CRITERIOS ESPECÍFICOS DE ACREDITACIÓN ENTIDADES DE CERTIFICACIÓN DIGITAL

SIG
SISTEMA INTEGRADO DE GESTIÓN

CEA-3.0-07 (Antes CEA-4.1-10)
Versión 2

PROCESO NIVEL 1:		
3.0 PROCESO DE PRESTACIÓN DEL SERVICIO		
ELABORÓ:	**REVISÓ:**	**APROBÓ:**
Fecha: 2021-12-30 COORDINADOR SECTORIAL GRUPO TÉCNICO ASESOR DE ECD	Fecha: 2021-06-29 DIRECTOR TÉCNICO NACIONAL PARTES INTERESADAS (CONSULTA PÚBLICA 2021-06-01 HASTA 2021-02-06) CONSULTA- COMITÉ TÉCNICO CONSEJO DIRECTIVO DE ONAC (2021-06-30)	Fecha: 2021-07-02 DIRECTOR EJECUTIVO

TABLA DE CONTENIDO

1. PROPÓSITO

Estos criterios específicos establecen los requisitos 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 con lo establecido en la Ley 527 de 1999, el Decreto Ley 019 de 2012, los capítulos 47 y 48 del título 2 de la parte 2 del libro 2 del Decreto Único del Sector Comercio, Industria y Turismo – DURSCIT y los reglamentos que los modifiquen o complementen.

2. AUTORÍA

Este documento fue elaborado por el Organismo Nacional de Acreditación de Colombia, ONAC; en su realización y revisión participaron el Grupo Técnico Asesor – GTA, dentro de sus participantes se destacan, Director Técnico de ONAC, el Coordinador Sectorial de Entidades de Certificación Digital de ONAC, Dirección del sistema gestión de ONAC, Dirección de Gestión, Desarrollo y Mejora de ONAC, expertos técnicos de las partes interesadas, un representante del Ministerio de Comercio, Industria y Turismo, un representante del Archivo General de la Nación, y un representante del Ministerio de Tecnologías de la Información y las Comunicaciones.

3. INTRODUCCIÓN

Los presentes Criterios Específicos de Acreditación – CEA se fundamentan en las siguientes normas: Ley 527 de 1999 *"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"*; Decreto Ley 019 de 2012 *"Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública"* artículos 160 a 163; capítulos 47 *"firma electrónica"* y 48 "*acreditación de las entidades de certificación"* del título 2 de la parte 2 del libro 2 del Decreto Único del Sector Comercio, Industria y Turismo – DURSCIT; y capítulo 7 del título 1 de la parte 2 del libro 2 *"Subsistema nacional de la calidad"*. 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 Entidades de Certificación Digital (ECD).

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

Este documento, se desarrolla en el ámbito del sector reglamentario de la acreditación, atendiendo el mandato del Gobierno Nacional establecido en el Decreto Ley 019 de 2012 y reglamentado por el capítulo 48 del DURSCIT y las demás regulaciones que lo modifiquen o complementen.

En los criterios específicos de acreditación CEA se utilizan las siguientes formas verbales:

- "debe" indica un requisito;
- "debería" indica una recomendación;
- "puede" indica un permiso, una posibilidad o una capacidad.

4. ALCANCE

Los conceptos y directrices dados en este documento deben ser aplicados en la prestación de los servicios de certificación digital que ofrezcan los organismos evaluadores de la conformidad que soliciten o mantengan su acreditación ante ONAC. Así mismo, estos Criterios también son aplicables a aquellos organismos en proceso de acreditación y cuyo cumplimiento será verificado en evaluaciones iniciales, de seguimiento, de reevaluación y extraordinarias para la acreditación.

5. JUSTIFICACIÓN

Este documento establece los Criterios Específicos de Acreditación (CEA) y se elabora con el fin de que las entidades de certificación digital (ECD), puedan acreditarse como organismo de evaluación de la conformidad ante el Organismo Nacional de Acreditación de Colombia – ONAC; es decir, para prestar servicios de certificación digital de acuerdo con lo establecido en la Ley

527 de 1999 donde se reglamenta el acceso y el uso de los mensajes de datos, el Decreto Ley 019 de 2012 y los capítulos 47 y 48 del título 2 del libro 2 de la parte 2 del DURSCIT y las normas que los modifiquen o complementen.

El artículo 160 del Decreto Ley 019 de 2012, reglamentado por el artículo 2.2.2.48.1.2., del DURSCIT, 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 entidades de certificación."

