CRITERIOS ESPECÍFICOS DE ACREDITACIÓN
ENTIDADES DE CERTIFICACIÓN DIGITAL

CEA-4.1-10
Versión 01

ELABORÓ:2014-11-04 *DIRECTOR TÉCNICO* *COORDINADOR SECTORIAL ECD* *GRUPO TÉCNICO ASESOR GTA-ECD*	*REVISÓ: 2015-07-03* *COMITÉ TÉCNICO – CONSEJO DIRECTIVO* *2014-12-18* *CONSULTA PÚBLICA:* *2015-02-02 – 2015-03-02* *GRUPO TÉCNICO ASESOR GTA* *2015-07-03*	*APROBÓ: 2015-08-11* *DIRECTOR EJECUTIVO*

TABLA DE CONTENIDO

1. OBJETIVO

Establecer los Criterios Específicos de Acreditación (CEA), que deben ser cumplidos para obtener la Acreditación como Entidad de Certificación Digital - ECD, ante el Organismo Nacional de Acreditación de Colombia – ONAC; es decir para prestar servicios de certificación digital de acuerdo a lo establecido en la Ley 527 de 1999, el Decreto Ley 0019 de 2012, el Decreto 333 de 2014, el Decreto 1471 de 2014 y los reglamentos que los modifiquen o complementen.

2. AUTORÍA

Este documento fue preparado por el Organismo Nacional de Acreditación de Colombia, ONAC; en su revisión participaron los miembros del Grupo Técnico Asesor – GTA, compuesto por: un representante del Comité Técnico del Consejo Directivo de ONAC, el Director Técnico de ONAC, el Coordinador Sectorial de Entidades de Certificación Digital de ONAC, un experto técnico en representación de las Entidades de Certificación Digital abiertas, un experto técnico en representación de las Entidades de Certificación Digital cerradas, dos expertos técnicos de ONAC, un representante del Ministerio de Comercio, Industria y Turismo, un representante de la Superintendencia de Industria Comercio, y, un representante del Archivo General de la Nación.

3. INTRODUCCIÓN

Con base en los artículos 160 a 163 del Decreto Ley 0019 de 2012, la Ley 527 de 1999 el Decreto 333 de 2014 y el Decreto 1471 de 2014, las Entidades de Certificación Digital - ECD deben acreditarse ante el Organismo Nacional de Acreditación de Colombia - ONAC, de acuerdo con los Criterios Específicos de Acreditación - CEA que él establezca, por ser el designado para diseñar y desarrollar el servicio de acreditación para las ECD con el fin de dar cumplimiento a estos mandatos del Gobierno Nacional de Colombia.

La denominación Entidades de Certificación Digital – ECD, usada en este documento y para todo el programa de acreditación, se establece con el fin de particularizar y diferenciar este tipo de organizaciones de los demás Organismos de Certificación que ONAC acredita.

4. ALCANCE

4.1. El artículo 160 del Decreto Ley 0019 de 2012 y en el artículo 2 del Decreto 333 de 2014, establece quiénes están obligados a acreditarse ante ONAC y por ende a cumplir con estos Criterios Específicos de Acreditación, así:

1. Las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero, incluidas las cámaras de comercio y las notarías, que pretendan ser acreditadas como ECD.
2. Las Entidades de Certificación Digital abiertas o cerradas que hubieren sido autorizadas por la Superintendencia de Industria y Comercio y que pretendan continuar prestando servicios de certificación digital como ECD.
3. Las ECD acreditadas o en proceso de acreditación por ONAC.

4.2. El Artículo 161 del Decreto Ley 0019 de 2012, modificando la Ley 527 de 1999, establece las actividades que pueden realizar las ECD para prestar servicios de certificación digital, así:

"ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACIÓN. El artículo 30 de la Ley 527 de 1999, quedará así:
Las entidades de certificación acreditadas por el Organismo Nacional de Acreditación de Colombia para prestar sus servicios en el país, podrán realizar, entre otras, las siguientes actividades:

1. *Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.*
2. *Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.*
3. *Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999.*
4. *Ofrecer o facilitar los servicios de generación de los datos de creación de las firmas digitales certificadas.*
5. *Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.*
6. *Ofrecer o facilitar los servicios de generación de datos de creación de las firmas electrónicas.*
7. *Ofrecer los servicios de registro, custodia y anotación de los documentos electrónicos transferibles.*
8. *Ofrecer los servicios de archivo y conservación de mensajes de datos y documentos electrónicos transferibles.*
9. *Cualquier otra actividad relacionada con la creación, uso o utilización de firmas digitales y electrónicas."*

4.3. El numeral 1 del Artículo 11 del Decreto 333 de 2014 establece que los servicios de certificación digital que preste la ECD, deben estar Acreditados, así:

El Artículo 11 del Decreto 333 de 2014. Infraestructura y recursos, establece: "*En desarrollo de lo previsto en el literal b) del artículo 29 de la Ley 527 de 1999, la entidad de certificación deberá contar con un equipo de personas, una infraestructura física, tecnológica y unos procedimientos y sistemas de seguridad, tales que: 1. Puedan generar las firmas digitales y electrónicas propias y que además, les permita prestar todos los servicios para los que soliciten la acreditación...".*

El artículo 30 de la Ley 527 de 1999, quedó así: *Las entidades de certificación acreditadas por el Organismo Nacional de Acreditación de Colombia para prestar sus servicios en el país, podrán realizar entre otras, las siguientes actividades…* (subraya fuera de texto original)

Por lo anterior, el alcance de acreditación otorgado por ONAC a las ECD corresponderá a los servicios de certificación digital para los cuales solicite acreditación y demuestre su competencia en el contexto del presente Criterio Específico de Acreditación.

Estos Criterios deben ser aplicados por las ECD. ONAC evaluará su cumplimiento junto con los requisitos establecidos en las Reglas del Servicio de Acreditación, R-AC-01, en el desarrollo de evaluaciones de otorgamiento, vigilancia, ampliación, extraordinarias y de renovación de la acreditación.

5. JUSTIFICACIÓN

Este documento, se desarrolla en el ámbito del sector reglamentario de la acreditación, atendiendo el mandato del Gobierno Nacional establecido en el Decreto Ley 0019 de 2012 y del ente regulador, establecido en el Decreto 333 de 2014 emitido por el Ministerio de Comercio Industria y Turismo, y, las demás regulaciones que lo modifiquen o complementen.

6. DOCUMENTOS DE REFERENCIA

	DOCUMENTO	TITULO/CONTENIDO
1	ISO/IEC 17000	Evaluación de la Conformidad. Vocabulario y principios generales.
2	ISO/IEC 17065	Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios.
3	ISO 9001	Sistema de gestión de la calidad. Requisitos.
4	NTC GP1000	Norma técnica de calidad en la gestión pública.
5	ISO/IEC 27001	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos
6	ISO/IEC 20000	Tecnología de la información. Gestión de la calidad de los servicios TI
7	ISO 19011	Directrices para la auditoría de Sistemas de Gestión.
8	ISO 31000	Gestión de Riesgos.
9	ISO 22301	Sistema de Gestión de la Continuidad del Negocio (SGCN)
10	ISO 25000	SQuaRE (System and Software Quality Requirements and Evaluation)
11	ISO 21188	Public key infrastructure for financial services -- Practices and policy framework
12	ISO 15836	Information and documentation -- The Dublin Core metadata element set (XML)
13	Ley 527 de 1999	Ley de comercio electrónico, que deben cumplir las ECD
14	Decreto ley 0019 de 2012	En los artículo 160 a 163 se sustituye la autorización que la SIC otorgaba a las Entidades de Certificación, por la acreditación que las Entidades de Certificación que fueron autorizadas por la SIC y las ECD, deben obtener de ONAC.
15	Decreto 333 de 2014	Reglamenta el artículo 160 del Decreto Ley 0019 de 2012.
16	Decreto 1595 de 2015	Por el cual se dictan normas relativas al Subsistema Nacional de la Calidad y se modifica el capítulo 7 y la sección 1 del capítulo 8 del título 1 de la parte 2 del libro 2 del Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, Decreto 1074 de 2015, y se dictan otras disposiciones.

7. SIGLAS Y/O ABREVIATURAS

SIGLA	DEFINICIÓN
AICPA	American Institute of Certified Public Accountants
ANSI	American National Standards Institute
CA	Cetification Authority (Autoridad de Certificación)
CPA	Chartered Professional Accountants Of Canada
PC	Políticas de los certificados
CRL	Lista de Certificados Revocados
DPC	Declaración de prácticas de certificación
ECD	Entidad de Certificación Digital que prestan servicios de certificación digital y equivale a una Entidad

SIGLA	DEFINICIÓN
	Certificadora definida en la ley 527 de 1999. También se debe entender como un Organismo de Evaluación de la Conformidad – OEC de acuerdo con lo definido en la ISO/IEC 17000.
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards (FIPS, en español Estándares Federales de Procesamiento de la Información) son estándares anunciados públicamente desarrollados por el gobierno de los Estados Unidos para la utilización por parte de todas las agencias del gobierno no militares y por los contratistas del gobierno. Muchos estándares FIPS son versiones modificadas de los estándares usados en las comunidades más amplias (ANSI, IEEE, ISO, etc.)
GP	Gestión Pública
GTA	Grupo Técnico Asesor
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LDAP	Lightweight Directory Access Protocol
MINCIT	Ministerio de Comercio, Industria y Turismo de Colombia
MLA	Acuerdo Multilateral de Reconocimiento.
NTC	Norma Técnica Colombiana
OEC	Organismo de Evaluación de la Conformidad. Para su correcta interpretación, debe entenderse que ECD equivale a OEC dando alcance así al art.160 del decreto ley 019 de 2012.
ONAC	Organismo Nacional de Acreditación de Colombia
OCSP	Servicio del estado del certificado en línea
PKCS	Public-Key Cryptography Standards. Estándares de criptografía de llave pública concebidos y publicados por los laboratorios de RSA. Anexo G
PKI	Infraestructura de llave pública
RA	Autoridad de Registro
RC	Requisitos de Certificación
RFC	Request for Comments son una serie de publicaciones del Internet Engineering Task Force (IETF) que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc.
RSA	Rivest, Shamir y Adleman. Es un sistema criptográfico de llave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.
SHA	Secure Hash Algorithm (Algoritmo de seguridad HASH)
SSL	Secure Sockets Layer: capa de conexión segura. Protocolo criptográfico que proporciona comunicaciones seguras por una red, comúnmente Internet.

SIGLA	DEFINICIÓN
TSA	Time Stamp Authority, (Autoridad de sellado de tiempo).
TLS	Transport Layer Security: seguridad de la capa de transporte. Protocolo criptográfico que proporciona comunicaciones seguras por una red, comúnmente Internet
TICs	Tecnología de Información y Comunicaciones
VA	Validation Authority (Autoridad de validación)

8. DEFINICIONES Y CONVENCIONES

Para la aplicación de este documento, se deben considerar en su orden jerárquico: las definiciones establecidas en las leyes, reglamentos, documentos de referencia y las siguientes:

8.1. Algoritmo: es un conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien deba realizar dicha actividad. Dados un estado inicial y siguiendo los pasos sucesivos se llega a un estado final y se obtiene una solución.

8.2. Apelación: solicitud, presentada por una entidad de certificación digital, para reconsiderar cualquier decisión adversa tomada por el Organismo de Acreditación con relación a su estado de acreditación.

8.3. Autoridad de sellado de tiempo (TSA): Entidad de confianza que emite sellos de tiempo.

8.4. Autoridad de validación (VA): Entidad de confianza que proporciona información sobre la validez de los certificados digitales.

