Certificado de Firma de código. OID: 1.3.6.1.4.1.17326.10.12.2

Los certificados de para la firma de código permiten, como su nombre indica, que los desarrolladores apliquen una firma electrónica sobre el código que desarrollan: ActiveX, applets java, macros para Microsoft Office, etc. estableciendo de esta forma, en dicho código, garantías de integridad y autenticidad.

Certificado de Servidor Seguro SSL. OID: 1.3.6.1.4.1.17326.10.11.2.1

Emitidos a aplicativos servidores de páginas HTML en Internet mediante protocolo SSL/TLS o HTTPS. Este protocolo es necesario para la identificación y el establecimiento de canales seguros entre el navegador del usuario o tercero que confía y el servidor de páginas HTML del Firmante/Suscriptor.

(Este certificado no se encuentra dentro del alcance de acretiacion)

Certificado de Sello de Tiempo (Estampado Cronológico). OID: 1.3.6.1.4.1.17326.10.13.1.3

El time stamping o sellado de tiempo es el complemento ideal a la seguridad que ofrecen los certificados digitales de identidad. Mediante la aplicación del sellado de tiempo garantizamos el momento exacto en el que se produjo la firma de un documento. El Servicio de Sellado de Tiempo de AC Camerfirma está basado en la especificación del estándar RCF 3161– Internet X. 509 Public Key Infrastructure, ETSI TS 102 023, Time-Stamp Protocol, Electronic Signatures and Infrastructures (ESI) Policy requirements for time-stamping authorities y ETSI TS 101 861, Time stamping profile. Actualmente el servicio de sincronización de tiempos de Camerfirma está sincronizado con la hora legal para Colombia provista por el Instituto Nacoional de Metrología de Colombia.

1.2.2 Autoridad de las Políticas

La actividad de la SubCA podrá ser sometida a la inspección de la Autoridad de las Políticas (PA) o por personal delegado por la misma.

Para las jerarquías descritas en este documento la Autoridad de las Políticas es el departamento jurídico de la SubCA. El departamento jurídico de la SubCA constituye por lo tanto la Autoridad de las Políticas (PA) de las Jerarquías y Autoridades de Certificación descritas anteriormente siendo responsable de la administración de la DPC.

Puede contactar con la Autoridad de las Políticas (PA) en:

Nombre:	Dpto. Jurídico de la CITISEG SAS
Dirección e-mail:	gestion.juridica@citiseg.com
Dirección:	Carrera 13A # 29-26, local 142
Teléfono:	3837295
Fax:	3837295
URL	http://www.citiseg.com/contacto

En lo que se refiere al contenido de esta DPC, se considera que el lector conoce los conceptos básicos de PKI, certificación y firma digital, recomendando que, en caso de desconocimiento de dichos conceptos, el lector se informe a este respecto. En la Web de la SubCA se puede encontrar información general sobre el uso de la firma digital y los certificados digitales.

1.3 Nombre del Documento e Identificación

Nombre del documento:	Declaración de Prácticas de Certificación
Versión:	5
Fecha de emisión:	10/08/2017
Fecha de expiración:	No aplicable
Localización:	http://citiseg.com/declaracion-practicas-certificacion-dpc/
Página web	http://citiseg.com/declaracion-practicas-certificacion-dpc/

1.4 Comunidad y Ámbito de Aplicación.

1.4.1 Autoridad de Certificación (AC).

Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Firmante (Suscriptor) y el Tercero que confía, en las relaciones electrónicas, vinculando una determinada clave pública con una persona.

A los efectos de la presente DPC, la Autoridad de Certificación Raíz e Intermedia de Nivel 1, son gestionadas por AC Camerfirma SA, mientras que la Autoridad de Certificación Intermedia de Nivel 2 es gestionada por la SubCA.

La información relativa a la AC está disponible en la web de la la SubCA, dirección indicada en la sección 1.3.

1.4.2 Prestador de Servicios de Certificación (PSC)

Esta DPC define al Prestador de Servicios de Certificación (PSC) como aquella entidad que presta los servicios concretos relativos al ciclo de vida de los certificados y servicios asociados como la emisión de sellos de tiempo (estampado cronológico), provisión de dispositivos de firma o servicios de validación.

A los efectos de la presente DPC, la SubCA es el PSC.

Nombre o Razón Social:	CITISEG SAS
NIT:	900.760.499-6
Nº Matrícula de Cámara Comercio:	02487553 del 15 de agosto de 2014
Estado Activo en Cámara Comercio:	Activo
Domicilio Social y de correspondencia:	Carrera 13A # 29-26, local 142
Teléfono:	PBX 3837295
Fax:	2441929 Ext. 1006
Email:	info@citiseg.com
Web:	http://citiseg.com/
Oficina Responsable de peticiones, consultas y quejas de los suscriptores y usuarios:	Citiseg

Para PQRSA se informa al usuario a través de la web: www.citiseg.com el proceso a seguir.

1.4.3 Proveedor de Servicios de certificación

Los proveedores de servicios de certificación son terceros que prestan su infraestructura o servicios tecnológicos al PSC, cuando la entidad de certificación así lo requiere y garantizan la continuidad del servicio a los suscriptores durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

A efectos de esta DPC, el Proveedor de Servicios de Certificación es la empresa AC Camerfirma.

Nombre o Razón Social:	AC Camerfirma SA
Domicilio Social y de correspondencia:	Calle Ribera del Loira, 12 28042, Madrid, España
Teléfono:	+34 (91) 4119661
Fax:	+34 (91) 5610769
Email:	info@camerfirma.com
Web:	http://www.camerfirma.com

1.4.4 Autoridad de Registro (AR)

Una Autoridad de Registro (AR) es la responsable de la gestión de las solicitudes, identificación y registro de los solicitantes del Certificado y cualquier responsabilidad específica establecida en esta DPC y Políticas de Certificación. Las AR son autoridades delegadas por el PSC, aunque el PSC es en última instancia el responsable del servicio. El PSC puede ejercer en cualquier momento las labores de AR.

A los efectos de la presente DPC podrán actuar como AR:

- El Prestador de Servicios de Certificación (la SubCA).
- Cualquier agente nacional o internacional que tenga una relación contractual con el PSC y haya superado los procesos de alta y auditoría establecidos por el PSC.

1.4.5 Firmante/ Suscriptor

Firmante/Suscriptor se refiere al titular del certificado cuando éste sea un individuo o compañía. Cuando se emita a nombre de un dispositivo hardware o aplicativo informático, se considerará Firmante/Suscriptor el individuo o compañía asociada al certificado emitido.

Antes de emitir el certificado, el Firmante/Suscriptor es considerado como Solicitante.

1.4.6 Tercero que confía o usuario

En esta DPC se entiende por tercero que confía o usuario a la persona que recibe una transacción electrónica realizada con un certificado emitido por la SubCA y que voluntariamente confía en el certificado emitido por esta.

1.4.7 Entidad

La Entidad es la empresa u organización con la que el Firmante/Suscriptor mantiene una vinculación, según se define en los campos determinados de cada certificado. Y así:

- En los certificados de pertenencia a empresa y de función pública, la entidad está vinculada al Firmante/Suscriptor a través de una relación contractual (laboral, mercantil, como colegiado, funcionario público, etc.)

- En los certificados de representante de empresa, la entidad está representada por el Firmante/Suscriptor que cuenta con amplios poderes de representación.

Como excepción a lo anteriormente expuesto, en los certificados de persona jurídica la Entidad coincide con la figura del Firmante/ Suscriptor.

Como regla general, la Entidad está identificada en el campo de organización en el certificado y su número de identificación fiscal se introduce en un campo del certificado para este fin.

1.4.8 Solicitante

Se entenderá por Solicitante la persona física que solicita el Certificado a la SubCA bien sea directamente o a través de un representante autorizado. El solicitante una vez emitido el certificado será considerado como Firmante/Suscriptor.

1.4.9 Responsable de los certificados

Esta DPC considera que, para los certificados expedidos a particulares, el titular del certificado (el firmante/suscriptor) es la persona responsable del mismo.

La DPC considera que la persona que hace la petición (el solicitante) es responsable de los certificados emitidos a empresas. Esta persona debe ser identificada en el certificado, incluso si la solicitud se realiza a través de un tercero. Para los certificados que contienen poderes de representación, esta DPC considera parte responsable tanto al firmante/suscriptor como a la persona o empresa representada.

1.4.10 TSA-TSU

Una TSA (Autoridad de Sellado de tiempo) es un elemento de confianza en el que el usuario (suscriptores y terceras partes receptoras de sellos) confían para la emisión de sellos de tiempo. La TSA tiene la responsabilidad última sobre todos los servicios relacionados con la emisión de los sellos de tiempo. La TSA tiene la responsabilidad sobre las TSU (Unidades de sellado de tiempo) las cuales emiten los sellos de tiempo en representación de la TSA.

El servicio de sellado de tiempo se compone de una autoridad TSA y una Unidad de Sellado de Tiempo (Estampado Cronológico). Esta última tiene asociada una clave privada que utiliza para la firmar de los sellos de tiempo.

Existe una autoridad de Sellado de tiempo TSA que emite certificados a TSU. Las TSU (Unidades de Sellado de Tiempo) pueden emitir sellos de tiempo en nombre de la TSA. Estas a su vez podrán emitir sellos de tiempo.

En el esquema establecido para el servicio de sellado de tiempo, la TSU emite sellos de tiempo desde claves gestionadas en dispositivo hardware y con las garantías de servicio descritas en este documento.

Los sellos de tiempo se distinguirán por las TSU emisora y por el OID de política descrito en él.

1.4.11 Ámbito de Aplicación y Usos

Esta DPC cumple e incluye las Políticas de Certificación de los certificados indicados en el apartado 1.2.1 de la presente DPC.

Los certificados de la SubCA pueden ser utilizados de acuerdo con la legislación colombiana y esta DPC y políticas. En particular, los certificados sólo pueden utilizarse para los fines para los que fueron emitidos y sujetos a los campos estándar del certificado "Key Usage" y "Extended Key Usage" y siempre que no violen el uso prohibido y no autorizado.

1.4.11.1 Usos Prohibidos y no Autorizados

Los certificados sólo podrán ser empleados con los límites y para los usos para los que hayan sido emitidos en cada caso y están sujetos a los límites establecidos definidos en las políticas de certificación incluidas en estas DPC.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un error pudiera directamente comportar la muerte, lesiones personales o daños medioambientales severos.

Los certificados no pueden utilizarse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados u otros mensajes de información de estado de certificados o validación de firmas.

El uso de los certificados digitales en operaciones que contravienen las Políticas de Certificación aplicables a cada uno de los Certificados, la DPC o los Contratos que la AC firma con las AR ó los Firmantes/Suscriptores tendrán la consideración de usos indebidos, a los efectos legales oportunos, eximiéndose por tanto la AC en función de la legislación vigente de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

La SubCA no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de la SubCA emitir valoración alguna sobre dicho contenido, asumiendo por tanto el Firmante/Suscriptor cualquier responsabilidad sobre los datos o contenido sobre el que se usa el certificado. Asimismo, el Firmante/Suscriptor será responsable de las consecuencias de cualquier uso de estos datos fuera de los límites y condiciones de uso recogidas en las Políticas de Certificación aplicables a cada Certificado, la DPC y los contratos de la AC con los Firmantes, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

La SubCA incorpora información en el certificado sobre las limitaciones de uso, tanto en los campos estándar, en los atributos “key usage” (uso de certificado) y “basic constraints” (restricciones básicas), marcados como críticos en el certificado y por lo tanto de cumplimiento obligatorio por cualquier aplicación que lo utilice, o bien mediante textos incorporados en el campo “user notice” (notificación del usuario) de uso “no crítico” pero de obligado cumplimiento por parte del titular y del usuario del certificado.

Una vez el certificdo haya sido revocado o perdido su vigencia el suscriptor debe dejar de utilizar el certificado en todo el material publicitario que contenga alguna referencia.

1.5 Normativa aplicable

La SubCA viene obligada al cumplimiento de requerimientos marcados en la legislación española y colombiana vigentes, como entidad mercantil prestadora de servicios de certificación digital (en adelante, normativa ó legislación vigente).

La principal legislación aplicable es:

Colombiana:

- Ley 527 de 1999, por medio de la cual se define y reglamenta 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.

- Decreto-Ley 19 de 2012, por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- Decreto 333 de 2014, por el cual se reglamenta el artículo 160 del Decreto-ley 19 de 2012.

1.6 Contacto Técnico

Esta DPC está administrada y gestionada por la Autoridad de Políticas según se describe en el apartado correspondiente**¡Error! No se encuentra el origen de la referencia.** y puede contactarse por los medios allí expuestos.

De manera adicional, es posible contactar con el Departamento Técnico para aquellas cuestiones técnicas respecto a la gestión de los certificados que no pueda resolver la Autoridad de Políticas.

Nombre:	Dpto. Técnico de la SubCA
Dirección e-mail:	soporte.nivel1@citiseg.com.co
Dirección:	Carrera 13A # 29-26, local 142
Teléfono:	244 29 29 ext. 3333
Fax:	2441929
URL	http://www.citiseg.com/contacto

2 CLÁUSULAS GENERALES

2.1 Obligaciones

2.1.1 Obligaciones de la SubCA y la CACamerfirma España

En conformidad con lo establecido en las Políticas de Certificación y la presente DPC, y en conformidad con la legislación vigente en materia de prestación de servicios de certificación, la SubCA y la CA se compromete a:

- Respetar lo dispuesto en esta DPC y en las Políticas de Certificación, así como requerir a los proveedores que pueda emplear para la prestación de los servicios de certificación que cumplan estas obligaciones.
- Proteger sus claves privadas y mantenerlas de forma segura.
- Emitir certificados conforme a esta DPC, a las Políticas de Certificación, a los estándares técnicos de aplicación y a lo solicitado o acordado con el suscriptor.
- Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos.
- Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente.
- Publicar los certificados emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.
- Suspender y revocar los certificados según lo dispuesto en esta Política y publicar las mencionadas revocaciones en la CRL.
- Informar a los Firmantes/Suscriptores de la revocación o suspensión de sus certificados, en tiempo y forma, de acuerdo con la legislación vigente.
- Publicar esta DPC y las Políticas de Certificación correspondientes en su página Web.
- Informar sobre las modificaciones de esta DPC y de las Políticas de Certificación a los Firmantes/Suscriptores y a las AR que estén vinculadas a ella.
- No almacenar ni copiar los datos de creación de firma del Firmante/Suscriptor.
- Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia, en su caso.
- Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida o destrucción o falsificación.
- Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente.
- Atender oportunamente las solicitudes y reclamaciones de los suscriptores.
- Disponer de un canal de comunicación de atención permanente a suscriptores y terceros, que permita las consultas y la pronta solicitud de revocación de certificados por los suscriptores, según indica el art. 15.12 del Decreto 333 de 2014.
- Informar a la Superintendencia de Industria y Comercio y al ONAC, de manera inmediata, la ocurrencia de cualquier evento que comprometa o pueda comprometer la prestación del servicio, según indica el art. 15.7 del Decreto 333 de 2014.