El Artículo 161 del Decreto Ley 019 de 2012, que modificó el artículo 30 de la Ley 527 de 1999, establece las actividades que pueden realizar las ECD para prestar servicios de certificación digital, 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."*

El DURSCIT en su artículo 2.2.2.48.3.2. *Infraestructura y recursos*, establece que:

> *"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, modificado por el artículo 161 del Decreto 019 del 2012, establece lo siguiente: *"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".*

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 de los presentes Criterios Específicos de Acreditación -CEA.

Estos Criterios deben ser cumplidos por las ECD para su respectiva acreditación, por tal motivo, ONAC evaluará dicho cumplimiento con base en el presente CEA, con los requisitos establecidos en las Reglas del Servicio de Acreditación, y los demás documentos considerados en el Sistema de Gestión de ONAC.

6. DOCUMENTOS DE REFERENCIA

Las normas que a continuación se indican son indispensables para la aplicación de este CEA. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición de la norma (incluyendo cualquier modificación de ésta).

- **ISO/IEC 17000**: Evaluación de la conformidad. Vocabulario y principios generales.
- **ISO/IEC 17011:** Evaluación de la conformidad. Requisitos generales para los organismos de acreditación que realizan la acreditación de organismos de evaluación de la conformidad

- **Decreto Único del Sector Comercio, Industria y Turismo - DURSCIT, 1074 de 2015.** Que compila todas las normas que rigen los sectores de comercio, industria y turismo del país, y entre ellas las relacionadas con el Subsistema Nacional de la Calidad, las de firmas electrónicas y firmas digitales, y la acreditación de las entidades de certificación digital.
- **Ley 527 de 1999:** que regula el acceso y el uso de los mensajes de datos
- **Decreto 019 de 2012, Artículos 160 a 163,** que suprime la actividad de autorización de entidades de certificación digital por parte de la Superintendencia de Industria y Comercio, y establece la obligación de acreditarse ante el Organismo Nacional de Acreditación de Colombia – ONAC.
- **Decreto 620 de 2020:** Lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- **Ley 2106 del 2019:** Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- **Ley 1581 del 2012**: Por la cual se dictan disposiciones generales para la Protección de Datos Personales.
- **ISO 9001** Sistema de gestión de la calidad. Requisitos.
- **ISO/IEC 27001** Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos
- **ISO/IEC 20000** Tecnología de la información. Gestión de la calidad de los servicios TI
- **ISO 19011** Directrices para la auditoría de Sistemas de Gestión.
- **ISO 31000** Gestión de Riesgos.
- **ISO 22301** Sistema de Gestión de la Continuidad del Negocio (SGCN)
- **ISO/IEC 27006** Tecnologías de la información, técnicas de seguridad, requisitos para organismos que proveen auditoria y certificación de sistemas de gestión de seguridad de la información.
- **ISO/IEC 25000** SQuaRE (System and Software Quality Requirements and Evaluation)
- **ISO 21188** Public key infrastructure for financial services -- Practices and policy framework
- **ISO 15836** Information and documentation -- The Dublin Core metadata element set (XML)
- **ISO/IEC 27037** Guidelines for identification, collection, acquisition and preservation of digital evidence
- **NTC 14721:2018** Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS). Modelo de referencia
- **ISO 20104:2015** Sistemas de transferencia de información y datos espaciales - Especificación de interfaz productor-archivo (PAIS)
- **ISO 20652:2006** Sistemas espaciales de transferencia de datos e información - Interfaz productor-archivo - Metodología Resumen estándar
- **Ley 1898 de 2018**. artículo 13.10 Autenticación y Certificados Digitales.
- **NIST 800-63** Directrices de identidad digital

7. DEFINICIONES Y CONVENCIONES

Para la aplicación de este documento se deben considerar las definiciones establecidas en las siguientes normas y reglamentación en su versión vigente o las que las actualicen o sustituyan, tales como; normas, ISO/IEC 17000, ISO/IEC 17011 e ISO/IEC 27000, ISO 9000, las establecidas en el Decreto 620 de 2020, y en el capítulo 48 del DURSCIT, además de los siguientes:

SIGLA	DEFINICIÓN
ANSI	American National Standards Institute
Autoridad de Registro (RA):	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.
Autoridad de sellado de tiempo (TSA)	Time Stamp Authority, (Autoridad de sellado de tiempo)
Autoridad de Certificación (CA)	Entidad de confianza, responsable de emitir y revocar los certificados.
CA raíz	Autoridad certificadora de primer nivel, base de confianza
CA subordinada	Autoridad certificadora de segundo nivel o más niveles
Centro de procesamiento de datos (CPD)	También conocido como Data Center, y se refiere al espacio donde se concentran los recursos ya sean On premise o Cloud, necesarios para el procesamiento de la información de una entidad de certificación digital.
DPC	Declaración de prácticas de certificación. Documento oficial presentado por la Entidad de Certificación Digital, en el cual