8.5. OID: Identificador único de objeto (Object identifier). OID. Acrónimo del término en idioma inglés “Object Identifier”, que consiste en un número único de identificación asignado en base a estándares internacionales y comúnmente utilizado para identificar documentos, sistemas, equipos, etc., con la finalidad, entre otras cosas, de conocer el origen, la titularidad y la antigüedad del objeto identificado.

8.6. CA raíz: Autoridad certificadora de primer nivel, base de confianza.

8.7. CA subordinada: Autoridad certificadora de segundo nivel o más niveles.

8.8. Caracterización de procesos y servicios: Descripción documentada de las características generales del proceso o servicio que establece la relación con los demás procesos internos o externos de la organización, los insumos y salidas del proceso, los proveedores y clientes, los riesgos y controles, y su interacción.

8.9. Certificado digital: mensaje de datos electrónico firmado por la entidad de certificación digital, el cual identifica tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la llave pública de éste último.

8.10.

8.11. Cliente: En los servicios de certificación digital, el término cliente identifica a la persona natural o jurídica con la cual la ECD establece una relación comercial.

8.12. Datos de Creación de Firma (Llave privada): son valores numéricos únicos que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.

8.13. Datos de Verificación de Firma (Llave pública): son los datos, como códigos o claves criptográficas públicas, que son utilizados para verificar que una firma digital fue generada con la llave privada del suscriptor.

8.14. Declaración de Prácticas de Certificación (DPC): Es el documento en el que consta de manera detallada los procedimientos que aplica la ECD para la prestación de sus servicios. Una declaración de las prácticas que una ECD emplea para emitir, gestionar, revocar y renovar certificados sin y con cambio de claves.

8.15. Entidad de Certificación De acuerdo con lo indicado en la Ley 527 de 1999, Artículo 2, Literal d, es aquella persona natural o jurídica que, autorizada conforme a dicha Ley, está facultada para emitir certificados digitales en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la

transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

8.16. Entidades de Certificación Digital – ECD: Denominación que se establece con el fin de particularizar y diferenciar este tipo de organizaciones como Entidades de Certificación de los demás Organismos de Certificación que ONAC acredita.

8.17. Entidad de certificación abierta: la que ofrece al público en general, servicios propios de las ECD, tales que: su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, y recibe remuneración.

8.18. Entidad de certificación cerrada: entidad que ofrece servicios propios de las entidades de certificación solo para el intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello.

8.19. Autoridad de Registro (RA): Persona jurídica, con excepción de los notarios públicos, o parte interna de las ECD necesariamente independiente de su CA, que acorde con la normatividad vigente, es la encargada de recibir las solicitudes relacionadas con certificación digital, para:

- Registrar las peticiones que hagan los solicitantes para obtener un certificado.
- Comprobar la veracidad y corrección de los datos que aportan los usuarios en las peticiones.
- Enviar las peticiones que cumplen los requisitos a una CA para que sean procesadas.

8.20. Firma Digital: Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático reconocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

8.21. Función Hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.

8.22. Lista de Certificados Digitales Revocados (CRL): es aquella relación que debe incluir todos los certificados revocados por la entidad de certificación digital.

8.23. Log: Servicio de registro de eventos del sistema de información, dejando la información anterior y la actual, identifica quién y cuándo se realizó el evento.

8.24. Neutralidad tecnológica: principio de no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente, así mismo la no discriminación, preferencia o restricción de ninguna de las diversas técnicas o tecnologías que pueden utilizarse para firmar, generar, comunicar, almacenar o archivar electrónicamente información.

8.25. Niveles de seguridad: son los diversos niveles de garantía que ofrecen las variables de firma electrónica cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma electrónica para enviar o recibir mensajes de datos o documentos electrónicos.

8.26. Organismo relacionado: entidad que está relacionada con la ECD porque comparten propietarios comunes, tiene acuerdos contractuales con las mismas ECD, o pertenece al mismo grupo corporativo en el cual está la ECD.

8.27. PKI: Infraestructura de llave pública (Public key infraestructure): es el conjunto de hardware, software, políticas, procedimientos y elementos tecnológicos que, mediante la utilización de un par de claves criptográficas, una privada que sólo posee el suscriptor del servicio y una pública, que se incluye en el certificado digital, logran:

- Identificar al emisor de un mensaje de datos electrónico.
- Impedir que terceras personas puedan observar los mensajes que se envían a través de medios electrónicos.
- Impedir que un tercero pueda alterar la información que es enviada a través de medios electrónicos.
- Evitar que el suscriptor del servicio de certificación digital que envió un mensaje electrónico pueda después negar dicho envío.

8.28. Políticas de Certificado (PC): Es el conjunto de reglas que indica los requisitos de un certificado en una comunidad y/o clase en particular, en el marco de los requisitos legales, reglamentarios, y con requisitos de seguridad comunes.

8.29. Proveedor: El término "proveedor", incluye a organizaciones, personas, fabricantes, distribuidores, ensambladores de tecnología y otros que suministran productos, bienes y servicios. Entre los proveedores de las ECD están: Entidades recíprocas, empresas de tecnología que prestan servicios en sus diferentes modalidades como son: hosting, colocation, repositorio documental (electrónico o físico), proveedor de dispositivos, proveedor de telecomunicaciones, etc.

8.30. Queja: expresión de insatisfacción, diferente de la apelación, presentada por una persona u organización a una ECD o a un organismo de acreditación, relacionada con las actividades de uno de los dos, para la cual se espera respuesta.

8.31. Requisitos de certificación (RC): Es el conjunto de obligaciones establecidas en la ley Colombiana, para el solicitante del servicio de certificación digital debe demostrar cumplimiento ante la ECD, para ser suscriptor del producto que solicita.

8.32. Revocación: Para este documento, es el proceso por el cual se inhabilita el Certificado Digital emitido y se da por terminado su periodo de validez de uso a partir de la fecha de revocación; al presentarse alguna de las causas establecidas en la Declaración de Prácticas de Certificación. .

8.33. Estampado cronológico: (Time stamping en Ingles). Mensaje de datos firmado digitalmente y con sello de tiempo por una TSA que vincula a otro mensaje de datos con un momento de tiempo concreto, el cual permite establecer con una prueba que estos datos existían en ese momento y que no sufrieron ninguna modificación a partir del momento en que se realizó el estampado

8.34. Servicio del estado del certificado en línea OCSP: Actividad de consulta en tiempo real al sistema de la ECD, sobre el estado de un certificado digital a través del protocolo OCSP

8.35. Servicio de certificación digital: Conjunto de actividades certificación que ofrece la ECD para certificar el origen e integridad de mensajes de datos, basados en las firmas digitales o electrónicas, estampado de tiempo, así como en la aplicabilidad de estándares técnicos admitidos y vigentes en infraestructura de llave pública – PKI.

8.36. Solicitante: persona natural o jurídica que con el propósito de obtener servicios de certificación digital de una ECD, demuestra el cumplimiento de los requisitos establecidos en la DPC y PC de éstas, para acceder al servicio de certificación digital.

8.37. Suscriptor: persona natural o jurídica a cuyo nombre se expide un certificado digital.

8.38. Token: Dispositivo hardware criptográfico suministrado por una ECD, el cual contiene el certificado digital y la llave privada del suscriptor.

8.39. Uptime: Compromiso en término de porcentaje de tiempo disponible de un sistema de información, que la empresa proveedora de éste se compromete a ofrecer a su cliente por año.

8.40. Usabilidad: es un término proveniente del inglés "usability", empleado para denotar la forma en la que una persona puede emplear una herramienta particular de manera efectiva, eficiente y satisfactoria, en función de lograr una meta específica.

8.41. Webtrust: Sello de confianza en Internet otorgado por AICPA / CPA

9. REGLAS DEL SERVICIO DE ACREDITACIÓN

Tanto las Entidades de Certificación autorizadas por la SIC que desean continuar prestando servicios de certificación digital, como las demás ECD para obtener y mantener su acreditación ante ONAC, deben dar cumplimiento a las Reglas del Servicio de Acreditación establecidas por ONAC en el documento R-AC-01; el Reglamento para el uso de símbolos de acreditado y/o asociado R-AC-1.4-03, y, los demás procedimientos, circulares y documentos que establezca ONAC pertinentes al proceso y mantenimiento de la acreditación.

10. REQUISITOS DE ACREDITACIÓN PARA ENTIDADES DE CERTIFICACIÓN DIGITAL

ONAC, en cumplimiento de la obligación establecida en el artículo 160 del Decreto Ley 0019 de 2012 y en el Decreto reglamentario 333 del 19 de febrero de 2014, así como en la ley 527 de 1999 en sus artículos 2 literal d), artículo 29 y artículo 30 modificado por el Decreto Ley 0019 de 2012, artículo 42 del decreto 1471 de 2014, establece las reglas del servicio de acreditación en el documento R-AC-01 y los Criterios Específicos de Acreditación para Entidades de Certificación Digital en el presente documento CEA-4.1-10, tomando para ello como documento de referencia la norma internacional ISO/IEC 17065, así como también los modelos y estándares técnicos de Infraestructura de llave pública (PKI) que se encuentren vigentes y sean aceptados internacionalmente de manera que no comprometen la seguridad de algún componente de la PKI.

10.1. REQUISITOS DE CERTIFICACIÓN (RC)

Las ECD deben asegurar que todos los suscriptores han cumplido los requisitos definidos en las leyes colombianas y las disposiciones emitidas por los entes reguladores para obtener el servicio de certificación digital solicitado. Estos requisitos deben ser parte de la Declaración de Prácticas de Certificación (DPC) y las políticas de cada tipo de certificado (PC) citando la fuente de regulación.

10.2. REQUISITOS GENERALES

10.2.1. TEMAS LEGALES Y CONTRACTUALES

La ECD debe cumplir los requisitos de la ley 527 de 1999, el decreto 333 de 2014 y los demás reglamentos que los modifiquen o complementen.

10.2.1.1. Responsabilidad legal

La ECD debe estar formal y legalmente constituida como una persona jurídica en los términos del Artículo 160 del Decreto Ley 0019 de 2012.

10.2.1.2. Declaración de Prácticas de Certificación

10.2.1.2.1. La ECD debe suscribir un acuerdo de las condiciones para proporcionar servicios de certificación digital con el suscriptor del mismo. La Declaración de Prácticas de Certificación, debe tener en cuenta las responsabilidades de la ECD y de sus suscriptores.

10.2.1.2.2. La ECD debe asegurar que su Declaración de Practicas de Certificación exige al suscriptor cumplir, por lo menos, con lo siguiente:

a) los requisitos del servicio de certificación digital respectivo (véase numeral 10.1), incluyendo la implementación de los cambios cuando los comunica la ECD (véase 10.5.8);

b) que las declaraciones sobre la certificación son coherentes con el alcance del servicio de certificación digital (véase 10.8);
c) no utilizar su certificación digital de manera que contravenga la ley u ocasione mala reputación para la ECD, y no hace ninguna declaración relacionada con su certificación digital que la ECD pueda considerar engañosa o no autorizada;
d) que inmediatamente después de la cancelación o la terminación de la certificación digital, el suscriptor deja de utilizarla en todo el material publicitario que contenga alguna referencia a ella, y emprende las acciones exigidas por el servicio de certificación digital (por ejemplo, la devolución de los documentos de la certificación) y cualquier otra medida que se requiera;
e) que 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;
f) los requisitos que pueda prescribir el servicio de certificación digital con relación al uso de las marcas de conformidad y a la información relacionada con el servicio. No aplica para ECD cerradas.
g) informar a la ECD, sin retraso, acerca de los cambios que pueden afectar el servicio de certificación digital que le fue expedido por la ECD.