- Permitir y facilitar la realización de las auditorías por parte del ONAC de conformidad con lo dispuesto en el artículo 162 del Decreto-ley 19 de 2012, de acuerdo con los requerimientos de la Ley 527 de 1999 y el Decreto 333 de 2014.
- Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas digitales y certificados emitidos, según indica la Ley 527 de 1999.
- Salvaguardar la imparcialidad e independencia de las actividades de certificación de Citiseg; para esta actividad se dispuso de un comité de imparcialidad e independencia que vigila y monitorea los riesgos que comprometan este aspecto, cualquier conflicto de interés que sea detectado por parte del público en general puede ser reportado en http://citiseg.com/contacto/ y se direccionará a esta instancia.
- Informar a los suscriptores que sus proveedores críticos cumplen con los requisitos de acreditación para ECD como soporte de su contratación y del cumplimiento de los requisitos solicitados tanto administrativos como técnicos. Se consideran como proveedores críticos: ECD recíprocas, y data center.
- Informar oportunamente la modificación o actualización de servicios incluidos en el alcance de su acreditación, en los términos que establezcan los procedimientos, reglas y requisitos del servicio de acreditación del ONAC.

  Para ampliar información sobre la DPC de la CA Camerfirma España, dirigirse al link http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/

2.1.2 Obligaciones de la AR

Las AR son las entidades delegadas por la SubCA para realizar las labores de registro de los suscriptores en el ámbito de la emisión de certificados. Por lo tanto, las AR también se comprometen a cumplir las obligaciones definidas en las Prácticas de Certificación para la emisión de certificados, y en particular:

- Respetar lo dispuesto en esta DPC y en las Políticas de Certificación incluidas.
- Proteger sus claves privadas.
- Comprobar la identidad de los Firmantes/Suscriptores y Solicitantes de los certificados.
- Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
- Proporcionar al suscriptor, en caso de certificados individuales, o al futuro poseedor de claves, en caso de certificados de organización, acceso al certificado.
- Entregar, en su caso, el dispositivo criptográfico correspondiente.
- Archivar, por el periodo dispuesto en la legislación vigente, los documentos suministrados por el solicitante o suscriptor, garantizando su protección y confidencialidad.
- Respetar lo dispuesto en los contratos firmados con la SubCA y con el Firmante/Suscriptor.
- Informar a la SubCA de las causas de revocación, cuando sean conocidas.

2.1.3 Obligaciones del Firmante/Suscriptor

El Firmante/Suscriptor estará obligado a cumplir con lo dispuesto por la normativa vigente y a:

- Usar el certificado según lo establecido en la presente DPC y en las Políticas de Certificación aplicables, manteniendo su control y seguridad.

- Respetar lo dispuesto en los documentos firmados con la SubCA y la AR.
- Informar a la mayor brevedad posible de la existencia de alguna causa de suspensión o revocación.
- Notificar cualquier inexactitud o cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- No utilizar la clave privada ni el certificado una vez la SubCA solicita o informa de la suspensión o revocación del mismo, o una vez ha expirado el plazo de validez del certificado.
- Hacer uso del certificado digital con el carácter de personal e intransferible y, por tanto, asumir la responsabilidad por cualquier actuación que se lleve a cabo en contravención de esta obligación, así como cumplir las obligaciones que sean específicas de la normativa aplicable a las dichas certificaciones digitales.
- Autorizar a la SubCA para proceder al tratamiento de los datos personales contenidos en los certificados, en conexión con las finalidades de la relación electrónica y, en todo caso, para cumplir las obligaciones legales de verificación de certificados.
- Responsabilizarse de que toda la información incluida, por cualquier medio, la solicitud del certificado y en el mismo certificado sea exacta, completa para la finalidad del certificado y esté actualizada en todo momento.
- No utilizar la clave privada, el certificado electrónico o cualquier otro soporte técnico entregado por el prestador de servicios de certificación correspondiente para realizar ninguna transacción prohibida por la ley aplicable.
- Al hacer referencia al servicio de certificación digital en medios de comunicación, tales como documentos, folletos o publicidad, el suscriptor informa que cumple con los requisitos especificados en las Políticas de Certificación Digital.
- No se debe utilizar la marca de certificación digital en un certificado digital no acreditado o en condición de revocación, vencimiento o cualquier otro estado que incumpla las condiciones dispuestas en este documento y las Politicas de Cetificación por Servico.

Si el suscriptor genera sus propias claves, se obliga a:

- Generar sus claves de suscriptor utilizando un algoritmo reconocido como aceptable para la firma electrónica, en su caso cualificado, o el sello electrónico, en su caso calificado.
- Crear las claves dentro del dispositivo de creación de firma o de sello, utilizando un dispositivo seguro cuando proceda.
- Utilizar longitudes y algoritmos de clave reconocidos como aceptables para la firma electrónica.

2.1.4 Obligaciones del Solicitante del certificado

El Solicitante de un certificado (ya sea de forma directa o a través de un tercero autorizado) se compromete a cumplir con las disposiciones legales y a:

- Utilizar el certificado de acuerdo con la presente DPC y las Políticas de Certificación aplicables.
- Respetar las disposiciones establecidas en los documentos suscritos con la SubCA y la RA.
- Reportar cualquier causa de suspensión / revocación tan pronto como sea posible.

- Reporte cualquier cambio en los datos proporcionados para crear el certificado durante su período de validez.
- No utilizar la clave privada ni el certificado una vez la SubCA solicita o informa de la suspensión o revocación del mismo, o una vez ha expirado el plazo de validez del certificado.

2.1.5 Obligaciones del Tercero de confianza/Usuario

Será obligación del Tercero que confía cumplir con lo dispuesto en la normativa vigente y a:

- Verificar la validez de los certificados antes de realizar cualquier operación basada en los mismos. la SubCA dispone de diversos mecanismos para realizar dicha comprobación, como el acceso a listas de revocación o a servicios de consulta en línea como OCSP, todos estos mecanismos están descritos en la página Web de la SubCA indicada en la sección 1.3.
- Conocer y respetar las garantías, limitaciones y responsabilidades aplicables con la aceptación y uso de los certificados de confianza, y aceptar estar sujeto a ellas.

2.1.6 Obligaciones de la Entidad

En el caso de aquellos certificados que impliquen vinculación a una Entidad, la Entidad estará obligada a solicitar a la AR la revocación o suspensión del certificado cuando el Firmante/Suscriptor cese dicha vinculación respecto a la organización.

2.1.7 Obligaciones respecto al Repositorio

La SubCA dispone de un servicio de consulta de certificados emitidos y listas de revocación. Estos servicios están disponibles públicamente en su página Web.

Esta información es custodiada dentro de una base de datos relacional con medidas de integridad y acceso que permiten su custodia de acuerdo con las exigencias de las Políticas de Certificación.

La SubCA publica los certificados emitidos, las listas de revocación, políticas y prácticas de certificación sin coste.

2.2 Responsabilidad

Responsabilidad de la SubCA

La SubCA será responsable de los daños y perjuicios ocasionados a los usuarios por sus servicios, ya sea al Firmante/Suscriptor o al Tercero que confía, y a otros terceros en los términos establecidos en la legislación vigente y en las Políticas de Certificación.

De igual forma, AC Camerfirma SA será responsable de los servicios prestados a la SubCA en los términos previstos por el acuerdo suscrito entre ambos.

En cumplimiento con lo establecido en el artículo 9 del Decreto 333 de 2014, la SubCA ha suscrito una póliza de seguro con una entidad aseguradora autorizada de acuerdo con la legislación colombiana, que ampara entre otros aspectos los perjuicios contractuales y extracontractuales de los suscriptores y terceros de buena fe exenta de culpa derivados de errores y omisiones, o de actos de mala fe de los administradores, representantes legales o empleados de la SubCA en el desarrollo de sus actividades.

La SubCA será responsable de:

- La exactitud de toda la información contenida en el certificado en la fecha de su emisión, mediante la confirmación de los datos del solicitante y las prácticas de RA.

- La garantía de que, en el momento de la entrega del certificado, obra en poder del Firmante/Suscriptor la clave privada correspondiente a la clave pública dada o identificada en el certificado cuando el proceso así lo requiera, mediante la utilización de peticiones estandarizadas en formato PKCS#10.
- La garantía de que la clave pública y privada funcionan conjunta y complementariamente, utilizando dispositivos y mecanismos criptográficos certificados.
- La correspondencia entre el certificado solicitado y el certificado entregado.
- Cualquier responsabilidad que se establezca por la legislación vigente.

Responsabilidad de las AR

Las AR suscriben un contrato de prestación de servicio con la SubCA mediante el cual la SubCA delega las funciones de registro en las AR, consistentes fundamentalmente en:

1. Obligaciones previas a la emisión de un certificado.
    - Informar adecuadamente a los solicitantes de la firma de sus obligaciones y responsabilidades.
    - La adecuada identificación de los solicitantes, que deben ser personas capacitadas o autorizadas para solicitar un certificado digital.
    - Verificar la validez y vigencia de los datos de los solicitantes y de la Entidad, en el caso de que exista una relación de vinculación o representación.
    - Acceder a la aplicación de Autoridad de Registro para gestionar las solicitudes y los certificados emitidos.

2. Obligaciones una vez emitido el certificado.
    - Suscribir los contratos de Prestación de Servicios de Certificación Digital con los solicitantes.
    - El mantenimiento de los certificados durante su vigencia (extinción, suspensión, revocación).
    - Archivar las copias de la documentación presentada y los contratos debidamente firmados por los solicitantes en conformidad con Políticas de Certificación publicadas por la SubCA y la legislación vigente.

Así pues, las AR se responsabilizan de las consecuencias en caso de incumplimiento o cumplimiento incorrecto de sus labores de registro, y a través del cual se comprometen a respetar además las normas reguladoras internas de la la SubCA (Políticas y DPC), las cuales deberán tenerse en cuenta por parte de las AR y deberán servirles como guías de orientación.

En caso de reclamación por un Firmante, una Entidad, o un usuario, la AR deberá aportar la prueba de la actuación diligente y si se constata que el origen de la reclamación radica en un error en la validación o comprobación de los datos, la AC podrá, en virtud de los acuerdos firmados con las AR, hacer responsable a la AR de las consecuencias. Porque, aunque legalmente sea la AC la entidad responsable frente al Firmante, una Entidad, o Tercero que Confía, y que para ello dispone de un seguro de responsabilidad civil, según el acuerdo vigente y las Políticas vinculantes, la AR tiene como obligación contractual "identificar y autenticar correctamente al Solicitante y, en su caso, a la Entidad que corresponda", y en su virtud deberá responder frente a la SubCA de sus incumplimientos.

Por supuesto, no es intención de la SubCA descargar todo el peso de la asunción de responsabilidad a las AR en cuanto a los posibles daños cuyo origen vendría de un incumplimiento de las tareas delegadas a las AR. Por esta razón, al igual que lo previsto para la AC, la AR se ve sometida a un régimen de control que será ejercido por la SubCA, no solamente a través de la comprobación de archivos y procedimientos de conservación de archivos de la AR, sino también mediante la realización de auditorías para evaluar los recursos empleados y el conocimiento y control de los procedimientos operativos empleados para ofrecer los servicios de AR.

Responsabilidad de los suscriptores

Los suscriptores serán responsables por la falsedad, error u omisión en la información suministrada a la SubCA o AR y por el incumplimiento de sus deberes como suscriptor (art. 40, Ley 527 de 1999).

2.2.1 Exoneración de responsabilidad de SubCA y AR

Según la legislación vigente, la responsabilidad de la SubCA y de la AR no se extiende a aquellos supuestos en los que la utilización indebida del certificado tiene su origen en conductas imputables al Firmante y al Tercero de confianza por:

- No haber proporcionado la información correcta, inicial o posteriormente como consecuencia de modificaciones de las circunstancias reflejadas en el certificado electrónico, cuando su inexactitud no haya podido ser detectada por el Prestador de Servicios de Certificación.
- Haber incurrido en negligencia con respecto a la conservación de los datos de creación de firma y a su confidencialidad.
- No haber solicitado la suspensión o revocación del certificado electrónico en caso de duda sobre el mantenimiento de la confidencialidad.
- Haber utilizado la firma después de haber expirado el periodo de validez del certificado electrónico.
- Superar los límites que figuren en el certificado electrónico.
- En conductas imputables al Tercero que confía si éste actúa de forma negligente, es decir cuando no compruebe o tenga en cuenta las restricciones que figuran en el certificado en cuanto a sus posibles usos y límite de número de transacciones; o cuando no tenga en cuenta el estado de vigencia del certificado.
- De los daños ocasionados al firmante o terceros que confía por la inexactitud de los datos que consten en el certificado electrónico, si éstos le han sido acreditados mediante documento público, inscrito en un registro público, si así resulta exigible.

La SubCA y las AR tampoco serán responsables en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.
- Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y en las Políticas de Certificación.
- Por el uso indebido o fraudulento de los certificados o CRL’s emitidos por la AC.
- Por el uso de la información contenida en el Certificado o en la CRL.

- Fraude en la documentación presentada por el Solicitante.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación o suspensión.
- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Por el incumplimiento de las obligaciones establecidas para el Firmante/Suscriptor o Terceros que confían en la normativa vigente, en las Políticas de Certificación o en esta DPC.
- Por la no recuperación de documentos cifrados con la clave pública del Firmante.

2.2.2 Límite de responsabilidad en caso de pérdidas por transacciones

El límite monetario del valor de las transacciones se expresa en el propio certificado mediante la inclusión de una extensión "qcStatements", (OID 1.3.6.1.5.5.7.1.3), tal como se define en la RFC 3039. La expresión del valor monetario se ajustará a lo dispuesto en la sección 5.2.2 de la norma TS 101 862 de la ETSI (European Telecommunications Standards Institute, www.etsi.org).