SIGLA	DEFINICIÓN
	define normas y prácticas de la Autoridad de Certificación para la prestación de los servicios de certificación digital.
Entidad de Certificación (ECD)	Aplican las definiciones establecidas en la Ley 527 del 1999 Artículo 2o. Definiciones
DSA (DSA, Digital Signature Algorithm)	Algoritmo estándar del Gobierno Federal de los Estados Unidos de América o FIPS para firmas digitales. Obtiene la clave pública y clave privada que se utilizan posteriormente para firmar un archivo en forma digital.
ETSI	European Telecommunications Standards Institute
Common Criteria	Es una clasificación de categoría asignada a un producto o sistema de TI después de una evaluación de seguridad
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.)
Firma Digital	Aplican las definiciones establecidas en la Ley 527 del 1999 Artículo 2o. Definiciones
Firma electrónica	Aplican las definiciones establecidas en el DURSCIT artículo 2.2.2.47.1. *Definiciones*, y Ley 527 de 1999 Artículo 7 Firma.
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
HSM	Hardware Security Module
LDAP	Lightweight Directory Access Protocol
Lista de Certificados Digitales Revocados (CRL)	Es aquella lista de certificados digitales que han sido revocados por la autoridad de certificación (CA), que no han cumplido su fecha de vencimiento programada y que ya no deben ser confiables
Log	ISO/IEC 27001:2013 control anexo A Seguridad operacional: A.12.4.
Neutralidad tecnológica	El principio de neutralidad tecnológica de acuerdo con la Ley 1341 del 2009 y el Artículo 2.2.2.47.2., establecido en el DURSCIT, en este sentido, este principio es aplicable a la actividad adelantada por las Entidades de Certificación Digital, siempre y cuando se dé cumplimiento a los criterios establecidos en el presente documento.
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
OID	Identificador único de objeto (Object identifier). OID, 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
PKCS	Public-Key Cryptography Standards. Estándares de

SIGLA	DEFINICIÓN
	criptografía de llave pública concebidos y publicados por los laboratorios de RSA
Política	Se refiere a las intenciones y la dirección de una organización expresadas formalmente por su alta dirección.
Política de Certificación (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.
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
Revocación	Para este documento, es el proceso por el cual se inhabilita los certificados en relación con las firmas digitales de personas naturales o jurídicas 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
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
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
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
Solicitante	Persona natural o jurídica que solicita el servicio de certificación digital a la ECD
Suscriptor	Persona natural o jurídica que contrata el servicio de certificación digital a la ECD. En el caso de la actividad de emisión de certificados digitales, también será la persona natural o jurídica a cuyo nombre se expide un certificado digital.
TLS	Transport Layer Security: seguridad de la capa de transporte. Protocolo criptográfico que proporciona comunicaciones seguras por una red, comúnmente Internet
Token	Dispositivo hardware criptográfico suministrado por una ECD, el cual contiene el certificado digital y la llave privada del suscriptor
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
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

SIGLA	DEFINICIÓN
VA	Validation Authority (Autoridad de validación)

8. DISPOSICIONES GENERALES

8.1 TEMAS LEGALES

8.1.1 La Entidad de Certificación Digital, debe estar constituida formal y legalmente responsable de todas sus actividades de certificación, como una persona jurídica en los términos del Artículo 160 del Decreto Ley 019 de 2012 y el capítulo 48 del DURSCIT.

8.1.2 La ECD debe cumplir los requisitos de la Ley 527 de 1999, los capítulos 47 y 48 del DURSCIT, el Decreto Ley 019 de 2012 y los demás reglamentos que los modifiquen, complementen o sustituyan.

8.2 GESTIÓN DE LA IMPARCIALIDAD

8.2.1 La ECD debe actuar de manera imparcial en relación con las actividades de certificación digital.

8.2.2 La ECD debe establecer su estructura a través de la implementación de políticas y procedimientos documentados, orientados a gestionar la imparcialidad y asegurarse de que las actividades de certificación se realizan con imparcialidad. La ECD debe tener el compromiso de imparcialidad de la alta dirección de las actividades de certificación.

8.2.3 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

8.2.4 La ECD debe ser responsable de la imparcialidad de sus actividades de certificación y no debe permitir que presiones comerciales, financieras o de otra índole comprometan dicha imparcialidad.