10.2.1.3.1 La ECD debe ejercer control, sobre los servicios de certificación digital acreditados, respecto a la propiedad y el uso de símbolos, certificados, cualquier otro mecanismo para indicar que el servicio de certificación digital está acreditado.

10.2.1.3.2 Las referencias al alcance de acreditación otorgado, o el uso engañoso del alcance de acreditación otorgado, los símbolos, los certificados, y cualquier otro mecanismo para indicar que un servicio de certificación digital, o que la ECD está acreditada, en la documentación o en otra publicidad, estarán sujetas al cumplimiento de las Reglas de Acreditación de ONAC R-AC-01 y R-AC-1.4-03.

10.2.2. GESTIÓN DE LA IMPARCIALIDAD

10.2.2.1. Las ECD deben actuar de manera imparcial.

10.2.2.2. La ECD debe emprender acciones preventivas y correctivas para responder ante cualquier riesgo que comprometa su imparcialidad, ya sea que se derive de las acciones de cualquier persona, organismo u organización, o de sí misma.

10.2.2.3. Todo el personal y los comités de la ECD (sean internos o externos), que puedan tener influencia en las actividades de certificación deben actuar con imparcialidad.

NOTA 1: La identificación de riesgos que comprometa la imparcialidad de la ECD se puede basar en la propiedad, el gobierno, la gestión, el personal, los recursos compartidos, las finanzas, los contratos, el mercadeo (incluyendo el posicionamiento de la marca), y el pago de comisiones por ventas u otros incentivos o la remisión suscriptores nuevos, etc.

NOTA 2: La identificación, valoración y gestión de los riesgos puede realizarse de acuerdo a lo establecido en la norma ISO 31000.

10.2.2.4. Si se identifica un riesgo para la imparcialidad, la ECD debe poder demostrar la manera en que elimina o minimiza tal riesgo. Esta información debe estar disponible para el mecanismo especificado en 10.3.2.

10.2.2.5. La ECD debe documentar y demostrar el compromiso de imparcialidad de la alta dirección (véase 10.3.1).

10.2.2.6. La ECD debe ser responsable de la imparcialidad de su actividad y no debe permitir que las presiones comerciales, financieras u otras comprometan su imparcialidad.

10.2.2.7. La ECD debe identificar los riesgos a su imparcialidad de manera continua. Se deben incluir aquellos riesgos que se derivan de sus actividades, sus relaciones o las relaciones de su personal (véase 10.2.2.3). Sin embargo, dichas relaciones no necesariamente pueden presentar riesgo a su imparcialidad.

10.2.2.8. Cuando la ECD ofrece los servicios de certificación digital que se van a certificar, y a la vez ofrece o suministra consultoría (véase 10.3.2), el personal administrativo, de gestión, técnico de la PKI, de la ECD asociado a las actividades de consultoría, debe mantener completa independencia y autonomía respecto al personal del proceso de revisión y toma de decisión sobre la certificación de la misma ECD.

NOTA Para el personal de RA, se estipulan requisitos de imparcialidad adicionales en las secciones 10.4 y 10.10

10.2.3. RESPONSABILIDAD Y FINANCIACIÓN

10.2.3.1. La ECD debe tener los seguros para cubrir las responsabilidades que se deriven de sus operaciones, establecidas en el Decreto 333 de 2014 y el Decreto 1471 de 2014.

10.2.3.2. La ECD debe tener la estabilidad financiera y los recursos que se requieren para sus operaciones que se encuentran establecidos en el Decreto 333 de 2014.

10.2.4. CONDICIONES NO DISCRIMINATORIAS

10.2.4.1. Las políticas y los procedimientos bajo los cuales opera la ECD, así como la administración de éstos, no deben ser discriminatorios. No se deben utilizar procedimientos que impidan o inhiban el acceso de los solicitantes a los servicios.

10.2.4.2. Los servicios de certificación digital de la ECD deben ser accesibles a todos los solicitantes cuyas solicitudes estén dentro del alcance de su acreditación.

10.2.4.3. El acceso a un servicio de certificación digital no debe depender del tamaño del solicitante o suscriptor ni de la membresía de cualquier asociación o grupo, tampoco debe depender del número de certificaciones ya emitidas. No deben existir condiciones indebidas, sean financieras u otras.

10.2.4.4. Una ECD puede declinar la aceptación de una solicitud o el mantenimiento de un contrato para la certificación cuando existen razones fundamentadas y demostradas, por ejemplo, la participación del solicitante y/o suscriptor en actividades ilegales, o temas similares relacionados con el suscriptor.

10.2.4.5. La ECD en el contexto de la acreditación, debe delimitar sus requisitos, revisión y decisión de certificación a aquellos asuntos relacionados específicamente con el alcance de acreditación otorgado por ONAC.

10.2.5. CONFIDENCIALIDAD

10.2.5.1. La ECD es responsable, a través de compromisos de cumplimiento legal, de la gestión de toda la información obtenida o creada durante el desempeño de las actividades de certificación digital. Con excepción de la información que el suscriptor pone a disposición del público, o cuando existe acuerdo suscrito entre la ECD y el suscriptor (por ejemplo, con fines de responder a los reclamos), toda otra información se considera información de propiedad y se debe considerar confidencial. La ECD debe informar al suscriptor, con anticipación, acerca de la información que pretende poner a disposición del público.

10.2.5.2. Cuando se exige a la ECD, por ley o autorización en las disposiciones contractuales, la divulgación de información confidencial, el suscriptor o la persona implicada debe, a menos que lo prohíba la ley, ser notificada de la información suministrada.

10.2.5.3. La información acerca del suscriptor obtenida en fuentes diferentes del suscriptor (por ejemplo, de un reclamante o de los reguladores) debe ser tratada como confidencial.

10.2.6. INFORMACIÓN DISPONIBLE AL PÚBLICO

La ECD debe mantener (a través de publicaciones, medios electrónicos u otros medios) y poner a disposición según solicitud, la siguiente información:

a) información sobre los servicios de certificación digital acreditados por ONAC, incluyendo los procedimientos de revisión, las reglas y los procedimientos para otorgar y mantener, el alcance de la certificación, o para cancelar o negar la certificación digital;
b) descripción de los derechos y deberes de solicitantes y suscriptores, que incluya requisitos, restricciones o limitaciones del uso del nombre de la ECD y de la marca de certificación, y sobre la manera de hacer referencia a la certificación digital otorgada;
c) información sobre los procedimientos para el manejo de reclamos y apelaciones.

10.3. REQUISITOS ESTRUCTURALES

10.3.1. ESTRUCTURA ORGANIZACIONAL Y ALTA DIRECCIÓN

10.3.1.1. Las actividades de certificación digital deben estar estructuradas y gestionadas de manera que salvaguarden la imparcialidad, la accesibilidad al servicio y la confidencialidad

10.3.1.2. La ECD debe documentar su estructura organizacional indicando los deberes, las responsabilidades y las autoridades de la dirección, y de todo el personal involucrado en el servicio de certificación digital y de todos los comités. Cuando la ECD es una parte definida de una entidad legal, la estructura debe incluir la línea de autoridad y la relación con otras partes dentro de la misma ECD.

10.3.1.3. La estructura de dirección de la ECD debe identificar la junta directiva, el representante legal, el responsable de la alta dirección, el grupo de personas o la persona con autoridad y responsabilidad total de cada una de las siguientes actividades:

a) desarrollo de políticas relacionadas con la operación de la ECD;
b) supervisión de la implementación de las políticas y los procedimientos;
c) supervisión de las finanzas de la ECD;
d) desarrollo de las actividades de certificación digital;
e) desarrollo de los requisitos de la certificación digital;
f) revisión (véase 10.5.3);
g) decisiones sobre la certificación digital (véase 10.5.5);
h) delegación de la autoridad en los comités o el personal, según se requiera, para emprender a su nombre las actividades definidas;
i) disposiciones contractuales;
j) suministro de los recursos adecuados para las actividades de certificación digital;
k) respuesta a reclamos y apelaciones;
l) requisitos de competencia del personal;
m) sistemas de gestión de la ECD (véase sección 10.6).

10.3.1.4. La Entidad de Certificación Digital debe tener reglas formales para la asignación, los términos de referencia y la operación de los comités involucrados en el proceso de certificación digital (véase sección 10.5). Tales comités no deben tener presiones de tipo comercial, financiero u otras que puedan influir en las decisiones. La ECD debe conservar la autoridad de asignar o retirar a los miembros de tales comités.

10.3.2. MECANISMO PARA SALVAGUARDAR LA IMPARCIALIDAD

10.3.2.1. La ECD, debe definir el mecanismo de gestión de riesgos para salvaguardar su imparcialidad, asegurar la eficacia del mismo y cumplir los requisitos en este numeral, preferiblemente sustentada en la norma ISO 31000. El mecanismo debe proveer elementos de entrada sobre:

a) las políticas y los principios relacionados con la imparcialidad de sus actividades de certificación digital;
b) consideraciones comerciales u otras que eviten la realización imparcial de las actividades de certificación digital;
c) temas que afecten a la imparcialidad y la confianza en la certificación digital, incluyendo la apertura.

NOTA 1: Se pueden asignar otras tareas y deberes (por ejemplo, tomar parte en el proceso de toma de decisiones) al mecanismo, siempre que dichas tareas y deberes no comprometan su papel principal en la preservación de la imparcialidad.

NOTA 2: Un posible mecanismo puede ser un comité que establecen uno o más organismos de certificación digital, una autoridad gubernamental o una parte equivalente.

NOTA 3: Un solo mecanismo para varios servicios de certificación digital puede satisfacer este requisito.

El mecanismo debe estar documentado formalmente para garantizar acceso a toda la información necesaria para poder llevar a cabo todas sus funciones.

10.3.2.2. Si la alta dirección de la Entidad de Certificación Digital no tiene en cuenta las recomendaciones del mecanismo mencionado, el mecanismo debe permitir a cualquier parte involucrada a emprender acción independiente (por ejemplo, informando a las autoridades, los organismos de acreditación, las partes involucradas). Al emprender la acción adecuada, se deben respetar los requisitos de confidencialidad establecidos en 10.2.5 con respecto al suscriptor y a la Entidad de Certificación Digital.

No se deben seguir las recomendaciones que estén en conflicto con los procedimientos operativos de la Entidad de Certificación Digital o con otros requisitos obligatorios. La dirección debe documentar la justificación tras la decisión de no cumplir con estos elementos y conservar el documento para su revisión por parte del personal correspondiente.

10.3.2.3. Aunque en el mecanismo pueden no estar representados todos los intereses, la ECD debe identificar e invitar a las partes interesadas significativas.

NOTA 1: Dichas partes interesadas pueden incluir a suscriptores de la ECD, usuarios de los suscriptores, fabricantes, proveedores, usuarios, expertos en evaluación de la conformidad, representantes de los gremios industriales, representantes de los organismos reguladores del gobierno u otros servicios gubernamentales, y representantes de organizaciones no gubernamentales, incluyendo a las organizaciones de consumidores. Puede ser suficiente tener un representante de cada parte interesada en el mecanismo.

NOTA 2: Estos intereses pueden estar limitados, dependiendo de la naturaleza del servicio de certificación digital.

10.4. REQUISITOS PARA LOS RECURSOS

10.4.1. PERSONAL DE LA ECD

10.4.1.1. Generalidades

10.4.1.1.1. La ECD debe emplear y demostrar que cuenta con capacidad operativa suficiente de personal para cubrir sus operaciones relacionadas con los servicios de certificación digital, las normas y otros documentos normativos aplicables.

El personal que trabaja normalmente para la ECD, debe tener un contrato legal que lo ubique dentro del control y los sistemas/procedimientos de gestión de la ECD (véase 10.4.1.3).