Si la extensión del certificado anteriormente expuesta no lo contradice, el límite máximo que la SubCA permite en las transacciones económicas realizadas es de 0 (cero) pesos.

2.3 Responsabilidad financiera

La SubCA, en su actividad como PSC, dispone de un seguro de responsabilidad civil que contempla sus responsabilidades para indemnizar por daños y perjuicios que se puedan ocasionar a los usuarios de sus servicios: el Firmante/Suscriptor y el Tercero que confía, y a terceros; por un importe conjunto de 3.700.000 euros.

Adicionalmente, Citiseg SAS cuenta con los amparos por responsabilidad civil contractual y extracontractual respecto de los eventos que puedan ocurrir en ejecución de sus actividades como Entidad de Certificación Digital (ECD).

2.4 Condiciones no discriminatorias

La CA y la SubCA manifiesta que los procesos bajo los cuales opera y los servicios que ofrece no están sujetos a la discriminación bajo ninguna circunstancia y son accesibles a los solicitantes de los mismos toda vez que las solicitudes estén dentro del alcance definido, La CA y la SubCA puede rechazar una solicitud únicamente si este rechazo esta soportado en razones fundamentadas y demostrables.

2.5 Interpretación y ejecución

2.5.1 Legislación

La ejecución, interpretación, modificación o validez de la presente DPC se regirá por lo dispuesto en las legislaciones colombiana y española vigentes.

2.5.2 Independencia

La invalidez de una de las cláusulas contenidas en esta DPC no afectará al resto del documento. En tal caso se tendrá la mencionada cláusula por no incluida.

2.5.3 Notificación

Cualquier notificación referente a la presente DPC se realizará por correo electrónico o correo certificado a la Autoridad de Políticas indicada en el apartado correspondiente de este documento o mediante correo certificado dirigido a cualquiera de las direcciones referidas en el apartado 1.6 Contacto Técnico.

2.5.4 Procedimiento de resolución de disputas

Toda controversia o conflicto que se derive del presente documento se resolverá definitivamente, mediante el arbitraje administrado por el organismo de Arbitraje correspondiente, de conformidad con su normativa legal, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo o decisión que se dicte.

2.6 Tarifas

2.6.1 Tarifas de emisión de certificados y renovación

Los precios de los servicios de certificación o cualquiera de los otros servicios relacionados están disponibles para los usuarios en la página Web de la SubCA indicada en el apartado 1.3.

El precio específico estará publicado para cada tipo de certificado.

2.6.2 Tarifas de acceso a los certificados

El acceso a los certificados emitidos es gratuito, no obstante, la SubCA implementa controles para evitar los casos de descarga masiva de certificados. Cualquier otra circunstancia que a juicio de la SubCA deba ser considerada a este respecto se publicara en la página Web indicada en el apartado 1.3.

2.6.3 Tarifas de acceso a la información relativa al estado de los certificados o certificados revocados

La SubCA provee un acceso gratuito a la información relativa al estado de los certificados o de los certificados revocados a través de Listas de Certificados Revocados (CRL) o mediante acceso vía Web en la dirección Internet indicada en el apartado 1.3.

La SubCA se reserva el derecho a facturar por servicios de validación de valor añadido como OCSP. Las tarifas de estos servicios estarán publicadas en la dirección web indicada en el apartado 1.3.

2.6.4 Tarifas de acceso a Políticas de Certificación

El acceso al contenido de la presente DPC y Políticas es gratuito, en la dirección Web de la SubCA indicada en el apartado 1.3.

2.6.5 Política de reintegros

La SubCA no tiene una política específica de reintegros, y se adhiere en general a las regulaciones actuales.

2.7 Publicación y repositorios

2.7.1 Publicación de información de la AC

De manera general la SubCA publica las siguientes informaciones en su repositorio:

- Un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida, o extinguida.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- La política general de certificación y, cuando sea conveniente, las políticas específicas.
- Los perfiles de los certificados y de las listas de revocación de los certificados.
- La Declaración de Prácticas de Certificación.
- Los instrumentos jurídicos vinculantes con suscriptores y verificadores.

Todo cambio en las especificaciones o condiciones del servicio será comunicado a los usuarios por la Entidad de Certificación, a través del depósito.

2.7.1.1 Políticas y Prácticas de Certificación

La presente DPC que incluye las Políticas de Certificación está disponible públicamente en el sitio web de la la SubCA, indicado en el apartado 1.3 AR-PT-03 POLITICAS DE CERTIFICACIÓN POR SERVICIO.

2.7.1.2 Términos y condiciones.

Los usuarios pueden encontrar los términos y condiciones de servicio de la SubCA ya sea a través del contrato físico en el proceso de emisión de certificados o en su sitio web indicado en el apartado 1.3.

2.7.1.3 Difusión de los certificados

Se podrá acceder a los certificados emitidos siempre que el Firmante/Suscriptor de su consentimiento en la página web indicada en el apartado 1.3.

Las Claves Raíz e Intermedias de Nivel 1 en las jerarquías de Camerfirma se pueden descargar desde http://www.citiseg.com.co. Las Claves intermedias de Nivel 2 se pueden descargar desde el sitio web de la SubCA, indicado en el apartado 1.3.

Los certificados de usuario final se pueden consultar desde el sitio web en modo seguro, introduciendo el email del suscriptor. La respuesta del sistema, si encuentra un suscriptor con ese email, es una página con todos los certificados asociados, ya estén activos, caducados, o revocados. Este servicio de consulta no es gratuito, ni se pueden descargar certificados de forma masiva.

Se podrá ofrecer esta información a través de un servicio LDAP. En el momento en que este servicio este a disposición del cliente se describirán en estas DPC los detalles del servicio.

2.7.2 Frecuencia de publicación

La SubCA publica los certificados inmediatamente después de haber sido emitidos y siempre tras la aprobación del Firmante/Suscriptor.

La SubCA publica de forma inmediata cualquier modificación en las Políticas y la DPC, en su página Web indicada en el apartado 1.3, manteniendo un histórico de versiones.

2.7.3 Control de acceso

La SubCA publica certificados y CRL en su sitio web. Se requiere la dirección de correo electrónico del titular del certificado para acceder al directorio de certificados y se debe pasar un control "anti-bot" para eliminar la posibilidad de búsquedas y descargas masivas.

El acceso a la información de revocación, así como a los certificados emitidos por la SubCA es libre y gratuito.

2.8 Auditorías

Tanto AC Camerfirma SA como la SubCA son empresas comprometidas con la seguridad y la calidad de sus servicios.

Los objetivos de AC Camerfirma SA en relación con la seguridad y la calidad han supuesto obtener las certificaciones ISO/IEC 27001:2005 e ISO/IEC 20000-1:2011 sobre la infraestructura y sistemas que opera sus operaciones como Auditoridad de Certificación, recibiendo anualmente auditorías internas y externas de su Sistema de Certificación. De manera adicional, está sujeta a auditorías periódicas anuales, como el sello Webtrust para CA, Webtrust SSL Baseline con Seguridad de Red y Webtrust EV, los cuales aseguran que los documentos de políticas y DPC tienen un formato y alcance adecuado a la vez que están completamente alineadas con su operativa como CA.

La SubCA, al encontrarse dentro de la jerarquía de AC Camerfirma SA, según lo expuesto en el apartado 1.2.1, se ve sometida a auditorías que garantizan que sus DPC y Políticas de Certificados se encuentran alineadas con la DPC de Camerfirma y las buenas prácticas internacionales y que los certificados son gestionados acorde a las mismas garantizando el cumplimiento de los procedimientos internos.

Adicionalmente, en cumplimiento del art. 14 del Decreto 333 de 2014, se deberá realizar una auditoría, con su correspondiente informe, que dictamine que la SubCA actúa o está en capacidad de actuar, de acuerdo con los requerimientos de la Ley 527 de 1999, lo previsto en el Decreto 333 de 2014 y en las normas que los sustituyan, complementen o reglamenten. Así mismo, evaluará todos los servicios a que hace referencia el literal d) del artículo 2º de la Ley 527 de 1999 y que sean prestados o pretenda prestar la SubCA. Dicho informe de auditoría quedará a disposición de la Organización Nacional de Acreditación de Colombia (ONAC).

Las Autoridades de Registro están sujetas a un proceso de auditoría interna que se realiza periódicamente con una frecuencia no superior a 2 años.

2.8.1 Frecuencia de las auditorias

La frecuencia de las auditorías a las que se somete la SubCA es anual.

2.8.2 Identificación y calificación del auditor

Las auditorias son realizadas por empresas de auditoría especializadas en PKI y de reconocido prestigio en este tipo de auditorías. Por tanto, los auditores cuentan con la cualificación adecuada para la correcta ejecución de este tipo de auditorías.

2.8.3 Relación entre el auditor y la SubCA

Las empresas de auditoría son de reconocido prestigio con departamentos especializados en la realización de auditorías en el ámbito de la PKI y que mantienen la independencia de auditoría en todo momento, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con la SubCA.

2.8.4 Tópicos cubiertos por la auditoria

La auditoría verifica:

- Que la SubCA cumple con los requerimientos de las Políticas de Certificación que gobiernan la emisión de los distintos certificados digitales.
- Que la DPC se ajusta a lo establecido en las Políticas, con lo acordado por la Autoridad que aprueba la Política y con lo establecido en la normativa vigente.
- Que la SubCA gestiona de forma adecuada sus sistemas de información para cumplir con la DPC y Políticas de Certificación.
- Cumplimiento de la legislación vigente en el ámbito de entidades de certificación y certificados digitales.

2.9 Confidencialidad

2.9.1 Tipo de información a mantener confidencial

La SubCA considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que le haya otorgado el carácter de confidencialidad, a no ser que exista una imposición legal.

La SubCA dispone de una adecuada política de tratamiento de la información y de los modelos de acuerdo que deberán firmar todas las personas que tengan acceso a información confidencial.

La SubCA cumple en todo caso con la normativa vigente en materia de protección de datos conforme a lo dispuesto en la ley 1581 de 2012.

La obligación de confidencialidad no se extiende en ningún caso a:

• Información que fuera del dominio público previamente a la fecha en la cual hubiere sido entregada a la correspondiente parte.
• Información que se haya hecho pública lícitamente durante la vigencia del presente proceso.
• Información que deba ser entregada por mandato legal a las autoridades de cualquier orden.

2.9.2 Tipo de información considerada no confidencial

La SubCA considera como información no confidencial la siguiente:

- La contenida en la presente DPC que incluye las Políticas de Certificación.
- La información contenida en los certificados que el Firmante/Suscriptor haya otorgado su consentimiento.
- La información referente al estado de los certificados (vigente, suspendido o revocado).
- Cualquier información cuya publicidad sea impuesta por la normativa vigente.

2.9.3 Divulgación de información de revocación / suspensión de certificados

La SubCA difunde la información relativa a la suspensión o revocación de un certificado mediante la publicación periódica de las correspondientes CRL.

La SubCA proporciona un servicio de consulta de CRL y Certificados en el sitio de Internet indicado en el apartado 1.3.

2.9.4 Envío de información a la Autoridad Competente

La SubCA proporcionará la información solicitada por la autoridad competente en los casos y forma establecidos legalmente.

2.10 Derechos de los suscriptores

1. Usar el certificado de conformidad con las Políticas de Certificación de cada tipo de certificado establecidas en la DPC.
2. A que la ECD le preste los servicios en las condiciones previstas en la normativa vigente y en lo previsto en la PC y DPC.
3. Su información sea tratada conforme a la política de protección de datos personales.
4. Se conserve de forma adecuada la información sobre los certificados que le hayan sido emitidos conforme a la normativa vigente.
5. A solicitar la revocación de sus certificados ya sea por su voluntad o por compromiso de su clave privada.

2.11 Derechos de propiedad intelectual

La propiedad intelectual de esta DPC pertenece a la SubCA a AC Camerfirma

3 IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 Registro inicial

3.1.1 Tipos de nombres

El Firmante/Suscriptor se describe en los certificados por un nombre distintivo (DN o distinguished name) conforme al estándar X.500.

Las descripciones del campo DN están reflejadas en cada una de las fichas de perfil de los certificados. Ver apartado 7.1.

3.1.2 Seudónimos

En general no se pueden utilizar seudónimos para identificar una organización. Los certificados personales pueden utilizar seudónimos en lugar del nombre real del poseedor de la clave correspondiente al certificado, siempre que en caso necesario se pueda determinar esta identidad. El pseudónimo constará como tal de manera inequívoca.

La admisión o no de pseudónimos es tratada en cada una de las Políticas de certificación. En caso de ser necesarios, la SubCA utilizara el seudónimo en el atributo CN del nombre del Firmante/Suscriptor guardando confidencialmente la identidad real del Firmante/Suscriptor.

El cálculo del seudónimo en aquellos certificados donde se permita, se realiza de manera que se identifica unívocamente al titular real del certificado anexando al número de serie del certificado más un acrónimo de la organización.

El uso de anónimos está totalmente prohibido.

3.1.3 Reglas utilizadas para interpretar varios formatos de nombres

La SubCA atiende en todo caso a lo marcado por el estándar X.500 de referencia en la ISO/IEC 9594.

3.1.4 Unicidad de los nombres

El atributo DN se encuentra construido de tal forma que no es posible que dos suscriptores dispongan de un mismo DN. De este modo no es posible asignar un DN existente a un suscriptor distinto.

3.1.5 Procedimiento de resolución de disputas de nombres

La SubCA no tiene responsabilidad en el caso de resolución de disputas de nombres. La asignación de nombres se realizará basándose en su orden de entrada y tras comprobar la documentación requerida para cada tipo de certificado.

La SubCA no arbitrará este tipo de disputas, que deberán ser resueltas directamente por las partes. La SubCA en todo caso se atiene a lo dispuesto en el apartado 2.5.4 de esta DPC.

3.1.6 Reconocimiento, autenticación y función de las marcas registradas

La SubCA no asume compromisos en la emisión de certificados respecto al uso de una marca comercial. La SubCA no permite deliberadamente el uso de un nombre cuyo derecho de uso no sea propiedad del Firmante/Suscriptor. Sin embargo, la SubCA no está obligada a buscar evidencias de la posesión de marcas registradas antes de la emisión de los certificados

3.1.7 Métodos de prueba de la posesión de la clave privada

La SubCA emplea diversos circuitos para la emisión de certificados donde la clave privada se gestiona de diferente forma. La clave privada puede ser generada tanto por el usuario como por la SubCA.