8.2.5 La ECD debe identificar y gestionar los riesgos para su imparcialidad de manera continua. Se deben incluir los riesgos que se derivan de sus actividades, de las relaciones con los organismos relacionados, o las relaciones de su personal.

NOTA 1 Una relación que presenta riesgo para la imparcialidad de la ECD puede basarse en factores tales como la propiedad, la estructura directiva, la gestión, el personal, los recursos compartidos, la situación financiera, los contratos, el marketing (incluido el posicionamiento de marca) y el pago de una comisión sobre las ventas u otro incentivo concerniente a nuevos clientes, etc.

8.2.6 La ECD debe documentar y ser capaz de demostrar cómo elimina, minimiza o gestiona dichos riesgos para su imparcialidad que surjan de sus actividades de certificación. Se deben considerar las fuentes potenciales de riesgos para su imparcialidad identificadas, ya sea que surjan de las actividades internas de la ECD, como de la asignación de responsabilidades al personal, o de actividades de otras personas, organismos u organizaciones, deben estar cubiertas.

8.2.7 Cuando la ECD ofrece o suministra consultoría, el personal administrativo, de gestión, y técnico de la ECD asociado a las actividades de consultoría, debe mantener completa independencia respecto al personal del proceso de revisión y toma de decisión sobre la certificación de la misma ECD.

8.2.8 Como mecanismo para salvaguardar la imparcialidad, la ECD debe tener en cuenta a las partes interesadas, en la gestión de imparcialidad.

9. REQUISITOS GENERALES

9.1 RESPONSABILIDAD LEGAL Y FINANCIAMIENTO

9.1.1. La ECD debe tener los recursos financieros necesarios para la operación y mantener la estabilidad financiera y los recursos que se requieren para sus operaciones, que se encuentran establecidos en el capítulo 48 del DURSCIT, Artículo 2.2.2.48.2.4. Patrimonio mínimo.

Para las ECD de naturaleza pública, el cumplimiento de esta disposición se podrá demostrar a través de cualquier medio que permita garantizar la disponibilidad de recursos por el año en curso, y/o periodos venideros, y de esta manera, se

garantice la correcta operación.

9.1.2. La ECD debe tener las garantías para cubrir las responsabilidades que se deriven de sus operaciones, establecidas en el capítulo 48 del DURSCIT, Artículo 2.2.2.48.2.5. *Garantías*.

NOTA 2 Esta disposición no es aplicable para las ECD cerradas.

9.2 CONDICIONES NO DISCRIMINATORIAS

9.2.1 No se debe restringir el acceso a los servicios de certificación digital por razones financieras u otras condiciones limitantes indebidas, tales como la membresía a una asociación o a un grupo. 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, si la ECD tiene contemplado en sus políticas y/o procedimientos la no emisión de un certificado en relación con las firmas electrónicas o digitales de personas naturales o jurídicas, o cualquier otro servicio de certificación digital que se encuentre cubierto en el alcance acreditado, lo deberá sustentar con la reglamentación vigente.

9.2.2 Los servicios de certificación digital de la ECD deben ser accesibles a todos los solicitantes cuyas solicitudes estén dentro del alcance de su acreditación. Esto incluye la aplicación del principio de neutralidad tecnológica que se encuentra registrado en las definiciones y convenciones del presente documento.

9.2.3 El acceso a un servicio de certificación digital no debe depender de alguna característica del solicitante o suscriptor diferente a las definidas en la Política de Certificación (PC), 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.

9.3 CONFIDENCIALIDAD

9.3.1 La ECD debe establecer e implementar políticas y procedimientos documentados para el mantenimiento y la divulgación de la información.

9.3.2 La ECD es responsable, a través de acuerdos ejecutables legalmente, de mantener la confidencialidad de toda la información obtenida durante el proceso de certificación digital. Estos acuerdos deben cubrir a todo el personal de la ECD.

9.3.3 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.

9.3.4 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.

9.3.5 La ECD debe suscribir acuerdos de confidencialidad, con el fin de asegurar que las actividades de los proveedores de servicios relacionados con la certificación digital no comprometan la confidencialidad.

9.3.6 La información acerca del suscriptor obtenida en fuentes ajenas al mismo (por ejemplo, de un reclamante o de los reguladores) debe ser tratada como confidencial, excepto cuando la misma sea de carácter público.

9.4 INFORMACIÓN DISPONIBLE AL PÚBLICO

La ECD debe mantener pública sin solicitud previa la DPC y PC cumpliendo con las disposiciones del capítulo 48 del DURSCIT, Artículo 2.2.2.48.3.1. Declaración de Prácticas de Certificación (DPC) y al estándar RFC 3647 o el que lo reemplace o actualice.