10.4.1.1.2. El personal debe ser competente para realizar las funciones que desempeña.

10.4.1.1.3. El personal, incluyendo a los miembros de los comités, el personal de organismos externos o el personal que actúa a nombre de la ECD, debe mantener la confidencialidad de toda información obtenida o creada durante la ejecución de las actividades de certificación digital, con la excepción de lo exigido por la ley o por el servicio de certificación digital.

10.4.1.2. Gestión de la competencia para el personal involucrado en el proceso de certificación digital

10.4.1.2.1. La ECD debe establecer, implementar y mantener un procedimiento para la gestión de las competencias del personal que participa en el proceso de certificación digital (véase sección 10.5). El procedimiento debe exigir a la ECD que:

a) determine los criterios para la competencia del personal para cada función en el proceso de certificación digital, tomando en consideración los requisitos de los servicios de certificación digital;
b) identifique las necesidades de entrenamiento y suministre, según necesidad, programas de entrenamiento sobre procesos de certificación digital, requisitos, metodologías, actividades y otros requisitos pertinentes del servicio de certificación digital;
c) demuestre que el personal tiene las competencias requeridas para los deberes y las responsabilidades que ellos acometen;
d) autorice formalmente al personal para las funciones en el proceso de certificación digital;
e) monitoree el desempeño del personal.

10.4.1.2.2. La ECD debe mantener los siguientes registros sobre el personal involucrado en el proceso de certificación digital (véase sección10.5):

a) nombre y dirección;
b) cargo que desempeña;
c) cualificación educativa y estatus profesional;
d) experiencia y entrenamiento;
e) evaluación de la competencia;
f) monitoreo del desempeño;
g) autorizaciones que tiene dentro de la Entidad de Certificación Digital y su vigencia;
h) fecha de la actualización más reciente de cada registro.

10.4.1.3. Contrato con el personal

La ECD debe exigir al personal involucrado en el proceso de certificación digital que firmen un contrato u otro documento de vinculación contractual mediante el cual se comprometa a:

a) cumplir con la reglas definidas por la ECD, incluyendo las relacionadas con la confidencialidad (véase 10.2.5) y su independencia de intereses comerciales y otros;
b) declarar toda asociación previa y/o actual de su parte, o de parte de su empleador, con:
    1) un proveedor o diseñador de productos, o
    2) un prestador o desarrollador de servicios, o
    3) un operador o desarrollador de procesos para la verificación o certificación a la cual van a ser asignados;
c) revelar toda situación que conozcan que le pueda representar a ellos o a la ECD un conflicto de intereses (véase 10.2.2).

Las ECD deben usar esta información como elemento de entrada para identificar los riesgos para la imparcialidad derivados de las actividades de dicho personal o por las organizaciones que los emplean (véase 10.2.2.3).

10.4.2. RECURSOS PARA LA SUBCONTRATACIÓN

10.4.2.1. En caso que la ECD acuda a lo dispuesto en los artículos 43 y 44 de la Ley 527 de 1999, únicamente lo podrá hacer con organismos que demuestren cumplir con los requisitos exigidos por ONAC a las ECD, establecidos en este documento; es decir los requisitos exigidos a las ECD son aplicables a los terceros, de manera tal que brindan confianza en los resultados, y que los registros están disponibles para justificar la confianza. La ECD no podrá subcontratar actividades diferentes a servicios de data center y las contempladas en los mencionados artículos de la Ley 527 de 1999.

10.4.2.2. La ECD debe tener un contrato legalmente vinculante con el organismo que suministra el servicio subcontratado, que incluya la confidencialidad y el conflicto de intereses, tal como se especifica en 10.4.1.3, literal c).

10.4.2.3. La ECD debe:

a) Ser responsable de todas las actividades subcontratadas con otro organismo;
b) Garantizar que el organismo que presta los servicios subcontratados y el personal que éste organismo utiliza no están involucrados, directamente ni a través de otro empleador de tal manera que la credibilidad e imparcialidad de los resultados pueda verse comprometida;
c) Tener políticas, procedimientos y registros documentados para la calificación, evaluación y monitoreo de todos los organismos que prestan servicios subcontratados utilizados para las actividades y servicios de certificación digital;
d) Mantener una lista de los proveedores de actividades subcontratadas por la ECD;
e) Implementar acciones correctivas para cualquier incumplimiento del contrato que se indica en 10.4.2.3 u otros requisitos en 10.4.2.2 del cual tenga conocimiento;
f) Informar al suscriptor con anticipación acerca de las actividades de subcontratación con el fin de brindarle la oportunidad de objetar.

NOTA: Si la evaluación y el monitoreo de las organizaciones que prestan las actividades a ser subcontratadas se llevan a cabo por parte de otras entidades (por ejemplo, por organismos de acreditación, organismos de evaluación de pares o autoridades gubernamentales), la ECD puede tomar en consideración el resultado de esta evaluación siempre que:
- tales servicios se presten según los requisitos del servicio de certificación digital;
- el alcance es aplicable al trabajo que se está realizando;
- la validez de las disposiciones para la evaluación y monitoreo se verifican con una periodicidad determinada por la ECD.

10.5. REQUISITOS DEL PROCESO - CICLO DE VIDA DEL CERTIFICADO DIGITAL

10.5.1. GENERALIDADES

10.5.1.1. Los servicios de certificación digital del alcance de acreditación de la ECD deben ser estructurados con una o más actividades de certificación digital y uno o más requisitos técnicos.

10.5.1.2. Los requisitos frente a los cuales se verifican los certificados digitales de un suscriptor deben ser aquellos que se encuentran en la DPC y PC.

10.5.1.3. Si se requieren explicaciones sobre la aplicación de la DPC y PC para un servicio de certificación digital específico, éstas deben ser formuladas por las personas pertinentes e imparciales o por los comités que tengan la competencia técnica necesaria, y la ECD debe ponerlas a disposición según solicitud.

10.5.2. SOLICITUD

En el caso de la solicitud, la RA debe obtener toda la información necesaria de acuerdo con el servicio de certificación digital establecido en la DPC y PC.
La información necesaria para la solicitud del servicio de certificación digital debe corresponder con la naturaleza y el tipo de servicio de certificación digital solicitado, de conformidad con lo definido en el documento de Declaración de Prácticas de Certificación Digital DPC y Políticas de certificados PC.
La información debe incluir, al menos, la siguiente

a) El servicio de certificación digital solicitado.
b) Las normas y/u otros documentos normativos para los cuales el solicitante busca la certificación digital (véase 10.5.1.2);
c) Los datos generales del solicitante, incluyendo su nombre, domicilio y todos los requisitos legales ;
d) Información general con respecto al solicitante, para el servicio de certificación digital para el cual se presenta la solicitud, de acuerdo con lo establecido en la DPC y las PC;

La ECD debe establecer los medios y mecanismos para recolectar esta información en diversos momentos, por ejemplo un formulario de solicitud.

10.5.3. REVISIÓN DE LA SOLICITUD

10.5.3.1. La RA debe ejecutar la revisión de la información obtenida (véase 10.5.2) con el fin de garantizar que:

a) La información acerca del solicitante es suficiente para realizar el proceso de certificación digital;
b) Se resuelve cualquier diferencia de entendimiento conocida entre la ECD y el solicitante, incluyendo el acuerdo con respecto a la DPC, documentos normativos u otros documentos reglamentarios;
c) Se define el alcance del servicio de certificación digital solicitado;
d) Se dispone de los medios para realizar todas las actividades de verificación;
e) La ECD tiene la competencia y la capacidad para llevar a cabo la actividad y servicios de certificación digital.
f) La ECD debe declinar una solicitud de un servicio de certificación digital, si el mismo no se encuentra en el alcance de la acreditación que le fue otorgado por ONAC.

10.5.4. REVISIÓN

10.5.4.1. La ECD debe asignar la función de la revisión a la RA para que revise toda la información.

10.5.4.2. El proceso y los resultados relacionados con la revisión deben estar documentados.

10.5.4.3. Las recomendaciones para la decisión sobre la certificación con base en la revisión deben estar documentadas.

10.5.5. DECISIÓN SOBRE LA CERTIFICACIÓN DIGITAL

10.5.5.1. La ECD debe ser responsable de sus decisiones relacionadas con la certificación digital.

10.5.5.2. La ECD para sus servicios de certificación digital, debe asegurar independencia e imparcialidad entre la funciones de revisión y de decisión de la certificación.

10.5.5.3. La persona o personas asignadas por la ECD para tomar la decisión sobre la certificación digital, deben ser empleadas o estar bajo otro tipo de contrato con uno de los siguientes entes:

a) La ECD (véase 10.4.1);
b) Una entidad bajo el control organizacional de la ECD (véase 10.5.5.4).

10.5.5.4. El control organizacional por parte de la ECD debe corresponder a uno de los siguientes:

- Propiedad total o mayoritaria de otra entidad por parte de la ECD;
- Participación mayoritaria por parte de la ECD en la junta directiva de otra entidad;

- Autoridad documentada de la ECD sobre otra entidad en una red de entidades legales (a la cual pertenece la ECD ya sea privada o pública), vinculada por propiedad o por el control de la junta directiva.

Nota: En el caso de las ECD gubernamentales, se puede considerar que otras partes del mismo gobierno están "vinculadas por propiedad" a la ECD.

10.5.5.5. Las personas empleadas o con otro tipo de contrato en entidades bajo el control organizacional de la ECD deben tener autoridad documentada.

10.5.5.6. La ECD debe notificar a los suscriptores las razones de la decisión de no otorgar la certificación digital.

10.5.6. DOCUMENTACIÓN DE LA CERTIFICACIÓN DIGITAL

10.5.6.1. La ECD debe suministrar al suscriptor la documentación formal de servicios de certificación digital que adquirió de forma que indique claramente el contenido del certificado digital y lo establecido en las DPC y PC, según servicios de certificación.

a) El nombre y la dirección de la ECD;
b) La fecha en que se otorga la certificación digital (esta fecha no debe ser anterior a la fecha en la cual se tomó la decisión sobre la certificación digital);
c) El nombre y la dirección del suscriptor;
d) El alcance de la certificación digital;
e) El término o la fecha de expiración de la certificación digital;
f) Toda otra información exigida para el servicio de certificación.

10.5.6.2. La documentación formal de la certificación digital debe incluir la firma de a quienes la ECD le ha asignado la responsabilidad de recibo, verificación y archivo.

10.5.6.3. La documentación formal de la certificación digital únicamente se puede emitir después o simultáneamente con las siguientes actividades:

a) Cuando se ha tomado la decisión de otorgar el alcance de la certificación digital (véase 10.5.6.1);
b) Se ha completado/firmado el acuerdo de Certificación Digital (véase 10.2.1.2).

10.5.7. DISPONIBILIDAD DE LA LISTA DE CERTIFICADOS REVOCADOS

En el caso del servicio de certificación digital, la ECD debe publicar y mantener la lista de certificados revocados en la CRL con una disponibilidad de consulta en línea 7x24x365, 99.9% uptime por año. Para Entidades de Certificación Cerradas corresponde como mínimo al 95% uptime por año.

10.5.8. CAMBIOS QUE AFECTAN LA CERTIFICACIÓN DIGITAL

10.5.8.1. Cuando el servicio de certificación digital introduce requisitos nuevos que afectan al suscriptor o al servicio de certificación digital, la ECD debe garantizar que estos cambios son comunicados a todos los suscriptores y a ONAC. La ECD debe verificar la implementación de los cambios y debe emprender las acciones exigidas por el servicio de certificación digital.

NOTA: En las DPC se establecen las disposiciones contractuales con los suscriptores para garantizar la implementación de estos requisitos.