El modelo de generación de claves utilizado viene indicado en el propio certificado, tanto en su identificador de Política como en el atributo Descripción del campo DN del certificado.

Generación de claves por parte de la SubCA

En el caso que se generen las claves por la SubCA, se emplean mecanismos que permiten garantizar que únicamente el suscriptor se encuentre en posesión de la clave privada. Las claves se entregan al suscriptor en mano o por correo mediante ficheros protegidos utilizando el Standard PKCS#11. La seguridad del proceso queda garantizada ya que la clave de acceso al fichero, que posibilita la instalación de este en las aplicaciones, es entregada por un medio distinto al utilizado en la entrega del P11 (correo, teléfono, entrega personal, SMS…) y únicamente el suscriptor tiene acceso a las dos partes (PKCS#11 y clave de protección).

En el caso de que las claves se generen en una tarjeta criptográfica (DSCF), las claves privadas no se pueden extraer del chip criptográfico de la tarjeta y el PIN es protegido por el suscriptor. Por lo que se garantiza en todo momento la posesión de la clave privada.

Generación de las claves por el suscriptor

En aquellos casos en los que el suscriptor genera su par de claves, se considera que el suscriptor dispone de un mecanismo de generación de claves homologado por el prestador, siendo la prueba de posesión de la clave privada en estos casos la petición recibida por la SubCA en formato PKCS#10. (Clave pública firmada por la clave privada).

Cuando el suscriptor crea previamente sus propias claves en un dispositivo criptográfico HSM y pide a la SubCA emitir un certificado digital con una política de generación de claves en dispositivo hardware, el suscriptor debe acompañar a la petición una declaración incorporando:

- El proceso seguido para la creación de las claves
- Las personas implicadas
- El entorno en el que se ha realizado
- El equipo HSM utilizado (modelo y marca)
- Políticas de seguridad empleadas: (tamaño de claves, parámetros de creación de la clave, exportable/no exportable y cualquier dato relevante adicional)
- La solicitud PKCS#10 generada.
- Incidencias presentadas y su resolución.

Este informe puede ser redactado y firmado bien por un tercero (empresa que realiza la instalación por el cliente) o por el cliente en una declaración responsable. El informe debe ser visado antes de la emisión del certificado por un responsable técnico de Camerfirma.

La SubCA se reserva el derecho a valorar el aval del tercero externo como valido o bien rechazarlo.

3.1.8 Autenticación de la identidad de un individuo, la entidad y su vinculación

Para realizar una correcta identificación de la identidad del Solicitante, de la entidad y de su vinculación, la SubCA a través de las Autoridades de Registro, exige:

- Identificación del Solicitante:
  Se exige la presencia física del Firmante/Suscriptor cuando éste es también Solicitante, o de un representante del Solicitante cuando éste es una entidad jurídica, así como la presentación de un documento oficial que acredite de forma fehaciente su identidad (NIT, Cédula de

Ciudadanía, tarjeta de identidad, pasaporte o cualquier otro documento admitido en derecho), siempre que contenga al menos la siguiente información:

a) Nombre y apellidos de la persona
b) Lugar y fecha de nacimiento
c) Número de identidad reconocido legalmente
d) Otros atributos de la persona que deban constar en el certificado

La presencia física no es obligatoria en los casos previstos en la legislación vigente

- Identificación de la entidad:

  Con carácter previo a la emisión y entrega de un certificado de organización o sello electrónico es necesario autenticar los datos relativos a la constitución y la personalidad jurídica de la entidad. Se exige la identificación de la entidad, por lo que la AR requerirá la documentación pertinente en función del tipo de entidad. Esta información varía dependiendo del tipo de entidad y está indicada en los manuales operativos de la AR y en la Web de la SubCA. En general serán datos relativos a la constitución y la personalidad jurídica de la entidad, y a la extensión y vigencia de las facultades o poderes de representación del solicitante, mediante los documentos públicos que los acrediten de forma fehaciente y la consulta al pertinente registro público, cuando se trate de datos que deben figurar en ella. Se comprobará:

  a) Nombre legal completo de la organización
  b) Estado legal de la organización
  c) Número de registro tributario
  d) Datos de identificación registral

- Identificación del dominio:

  Para los certificados SSL pretenden identifican a una entidad a cuyo nombre ha sido registrado un dominio. La RA utilizara los medios oportunos para asegurarse de la existencia de la organización y el control del dominio. Entre estos medios se cuentan bases registrales externas. El identificativo fiscal de la organización se incorporará en el contenido del certificado

- Identificación de la vinculación:

  Para los **Certificados de representante de empresa** se exige la documentación sobre la capacidad de **representación** del Firmante/Suscriptor respecto de la otra persona, por medio de la entrega de las escrituras notariales que demuestran sus poderes o facultades de representación. Se presentará un certificado expedido por el registro público correspondiente con menos de **10 días** de antigüedad. La AR puede disponer también de medios telemáticos para la consulta en línea del estado y nivel de representación del solicitante.

  Para los **Certificados de pertenencia a empresa** la AR debe obtener una acreditación documental de la vinculación de la persona física con la organización, mediante cualquier medio admitido en derecho. En general, será necesaria la presentación de una autorización firmada por un representante legal o apoderado general de la entidad.

  En los **Certificados de persona jurídica**, en los que el Firmante/ Suscriptor y el Solicitante son distintos, deberá demostrar documentalmente que el Solicitante tiene poderes suficientes para realizar dicha solicitud de certificado por cuenta del Firmante/ Suscriptor, mediante la presentación de un certificado del registro público correspondiente no superior a 10 días o

mediante consulta en línea realizada por la propia AR a los datos del registro público correspondiente.

En los **Certificados de Función Pública** no se exige la documentación acreditativa de la existencia de la administración pública. Se exige la documentación de identidad de la persona que actúa como responsable, en nombre de dicha Administración Pública, organismo o entidad de derecho público. El Solicitante / responsable se identificará ante la AR con un documento que acredite de forma fehaciente su identidad y un documento acreditativo de su pertenencia como empleado en la Administración Pública, organismo o entidad de derecho público donde consten además los datos identificativos de ésta.

En los **Certificados de Firma de Código** se identifican a una entidad, por lo que se comprobará la identidad de esta y de los solicitantes mediante el acceso a bases de datos externas.

La información de identificación de suscriptores de certificados personales, así como de poseedores de claves de certificados de organización, se debe realizar contrastando la información de la solicitud con la documentación aportada, electrónicamente o en soporte físico.

3.2 Renovación de la clave

Antes de renovar un certificado, la SubCA deberá comprobar que la información utilizada para verificar la identidad y demás datos del suscriptor y del poseedor de la clave sigue siendo válida.

Si cualquier información del suscriptor o del poseedor de la clave ha cambiado, se registrará adecuadamente la nueva información.

Antes de generar un certificado a un suscriptor cuyo certificado fue revocado (siempre que la causa de la revocación haya sido diferente del compromiso de la clave privada) la SubCA deberá comprobar que la información utilizada para verificar la identidad y el resto de datos del suscriptor y del poseedor de la clave, siguen siendo válidos.

La SubCA realiza renovaciones de certificados emitiendo siempre nuevas claves, por lo tanto, el proceso es similar al que se emplea cuando se realiza una emisión inicial.

En el caso de renovación los certificados cualificados o reconocidos para firma electrónica no se necesita presencia física, ya que se aplica la Ley 59/2003 que permite hasta un periodo de 5 años desde el último registro presencial. Una vez superado este plazo el suscriptor deberá realizar un proceso de emisión presencial. Si en el momento de la emisión del certificado no han trascurrido más de 5 años, la SubCA entiende que no es necesaria la presencia física del titular, independientemente de la duración de la caducidad del certificado emitido.

La SubCA realiza cuatro avisos (30 días, 15 días, 7 días, 1 día) vía email al suscriptor notificando que el certificado va a caducar, sugiriendo la realización del proceso de renovación. Si el certificado activo a renovar caduca antes de realizar la renovación, se deberá realizar un proceso de emisión nuevo.

El proceso de renovación se inicia en la página Web de la SubCA, indicada en el apartado 1.3. Para iniciar el proceso se necesita disponer del certificado activo a renovar.

Una vez identificado en el sistema de renovación, el sistema presenta al suscriptor los datos del certificado antiguo y pide la confirmación de dichos datos. El suscriptor puede modificar solo el email asignado al certificado. Si existen otros datos incorporados en el certificado que han cambiado, el certificado debe revocarse y proceder a realizar una emisión nueva.

Confirmados los datos, el sistema procede a realizar el cobro de los servicios de renovación si estos son pertinentes.

La petición se incorpora al aplicativo de RA donde el operador una vez revisados los datos y el pago, procede a pedir la emisión del certificado a la SubCA.

La SubCA emite un nuevo certificado tomando como inicio de validez la finalización del certificado a renovar.

3.3 Reemisión después de una revocación

La revocación implica la invalidez del certificado y, por tanto, no se podrá realizar la renovación automatizada. El solicitante deberá iniciar un proceso de emisión nueva.

En algunos casos la revocación se produce como consecuencia de un proceso de sustitución del certificado por error en su emisión. Siempre que refleje la situación actual, se reutilizara la documentación soporte entregada para la emisión del certificado sustituido y se eliminaría la personación física, si esta fuera requerida por la naturaleza del certificado.

La SubCA actualizará el número de años desde la última personación física al estado que tuviera el certificado a sustituir de la misma forma que si este proceso hubiera sido consecuencia de una renovación.

3.4 Solicitud de revocación

La forma de realizar las solicitudes de revocación se establece en el apartado siguiente.

3.5 Renovación de certificados sin renovación de claves

Bajo esta CPS no se renuevan certificados utilizando la misma clave.

3.6 Renovación de certificados con renovación de claves

Ver 3.2, 3.3

3.7 Modificación de certificados

Bajo esta CPS, la modificación de certificados implica la emisión o renovación de este. En la renovación del certificado se permite el cambio en el email.

4 REQUERIMIENTOS OPERACIONALES

Citise cuenta con el procedimiento AR-PR-01 PROCEDIMIENTO EMISION DE CERTIFICADOS FIRMA DIGITAL en el cual a partir de la solicitud y registro inicial se detalla el proceso de gestión y emisión de los certificados.

4.1 Solicitud de certificados

Las solicitudes de los certificados se realizan mediante el acceso a los formularios de solicitud en la página web de la SubCA (ver apartado 1.3). En la página web se encuentran los formularios necesarios para realizar la petición para cada tipo de certificado emitido por la SubCA en diferentes formatos y los dispositivos de generación de firma, si estos fueran necesarios.

Se establecen también circuitos de solicitud mediante lotes. En este caso, se enviará por el solicitante a la AR un fichero estructurado según un diseño prefijado por la SubCA con los datos de los solicitantes. La AR procederá a la carga de dichas peticiones en el aplicativo de RA.

Cuando el solicitante genera las claves, la solicitud de certificados se realiza entregando una petición de emisión de certificado estandarizada tipo PKCS#11 o CSR junto con los datos adicionales de la petición.

Para cada tipo de certificado el suscriptor debe aceptar los términos y condiciones de uso entre el suscriptor, la autoridad de registro y la autoridad de certificación. Este proceso se realiza bien mediante la firma manuscrita de un contrato, bien mediante una aceptación de términos visualizados en una página Web antes de proceder a la creación y descarga del certificado.

Con objeto de incorporar la integración de aplicaciones de terceros con la plataforma de gestión de certificados (STATUS), existe una capa de Web Services (WS) que ofrecen los servicios de emisión, renovación y revocación de certificados. Las llamadas a estos WS están firmadas por un operador de registro autorizado, por lo que las operaciones se realizan directamente en la plataforma.

La AR se asegurará que la solicitud de certificado se haya completado correctamente, de forma previa a la emisión del certificado.

4.2 Procesamiento de la solicitud de certificación

Una vez haya tenido lugar una petición de certificado, la AR debe verificar la información proporcionada, conforme a la sección correspondiente de esta política.

Si la información no es correcta, la AR debe denegar la petición. En caso de que los datos se verifiquen correctamente la AR aprobará la emisión del certificado.

En caso de un certificado cualificado, la documentación justificativa de la aprobación de la solicitud se ha de conservar debidamente registrada y con garantías de seguridad e integridad durante el plazo de 15 años desde la expiración del certificado, incluso todo en caso de pérdida anticipada de vigencia por revocación.

4.3 Petición de certificación cruzada

La SubCA no tiene actualmente ningún proceso de certificación cruzada activo.

4.4 Emisión de certificados

En certificados cualificados o reconocidos el suscriptor o solicitante utiliza un formulario Web para rellenar su solicitud y la confirmación de los datos. En respuesta el aplicativo solicitará mediante un mensaje de correo electrónico al suscriptor la presencia física en las instalaciones de la AR o en un lugar acordado con la documentación correspondiente. Si la solicitud se realiza con un certificado reconocido admitido por la SubCA no será necesaria la presencia física.

El operador de RA identificará físicamente al solicitante, mediante la aportación de documento identificativo válido, revisará la documentación aportada por el solicitante para la emisión del certificado y comprobará el pago de los servicios si fuera pertinente. Una vez realizadas estas operaciones el operador de RA validará con su firma electrónica la emisión del certificado.

Antes de comenzar una relación contractual, la SubCA, por sí misma o por medio de la AR, deberá informar al solicitante de los términos y condiciones relativos al uso del Certificado.

La operativa será diferente según el tipo de soporte del certificado:

- Certificados en HW: El usuario recibe en las dependencias de la AR el dispositivo de firma con los certificados y las claves generadas. Por otro lado, recibirá en la cuenta de correo asociada el código de acceso al dispositivo y el código de desbloqueo, así como una clave de revocación.

Como se ha comentado anteriormente, los certificados se pueden solicitar mediante lotes de peticiones. Estos lotes se entregan a la AR por el solicitante en un fichero estructurado que posteriormente se introduce en la plataforma de gestión de certificados.

El operador de RA posteriormente a la recopilación de la documentación y la comprobación de la identidad procederá a realizar la validación de los certificados bien uno a uno o en bloques.

Una vez aprobada la petición por el operador de RA, se le hará llegar al Firmante/Suscriptor un PIN necesario para la instalación de las claves y el certificado.

El Firmante/Suscriptor necesitará también para el proceso de creación de las claves y el certificado, un código que estará impreso en el contrato firmado con la AR y la AC.

Si la clave es generada por el suscriptor, este entregará a la SubCA una petición estandarizada tipo PKCS#10 y la SubCA enviará al usuario un certificado en formato PKCS#7. Si es el caso, el suscriptor deberá entregar a la SubCA un informe de auditoría confirmando la generación de las claves en un entorno hardware antes de que la SubCA emita el certificado.