Adicionalmente, la ECD debe mantener pública y poner a disposición a siguiente información:

a) Todos los servicios de certificación digital que han sido acreditados por ONAC (alcance de acreditación), adicionalmente

debe estar disponible al público los servicios que no se encuentran bajo el alcance de acreditación.

b) Políticas de Certificación (PC) según el capítulo 48 del DURSCIT, Artículo 2.2.2.48.3.1.
c) 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.
d) Información sobre los procedimientos para el tratamiento de PQRS (petición, queja, reclamo y solicitud), recibidas de las partes relacionadas.

Si la ECD tiene CA subordinadas o subcontratadas, involucradas en el alcance de la acreditación, debe incluir esta misma información respecto a cada una de ellas.

La ECD debe mantener disponible al público la política de certificación (PC), la cual debe contener:

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 capítulo 48 del DURSCIT, Artículo 2.2.2.48.3.4. Certificaciones recíprocas.
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.

La ECD debe mantener disponible al público la documentación relativa al 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.

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.

La información proporcionada por la ECD, incluyendo la publicidad, debe cumplir los parámetros y características contenidas en la normatividad vigente, siendo exacta, de fácil acceso y no inducir al error.

Toda la información que debe mantenerse disponible al público debe garantizarse como mínimo a través del portal o página WEB de la ECD.

10. REQUISITOS RELATIVOS A LA ESTRUCTURA

10.1 DIRECCIÓN Y ESTRUCTURA DE LA ORGANIZACIÓN

La estructura, composición y la gestión de la Entidad de Certificación Digital, debe dar cumplimiento a lo siguiente:

10.1.1 Las actividades de la ECD se deben estructurar y gestionar de modo que se salvaguarde la imparcialidad, la accesibilidad al servicio y la confidencialidad.

10.1.2 La ECD debe mantener actualizada y documentada su estructura organizacional, que describa las funciones y líneas de autoridad de la organización donde se identifique entre otras a la alta dirección, el representante legal, el representante de la dirección, las funciones con responsabilidad en la operación de la ECD y las funciones responsables de la RA. 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.

10.1.3 La ECD debe documentar los deberes y responsabilidades de la dirección, de todo el personal involucrado en el servicio de certificación digital y de todos los comités necesarios para la operación de la ECD, en especial deben identificar las funciones con autoridad y responsabilidad total de cada una de las siguientes actividades:

a) Desarrollo de políticas relacionadas con la operación de la ECD.
b) La implementación de las políticas y los procedimientos.

c) Las finanzas de la ECD.
d) El diseño y desarrollo de los servicios de certificación digital y la gestión de cambios.
e) La implementación de los requisitos de la certificación digital.
f) La revisión de la solicitud.
g) La toma de decisiones sobre la certificación digital.
h) La delegación de la autoridad en los comités o el personal, según se requiera, para emprender a su nombre las actividades definidas.
i) Los acuerdos contractuales.
j) El suministro de los recursos adecuados para las actividades de certificación digital.
k) La respuesta a reclamos o PQRS.
l) La gestión de competencia del personal.
m) Los sistemas de gestión de la ECD.

10.1.4 La ECD debe tener reglas formales documentadas para la asignación, los términos de referencia y la operación de los comités involucrados en el proceso de certificación digital. Tales comités no deben tener presiones de tipo comercial, financiero u otras que puedan influir en las decisiones. La ECD debe conservar la autoridad.

10.1.5 Roles de la RA.

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

a) Agentes de la RA: Usuarios de la RA con privilegios. Son responsables por las operaciones diarias, tales como la revisión y aprobación de solicitudes.
b) Administrador: La persona responsable de administrar y configurar la RA.
c) System auditor: Auditor de los sistemas de información de la RA, diferente al rol de auditor interno de sistemas de gestión.

10.2 REQUISITOS DEL PERSONAL

10.2.1 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 para la ECD, debe tener un contrato laboral que identifique su rol en el sistema de gestión de la ECD.

10.2.2 La ECD debe definir los requisitos de competencia para el personal involucrado en el proceso de certificación. El personal debe ser competente para desempeñar sus tareas y responsabilidades específicas.

10.2.3 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. El procedimiento debe definir requisitos para:

a) Determinar 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) Identificar las necesidades de formación y suministrar, según necesidad, la formación y entrenamiento requeridos sobre procesos de certificación digital, requisitos, metodologías, actividades y otros requisitos pertinentes del servicio de certificación digital.

c) Demostrar que el personal tiene las competencias requeridas para los deberes y las responsabilidades que ellos adelantan.

d) Autorizar formalmente al personal para las funciones en el proceso de certificación digital.

e) Monitorear el desempeño del personal.