10.5.8.2. La ECD debe considerar cualquier cambio que afecta a la certificación digital, incluyendo los indicados por el suscriptor, y debe decidir sobre la acción a seguir. Los cambios que afectan la certificación digital pueden incluir información nueva relacionada con el cumplimiento de los requisitos de la acreditación obtenida por la ECD después de haber establecido los servicios de certificación digital.

10.5.8.3. Todo cambio que las ECD pueden llegar a tener que implementar en su infraestructura PKI que afecte la certificación digital y por ende a sus suscriptores, debe ser avisado a los suscriptores y anunciado con anterioridad a ONAC de acuerdo al R-AC-01, para determinar necesidades de evaluación adicional; así como también la ECD debe informar las acciones que determine pertinentes.

10.5.9. REVOCACIÓN DE LA CERTIFICACIÓN DIGITAL

10.5.9.1. Una certificación digital debe tener establecido en su DPC las reglas para revocar ya sea por solicitud del suscriptor, o cuando la ECD conoce tiene indicios o confirmación de alguna de las siguientes situaciones:

- Por compromiso de la seguridad en cualquier motivo, modo, situación o circunstancia.
- Por muerte o incapacidad sobrevenida del suscriptor.
- Por liquidación de la persona jurídica representada que consta en el certificado digital
- Por la confirmación de que alguna información o hecho contenido en el certificado digital es falso.
- Por la ocurrencia de hechos nuevos que provoquen que los datos originales no correspondan a la realidad.
- Por orden judicial o de entidad administrativa competente.
- Por pérdida, inutilización del certificado digital que haya sido informado a la ECD.
- Por la terminación del contrato de suscripción, de conformidad con las causales establecidas en el contrato.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la confiabilidad del certificado digital.
- Por el manejo indebido por parte del suscriptor del certificado digital.
- Por el incumplimiento del suscriptor o de la persona jurídica que representa o a la que está vinculado a través del Contrato del Servicio de Certificación Digital proporcionado por la ECD.

10.5.9.2. En caso que se revoque un certificado digital, posteriormente el mismo NO podrá ser rehabilitado por la ECD.

10.5.9.3. Para cualquier cambio de estado de un certificado digital, la ECD debe establecer en la DPC las condiciones e informar al suscriptor sobre las decisiones tomadas.

10.5.9.4. Cuando las acciones a seguir respecto al cambio de estado de un certificado digital, incluyen la revisión o decisión sobre la certificación digital, se deben cumplir los requisitos de 10.5.5 o 10.5.6 respectivamente.

10.5.10. REGISTROS

10.5.10.1. La ECD debe conservar registros que demuestren que se han cumplido eficazmente todos los requisitos del proceso de certificación digital (los de este documento y los de los servicios de certificación digital).

10.5.10.2. La ECD debe garantizar la confidencialidad de los registros en cualquier instancia del servicio de certificación digital. Los registros se deben transportar, transmitir, transferir y conservar de manera que se garantice la confidencialidad (véase también 10.2.5) y protección de datos.

10.6. REQUISITOS DEL SISTEMA DE GESTIÓN

La ECD debe establecer y mantener un sistema de gestión que sea capaz de lograr el cumplimiento de los requisitos del presente documento CEA, el *"Artículo 11 del Decreto 333 de 2014. Infraestructura y recursos, establece: En desarrollo de lo previsto en el literal b) del artículo 29 de la Ley 527 de 1999, la entidad de certificación deberá contar con un equipo de personas, una infraestructura física, tecnológica y unos procedimientos y sistemas de seguridad, tales que: 1. Puedan generar las firmas digitales y electrónicas propias y que además, les permita prestar todos los servicios para los que soliciten la acreditación…"*. La ECD debe realizar el aseguramiento de la calidad de los servicios de certificación digital acreditados.

El sistema de gestión de la ECD, debe cumplir como mínimo con los siguientes aspectos:

1. Documentación general del sistema de gestión (manuales, políticas, procedimientos, definición de responsabilidades, etc.);
2. Control de documentos;
3. Control de registros;
4. Auditoría interna;
5. Revisión por la dirección;
6. Acciones correctivas;
7. Acciones preventivas.
8. Quejas, Reclamos y Apelaciones.

Adicionalmente, la ECD debe demostrar la implementación del modelo de gestión de calidad PHVA (Planear, Hacer, Verificar y Actuar), para cada uno de los servicios de certificación digital que solicita en el alcance de la acreditación.

Para cada servicio de certificación digital, la ECD debe definir como mínimo lo siguiente:

1. Alcance del servicio de certificación digital
2. Planificación de la realización
3. Procesos relacionados con el cliente
4. Caracterización de los servicios
5. Diseño y desarrollo del servicio
6. Medición, seguimiento y validación del servicio
7. Aseguramiento de la calidad del servicio
8. Proceso de aceptación
9. Control de cambios
10. Producción y modelo de prestación del servicio

La caracterización de los procesos y servicios de certificación debe contener como mínimo:

1. Nomenclatura, versión y fecha de última actualización
2. Objeto
3. Roles y responsables.
4. Proveedores e insumos, o entradas y productos, o salidas y usuarios o clientes.
5. Recursos asociados a la gestión del proceso.
6. Riesgos y controles asociados e indicadores del proceso.
7. Requisitos relacionados con el proceso y documentos y registros del mismo.
8. Flujograma del proceso o servicio.

10.6.1. QUEJAS, RECLAMOS Y APELACIONES

10.6.1.1. La ECD debe tener un procedimiento documentado para recibir, evaluar y tomar decisiones acerca de las quejas, reclamos y las apelaciones. Debe registrar y rastrear las quejas, reclamos y las apelaciones, así como las acciones que se han emprendido para resolverlas.

10.6.1.2. La ECD debe registrar y confirmar si un reclamo o una apelación se relaciona con las actividades de certificación digital de las cuales es responsable y, si es así, debe tratarlas y dar respuesta.

10.6.1.3. La ECD debe ser responsable de reunir y verificar toda la información necesaria para alcanzar una decisión sobre la queja, reclamo o la apelación.

10.6.1.4. La decisión que resuelve la queja, reclamo o la apelación debe ser tomada, revisada y aprobada por personas que no estén involucradas en las actividades de certificación digital relacionadas con el reclamo o la apelación.

10.6.1.5. Siempre, la ECD debe suministrar al reclamante una notificación formal sobre el resultado y la finalización del proceso de reclamación.

10.6.1.6. La ECD debe suministrar al apelante una notificación formal del resultado y la finalización del proceso de apelación.

10.6.1.7. La ECD debe emprender las acciones posteriores necesarias para resolver el reclamo o la apelación.

10.7. DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)

Las ECD deben definir la Declaración de Prácticas de Certificación (DPC), acogidas a las leyes Colombianas, a las disposiciones de los entes reguladores y al estándar RFC 3647 o el estándar que lo reemplace o actualice.

La DPC, además de incluir las disposiciones reglamentarias, debe incluir como mínimo los siguientes requisitos:

1. La identificación de la ECD debe tener: nombre, razón o denominación social de la entidad, NIT, número de matrícula de cámara de comercio, certificado de existencia y representación legal y estado activo en Cámara de Comercio, domicilio social y de correspondencia, teléfono, fax, dirección de correo electrónico y la oficina responsable dentro de la ECD de las peticiones, consultas y reclamos de los suscriptores y usuarios. Si la ECD tiene entidades subordinadas o subcontratadas, involucradas en el alcance de la acreditación, debe incluir esta misma información respecto de cada una de ellas.
2. La política de manejo de los certificados, debe tener:
   a. Los requisitos de los servicios de certificación digital, requisitos internos de la ECD, y el procedimiento de expedición de certificados, los procedimientos de identificación del suscriptor y de las Entidades recíprocas, de acuerdo con lo previsto en el artículo 43 de la Ley 527 de 1999.
   b. Los tipos de certificados (según políticas de certificados) y servicios que ofrece,
   c. El procedimiento para la actualización de la información contenida en los certificados.
   d. El procedimiento, las verificaciones, la oportunidad y las personas que podrán invocar las causales de revocación de los certificados.
   e. La Información sobre el sistema de seguridad para proteger la información que se recopila con el fin de expedir los certificados.
3. El manejo de la información que se obtiene de los suscriptores de acuerdo a las normas aplicables en la materia, detallando:
   a. El manejo de la información de naturaleza confidencial.
   b. Los eventos en que se revelará la información confidencial dada por el suscriptor, de acuerdo con las normas vigentes.
4. Las garantías que ofrece la entidad para el cumplimiento de las obligaciones que se deriven de sus actividades y los clausulados de los seguros que protegen a los terceros por los perjuicios que pueda causar la entidad y/o los reglamentos de los contratos de fiducia constituidos para el efecto.
5. El procedimiento de seguridad para el manejo de incidentes debe cumplir con el anexo A de la norma ISO/IEC 27001. Entre otros eventos que debe registrar están:

a. Cuando la seguridad de la llave privada de la entidad de certificación se ha visto comprometida.
b. Cuando el sistema de seguridad de la entidad de certificación ha sido vulnerado.
c. Cuando se presenten fallas en el sistema de la entidad de certificación que comprometan la prestación del servicio.
d. Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratado por el suscriptor.
e. Cuando se presente cualquier otro evento o incidente de seguridad de la información.

6. La ECD debe Informar que se tiene establecido y probado el plan de continuidad y contingencia encaminado a garantizar la continuidad del servicio de certificación, en caso de que ocurra algún evento que comprometa la prestación del servicio.
7. La ECD debe informar 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.
8. La ECD debe informar y presentar las políticas y procedimientos para resolver las quejas, apelaciones y disputas recibidas de las partes relacionadas.
9. La ECD debe Informar a los consumidores y al público en la página web principal de la ECD, las actividades y servicios acreditados atendiendo a lo establecido en el documento R-AC-1.4-03 de ONAC.
10. La ECD debe Informar a los consumidores y al público en la página web principal de la ECD, la información general de la ECD como lo es naturaleza, tipo de empresa, etc.
11. Es responsabilidad de la ECD, informar a sus proveedores y ECD recíproca, que hace extensivo el cumplimiento de los requisitos de este documento a ellos, cuando les corresponda.

10.8. POLITICAS DE CERTIFICADOS (PC)

La ECD debe definir o utilizar una o varias políticas para cada uno de sus servicios de certificación digital, generados a través de las actividades desarrolladas por la ECD, detallando: deberes, derechos, condiciones comerciales, independencia e imparcialidad de la ECD, acogidas a las leyes Colombianas y entes reguladores (Literal i, Artículo 32 de la ley 527 de 1999). Estas políticas podrán formar parte de la DPC.

Las PC, además de incluir las disposiciones reglamentarias y legales, deben acoger las recomendaciones de RFC 3647 e incluir como mínimo los siguientes requisitos:

1. Las obligaciones de la ECD y de los suscriptores del certificado digital y las precauciones que deben observar los terceros que confían en el certificado digital.
2. La información que se le va a solicitar a los suscriptores.
3. Los límites de responsabilidad de la ECD en cada uno de sus servicios y por cada documento firmado.
4. La vigencia de cada uno de los tipos de certificados digitales.
5. Las tarifas de expedición de certificados y los servicios que incluyen. No aplica para las ECD cerradas.
6. Modelos y minutas de los contratos de suscripción que utilizará la ECD para la prestación de sus servicios de certificación digital. En caso de prever su existencia, texto de las cláusulas compromisorias que establezcan el procedimiento jurídico para la resolución de conflictos, especificando como mínimo la jurisdicción y ley aplicable en el caso en que alguna de las partes no tenga domicilio en el territorio colombiano.
7. Requisitos de los servicios de certificación digital: Acorde a los entes reguladores, las ECD deben publicar las políticas específicas que establecen los requisitos y fuente reguladora para prestar cada uno de los servicios de certificación digital.