4.5 Aceptación de certificados

Una vez que el certificado ha sido entregado o descargado, el usuario dispone de siete días para comprobar que funciona correctamente y que los datos del mismo se corresponden con la realidad.

Si el certificado no se ha emitido correctamente debido a problemas técnicos o contiene datos erróneos, el certificado será revocado y uno nuevo emitido.

4.6 Suspensión y revocación de certificados

4.6.1 Aclaraciones previas

Se entenderá por revocación aquel cambio en el estado de un certificado motivado por la pérdida de validez de este en función de alguna circunstancia distinta a la de su caducidad.

La suspensión por su parte supone una revocación con causa de suspensión, esto es, se revoca un certificado temporalmente hasta que se decida si debe ser revocado definitivamente o activado.

La extinción de la vigencia de un certificado electrónico por causa de revocación o suspensión producirá efectos frente a terceros desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación (publicación de una lista de certificados revocados o consulta en servicio OCSP).

En general, las causas de suspensión de certificados serán las causas legalmente establecidas en la normativa vigente en materia de firma electrónica que resulte aplicable a la SubCA.

La SubCA mantiene los certificados revocados en la lista de revocación hasta el fin de su validez. Posteriormente, se eliminan de la lista de certificados revocados. Solo se eliminará de la Lista de revocación un certificado cuando se produzca alguna de las dos siguientes situaciones.

- Caducidad del certificado
- Certificado revocado por causa de suspensión que una vez revisado no se encuentran causas para su revocación definitiva.

4.6.2 Causas de revocación y documentos justificativos

Como norma general se procederá a la revocación de un certificado cuando existan:

- Circunstancias que afectan la información contenida en el certificado.
    - Modificación de alguno de los datos contenidos en el certificado.
    - Descubrimiento que alguno de los datos aportados en la solicitud de certificado es incorrecto, así como la alteración o modificación de las circunstancias verificadas para la expedición del certificado.
    - Descubrimiento que alguno de los datos contenidos en el certificado es incorrecto.
- Circunstancias que afectan la seguridad de la clave o del certificado.
    - Compromiso de la clave privada o de la infraestructura o sistemas de la Entidad de Certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de este incidente.
    - Infracción, por la Entidad de Certificación, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta DPC.
    - Pérdida o compromiso, o sospecha de compromiso, de la seguridad de la clave o del certificado del suscriptor o del responsable de certificado.
    - Acceso o utilización no autorizada, por un tercero, de la clave privada del suscriptor o del responsable de certificado.
    - El uso irregular del certificado por el suscriptor o del responsable de certificado, o falta de diligencia en la custodia de la clave privada.

- Circunstancias que afectan la seguridad del dispositivo criptográfico.
    - Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
    - Pérdida o inutilización por daños del dispositivo criptográfico.
    - Acceso no autorizado, por un tercero, a los datos de activación del suscriptor o del responsable de certificado.
- Circunstancias que afectan al suscriptor o responsable del certificado.
    - Finalización de la relación entre Entidad de Certificación y suscriptor o responsable del certificado.
    - Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al suscriptor o responsable del certificado.
    - Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de éste.
    - Infracción por el suscriptor o responsable del certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento jurídico correspondiente o en esta Declaración de Prácticas de Certificación.
    - La incapacidad sobrevenida o la muerte del suscriptor o responsable del certificado.
    - La extinción de la persona jurídica suscriptora del certificado, así como la finalidad de la autorización del suscriptor al responsable del certificado o la finalización de la relación entre suscriptor y responsable del certificado.
    - Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en esta DPC.
- Otras circunstancias.
    - La suspensión del certificado digital por un periodo superior al establecido en esta DPC.
    - La finalización del servicio de la Entidad de Certificación, de acuerdo con lo establecido en la sección en esta DPC.
    - Por Orden Judicial o de entidad administrativa competente, según Ley 527 de 1999.

Para justificar la necesidad de revocación que se alega se deberán presentar ante la AR o la SubCA los documentos correspondientes, en función de la causa que motiva la solicitud.

Si la entidad a la que se dirige la solicitud de revocación no dispone de toda la información necesaria para determinar la revocación de un certificado, pero tiene indicios de su compromiso puede decidir la suspensión.

En este caso se considerará que las actuaciones realizadas durante el período de suspensión no son válidas, siempre que el certificado finalmente sea revocado. Serán válidas, en cambio, si se levanta la suspensión y el certificado vuelve a pasar a la situación de válido.

El instrumento jurídico que vincula a la Entidad de Certificación con el subscriptor establecerá que el suscriptor deberá solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias indicadas anteriormente.

Los suscriptores disponen de los códigos de revocación que pueden usar en los servicios de revocación vía Web o llamando al área de soporte.

4.6.3 Quién puede solicitar la revocación

La revocación de un certificado podrá solicitarse por:

- El Firmante/Suscriptor
- El Solicitante responsable
- La Entidad (a través de un representante de la misma)
- La AR ó la AC tras haber autenticado la orden de revocación.

Cualquiera establecido en las políticas de certificación concretas.

4.6.4 Procedimiento de solicitud de revocación

Todas las solicitudes deberán realizarse:

- A través del Servicio de Revocación on line, accediendo al servicio de revocación localizado en la página de la Web de la SubCA (ver apartado 1.3) e introduciendo el PIN de revocación. Este medio de revocación es accesible sólo para el Firmante/Suscriptor.
- A través de la personación física en la AR en horario de atención al público del Firmante/Suscriptor o Solicitante y mostrando documento identificativo.
- Enviando a la SubCA un documento firmado por un representante suficiente de la Entidad solicitando la revocación del certificado.

La SubCA mantiene en su página Web toda la información relativa a los procesos de revocación de los certificados.

Cuando se produce una suspensión, la SubCA tendrá una semana para decidir el estado definitivo del certificado: (revocado o activo). En caso de no tener en este plazo toda la información necesaria para la verificación y validación de la solicitud de revocación, la SubCA revocará definitivamente el certificado.

En el caso de producirse una suspensión del certificado, se enviará un comunicado mediante email al Firmante/Suscriptor comunicando la fecha de suspensión y la causa de la misma.

La AR recibirá un correo del sistema informándole que se ha producido una suspensión del certificado.

Si finalmente la suspensión no da lugar a la revocación definitiva y el certificado tiene que ser de nuevo activado, el Firmante/Suscriptor recibirá un correo indicando el nuevo estado del certificado.

Tanto el servicio de gestión de las revocaciones como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencias ó el plan de continuidad de negocio de la SubCA. Estos servicios estarán disponibles las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de la SubCA, esta realizará todos los esfuerzos posibles para asegurar que estos servicios no se encuentren inaccesibles durante un periodo máximo de 24 horas.

4.6.5 Periodo de revocación

Para dar cumplimiento al art. 7º.7 del Decreto 333 de 2014, la SubCA cuenta con un mecanismo de ejecución inmediata para revocar los certificados digitales expedidos a los suscriptores, a petición de estos o cuando se tenga indicios de que ha ocurrido alguno de los eventos previstos en el artículo 37 de la Ley 527 de 1999 (ver apartado 4.6.2).

La revocación de un certificado se realiza de manera inmediata tras la verificación de la solicitud de revocación, transcurrido un plazo máximo de 24 horas entre la solicitud de la revocación y la revocación efectiva.

Los certificados que han sido revocados no son objeto de rehabilitación por parte de Citiseg.

4.6.6 Periodo de suspensión

No exite periodo de suspensión

4.6.7 Procedimiento para la solicitud de suspensión

La suspensión de un certificado es un estado excepcional que se produce al no poder verificar la identidad de la persona que realiza la solicitud de revocación. Por tanto, no es posible realizar una solicitud de suspensión.

4.6.8 Límites del periodo de suspensión

Un certificado se mantendrá en estado suspendido el menor tiempo posible. En cualquier caso, la decisión de revocar o no un certificado se adoptará en un periodo máximo de una semana.

Durante este tiempo el certificado permanece suspendido, mientras se decide si volver a activar la eficacia del mismo ó revocarlo definitivamente basándose en la información obtenida hasta ese momento respecto a las causas que han provocado dicha suspensión.

La SubCA supervisará mediante un sistema de alertas de la plataforma de gestión de certificados que el periodo de suspensión marcado por esta DPC no se sobrepasa.

4.6.9 Frecuencia de emisión de CRLs

Las CRLs se emiten y publican de manera inmediata cuando se produce un cambio de estado en algún certificado (revocación o suspensión) o cada 24 horas si no se ha procucido ninguna revocación o suspensión.

Adicionalmente, la SubCA notificará la revocación del certificado al suscriptor correspondiente en el plazo de 24 horas, según indica el art. 15.16 del Decreto 333 de 2014.

La CRL de la subordinada se emite cuando se produzcan cambios en el estado del certificado o cada 12 meses.

4.6.10 Requisitos de comprobación de CRL

Los terceros que confían deben comprobar el estado de los certificados en los cuales va a confiar, debiendo comprobar en todo caso la última CRL emitida, que podrá descargarse desde la página Web de la SubCA (ver apartado 1.3).

4.6.11 Disponibilidad de comprobación on-line de la revocación

LA SubCA proporciona un servicio on-line de comprobación de revocaciones vía HTTP en su página web (ver apartado 1.3) y también mediante consultas OCSP en http://ocsp.citiseg.com.co.

Las direcciones de acceso a estos servicios vienen referenciadas en el certificado digital. Para las CRL y ARL en la extensión puntos de distribución de CRL “CRL distribution Point” y la dirección de OCSP en la extensión Acceso a la Información de la Autoridad “Authority Information Access”.

En los certificados puede aparecer más de una dirección de acceso a las CRL para garantizar su disponibilidad.

Los datos técnicos de acceso al servicio OCSP así como los certificados de validación de las respuestas OCSP se encuentran publicados en la Web de la SubCA (ver apartado 1.3).

Estos servicios estarán disponibles las 24 horas del día los 7 días de la semana.

La SubCA realizará todos los esfuerzos necesarios para que el servicio nunca se encuentre inaccesible de forma continua más de 24 horas, siendo este un servicio crítico en las actividades de la SubCA y por lo tanto tratado de forma adecuada en el Plan de contingencias y de continuidad de negocio.

En caso necesario, la SubCA suministrará información a los verificadores sobre el funcionamiento del servicio de información de estado de certificados.

4.6.12 Requisitos de la comprobación on-line de la revocación

Para realizar la comprobación de una revocación el Tercero que confía deberá conocer el e-mail asociado al certificado que se desea consultar si se realiza mediante acceso Web y, el número de serie y la autoridad de certificación si se realiza mediante otros mecanismos.

Los requisitos para acceder al servicio OCSP y los certificados necesarios para su validación estarán actualizados en la página web de la SubCA (ver apartado 1.3) y los requisitos técnicos serán los dispuestos por la RFC 6960.

4.6.13 Otras formas de divulgación de información de revocación disponibles

Los mecanismos que la SubCA pone a disposición de los usuarios, estarán publicados en su página Web (ver apartado 1.3).

4.6.14 Requisitos de comprobación para otras formas de divulgación de información de revocación

No estipulado.

4.6.15 Requisitos especiales de revocación por compromiso de las claves

No estipulado.

4.7 Procedimientos de Control de Seguridad

La SubCA está sujeta a las validaciones anuales de AC Camerfirma SA para garantizar una correcta gestión de la seguridad en los sistemas de información necesarios para la prestación del servicio como CA.

4.7.1 Tipos de eventos registrados

La SubCA registra y guarda los LOG´s de todos los eventos relativos al sistema de seguridad de la AC. Se registrarán los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los LOGs.

- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los dispositivos que contienen las claves y datos de activación

4.7.2 Frecuencia de procesado de Logs

La SubCA revisa sus LOGs cuando se produce una alerta del sistema motivada por la existencia de algún incidente, o al menos de forma periódica.

La SubCA mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.

Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

4.7.3 Periodos de retención para los LOGs de auditoría

La SubCA almacena la información de los LOGs al menos durante 5 años.

4.7.4 Protección de los LOGs de auditoría

Los logs de los sistemas son protegidos de su manipulación mediante la firma de los ficheros que los contienen y son almacenados en dispositivos ignífugos.

Se protege su disponibilidad mediante el almacén en instalaciones externas al centro donde se ubica la SubCA.

El acceso a los ficheros de Logs está reservado solo a las personas autorizadas (Auditor).

Los dispositivos son manejados en todo momento por personal autorizado.

Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de LOGs de auditoría.

4.7.5 Procedimientos de backup de los Logs de auditoría

La SubCA dispone de un procedimiento adecuado de backup de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

La SubCA tiene implementado un procedimiento de back up seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo.

Adicionalmente se mantiene copia en centro de custodia externo.

4.7.6 Sistema de recogida de información de auditoría

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo, la red y por el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado, todo ello compone el sistema de acumulación de registros de auditoría.

4.7.7 Notificar a la parte que causó el evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no será necesario enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

Se podrá comunicar si el resultado de su acción ha tenido éxito o no, pero no que se ha auditado la acción.

4.7.8 Análisis de vulnerabilidades

La SubCA realizará una revisión de los riesgos de seguridad del sistema. Esta revisión cubrirá todos los riesgos que puedan afectar a la emisión de los certificados y se realizará anualmente.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

4.8 Archivos de registro o Log

4.8.1 Tipo de archivos registrados

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por la SubCA o por las AR's:

- Todos los datos de auditoría de sistema.
- Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y los datos relativos a su identificación y su ubicación.
- Solicitudes de emisión y revocación de certificados.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación

LA SubCA es responsable del correcto archivo de todo este material.

4.8.2 Periodo de retención para el archivo

Los certificados, los contratos con los Firmantes/Suscriptores y cualquier información relativa a la identificación y autenticación del Firmante/Suscriptor serán conservados durante al menos 15 años.

4.8.3 Protección del archivo

La SubCA asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas.

4.8.4 Procedimientos de backup del archivo

La SubCA realiza copias de respaldo diarias y semanales de todos sus documentos electrónicos para casos de recuperación de datos.

La SubCA dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

4.8.5 Requerimientos para el sellado de tiempo (estampado cronológico) de los registros

Los registros están fechados con una fuente fiable vía NTP desde el ROA, GPS y sistemas de sincronización vía Radio.