10.2.4 La ECD debe mantener actualizados los registros del personal, incluyendo la información de nombre y dirección; cargo que desempeña; cualificación educativa y estatus profesional; experiencia y entrenamiento; evaluación de la competencia; monitoreo del desempeño; autorizaciones que tiene dentro de la ECD y su vigencia con la fecha de la

actualización más reciente de cada registro.

10.2.5 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.

10.2.6 La ECD debe requerir a su personal que firme un documento por el cual se compromete a cumplir las reglas definidas por la ECD, incluidas aquellas relativas a la confidencialidad, la imparcialidad y los conflictos de intereses.

10.3 CONTRATACIÓN EXTERNA

10.3.1 En caso de que la ECD contrate de forma externa servicios o productos, relacionados con las actividades acreditadas en alcance, únicamente lo debe hacer con organismos que demuestren cumplir con los requisitos evaluados por ONAC a las ECD, establecidos en este documento; es decir los requisitos evaluados 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.

10.3.2 La ECD no podrá subcontratar la decisión dentro de la actividad de certificación digital.

Teniendo en cuenta las funciones de la RA, la ECD podrá subcontratar la recepción de solicitudes relacionadas con la certificación digital y el registro de las peticiones que hagan los solicitantes con un departamento externo o persona jurídica diferente a la ECD, siempre y cuando se demuestre que las funciones de comprobación de veracidad, y corrección de los datos que aportan los usuarios, así como el envío a una CA de las peticiones que cumplen los requisitos se mantiene como función propia de la ECD. Esta distribución de funciones de la RA deberá mantenerse documentada, de tal manera que permita el entendimiento adecuado de tal situación, frente al cumplimiento del numeral 10.4.5 y en general del presente CEA-3.0-07.

10.3.3 Cuando La ECD contrata externamente servicios relacionados con la certificación debe:

a) Asumir la responsabilidad total por el trabajo contratado externamente.
b) Evaluar y seleccionar a los proveedores de productos y servicios relacionados con las actividades de certificación digital.
c) Evaluar y hacer el seguimiento del desempeño el proveedor de productos y servicios relacionados con la certificación de acuerdo con sus procedimientos documentados.
d) Tener registros que demuestren que el proveedor de productos y servicios relacionados con la certificación cumple todos los requisitos pertinentes del trabajo contratado externamente y mantener una lista del proveedor de productos y servicios relacionados con la certificación.

10.3.4 La ECD debe tener un acuerdo ejecutable legalmente que cubra los acuerdos, incluyendo la confidencialidad y los conflictos de intereses, con cada proveedor de productos y servicios relacionados con la certificación.

10.3.5 Para que la confianza de calidad y seguridad de los servicios de certificación digital no se vea comprometida, la contratación que adelante la ECD, debe asegurar que sus contratistas no afecten el cumplimiento de los requisitos de los criterios específicos de acreditación, en el contexto que la subcontratación involucre. Para esto, la ECD debe adoptar los controles del Anexo A de la ISO/IEC 27001 aplicables a las actividades desarrolladas por estos subcontratistas, y los cuales podrán ser parte del alcance de la evaluación en el proceso de otorgamiento, mantenimiento o renovación de la acreditación de la ECD de conformidad con el capítulo 48 del DURSCIT, Artículo 2.2.2.48.3.3. Infraestructura prestada por un tercero, en el contexto de los requisitos establecidos para cada actividad.

10.4 REQUISITOS TÉCNICOS

10.4.1 Los requisitos técnicos deben dar cumplimiento al presente CEA-3.0-07 y sus anexos técnicos para los servicios establecidos de conformidad con el Decreto Ley 019 del 2012, manteniendo 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.

10.4.2 La ECD debe tener la infraestructura técnica y equipos de acuerdo con lo establecido en el capítulo 48 del DURSCIT, Artículo 2.2.2.48.3.2. Infraestructura y recursos y articulo 29, literal b) de la Ley 527 de 1999. La ECD debe contar con una infraestructura de llave pública (PKI), que cumpla las siguientes características:

1. Puedan generar las firmas digitales y electrónicas propias y que, además, les permita prestar todos los servicios para los que soliciten la acreditación.

2. Se garantice el cumplimiento de lo previsto en la Declaración de Prácticas de Certificación (DPC).

3. Se pueda calificar el sistema como confiable de acuerdo con el capítulo 48 del DURSCIT, Artículo 2.2.2.48.1.4. Sistema confiable.