8. La ECD en la PC debe informar los dispositivos criptográficos admitidos que ofrece, los riesgos asociados, y los compromisos de seguridad que contiene.

Tanto la Declaración de prácticas de certificación (DPC) como las Políticas de Certificados (PC), deben estar elaboradas con base en RFC 3647: Política de Certificados y Prácticas de Certificación Framework, y estar disponibles desde el "home page" o página web de la ECD.

10.9. REQUISITOS DE LA AUTORIDAD DE CERTIFICACIÓN (CA)

La ECD mantendrá controles necesarios para proporcionar seguridad tal que:

1. La seguridad se planea y gestiona, está dirigida para apoyar la CA y todos las partes relacionadas;
2. Los riesgos son identificados y gestionados con eficacia;
3. Gestiona los activos de información;
4. La seguridad de las instalaciones y del entorno físico de CA, sistemas y activos de información accedido por terceros se mantiene;
5. La seguridad de la información se mantiene cuando la responsabilidad de las funciones de CA han sido subcontratas a otra organización o entidad.

La ECD deberá mantener controles necesarios para:

1. Ceremonia de generación de la CA raíz
2. Logs de la CA y Bitácora de trabajo debidamente autorizada
3. Generación de las claves de la CA
4. Almacenamiento, copias de seguridad y recuperación de las claves de la CA
5. Distribución de la Llave pública de la CA
6. Uso de la Clave de la CA
7. Destrucción de la clave de la CA y de todas sus copias de seguridad con el registro de destrucción y su almacenamiento
8. Archivo de claves de la CA
9. Mantener offline o apagada la CA raíz
10. Debe ser un dispositivo criptográfico certificado para la CA raíz. ver anexo F.

Para el cumplimiento de estos objetivos de control, la ECD, debe implementar los requisitos técnicos admitidos (10.11) y vigentes, la norma internacional ISO/IEC 27001, los requisitos de aseguramiento (10.11.7) de éste documento, otras normas de referencia de mejores prácticas, y estándares técnicos reconocidos internacionalmente para la infraestructura de llave publica - PKI.

Una vez que las solicitudes han sido validadas y autorizadas por parte de la RA (autoridad de registro), la siguiente etapa correspondiente al ciclo de vida del certificado, es la generación del mismo, a cargo de la CA. Este proceso implica los siguientes pasos:

1. La CA recibe la solicitud de certificación previamente validada por la RA.
2. El certificado es armado por un dispositivo de firma que contiene la llave privada de la CA.

10.10. REQUISITOS AUTORIDAD DE REGISTRO (RA)

10.10.1. Requisitos de la RA:

1. Para las ECD cerradas, una RA debe ser un Departamento, División o Área de la misma ECD. Cuando se trate de un conglomerado de Empresas, la RA será una organización, persona jurídica independiente e imparcial, para ambos casos, independiente de las funciones administrativas, comerciales y técnicas de la ECD.
2. Para una ECD abierta, la función de RA la debe ejercer un departamento interno o externo, independiente al departamento técnico encargado de la administración técnica de la CA quien emite los certificados.
3. Una vez la RA ha verificado la documentación y tiene plena certeza que el solicitante es quien dice ser (Autenticación Exitosa), la RA debe remitir la solicitud a quienes deciden sobre el otorgamiento del certificado digital para garantizar la imparcialidad.
4. Cuando se toma la decisión de otorgar el certificado digital y ésta se encuentra documentada, se procede a realizar la inscripción a la CA para generar el certificado digital respectivo.
5. De acuerdo con las tablas de retención documental acordes a las regulaciones vigentes Artículo 38 Ley 527 de 1999, la RA debe custodiar todas las solicitudes y mantener la trazabilidad sobre la gestión de los certificados digitales.
6. La infraestructura de llaves públicas de la ECD, debe garantizar plenamente dicha independencia entre la RA y la CA.
7. Normalmente la RA podrá estar expuesta en INTERNET, para que el solicitante pueda interactuar con ella, sin embargo deben existir controles que garanticen la prestación del servicio.
8. La conexión entre la RA y la CA debe estar protegida, de modo que se garantice la confidencialidad y autenticación. Por ejemplo por SSL o TLS, entre otros métodos o protocolos seguros establecidos y validados.
9. La RA debe utilizar su certificado para identificarse a la entidad emisora (CA). Para la autorización, la autoridad competente comprobará si la RA pertenece a un grupo de su sistema de la RA en la ECD.
10. La RA debe confirmar que el certificado cumple la política de certificación y que está en consonancia con lo especificado en las prácticas de certificación.

10.10.2. Roles de la RA:

La RA debe soportar como mínimo los siguientes roles, los cuales no podrán ser desempeñados por la misma persona dentro del área o empresa designada:

1. Agentes de la RA: Usuarios de la RA con privilegios. Son responsables por las operaciones diarias, tales como la aprobación de solicitudes.
2. Register Administrador: La persona responsable por instalar y configurar la RA.
3. System auditor: Auditor

10.11. REQUISITOS TÉCNICOS

Los requisitos técnicos para en el entorno de infraestructura de llave pública – PKI, deben mantener el principio de neutralidad tecnológica y vigencia. Los requisitos técnicos pierden vigencia una vez se establezca que está comprometida la seguridad, o son declarados obsoletos, por lo que la ECD debe informar a ONAC y debe reemplazar por una nueva versión u otro estándar o componente, que no comprometa la seguridad y se encuentre vigente.

10.11.1. CONTENIDO DE LOS CERTIFICADOS

Los certificados deben cumplir con los requisitos exigidos en artículo 35 de la ley 527 de 1999, deben contener los requisitos del estándar ITU X-509 y como mínimo lo siguiente:

1. Nombre, dirección y domicilio del suscriptor.
2. Una Identificación única del suscriptor nombrado en el certificado
3. El nombre y el lugar donde realiza actividades la CA.
4. Llave pública del certificado.
5. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
6. El número de serie (único) del certificado.
7. Fecha de emisión y expiración del certificado.

La ECD debe remitir a ONAC, con frecuencia anual, para la realización de la etapa 1 de cada evaluación de la acreditación:

1. Archivo con los certificados emitidos y la información citada del 1 al 7 de este numeral.
2. Archivo con totales de control (emitidos, vigentes, revocados y expirados).

La información debe estar en medio magnético cd o dvd, con copia, en archivo txt, que contenga esta información, con títulos de campos y separados por punto y coma (;).

10.11.2. SUSPENSIÓN PARCIAL O TEMPORAL DEL SERVICIO

Conforme con lo dispuesto en el literal d) del artículo 32 de la ley 527 de 1999, la ECD no podrá suspender el servicio de la CRL, es decir debe cumplir una disponibilidad (uptime) del 99.9% 7x24x365 al año para la CRL. Para Entidades de Certificación Cerradas corresponde como mínimo al 95% uptime por año.

Para el resto de la plataforma tecnológica de PKI que requiera interrupciones por mantenimiento o actualización, la ECD debe informar a ONAC con anticipación de un mes, adjuntando el plan de trabajo, y posteriormente entregar el resultado frente a lo esperado después del trabajo realizado. En ningún caso la disponibilidad para el resto de la plataforma tecnológica de PKI podrá ser inferior al 95% de uptime por año. ONAC con la información recibida, determinará la necesidad de realizar una evaluación extraordinaria. Las ECD cerradas podrán definir porcentajes de disponibilidad diferentes, los cuales deben estar establecidos como acuerdos de niveles de servicio en la DPC.

10.11.3. CESACIÓN DE ACTIVIDADES DE LA ECD

Conforme con lo dispuesto en el artículo 163 del decreto 19 de 2012 que modifica el artículo 34 de la ley 527 de 1999, las ECD acreditadas por ONAC *"pueden cesar en el ejercicio de actividades, siempre y cuando garanticen la continuidad del servicio de certificación digital a quienes ya lo hayan contratado, directamente o a través de terceros, sin costos adicionales a los servicios ya cancelados".* Las ECD deberán informar 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

En concordancia de lo anterior, la ECD debe tener.

1. Un plan de continuidad del servicio.
2. Un plan que garantice la continuidad en alta disponibilidad de la publicación en los repositorios (CRL) propios.
3. La ECD debe tener un plan de seguridad que garantice la adecuada destrucción de la llave privada de la entidad.

La ECD debe cumplir los planes anteriores, mantener la documentación y registros de pruebas anuales en su sede principal y accesible a ONAC.

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

1. La terminación de su actividad o actividades y la fecha precisa de cesación.
2. Las consecuencias jurídicas de la cesación respecto de los certificados expedidos.
3. La posibilidad de que un suscriptor obtenga el reembolso equivalente al valor del tiempo de vigencia restante del certificado.
4. La autorización emitida por la Superintendencia de Industria y Comercio para que la ECD pueda cesar el servicio, y si es el caso, el operador de la CRL responsable de la publicación de los certificados emitidos por la ECD, 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 (2) meses siguientes a la segunda publicación.

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

10.11.4. ESTÁNDARES TÉCNICOS ADMITIDOS.

De acuerdo con lo indicado en la Ley 527 de 1999, Artículo 2, literal d), ECD: "*es aquella persona que, autorizada conforme a la presente ley, está facultada para prestar servicios de certificación digital en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.*"
De acuerdo con lo anterior, la ECD para prestar los servicios de certificación digital debe seleccionar o combinar cualquiera de las actividades citadas en el Artículo 161 del Decreto 19 de 2012, y debe asegurar el debido cumplimiento de los requisitos y estándares técnicos seleccionados o combinados de los siguientes anexos:

1. Actividades 1 3, 4 y 6 Clasificadas como: Servicio de emisión de certificados digitales. Ver anexo A
2. Actividad 2, y 9. Clasificada como: Servicios de generación y verificación de firmas digitales. Ver anexo B
3. Actividad 5. Clasificada como: Servicios de estampado cronológico. Ver anexo C
4. Actividades 7 y 8. Clasificadas como: Archivo, registro, conservación, custodia y anotación para los documentos electrónicos transferibles y mensajes de datos. Ver anexo D
5. Mecanismos de validación del estado del certificado Ver anexo E
6. Dispositivos criptográficos. Ver anexo F

Nota 1: Debe entenderse que si un estándar o un componente se encuentra actualizado por una nueva versión o reemplazado por otro estándar, es obligación de la ECD, informar a ONAC sobre las actualizaciones, presentar el plan de actualización para poder implementar los estándares vigentes.
Nota 2: Teniendo en cuenta el principio de Neutralidad tecnológica, la ECD en caso de usar una norma o estándar técnico que no se encuentre en los anexos mencionados anteriormente, debe informar a ONAC el requisito técnico objeto de evaluación de la conformidad bajo el cual solicita el alcance de su acreditación, citando la fuente y demostrando que no compromete la seguridad de los componentes de la PKI.

10.11.5. CERTIFICACIÓN DE CONFORMIDAD DE PRODUCTOS

La ECD debe demostrar que los dispositivos físicos criptográficos para el almacenamiento de certificados digitales y llave privada de los suscriptores, como los HSM de la misma, cumplen con los requisitos establecidos en el Anexo F, a través del certificado emitido por un Organismo Evaluador de la Conformidad acreditado bajo la norma internacional ISO/IEC 17065 (Certificación de Productos, Procesos y Servicios) ya sea por ONAC, o por un Organismo de acreditación extranjero, en cuyo caso debe ser miembro de acuerdo de reconocimiento multilateral para ese alcance (Ejemplo: MLA de IAF).