4.8.6 Sistema de recogida de información de auditoría

La SubCA dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

4.8.7 Procedimientos para obtener y verificar la información archivada

La SubCA dispone de procesos para verificar que la información archivada es correcta y accesible.

Asimismo, la SubCA dispone métodos adecuados para limitar la obtención de la información sólo a las personas autorizadas.

4.9 Cambio de clave

Antes de que el uso de la clave privada de la SubCA caduque se realizará un cambio de claves. La vieja SubCA y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por la SubCA vieja. Se generará una nueva SubCA con una clave privada nueva y un nuevo DN.

- El cambio de claves del suscriptor es realizado mediante la realización de un nuevo proceso de emisión (ver apartado Identificación del Solicitante:
  Se exige la presencia física del Firmante/Suscriptor cuando éste es también Solicitante, o de un representante del Solicitante cuando éste es una entidad jurídica, así como la presentación de un documento oficial que acredite de forma fehaciente su identidad (NIT, Cédula de Ciudadanía, tarjeta de identidad, pasaporte o cualquier otro documento admitido en derecho), siempre que contenga al menos la siguiente información:

  a) Nombre y apellidos de la persona
  b) Lugar y fecha de nacimiento
  c) Número de identidad reconocido legalmente
  d) Otros atributos de la persona que deban constar en el certificado

  La presencia física no es obligatoria en los casos previstos en la legislación vigente

- Identificación de la entidad:
  Con carácter previo a la emisión y entrega de un certificado de organización o sello electrónico es necesario autenticar los datos relativos a la constitución y la personalidad jurídica de la entidad. Se exige la identificación de la entidad, por lo que la AR requerirá la documentación pertinente en función del tipo de entidad. Esta información varía dependiendo del tipo de entidad y está indicada en los manuales operativos de la AR y en la

Web de la SubCA. En general serán datos relativos a la constitución y la personalidad jurídica de la entidad, y a la extensión y vigencia de las facultades o poderes de representación del solicitante, mediante los documentos públicos que los acrediten de forma fehaciente y la consulta al pertinente registro público, cuando se trate de datos que deben figurar en ella. Se comprobará:

a) Nombre legal completo de la organización
b) Estado legal de la organización
c) Número de registro tributario
d) Datos de identificación registral

Identificación del dominio:
Para los certificados SSL pretenden identifican a una entidad a cuyo nombre ha sido registrado un dominio. La RA utilizara los medios oportunos para asegurarse de la existencia de la organización y el control del dominio. Entre estos medios se cuentan bases registrales externas. El identificativo fiscal de la organización se incorporará en el contenido del certificado

- Identificación de la vinculación:

Para los **Certificados de representante de empresa** se exige la documentación sobre la capacidad de **representación** del Firmante/Suscriptor respecto de la otra persona, por medio de la entrega de las escrituras notariales que demuestran sus poderes o facultades de representación. Se presentará un certificado expedido por el registro público correspondiente con menos de 10 días de antigüedad. La AR puede disponer también de medios telemáticos para la consulta en línea del estado y nivel de representación del solicitante.

Para los **Certificados de Pertenencia a Empresa** la AR debe obtener una acreditación documental de la vinculación de la persona física con la organización, mediante cualquier medio admitido en derecho. En general, será necesaria la presentación de una autorización firmada por un representante legal o apoderado general de la entidad.

En los **Certificados de Persona Jurídica**, en los que el Firmante/ Suscriptor y el Solicitante son distintos, deberá demostrar documentalmente que el Solicitante tiene poderes suficientes para realizar dicha solicitud de certificado por cuenta del Firmante/ Suscriptor, mediante la presentación de un certificado del registro público correspondiente no superior a 10 días o mediante consulta en línea realizada por la propia AR a los datos del registro público correspondiente.
En los **Certificados de Función Pública** no se exige la documentación acreditativa de la existencia de la administración pública. Se exige la documentación de identidad de la persona que actúa como responsable, en nombre de dicha Administración Pública, organismo o entidad de derecho público. El Solicitante / responsable se identificará ante la AR con un documento que acredite de forma fehaciente su identidad y un documento acreditativo de su pertenencia como empleado en la Administración Pública, organismo o entidad de derecho público donde consten además los datos identificativos de ésta.

En los **Certificados de Firma de Código** se identifican a una entidad, por lo que se comprobará la identidad de esta y de los solicitantes mediante el acceso a bases de datos externas.

La información de identificación de suscriptores de certificados personales, así como de poseedores de claves de certificados de organización, se debe realizar contrastando la

información de la solicitud con la documentación aportada, electrónicamente o en soporte físico.

Renovación de la clave

4.10 Recuperación en caso de compromiso de la clave o desastre

La SubCA y el proveedor de servicios de certificación han desarrollado un Plan de contingencias para recuperar los sistemas críticos, y si fuera necesario un centro de datos alternativo.

El caso de compromiso de la clave raíz debe tomarse como un caso separado en el proceso de contingencia y continuidad de negocio. Esta incidencia afecta, en caso de sustitución de las claves, a los reconocimientos por diferentes aplicativos y servicios privados y públicos. Una recuperación de la efectividad de las claves en términos de negocio dependerá principalmente de la duración de estos procesos. El documento de contingencia y continuidad de negocio tratara los términos puramente operativos para que las nuevas claves estén disponibles, no así su reconocimiento por terceros.

Cualquier fallo en la consecución de las metas marcadas por este Plan de contingencias, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la SubCA para implementar dichos procesos

4.10.1 Compromiso de la clave

El Plan de contingencias de la SubCA trata el compromiso de la clave privada de la SubCA como una situación de desastre

En caso de compromiso de una clave raíz:

- Se informará a todos los Firmantes/Suscriptores, Tercero que confía y otras AC's con los cuales tenga acuerdos u otro tipo de relación del compromiso.
- Se indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.

4.10.2 Instalación de seguridad después de un desastre natural u otro tipo de desastre

La SubCA restablecerá los servicios críticos (revocación y publicación de revocados) de acuerdo con el plan de contingencias y continuidad de negocio existente.

La SubCA dispondrá de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación, como se describe en el plan de continuidad de negocio.

4.11 Cese de la AC

En el caso de que la AC decida cesar sus actividades acreditadas ante la ONAC, garantizará la continuidad del servicio de certificación digital a quienes ya lo hayan contratado sin costos adicionales a los servicios ya cancelados.

En todo caso, Citiseg informará a los entes oportunos de la cesación de los servicios, a ONAC y a la Superintendencia de Industria y Comercio, con una antelación de 30 días, según lo establecido en el artículo 17 decreto 333 de 2014.

Citiseg informará a todos los suscriptores mediante dos avisos publicados en diarios o medios de amplia circulación nacional, con un intervalo de 15 días, sobre:

La terminación de su actividad o actividades y la fecha precisa de cesación.

Las consecuencias jurídicas de la cesación respecto de los certificados expedidos.

La posibilidad de que un suscriptor obtenga el reembolso equivalente al valor del tiempo de vigencia restante del certificado.

La autorización emitida por la Superintendencia de Industria y Comercio para que Citiseg pueda cesar el servicio, y si es el caso, el operador de la CRL responsable de la publicación de los certificados emitidos por Citiseg, hasta cuando expire el último de ellos.

En todo caso los suscriptores podrán solicitar la revocación y el reembolso equivalente al valor del tiempo de vigencia restante del certificado, si lo solicitan dentro de los dos meses siguientes a la segunda publicación.

La terminación de la actividad o actividades se hará en la forma y siguiendo el cronograma presentado por Citiseg al ente de vigilancia y control y que éste apruebe.

En cualquier caso, Citiseg dispone de:

Un plan de continuidad del servicio.

Un plan que garantiza la continuidad en alta disponibilidad de la publicación en los repositorios (CRL) propios.

Citiseg garantiza la adecuada destrucción de la llave privada de la entidad en caso de ser necesario mediante la inicialización de los HSM y destrucción del Security World.

Los planes anteriores son mantenidos junto con la documentación relevante y pruebas anuales.

4.12 Acceso al servicio de sellado de tiempo

El método de comunicación entre las entidades y el servicio de sellado de tiempo se realizará mediante protocolo HTTPS con autentificación en cliente, con el fin de poder validar las peticiones realizadas.

5 CONTROLES DE SEGURIDAD FÍSICA, PROCEDIMENTAL Y DE PERSONAL

La SubCA está sujeta a las validaciones anuales de AC Camerfirma SA para garantizar una correcta gestión de la seguridad en los sistemas de información necesarios para la prestación del servicio como CA.

5.1 Controles de Seguridad física

La SubCA tiene establecidos controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones.

La política de seguridad física y ambiental aplicable a los servicios de generación certificados ofrece protección frente:

- Accesos físico no autorizados
- Desastres naturales
- Incendios
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura
- Inundaciones
- Robo
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del Prestador de Servicios de Certificación

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año, con asistencia en las 24 horas siguientes al aviso.

5.1.1 Ubicación y construcción

Las instalaciones de la SubCA están construidas con materiales que garantizan la protección frente a ataques por fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

En concreto, la sala donde se realizan las operaciones criptográficas es una caja de faraday con protección a radiaciones externas, doble suelo, detección y extinción de incendios, sistemas anti-humedad, doble sistema de refrigeración y sistema doble de suministro eléctrico.

5.1.2 Acceso físico

El acceso físico a las dependencias de la SubCA donde se llevan a cabo los procesos de cifrado está limitado y protegido mediante una combinación de medidas físicas y procedimentales.

Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Las instalaciones cuentan con detectores de presencia en todos los puntos vulnerables, así como Sistemas de alarma para detección de intrusismo con aviso por canales alternativos.

El acceso a las salas se realiza con lectores de tarjeta de identificación y gestionado por un sistema informático que mantiene un log de entradas y salidas automático.

El acceso a los elementos más críticos del sistema se realiza a través de tres zonas previas de paso con acceso limitado incrementalmente.

El acceso a los sistemas de certificación está protegido con 4 niveles de acceso. Edificio, Oficinas, CPD y Sala criptográfica.

5.1.3 Alimentación eléctrica y aire acondicionado

Las instalaciones de la SubCA disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos más un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado duplicado.

5.1.4 Exposición al agua

Las instalaciones de la SubCA están ubicadas en una zona de bajo riesgo de inundación. Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

5.1.5 Protección y prevención de incendios

Las salas donde se albergan los equipos informáticos disponen de sistemas automáticos de detección y extinción de incendios.

5.1.6 Sistemas de almacenamiento

Cada medio de almacenamiento extraible (cintas, cartuchos, disquetes, etc.) permanece solamente al alcance de personal autorizado.

La información con clasificación Confidencial, independientemente del dispositivo de almacenamiento se guarda en armarios ignífugos o bajo llave permanentemente, requiriéndose autorización expresa para su retirada.

5.1.7 Eliminación de residuos

Cuando haya dejado de ser útil, la información sensible es destruida en la forma más adecuada al soporte que la contenga.

- Impresos y papel: mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.
- Medios de almacenamiento: antes de ser desechados o reutilizados deben ser procesados para su borrado físicamente destruidos o hacer ilegible la información contenida.

5.1.8 Backup Externo

La SubCA utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos, el cual es independiente del centro operacional.

Se requiere autorización expresa para el acceso, depósito o retirada de dispositivos.

5.2 Controles procedimentales

5.2.1 Roles de confianza

Los roles de confianza se describen acontinuación, garantizando una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación, y con una concesión de mínimo privilegio, cuando sea posible.

Para determinar la sensibilidad de la función, se tendrán en cuenta los siguientes elementos:

- Deberes asociados a la función.
- Nivel de acceso.
- Monitorización de la función.
- Formación y concienciación.
- Habilidades requeridas.

Auditor Interno:

Responsable del cumplimiento de los procedimientos operativos. Es una persona externa al departamento de Sistemas de Información.

Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.

Administrador de Sistemas:

Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación

Administrador de AC.

Responsable de las acciones a ejecutar con el material criptográfico, o con la realización de alguna función que implique la activación de las claves privadas de las autoridades de certificación descritas en este documento, o de cualquiera de sus elementos.

Operador de AC.

Responsable necesario conjuntamente con el Administrador de AC de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de backup y mantenimiento de la AC.

Administrador de AR:

Persona responsable de aprobar las peticiones de certificación realizadas por el suscriptor.

Responsable de Seguridad:

Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de la SubCA.

5.2.2 Número de personas requeridas por tarea

La SubCA garantiza que al menos dos personas realizarán las tareas descritas en esta DPC, principalmente en la manipulación del dispositivo de almacenamiento de las claves de SubCA.

5.2.3 Identificación y autentificación para cada rol

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

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

El acceso a recursos se realiza dependiendo del activo mediante tarjetas criptográficas y códigos de activación.

5.2.4 Arranque y parada del sistema de gestión PKI.

El sistema de PKI se compone de los siguientes módulos:

Módulo de Gestión de AR, para lo cual se activarán o desactivarán los servicios del gestor de páginas especifico.

Modulo de gestión de solicitudes, para lo cual se activará o desactivará los servicios del gestor de páginas específico.

Módulo de gestión de claves, ubicado en el equipo HSM. Se activa o desactiva mediante encendido físico.

Modulo de BBDD, Gestión centralizada de los certificados y CRL gestionados, OCSP y TSA. Arranque y parada del servicio especifico del Gestor de BBDD.

Modulo OCSP. Servidor de respuestas de estado de los certificados en línea. Arranque y parada del servicio de sistema encargado de esta tarea.

Modulo TSA. Servidor de sellos de tiempos. Arranque y parada del servicio

El proceso de apagado de módulos seguiría la secuencia:

- Módulo de solicitud
- Módulo de AR
- Módulo OCSP
- Módulo TSA
- Módulo BBDD
- Módulo gestión de claves.

Se realizará el encendido en proceso inverso.

5.3 Controles de seguridad del personal

5.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación

Todo el personal que realiza tareas clasificadas o confiables, debe llevar al menos un año trabajando en su puesto y tener contrato laboral fijo.

Todo el personal esta cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

El personal en tareas clasificadas o confiables se encontrará libre de intereses personales que entren en conflicto con el desarrollo de la función que tenga encomendada.

LA SubCA se asegura de que el personal de registro o Administradores de RA es confiable para realizar las tareas de registro.

Los Administradores de RA habrán realizado un curso de preparación para la realización de las tareas de validación de las peticiones.

En general, la SubCA retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

5.3.2 Procedimientos de comprobación de antecedentes

La SubCA dentro de sus procedimientos de RRHH realiza las investigaciones pertinentes antes de la contratación de cualquier persona.