4. Los certificados expedidos por las entidades de certificación cumplan con:

    a. Los estándares técnicos nacionales e internacionales vigentes que cumplan con los criterios específicos de acreditación que para el efecto establezca el ONAC.

5. Se garantice la existencia de sistemas de seguridad física en sus instalaciones, un monitoreo permanente de toda su planta física, y acceso restringido a los equipos que manejan los sistemas de operación de la entidad.

6. El manejo de la clave privada de la entidad esté sometido a un procedimiento propio de seguridad que evite el acceso físico o de otra índole a la misma a personal no autorizado.

7. Cuente con un registro de todas las transacciones realizadas, que permita identificar el autor de cada una de las operaciones.

8. Los sistemas que cumplan las funciones de certificación solo sean utilizados con ese propósito y por lo tanto no deben realizar ninguna otra función.

9. Todos los sistemas que participen directa o indirectamente en la función de certificación estén protegidos por sistemas y procedimientos de autenticación y seguridad de conformidad con los estándares nacionales e internacionales vigentes y con los criterios específicos de acreditación que para el efecto establezca el ONAC.

10.4.3 La ECD debe establecer e implementar la metodología, mantener registros y controles necesarios para la generación de la CA Raíz, demostrando:

a) Ceremonia de generación de la CA raíz.
b) Logs de la CA y Bitácora de trabajo debidamente autorizada.
c) Generación de las claves de la CA.
d) Almacenamiento, copias de seguridad y recuperación de las claves de la CA.
e) Distribución de la Llave pública de la CA.
f) Uso de la Clave de la CA.
g) Destrucción de la clave de la CA y de todas sus copias de seguridad con el registro de destrucción y su almacenamiento.
h) Archivo de claves de la CA.
i) Mantener offline o apagada la CA raíz.
j) Debe ser un dispositivo criptográfico certificado para la CA raíz que cumpla con los criterios específicos de acreditación. Ver anexo F

10.4.4 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:

a) La CA recibe la solicitud de certificación previamente validada por la RA.
b) El certificado es generado por el software de la CA y firmado por un dispositivo criptográfico certificado ver anexo F, que contiene la llave privada de la CA.

10.4.5 Requisitos Generales de la RA (Autoridad de Registro): La ECD debe contar con una Autoridad de registro (RA), que cumpla las siguientes condiciones:

a) 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.
b) Para una ECD abierta, la función de la RA la debe ejercer un departamento interno o externo, independiente al departamento técnico encargado de la administración técnica de la CA.
c) De acuerdo con las tablas de retención documental acordes a las regulaciones vigentes Articulo 38 Ley 527 de 1999, la RA debe custodiar todas las solicitudes y mantener la trazabilidad sobre la gestión de los servicios de certificación digital.
d) Normalmente la RA podrá estar expuesta en INTERNET, para que el solicitante pueda interactuar con ella, sin embargo, deben existir controles que garanticen la calidad en la prestación del servicio y la seguridad de la información.
e) 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.
f) La RA debe utilizar su certificado para identificarse a la entidad emisora (CA), el cual debe cumplir con las políticas de certificación de la propia ECD. Para la autorización, la autoridad competente comprobará si la RA pertenece a un grupo de su sistema de la RA en la ECD.
g) La RA debe confirmar que el servicio de certificación digital cumple la política de certificación y que está en consonancia con lo especificado en las prácticas de certificación.
h) 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 para las actividades de emisión de certificados con relación a firmas electrónicas o digitales y garantizar la imparcialidad.
i) 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 o electrónico respectivo.
j) La infraestructura de llaves públicas de la ECD, debe garantizar plenamente dicha independencia entre la RA y la CA.

10.4.6 Centro de procesamiento de datos (CPD). La ECD debe contar con infraestructura tecnológica, garantizando como mínimo un CPD principal y uno alterno, cumpliendo con las características que aseguren la disponibilidad y seguridad. La ECD debe demostrar la fiabilidad en función del nivel de disponibilidad, redundancia y seguridad para el CPD principal y alterno, mediante la aplicación de los controles de referencia establecidos en el Anexo A de la norma técnica ISO/IEC 27001. Lo anterior en función de las áreas: telecomunicaciones, arquitectura, sistema eléctrico y sistema mecánico.

Cuando el centro de procesamiento de datos (CPD) sea administrado por un tercero, la entidad de certificación digital deberá demostrar su vinculación con aquél, asegurando la viabilidad de sus servicios bajo dichas condiciones, y la disponibilidad mediante acuerdos de niveles de servicio orientados a cubrir los elementos que serán producto de evaluación y supervisión por parte de ONAC.