La ECD cerrada podrá utilizar software para el almacenamiento de certificados digitales, éste debe ostentar la certificación FIPS 140-2 Level 2 o superior y garantizar la custodia de dicho software mediante la aplicación de los controles técnicos establecidos en la norma internacional ISO/IEC 27001.

En los dos casos, el organismo de certificación de producto o software deberá ser de "tercera parte", es decir, independiente de la entidad o empresa que ha fabricado el producto.

El organismo de certificación de producto debe sustentar el certificado emitido, en los resultados de ensayos de un laboratorio de evaluación de módulos criptográficos acreditado por ONAC, o si éste no existe, por un Organismo de Acreditación extranjero en cuyo caso debe ser miembro de acuerdo de reconocimiento multilateral del que ONAC haga parte, para ese alcance.

Los productos (dispositivos criptográficos), deben estar rotulados con la información establecida en los requisitos del Anexo F.

10.11.6. ESTÁNDARES Y PRÁCTICAS TÉCNICAS NO ADMISIBLES

La ECD no podrá usar estándares y tecnologías que estén obsoletos o han evidenciado comprometer la seguridad del servicio o de la PKI, entre otros están:

1. Cualquier algoritmo que use Criptografía de llave simétrica por ejemplo, DES.
2. Algoritmo de hash MD5. Algoritmo de reducción criptográfico de 128 bits.
3. No se permite la suspensión de certificados que no conduzca a un estado de revocación inmediato.
4. La red donde se encuentra la CA, debe estar aislada para no comprometer la clave de la CA. Para la ECD cerradas, para compartir físicamente o lógicamente la red de la CA con otras redes, la red de la PKI debe estar en una VLAN o VPN exclusiva para cualquiera de los dos casos debe estar aislada para no comprometer la clave de la CA.
5. El almacenamiento de la llave privada del suscriptor no puede ser almacenada en un medio no diseñado para tal fin, es decir sólo se admite el almacenamiento de la llave privada en dispositivos criptográficos certificados. Ver anexo F.
6. La plataforma tecnológica CA utilizada por la ECD, debe ser de uso exclusivo para las actividades que conforman el alcance de acreditación solicitado.
7. Solamente se permite HSM certificado. Ver anexo F.
8. La validez de un certificado digital para persona natural o jurídica, no puede ser superior a 2 años.
9. La actualización de las listas de la CRL deben estar en línea con la revocación de los certificados digitales, es decir con la RA.
10. No se permiten Claves RCA con longitud inferior a 1024 para certificados de entidad final.
11. No se permiten Claves inferiores a 2048 para CA.
12. PKCS#2, PKCS#4

Si la acreditación se otorgó con estándares técnicos o infraestructura que se encontraban vigentes en su momento y posteriormente la industria de PKI declara que pierde la vigencia por comprometer la seguridad, o por detección de vulnerabilidades, la ECD debe informar con anticipación a ONAC, para poder realizar la respectiva actualización.

10.11.7. REQUISITOS DE ASEGURAMIENTO

Los siguientes requisitos de aseguramiento se deben implementar y son objeto de cumplimiento por parte de las ECD como prerrequisito para obtener y mantener la acreditación por parte de ONAC.

ACTIVIDAD DE ASEGURAMIENTO	DESCRIPCION
1. Auditoría de Tercera Parte	Requisito reglamentario: artículo 14 del decreto 333 de 2014 Criterios: Ley 527 de 1999, reglamentos que lo modifican y/o complementen y CEA-4.1-10 de ONAC. Directriz de la auditoria: ISO 19011 Requisito: Empresa de auditoría legalmente constituida en Colombia en cuyo objeto social esté incluido: servicios de auditoría de sistemas, seguridad de la información e infraestructura de llave pública PKI. Debe contar o haber tenido el reconocimiento Web Trust, auditores profesionales en la ingeniería de sistemas o ingenierías afines los cuales deben demostrar: 10 años de experiencia en auditoria de sistemas, 5 años de experiencia en ISO/IEC 27001 y 5 años de experiencia en infraestructura de llave pública (PKI), Competencia y experiencia certificada. Auditor con formación en ISO/IEC 17065, ISO/IEC 27001, ISO 31000, PKI. Todos con tarjeta profesional vigente en Ingeniería. Frecuencia: Anual. Entregables: Informe de conformidad, no se permite con salvedad o razonabilidad. Imparcialidad: No puede ser realizada por la misma empresa o profesionales por más de dos veces consecutivas. En caso de que no existan en el país al menos una entidad que cumpla los requisitos para llevar a la auditoría de tercera parte, las ECD podrán hacer uso de empresas de auditoría extranjeras, siempre y cuando cumplan los requisitos que se exigen a las empresas de auditoría nacionales y se encuentre habilitadas en su país de origen para realizar este tipo de auditoría o sus equivalentes.
2. Ethical Hacking	Pruebas de penetración y escaneo de vulnerabilidades en la red. Imparcialidad: No puede ser realizado por la misma empresa que realiza la auditoría de tercera parte ni por la misma ECD. Las pruebas no podrán ser realizadas por la misma entidad por más de dos veces consecutivas. Debe ser realizada por ETHICAL HACKER preferiblemente certificados por EC-COUNCIL, o con experiencia en ETHICAL HACKER superior a 2 años. Debe incluir el análisis de riesgos de topología de red. Frecuencia: Anual

ACTIVIDAD DE ASEGURAMIENTO	DESCRIPCION
3. LOGs	Administración del Registro de auditoria transaccional y de seguridad utilizando el modelo PHVA Frecuencia: Permanente Retención: De acuerdo con lo definido por la entidad de vigilancia y control, el ente regulador o mínimo de 3 años.
4. SOC - Security Operation Center	Servicio de monitoreo y control de eventos de seguridad registrados en la plataforma computacional utilizando el modelo PHVA Frecuencia: Permanente
5. NOC - Network Operation Center	Servicio de monitoreo y control de disponibilidad y capacidad de los componentes de red utilizando el modelo PHVA Frecuencia: Permanente
6. BCP –DRP Plan de Continuidad y recuperación.	Implementado Sistema de Gestión de la Continuidad del Negocio (SGCN)
7. Militarización PKI	La ECD debe aislar los servidores de la red interna y externa mediante la instalación de un corta fuegos o firewall, VLAN o VPN en el cual deben ser configuradas las políticas de acceso y alertas pertinentes.
8. Protección de Datos	Conforme con los dispuesto en el numeral c. del artículo 32 de la ley 527 de 1999, la ECD debe tener un plan implementado que garantice la protección de la información confidencial de los suscriptores en concordancia con las leyes Habeas data, Protección de datos, y cualquier otra regulación que las modifiquen o complementen. Frecuencia: Permanente.

Tratándose de Entidades extranjeras que obren en calidad de ECD reciprocas, tanto la ECD nacional como la ECD recíproca, deben cumplir los requisitos de éste documento; lo mismo aplica para entidades recíprocas nacionales. Igualmente el cumplimiento se extiende a proveedores críticos de ambas empresas; dicho cumplimiento será evaluado por ONAC.

11. NOTAS ACLARATORIAS

No aplica

12. RESUMEN DE CAMBIOS

Versión	Fecha de emisión	Resumen de cambios
01	21-07-2015	Emisión del Documento

13. ANEXOS TÉCNICOS

ANEXO A: ACTIVIDADES 1,3, 4 Y 6. CLASIFICADAS COMO: EMISIÓN DE CERTIFICADOS DIGITALES *(firmas digitales)*.

REQUISITOS	ESTANDARES TÉCNICOS VIGENTES
1. Algoritmo de firma	Función hash y RSA SHA1 con RSA Encryption no recomendado, se admite hasta la siguiente revisión por declaración de vulnerabilidad de SHA1. SHA256 con RSA Encryption RSA con tamaño o longitud de clave no inferior a 1024. Para entidad final, se recomienda 2048. A partir de la próxima revisión RSA con longitud de clave no inferior a 2048 para CA, No se permiten Claves inferiores a 2048, se recomienda 4096. A partir de la próxima revisión RSA con longitud de clave no inferior a 4096 para CA. Se podrán aceptar otros algoritmos de uso extendido como por ejemplo: Algoritmo Hash: SHA-224, SHA-384, SHA-512 con RSA Encryption Algoritmo de llave pública: DSA, Curva elíptica.
2. Contenido del Certificado Digital	RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile, o más recientes ITU-T Recommendation X.509 | ISO/IEC 9594-8, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
3. Ciclo de vida de los certificados	RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. ETSI TS 102 042 - Policy requirements for certification authorities issuing public key certificate
4. LDAP repositorio de certificados (LDAP)	RFC 4523 - Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates
5. Generación de claves	Dispositivos criptográficos certificados, ver Anexo F.

ANEXO B: ACTIVIDAD 2 Y 9. CLASIFICADA COMO: SERVICIOS DE GENERACIÓN DE FIRMAS DIGITALES. (*generación y verificación de la altercación entre envío y recepción de firmas digitales*).

REQUISITOS	ESTANDARES TÉCNICOS VIGENTES
1. Formatos de Firma digital	RFC 5126 CMS Advanced Electronic Signatures (CAdES) RFC 5652 Cryptographic Message Syntax (CMS). ETSI TS 101 733 CMS Advanced Electronic Signatures (CAdES)
	W3C XML Advanced Electronic Signatures (XAdES) ETSI TS (EN) 101 903 XML Advanced Electronic Signatures (XAdES)
	ETSI TS(EN) 102 778 PDF Advanced Electronic Signature Profiles (PAdES)
	Para Cerradas: Si actualmente usa otros formatos, se aceptan siempre y cuando sean formatos que se encuentren vigentes por la industria PKI, y que no se encuentre comprometida su seguridad.
2. Dispositivo Criptográfico	Ver anexo F
3. Validación del estado del certificado	Ver anexo E

ANEXO C: ACTIVIDAD 5. CLASIFICADA COMO: SERVICIOS ESTAMPADO CRONOLÓGICO, *(estampado de tiempo)*.

PRODUCTO	REQUISITO O NORMA
1. **Protocolo estampado cronológico / time stamping**	RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) RFC 3126 Electronic Signature Formats for long term electronic signatures. RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification Protocolo ANSI ASC X9.95
2. Fuente de tiempo	Hora oficial de país, provista por el Instituto Nacional de Metrología. Los servidores se mantienen actualizados con lo hora UTC, mediante sincronización a través del protocolo NTP v4, conforme a: RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification
3. HSM para TSA	Anexo F de este documento
4. Políticas -TSA	RFC 3628 - Policy Requirements for Time-Stamping Authorities (TSAs) ETSI TS (EN) 102 023 Policy requirements for time-stamping authorities.

ANEXO D: ACTIVIDADES 7 Y 8. CLASIFICADAS COMO: ARCHIVO, REGISTRO, CONSERVACIÓN CUSTODIA Y ANOTACIÓN PARA LOS DOCUMENTOS ELECTRÓNICOS TRANSFERIBLES Y MENSAJES DE DATOS.

1. CUMPLIMIENTO LEGAL:

La ECD debe dar cumplimiento a las leyes, decretos, regulaciones y acuerdos emitidos al respecto, y las que lo modifiquen o complementen.