La SubCA nunca asigna tareas confiables a personal con menos de una antigüedad de un año.

5.3.3 Requerimientos de formación

El personal encargado de tareas de confianza ha sido formado de acuerdo a estas DPC.

5.3.4 Requerimientos y frecuencia de la actualización de la formación

La SubCA realiza los cursos de actualización necesarios para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas.

5.3.5 Frecuencia y secuencia de rotación de tareas

No estipulado.

5.3.6 Sanciones por acciones no autorizadas

La SubCA dispone de un régimen sancionador interno, descrito en su política de RRHH, para su aplicación cuando un empleado realice acciones no autorizadas pudiéndose llegar a su cese u otras acciones legales según sea el caso.

5.3.7 Requerimientos de contratación de personal

Los empleados contratados para realizar tareas confiables firman previamente las cláusulas de confidencialidad y de requerimientos operacionales de la SubCA. Cualquier acción que comprometa la seguridad de los procesos aceptados podría una vez evaluada dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la DPC, serán aplicados y

cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, la entidad de certificación será responsable en todo caso de la efectiva ejecución.

Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto de la SubCA.

5.3.8 Documentación proporcionada al personal

La SubCA pone a disposición de todo el personal la documentación donde se detallen las funciones encomendadas, en particular la normativa de seguridad y la DPC.

Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

6 CONTROLES DE SEGURIDAD TÉCNICA

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

Para la generación de la clave de la SubCA y AC Camerfirma SA se utilizan dispositivos criptográficos HSM que cumplen los requerimientos que se detallan en el FIPS 140-1, en su nivel 3. Los datos del equipo son: nShield PCI e+ 500 F3 de nCipher. Se disponen de otros HSM con la misma certificación para la emisión de respuestas OCSP.

Las claves correspondientes a la SubCA y Ac CAmerfirma SA fueron creadas en un entorno seguro mediante mecanismos software y bajo control dual y auditados por personal independiente que garantiza la integridad y seguridad del proceso.

Las claves se generaron en respectivas ceremonias de las que hay documentación detallada.

GLOBAL CHAMBERSIGN ROOT – 2016	**4.096**	**24 Años**
AC CAMERFIRMA COLOMBIA – 2016	**4.096**	24 años
AC CITISEG - 2016	**4.096**	24 años
Certificado de Persona Jurídica	2.048	1 año
Certificado de Persona Natural	2.048	1 año
Certificado de Pertenencia a Empresa	2.048	1 año
Certificado de Representante de Empresa	2.048	1 año
Certificado de Profesional Titulado	2.048	1 año
Certificado de Función Pública	2.048	1 año
Certificado de Comunidad Académica	2.048	1 año
Chambers of Commerce Root – 2008	**4.096**	**30 Años**
Camerfirma Corporate Server II – 2015	4096	22 años
Certificado SSL	2048	<3 años
Certificado de Sello electrónico de entidad	2048	<4 años
Camerfirma Codesign II – 2014	4096	23 años
Certificados Firma de código	2048	<4 años

Camerfirma TSA II – 2014	4096	23 años
ESTAMPADO CRONOLÓGICO	2048	6 años

6.1.2 Generación del par de claves del suscriptor

Las claves del Firmante/Suscriptor pueden ser creadas por el mismo mediante dispositivos hardware autorizados por la SubCA. Las claves son creadas usando el algoritmo de clave pública RSA. Las claves tienen una longitud mínima de 2048 bits.

En el caso de que el suscriptor genere las claves en un dispositivo criptográfico propio, la SubCA exigirá un informe técnico de auditoría que valorará antes de emitir un certificado con las claves generadas en un dispositivo hardware.

La SubCA dispone de controles para garantizar que las claves generadas se ajustan a lo descrito en su correspondiente Política de Certificación, no pudiendo emitir el certificado en el caso de que no se ajusten.

6.1.3 Entrega de la clave publica al emisor del certificado

El envío de la clave pública a la SubCA para la generación del certificado cuando el circuito así lo requiera, se realiza mediante un formato estándar, preferiblemente en formato PKCS#10 o X509 autoafirmado.

6.1.4 Entrega de la clave pública de la AC a los usuarios

El certificado de la SubCA y su fingerprint (huella digital) estarán a disposición de los usuarios en la página Web de laSubCA (ver apartado 1.3).

6.1.5 Tamaño y periodo de validez de las claves del emisor

Ver apartado 1.2.1 Jerarquía.

6.1.6 Tamaño y periodo de validez de las claves del suscriptor

Las claves privadas del Firmante/Suscriptor están basadas en el algoritmo RSA con una longitud mínima de 2048 bits. El periodo de uso de la clave pública y privada varía en función del tipo de certificado y se describen en cada Política de Certificación.

6.1.7 Parámetros de generación de la clave pública

La clave pública de la AC Raíz, de las SubCA y de los certificados de los suscriptores está codificada de acuerdo con RFC 5280 y PKCS#1. El algoritmo de generación de claves es el RSA.

6.1.8 Comprobación de la calidad de los parámetros

Los sistemas de emisión de certificados disponen de medidas de control que verifican los parámetros de las claves de modo que se ajusten a lo dispuesto en las Políticas de Certificación correspondientes.

6.1.9 Hardware de generación de claves

Las claves de los Firmantes/Suscriptores pueden ser generadas por ellos mismos en un dispositivo autorizado por la SubCA. Ver 6.1.2.

Las claves de la SubCA han sido generadas en un módulo criptográfico HSM acreditado FIPS-140-1 nivel 3.

6.1.10 Fines de uso de la clave

En el siguiente grafico se describen los usos de la clave para los distintos certificados emitidos. La solución adoptada para diferenciar rntre usos es la siguiente:

- Certificados para autenticación bit DS (puede combinarse con otros usos)
- Certificados para firma electrónica bit DS + NR (puede combinarse con otros usos)
- Certificados exclusivos de firma reconocida bit NR (NO puede combinarse con otros usos). Actualmente la SubCA no emite certificados exclusivos de firma electrónica reconocida pero este modelo marca las pautas a seguir para cuando sea incorporada.

AC:	DS	NR	KE	DE	KA	KCS	CRL	EO	DO
GLOBAL CHAMBERSIGN ROOT – 2016						✔	✔		
SubCA						✔	✔		
Certificado Persona Jurídica	✔	✔	✔						
Cert. Persona Natural	✔	✔	✔						
Cert. Pertenencia a Empresa	✔	✔	✔						
Cert. Representante Empresa	✔	✔	✔						
Cert. Profesional Titulado	✔	✔	✔						
Cert. Función Pública	✔	✔	✔						
Cert. Comunidad Académica	✔	✔	✔						
Chambers of Commerce Root - 2008						✔	✔		
Camerfirma Corporate Server II – 2015						✔	✔		
Certificado SSL	✔		✔						
Certificado de Sello electrónico de entidad	✔	✔	✔	✔ *	✔				
Camerfirma Codesign II – 2014						✔	✔		
Certificados Firma de código	✔	✔							
Camerfirma TSA II – 2014						✔	✔		
ESTAMPADO CRONOLÓGICO	✔	✔							

DS: Firma Digital
NR: No Repudio, "ContentCommitment"
KE: Cifrado de Clave
DE: Cifrado de Datos
KA: Acuerdo de clave
KCS: Firma de certificados
CRL: Firma de CRL
EO: Solo Cifrado
DO: Solo descifrado
(*) A pesar de que es posible técnicamente [SubCA] no se responsabiliza de su uso para estos fines

6.2 Protección de la clave privada

6.2.1 Clave privada de la SubCA

La clave privada de firma de la SubCA así como de AC Camerfirma SA es mantenida y usada en un dispositivo criptográfico seguro que cumple los requerimientos FIPS 140-1 nivel 3. Para las claves de las autoridades de OCSP y TSA se utiliza otro equipo HSM certificado FIPS 140-1 nivel 3.

Cuando la clave privada de la SubCA está fuera del dispositivo (backup) esta se mantiene cifrada y partida en diferentes dispositivos siendo necesario un número k de n para su recuperación siendo k un mínimo de 2. Este backup de la clave privada de la AC, es almacenada de forma segura y recuperada sólo por el personal autorizado según los roles de confianza, usando, al menos un control dual en un medio físico seguro.

6.2.2 Clave privada del suscriptor

La clave privada del suscriptor se puede almacenar en un dispositivo hardware.

Respecto a los dispositivos criptográficos con certificados para firma electrónica, aptas como dispositivos seguros de creación de firma, cumplen el nivel de seguridad CC EAL4+ y soportan los estándares PKCS#11 y CSP.

La SubCA utiliza los medios criptográficos permitidos en su solicitud de registro y que garantizan la creación de la firma electrónica.

La información respecto al tipo de creación y custodia de claves esta incorporada en el propio certificado digital permitiendo a Terceros que confían actuar en consecuencia.

La SubCA publicará los dispositivos permitidos para la generación y custodia de las claves en su página Web, indicada en el apartado 1.3.

6.3 Estándares para los módulos criptográficos

Ver apartado anterior.

6.3.1 Control multipersonal (n de entre m) de la clave privada

Se requiere un control multi-persona para la activación de la clave privada de la SubCA. En el caso de esta DPC, en concreto existe una política de 2 de 4 personas para la activación de las claves.

6.3.2 Custodia de la clave privada

La SubCA no almacena ni copia claves privadas de los suscriptores cuando estas son generadas por la SubCA. Para certificados en soporte hardware es el usuario quien genera y custodia la clave privada en la tarjeta criptográfica entregada por la SubCA.

6.3.3 Copia de seguridad de la clave privada

La SubCA realiza copias de backup de las claves privadas de la SubCA que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de las mismas. Del mismo modo, AC CAmerfirma SA realiza estas copias de seguridad. Tanto la generación de la copia como la recuperación de esta necesitan al menos de la participación de dos personas.

Estos ficheros de recuperación se almacenan en armarios ignífugos y en un centro de custodia externo. La SubCA y AC Camerfirma SA guardan actas de los procesos de gestión de las claves privadas de la SubCA y AC Camerfirma SA respectivamente.

6.3.4 Archivo de la clave privada

Las claves privadas de la SubCA así como de AC Camerfirma SA son archivadas por un periodo de al menos 10 años después de la emisión del último certificado. Se almacenarán en archivos ignífugos seguros y en un centro de custodia externo. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de la SubCA o de AC Camerfirma SA en el dispositivo criptográfico inicial. La SubCA y AC Camerfirma SA guardan actas de los procesos de gestión de las claves privadas de AC.

El suscriptor podrá almacenar las claves durante el tiempo que estime oportuno.

En el caso de que el suscriptor haya cifrado información con su certificado será responsabilidad suya mantener el acceso a dicha información a través de la clave privada asociada al certificado con el que cifro la información.

6.3.5 Introducción de la clave privada en el módulo criptográfico

Las claves de la SubCA y AC Camerfirma SA se crean en el interior de los dispositivos criptográficos en un proceso auditado por personal independiente. La introducción de la clave en el modulo criptográfico se realizará al menos con la participación de dos personas.

La SubCA y AC Camerfirma SA guardan actas de los procesos de gestión de las claves privadas de las respectivas CAs.

Las claves en hardware de los suscriptores se crean dentro del dispositivo criptográfico entregado por la SubCA.

Las claves asociadas a los suscriptores no pueden ser trasferidas

6.3.6 Método de activación de la clave privada

La activación de la clave privada de la SubCA y AC Camerfirma SA es realizada por la aplicación de gestión.

El acceso a la clave privada del suscriptor se realiza por medio de un PIN que conocerá solamente el suscriptor y que evitará tenerlo por escrito.

Las claves de la SubCA y de AC Camerfirma SA se activan por un proceso de m de n. Ver apartado 6.3.1.

La SubCA y AC Camerfirma SA guardan actas de los procesos de gestión de las claves privadas de las respectivas CAs.

6.3.7 Método de desactivación de la clave privada

La clave privada del suscriptor quedará desactivada una vez se retire el dispositivo criptográfico de creación de firma del dispositivo de lectura.

Para la desactivación de la clave privada de la SubCA o AC Camerfirma SA se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

La SubCA y AC Camerfirma SA guarda actas de los procesos de gestión de las claves privadas de las respectivas CAs.

6.3.8 Método de destrucción de la clave privada

Anteriormente a la destrucción de las claves de la SubCA se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o formatearán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de la SubCA o AC Camerfirma SA. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

Finalmente se destruirán de forma segura las copias de seguridad.

Las claves del suscriptor en hardware podrán ser destruidas mediante un software especial en las instalaciones de RA o de la SubCA.

La SubCA y AC Camerfirma SA guardan actas de los procesos de gestión de las claves privadas de AC.

6.4 Otros aspectos de la gestión del par de claves

6.4.1 Archivo de la clave pública

La SubCA y AC Camerfirma SA mantendrán sus archivos de documentación relativa a la gestión de los certificados por un periodo mínimo de quince (15) años siempre y cuando la tecnología de cada momento lo permita. Dentro de la documentación a custodiar se encuentran los certificados de clave pública emitidos a sus suscriptores y los certificados de clave pública propios.

6.4.2 Periodo de uso para las claves públicas y privadas

Un certificado de clave pública o privada no debe ser usado una vez haya expirado su período de validez. Una clave privada sólo se puede utilizar fuera del período establecido por el certificado digital para recuperar los datos cifrados.

6.5 Ciclo de vida del dispositivo seguro de almacenamiento de los datos de creación de firma (DSADCF) y del dispositivo seguro de creación de firma (DSCF)

Los certificados de la SubCA y AC Camerfirma SA se almacenan en un dispositivo seguro de creación de firma (Hardware) que cumple los requerimientos FIPS 140-1 Nivel 3.

El dispositivo hardware para los certificados de suscriptor es una tarjeta criptográfica o token USB que cumple los requerimientos de acreditación determinados en la legislación vigente ó al menos ITSEC E4+. Estos dispositivos estarán expuestos en la página Web de la SubCA.

La gestión de distribución del soporte la realiza el proveedor externo que lo distribuye a las autoridades de registro para su entrega al suscriptor.

El suscriptor o la RA utiliza el dispositivo para generar el par de claves y enviar la clave pública a la SubCA o AC Camerfirma SA.

La SubCA o AC Camerfirma SA envía un certificado de clave pública al suscriptor o la RA, que es introducido en el dispositivo.

El dispositivo es reutilizable y puede mantener de forma segura varios pares de claves.

La SubCA deberá, por si misma o por delegación de esta función, realizar todos los esfuerzos para asegurar que:

a) La preparación del DSADCF o DSCF es controlada de forma segura.

b) El DSADCF o DSCF es almacenado y distribuido de forma segura.

c) Si el propio sistema lo permite, que la activación y desactivación del DSADCF o DSCF es controlada de forma segura.

d) El DSADCF o DSCF no es usado por la SubCA o entidad delegada antes de su emisión.

e) El DSADCF o DSCF queda inhabilitado para su uso en caso de ser devuelto por el Firmante/Suscriptor.

f) Cuando el DSADCF o DSCF lleve asociado unos datos de activación (ej PIN), estos datos de activación y el dispositivo seguro de creación de firma serán preparados y distribuidos de forma separada.

6.6 Controles de seguridad informática

La SubCA emplea sistemas fiables para ofrecer sus servicios de certificación. La SubCA ha realizado controles y auditorías informáticas a fin de establecer una gestión adecuada de sus activos informáticos con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información en las operaciones de la SubCA, tanto la SubCA como AC Camerfirma SA son auditadas anualmente para garantizar que se mantienen los niveles apropiados de seguridad y se sigue el esquema de certificación sobre sistemas de gestión de la información ISO 27001/ISO 27002.

Los equipos informáticos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de la SubCA en los siguientes aspectos:

- Configuración de seguridad del sistema operativo
- Configuración de seguridad de las aplicaciones
- Dimensionamiento correcto del sistema
- Configuración de Usuarios y permisos
- Configuración de eventos de Log
- Plan de backup y recuperación
- Configuración antivirus
- Requerimientos de trafico de red

6.6.1 Requerimientos técnicos de seguridad informática específicos

Cada servidor de la SubCA incluye las siguientes funcionalidades:

- control de acceso a los servicios de la SubCA y gestión de privilegios
- imposición de separación de tareas para la gestión de privilegios
- identificación y autenticación de roles asociados a identidades
- archivo del historial del suscriptor y la SubCA y datos de auditoria
- auditoria de eventos relativos a la seguridad
- auto-diagnóstico de seguridad relacionado con los servicios de la SubCA

- Mecanismos de recuperación de claves y del sistema de la SubCA

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

6.6.2 Valoración de la seguridad informática

La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad.

6.7 Controles de seguridad del ciclo de vida

6.7.1 Controles de desarrollo del sistema

La SubCA posee un procedimiento de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada.

6.7.2 Controles de gestión de la seguridad

6.7.2.1 Gestión de seguridad

La SubCA desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un grupo para la gestión de la seguridad.

La SubCA exige mediante contrato las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

6.7.2.2 Clasificación y gestión de información y activos

La SubCA mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de la SubCA detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: Público, Uso interno y Confidencial.

6.7.2.3 Procedimientos de gestión

La SubCA dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos. En el documento de seguridad de la SubCA se desarrolla en detalle el proceso de gestión de incidencias.

La SubCA tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

Tratamiento de soportes y seguridad

Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

Plan de capacidad del sistema

El departamento de Sistemas de la SubCA mantiene un registro de las capacidades de los equipos. Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

Notificación de incidencias y respuesta

La SubCA dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica de la resolución de la incidencia.

Procedimientos operativos y responsabilidades

La SubCA define actividades, asignadas a personas con un rol de confianza, distintas a las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.7.2.4 Gestión de acceso al sistema

LA SubCA realiza todos los esfuerzos que razonablemente están a su alcance para garantizar que el acceso al sistema está limitado a las personas autorizadas. En concreto:

SubCA en general

- Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
- La SubCA dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- La SubCA dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones de certificación.
- El personal de la SubCA es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

Generación del certificado

- La autenticación para el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de la SubCA.

Gestión de la revocación

- La revocación se realizará mediante autenticación fuerte con tarjeta de un administrador autorizado.
- Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador de SubCA.

Estado de la revocación

- La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación por certificados para evitar el intento de modificación de la información del estado de la revocación.

6.7.2.5 Gestión del ciclo de vida del hardware criptográfico

La SubCA se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.

La SubCA registra toda la información pertinente del dispositivo para añadir al catálogo de activos.

El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

La SubCA realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

La clave privada de firma de la SubCA almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema de la SubCA así como sus modificaciones y actualizaciones son documentadas y controladas.

La SubCA posee un contrato de mantenimiento del dispositivo. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.7.3 Evaluación de la seguridad del ciclo de vida

No estipulado.

6.8 Controles de seguridad de red

La SubCA protege el acceso físico a los dispositivos de gestión de red y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se trasfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL.

6.9 Fuentes de Tiempo

La SubCA tiene un procedimiento de sincronización de tiempo coordinado con el Instituto Nacional de Metrología de Colombia.

6.10 Controles de ingeniería de los módulos criptográficos

Todas las operaciones criptográficas de la SubCA son realizadas en módulos validados al menos por FIPS 140-1 nivel 3.

7 PERFILES DE CERTIFICADO Y CRL

7.1 Perfil de certificado

Todos los certificados emitidos bajo esta DPC están en conformidad con el estándar X.509 versión 3, RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" y ETSI 101 867 "Qualified Certificate Profile".

El perfil común para todos los certificados es:

Campo	Descripción
Version	V3 (x509 estándar)
Serial number	Número de serie del certificado. Código único.
Issuer	Nombre distintivo de la SubCA que emite el certificado
not Before	Inicio de la validez del certificado
not After	Fin de la validez del certificado
Subject	Nombre distintivo del suscriptor
Extensions	Extensiones del certificado

7.1.1 Número de versión

La SubCA emite certificados X.509 Versión 3.

7.1.2 Extensiones del certificado

Los documentos de las extensiones de los certificados se encuentran detallados en documentos independientes adjuntos a esta CPS.

Este método de publicación permite mantener versiones de las políticas y DPC más estables y desligarlos de los frecuentes ajustes en los perfiles de los certificados.

7.1.3 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es 1.2.840.113549.1.1.11: SHA256 with RSA Encryption.

El identificador de objeto del algoritmo de la clave pública es 1.2.840.113549.1.1.1: rsaEncryption.

7.1.4 Restricciones de nombre

Los nombres contenidos en los certificados están restringidos a "Distinguished Names" X.500, que son únicos y no ambiguos.

7.1.5 Identificador de objeto (OID) de la Política de Certificación

Todos los certificados tienen un identificador de política:

Certificado	OID de la Política
Persona Jurídica	1.3.6.1.4.1.17326.20.1.3.2
Persona Natural	1.3.6.1.4.1.17326.20.1.4.2
Pertenencia a Empresa	1.3.6.1.4.1.17326.20.1.5.2
Representante de Empresa	1.3.6.1.4.1.17326.20.1.7.2

Certificado	OID de la Política
Profesional Titulado	1.3.6.1.4.1.17326.20.1.6.2
Función Pública	1.3.6.1.4.1.17326.20.1.2.2
Comunidad Académica	1.3.6.1.4.1.17326.20.1.1.2
Certificado SSL	1.3.6.1.4.1.17326.10.11.2.1
Sello de empresa	1.3.6.1.4.1.17326.10.11.3.1.1
Firma de Código	1.3.6.1.4.1.17326.10.12.2
Sello de tiempo	1.3.6.1.4.1.17326.10.13.1.3

7.2 Sellos de tiempo

El sello de tiempo tendrá seguirá las especificaciones de la RFC3161, disponiendo de la siguiente representación.

TimeStampResp ::= SEQUENCE {

status PKIStatusInfo,

timeStampToken TimeStampToken OPTIONAL }

El campo status está basado en la definición de la estructura PKIStatusInfo de la RFC2510:

PKIStatusInfo ::= SEQUENCE {

status

PKIStatus,

statusString PKIFreeText OPTIONAL,

failInfo PKIFailureInfo OPTIONAL }

Status: Si este campo está a cero o a uno indica que el sello viene en el mensaje de respuesta. Para cualquier otro valor indica que no viene en el mensaje de respuesta.

PKIStatus ::= INTEGER {

granted (0),

grantedWithMods (1),

rejection (2),

waiting (3),

revocationWarning (4),this message contains a warning that a revocation is imminent

revocationNotification (5)notification that a revocation has occurred}

StatusString: Se usa para indicar eventos de error.

FailInfo: indica las causas por las que no se ha generado el sello de tiempo. Siendo los posibles errores:

PKIFailureInfo ::= BIT STRING {

badAlg (0), Unrecognized or unsupported Algorithm Identifier

badRequest (2), Transaction not permitted or supported

badDataFormat (5), The data submitted has the wrong format

timeNotAvailable (14), The TSA's time source is not available

unacceptedPolicy (15), The requested TSA policy is not supported

unacceptedExtension (16), The requested extension is not supported

addInfoNotAvailable (17) The additional information requested could not be understood or is not available

systemFailure (25) the request cannot be handled due to system failure}

El campo timestampToken contiene el sello de tiempo generado. Se define como:

TimeStampToken ::= ContentInfo

contentType is id-signedData ([CMS])

Content is SignedData ([CMS])

ContentInfo es una estructura que encapsula la información firmada en una estructura TSTInfo. Está definida en la RFC2630 y tiene los siguientes campos:

TSTInfo ::= SEQUENCE {

version INTEGER { v1(1) },

policy TSAPolicyId,

messageImprint MessageImprint,

serialNumber INTEGER,

genTime GeneralizedTime,

accuracy Accuracy OPTIONAL,

ordering BOOLEAN DEFAULT FALSE,

nonce INTEGER OPTIONAL,

tsa [0] GeneralName OPTIONAL,

extensions [1] IMPLICIT Extensions OPTIONAL }

version: indica la versión del sello

policy: si se ha generado el sello, será igual al del mensaje de petición

messageImprint: será igual al del mensaje de petición

serialNumber: es un entero asignado por la TSA y debe ser único para cada sello que genere. Por tanto, un sello será identificado por el nombre de la TSA que lo generó y el número de serie asignado

genTime: es el instante de tiempo en el que se creó el sello. Tanto ISO como el IETF expresan el instante de tiempo referido a la escala UTC, para evitar confusiones con las horas locales. El formato debe ser el siguiente:

- CC YY MM DD hh mm ss Z
- CC representa el siglo (19-99)
- YY representa el año (00-99)
- MM representa el mes (01-12)
- DD representa el día (01-31)
- hh representa la hora (00-23)
- mm representa los minutos (00-59)
- ss representa los segundos (00-59)
- Z viene de zulu, que es como se conoce a la escala UTC

accuracy: en los casos que sea necesario, proporciona una precisión incluso de microsegundos:

Accuracy ::= SEQUENCE {

seconds [1] Integer OPTIONAL,

millis [2] Integer (1..999) OPTIONAL,

micros [3] Integer (1..999) OPTIONAL,

}

nonce: aparece si lo hace en el mensaje de petición, y tendrá el mismo valor tsa: sirve para identificar a la TSA extensions: están definidas en la RFC 2459

7.3 Perfil de CRL

El perfil de las CRL se corresponde con el propuesto en las Políticas de certificación correspondientes. Las CRL son firmadas por la subordinada que ha emitido los certificados.

El perfil del certificado de CRL se encuentra en un documento adjunto a esta CPS.

7.3.1 Número de versión

Las CRL emitidas por la SubCA son versión 2.

7.3.2 CRL y extensiones

Las extensiones de las CRL se encuentran en un documento adjunto a esta CPS.

8 ESPECIFICACIÓN DE LA ADMINISTRACIÓN

8.1 Autoridad de las Políticas

La Autoridad de las Políticas (PA) se establece en el apartado correspondiente. Es responsable de la administración de las Políticas y DPC.

8.2 Procedimientos de especificación de cambios

Esta DPC se modificará cuando se produzcan cambios relevantes en la gestión de cualquier tipo de certificados sujetos a ella. Se producirán al menos revisiones anuales en caso de que no se produzcan cambios en este tiempo para garantizar que siguen vigentes.

8.2.1 Elementos que pueden cambiar sin necesidad de notificación

Los cambios que puedan realizarse a esta DPC no requieren notificación excepto que afecten de forma directa a los derechos de los Firmantes/Suscriptores de los certificados, en cuyo caso deberán ser informados con objeto de que puedan presentar sus comentarios a la organización de la Administración de las Políticas dentro de los 15 días siguientes a la publicación del aviso.

8.2.2 Cambios con notificación

8.2.2.1 Lista de elementos

Cualquier elemento de esta DPC puede ser cambiado sin preaviso.

8.2.2.2 Mecanismo de notificación

Todos los cambios propuestos de esta DPC serán inmediatamente publicados en la Web de la SubCA, indicada en el apartado 1.3.

En este mismo documento existe un apartado de cambios y versiones donde se puede conocer los cambios producidos desde su creación y la fecha de dichas modificaciones

8.2.2.3 Periodo de comentarios

Los Firmantes/Suscritores y Terceros que confían, afectados pueden presentar sus comentarios a la organización de la Administración de las Políticas dentro de los 15 días siguientes a la recepción de la notificación.

8.2.2.4 Mecanismo de tratamiento de comentarios

Cualquier acción tomada como resultado de unos comentarios queda a la discreción de la PA.

8.3 Publicación y copia

Una copia de esta DPC estará disponible en formato electrónico en el sitio web de la SubCA, indicado en el apartado 1.3.

8.4 Procedimientos de aprobación de la DPC

La publicación de las revisiones de esta DPC deberá estar aprobada por la Dirección de la SubCA

Control de cambios

Fecha	Versión	Descripción del cambio	Justificación del cambio	Responsable
01-oct-2015	1	Creación del documento	Genera lineamientos de la dpc Citiseg SAS	RA/Benito Otero
20-abr-2015	2	Se incluye tanto la información de cumplimiento con la imparcialidad, como la ampliación de la información en caso de cese de actividad de la CA.	Corrección debido a no Conformidad detectada en evaluación realizada por el ONAC en diciembre de 2015.	RA/Rodrigo Caro
06-abr-2017	3	Se sustituye el certificado de CA raíz e intermedias	Certificados con algoritmo sha256WithRSAEncryption	RA/Rodrigo Caro
28-abr-2017	4	Se actualiza documento de acuerdo a observaciones de ONAC	Certificados con algoritmo sha256WithRSAEncryption	RA/Rodrigo Caro
16-ago-2017	5	Se actualiza documento de conformidad con la auditoria de vigilancia 2017	Se agrega una nota a la DPC donde se excluye del alcance de la acreditacion el certificado de Servidor Seguro SSL.	AR/Flor Mesa