2. SERVICIOS DE ARCHIVO, CUSTODIA Y CONSERVACIÓN:

a. ISO 639. Establecer códigos internacionalmente reconocidos
b. NTC 4095. NORMA GENERAL PARA LA DESCRIPCION ARCHIVISTICA
c. ISO TR/17068. Information and documentation. Trusted third party repository for digital records
d. GTC-ISO-TR 18492. Preservación a largo plazo de la información basada en documentos electrónicos
e. NTC-ISO 14641-1. Archivado electrónico. Parte 1: especificaciones relacionadas con el diseño y el funcionamiento de un sistema de información para la preservación de información electrónica
f. NTC-ISO 23081-1. Información y documentación. Procesos para la gestión de registros. Metadatos para los registros. Parte 1: principios
g. ISO 23081-2. Information and documentation. Managing metadata for record. Part 2: Conceptual and implementation issues.
h. ISO 23081-3. Information and documentation. Managing metadata for records. Part 3: Self-assessment method
i. ISO/IEC 11179-3. los registros de metadatos (MDR) – meta modelo Registro y atributos básicos
j. GTC-ISO-TR 26122. Información y documentación. Análisis de procesos de trabajo para registros.
k. ISO-TR 18128. Information and documentation. Risk assessment for records processes and systems.
l. GTC-ISO-TR 15801. Gestión de documentos. Información almacenada electrónicamente. Recomendaciones para la integridad y la fiabilidad.
m. ISO 14721. Space data and information transfer systems. Open archival information system (OAIS). Reference model.
n. NTC-ISO 30301. Información y documentación. Sistemas de gestión de registros. Requisitos.
o. NTC-ISO 30300. Información y documentación. Sistemas de gestión para registros. Fundamentos y vocabulario.
p. NTC-ISO 15489-1. Información y documentación. Gestión de documentos. Parte 1. Generalidades.
q. GTC-ISO-TR 15489-2. Información y documentación. Gestión de documentos. Parte 2. Guía
r. ISO 15836. Information and documentation. The Dublin Core metadata element set
s. ANSI/ARMA 19. Policy Design for Managing Electronic Messages
t. ARMA TR 24. Best Practices for Managing Electronic Messages
u. ARMA TR 23. Developing Electronic File Structures
v. BS 10008. Evidential weight and legal admissibility of electronic information. Specification
w. ISO/IEC 27005. Information technology -- Security techniques -- Information security risk management
x. ISO/IEC 27037. Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence

3. SERVICIOS DE DIGITALIZACIÓN Y MIGRACIÓN:

a. NTC 5985. Información y documentación. Directrices de implementación para digitalización de documentos
b. GTC-ISO-TR 15801. Gestión de documentos. Información almacenada electrónicamente. Recomendaciones para la integridad y la fiabilidad.

c. NTC-ISO 13008. Información y documentación. Proceso de conversión y migración de registros digitales
d. ISO/TR 13028. Directrices de aplicación para la digitalización de los registro

4. TRANSFERENCIA

a. NTC-ISO 12639. Tecnología gráfica - el intercambio de datos digitales de pre impresión - Tag formato de archivo de imagen para la tecnología de imagen (TIFF / IT)
b. ISO 32000 a gestión de documentos - Formato de Documento Portátil
c. ISO 19005 (PDF/A-2): Document Management - Electronic document file format for long term preservation (en caso de utilizarlos)
d. ISO 15444-1:2004 (JPEG).
e. ISO 13008. Información y documentación. Proceso de conversión y migración de registros digitales
f. ISO 9660. Procesamiento de la información - Volumen y estructura de archivos de CD-ROM para el intercambio de información
g. ISO 16363: Space data and information transfer systems -- Audit and certification of trustworthy digital repositories

5. SERVICIOS ASOCIADOS A SISTEMAS DE INFORMACIÓN:

a. NTC-ISO 16175-1. Información y documentación. Principios y requisitos funcionales para los registros en entornos electrónicos de oficina. Parte 1: información general y declaración de principios.
b. NTC-ISO 16175-2. Información y documentación. Principios y requisitos funcionales para los registros en entornos electrónicos de oficina. Parte 2: directrices y requisitos funcionales para sistemas de gestión de registros digitales.
c. ISO 16175-3. Information and documentation. Principles and functional requirements for records in electronic office environments. Part 3: Guidelines and functional requirements for records in business systems
d. ISO 22957. Document management. Analysis, selection and implementation of electronic document management systems (EDMS).
e. AIIM/ARMA TR48. Revised Framework for Integration of EDMS & ERMS Systems.

ANEXO E: MECANISMOS DE VALIDACIÓN DEL ESTADO DEL CERTIFICADO

1. CRL VALIDACIÓN ESTADO DE CERTIFICADOS.	RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile. ITU-T Recommendation X.509 ISO/IEC 9594-8 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
2. OCSP PROTOCOLO DEL ESTADO CERTIFICADO.	RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP RFC 2560 Protocolo OCSP (Protocolo de Estado de Certificado en Línea) X.509 Internet PKI Online Certificate Status Protocol – OCSP RFC 6960, de junio de 2013

ANEXO F: DISPOSITIVOS CRIPTOGRÁFICOS.

F.1 Generalidades

Este anexo provee los requisitos de seguridad y de certificación para los dispositivos criptográficos, que le permiten al suscriptor el uso de una firma digital en el marco del artículo 28 de la ley 527 de 1999, que la ECD debe ofrecer al solicitante y estar publicados en la DPC.

F.2 Requisitos de seguridad

Los requisitos de seguridad deben ser de alto nivel de forma que generen confianza a los suscriptores. Además de cumplir con requisitos certificado FIPS 140-2 level 3 o superior, entre otros están:

1. Que los dispositivos criptográficos que utiliza la ECD y ofrece a los solicitantes, se encuentren certificados por un organismo evaluador de la conformidad de acuerdo con lo establecido en este documento.
2. Que su método de creación y verificación sea confiable, seguro e inalterable y auditable para el propósito para el cual el mensaje fue generado.
3. Que al momento de creación de la firma digital, los datos con los que se creare se hallen bajo control exclusivo del suscriptor.
4. Que la firma digital cumpla con el artículo 28 ley 527 de 1999:
    a. *Es única a la persona que la usa.*
    b. *Es susceptible de ser verificada.*
    c. *Está bajo el control exclusivo de la persona que la usa.*
    d. *Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.*
    e. *Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.*

F.3 Requisitos de certificación de los productos o dispositivos criptográficos.

PRODUCTO O DISPOSITIVO CRIPTOGRAFICO	REQUISITO
Dispositivos criptográficos para el almacenamiento de certificados digitales y llave privada de los suscriptores.	Certificado FIPS 140-2 Level 3 o superior o, Longitud de Clave RSA 2048 o superior
Dispositivo criptográfico HSM "Hardware Security Module" (Módulo de Seguridad Hardware).	Certificado FIPS 140-2 Level 3 o superior, Longitud de Clave RSA 2048 o superior, exigible 4096 cuando se declare inseguro RSA 2048.

Nota: Consulta de ejemplos de certificación en anexo H numerales 19 y 20.

14. ANEXOS INFORMATIVOS

ANEXO G: RESUMEN DE LOS ESTANDARES PKCS

PKCS	Versión	Nombre	Comentarios
PKCS#1	2.1	Estándar criptográfico RSA	Ver RFC 3447. Define el formato del cifrado RSA.
PKCS#2	-	Obsoleto	Definía el cifrado RSA de resúmenes de mensajes, pero fue absorbido por el PKCS#1.
PKCS#3	1.4	Estándar de intercambio de claves Diffie-Hellman	Un protocolo criptográfico que permite a dos partes sin conocimiento previo una de la otra establecer conjuntamente una clave secreta compartida, utilizando un canal de comunicaciones inseguro.
PKCS#4	-	Obsoleto	Definía la sintaxis de la clave RSA, pero fue absorbido por el PKCS#1.
PKCS#5	2.0	Estándar de cifrado basado en contraseñas	Recomendaciones para la implementación de criptografía basada en contraseñas, que cubren las funciones de derivación de claves, esquemas de encriptación, esquemas de autenticación de mensajes, y la sintaxis ASN.1 que identifica las técnicas. Ver RFC 2898 y PBKDF2.
PKCS#6	1.5	Estándar de sintaxis de certificados extendidos	Define extensiones a la antigua especificación de certificados X.509 versión 1. La versión 3 del mismo lo dejó obsoleto.
PKCS#7	1.5	Estándar sobre la sintaxis del mensaje criptográfico	Ver RFC 2315. Usado para firmar y/o cifrar mensajes en PKI. También usado para la diseminación de certificados (p.ej. como respuesta a un mensaje PKCS#10). Fue la base para el estándar S/MIME, ahora basado en la RFC 5652, una actualización del estándar [[CMS] Cryptographic Message Syntax, utilizado para firmar digitalmente, obtener el digest, autenticar, o cifrar arbitrariamente el contenido de un mensaje (no confundir con Sistema de gestión de contenido -Content Management System-)].
PKCS#8	1.2	Estándar sobre la sintaxis de la información de llave privada	Ver RFC 5208.
PKCS#9	2.0	Tipos de atributos seleccionados	
PKCS#10	1.7	Estándar de solicitud de certificación	Ver RFC 2986. Formato de los mensajes enviados a una Autoridad de certificación para solicitar la certificación de una llave pública. Ver CSR.
PKCS#11	2.20	Interfaz de dispositivo criptográfico ("Cryptographic Token Interface" o cryptoki)	Define un API genérico de acceso a dispositivos criptográficos

PKCS#12	1.0	Estándar de sintaxis de intercambio de información personal	Define un formato de fichero usado comúnmente para almacenar llaves privadas con su certificado de llave pública protegido mediante clave simétrica.
PKCS#13	–	Estándar de criptografía de curva elíptica	(Aparentemente abandonado, la única referencia es una propuesta de 1998.)
PKCS#14	–	Generación de número pseudo-aleatorios	(Aparentemente abandonado, no hay publicada documentación al respecto)
PKCS#15	1.1	Estándar de formato de información de dispositivo criptográfico	Define un estándar que permite a los usuarios de dispositivo criptográficos identificarse con aplicaciones independientemente de la implementación del PKCS#11 (crytoki) u otro API. RSA ha abandonado las partes relacionadas con la tarjeta IC de este estándar, subsumidas por el estándar ISO/IEC 7816-15. 1

ANEXO H: REFERENTES DE CONSULTA DE INFRAESTRUCTURA DE LLAVE PÚBLICA - PKI

	Referentes PKI	Link
1	ANSI	http://www.ansi.org/
2	CAB CA / Browser fórum	https://cabforum.org/
3	Common Criteria Project Sponsoring Organization	http://www.commoncriteriaportal.org/
4	CWA	http://www.cen.eu/cen/Sectors/Sectors/ISSS/CWAdownload/Pages/Electronic%20Signatures.aspx
5	European Telecommunications Standards Institute - ETSI TS	http://www.etsi.org/website/homepage.aspx
6	Federal Information Processing Standard – FIPS	http://www.nist.gov/itl/fips.cfm
7	Forum PKI	http://www.oasis-pki.org/resources/techstandards/#majorrfcs
8	IEEE	http://www.ieee.org/index.html
9	International Organization for Standardization – ISO	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306
10	International Electrotechnical Commission – IEC	http://www.iec.ch/
11	Internet Engineering Task Force (IETF).	http://www.ietf.org/rfc.html
12	Massachusetts Institute of Technology – MIT	http://www.mit.edu/
13	Request for Comments – RFC	http://www.normes-internet.com/normes.php?rfc=rfc3647&lang=es http://www.rfc-es.org/ http://www.rfc-editor.org/search/rfc_search.php
14	National Institute of Standards and Technologies – NIST	http://www.nist.gov/index.html
15	Telecomunication Union (ITU - T).	http://www.itu.int/en/ITU-T/Pages/default.aspx
16	Uncitral	http://www.uncitral.org/uncitral/es/index.html
17	WEBTRUST	http://www.webtrust.org/item64428.aspx
18	The Dublin Core	http://www.dublincore.org/
19	Ejemplo lista de certificados FIPS 140 para dispositivos criptográficos	http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2014.htm
20	Ejemplo lista de laboratorios acreditados	http://csrc.nist.gov/groups/STM/testing_labs/