En relación con la ubicación de la CPD, la ECD debe cumplir con lo establecido en el capítulo III del Título V de la Circular Única Básica de la Superintendencia de Industria y Comercio

De cualquier manera, la demostración del cumplimiento de dichos controles y requisitos de parte de la ECD, debe ser verificable de manera adecuada.

10.5 REQUISITOS DE LA AUTORIDAD DE CERTIFICACIÓN (CA) PARA LAS ACTIVIDADES DE CERTIFICACIÓN DIGITAL.

10.5.1 Conforme al Artículo 32 de la Ley 527 de 1999 en su literal b), la ECD debe implementar los controles necesarios para proporcionar seguridad tal que garantice el cumplimiento de los siguientes controles:

a) La seguridad que se planea y gestiona, está dirigida para apoyar la correcta operación de la CA.
b) Los riesgos deben ser identificados y gestionados con eficacia.
c) Gestionar los activos de información.
d) Se debe mantener la seguridad de las instalaciones y del entorno físico de CA, sistemas y activos de información accedidos por terceros.
e) La seguridad de la información se mantiene cuando las responsabilidades de las funciones de la CA han sido subcontratas a otra organización o entidad.
f) La ECD deberá mantener controles necesarios para el servicio de emisión con relación de las firmas digitales.

10.5.2 Los certificados deben cumplir con los requisitos exigidos en artículo 35 de la ley 527 de 1999, por ende, deben contener por lo menos lo siguiente:

a) Nombre, dirección y domicilio del suscriptor.
b) Una Identificación única del suscriptor nombrado en el certificado
c) El nombre y el lugar donde realiza actividades la CA.
d) Llave pública del certificado.
e) La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
f) El número de serie (único) del certificado.
g) Fecha de emisión y expiración del certificado.

Adicionalmente, y a partir del otorgamiento de la acreditación, los certificados de entidad final generados por la ECD deben incluir el Código de acreditación asignado por ONAC, lo cual podrá ser incluido conforme a una extensión de certificado definido en el numeral 4.2 del RFC 5280.

10.6 REQUISITOS DE DISPONIBILIDAD

10.6.1 Conforme con lo dispuesto en el literal d) del artículo 32 de la ley 527 de 1999, la ECD no podrá suspender los servicios de certificación digital relacionados en el alcance de acreditación, es decir debe cumplir una disponibilidad (uptime) del 99.8% 7x24x365 al año. Para Entidades de Certificación Cerradas corresponde como mínimo al 95% (uptime) por año.

10.6.2 Para las plataformas tecnológicas que requiera interrupciones por mantenimiento o actualización, la ECD debe informar a ONAC con anticipación de tres meses, adjuntando el plan de trabajo, los riesgos asociados garantizando que los servicios de certificación digital relacionados en el alcance de acreditación, se encuentren cumpliendo el 99.8 % (uptime). 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.

10.6.3 Disponibilidad de la lista de certificados revocados para las actividades de emisión de certificados en relación con las firmas electrónicas o digitales para personas naturales y jurídicas. En el caso del servicio de validación de certificados digitales, la ECD debe publicar y mantener la lista de certificados revocados en la CRL y OCSP con una disponibilidad de consulta en línea 7x24x365, 99.8% uptime por año. Para Entidades de Certificación Cerradas corresponde como mínimo al 95% uptime por año.

10.7 CESACIÓN DE ACTIVIDADES DE LA ECD

10.7.1 Conforme con lo dispuesto en el artículo 163 del Decreto Ley 019 del 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 capítulo 48 del DURSCIT, Artículo 2.2.2.48.3.8. Cesación de actividades.

En concordancia de lo anterior, la ECD debe tener.

a) Un plan de continuidad de negocio para todos los servicios que se encuentren acreditados o en proceso de acreditación.
b) Un plan que garantice la continuidad en alta disponibilidad de la infraestructura prestada para los servicios acreditados.
c) La ECD debe tener un plan de seguridad que garantice la adecuada cesación en sus actividades como ECD.

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

10.7.3 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:

a) La terminación de su actividad o actividades y la fecha precisa de cesación.
b) Las consecuencias jurídicas de la cesación respecto a los servicios acreditados
c) La posibilidad de que un suscriptor obtenga el reembolso equivalente al valor del tiempo de vigencia restante sobre el servicio contratado.
d) 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.

10.7.4 En todo caso los suscriptores podrán solicitar la revocación y el reembolso equivalente al valor del tiempo de vigencia restante de los servicios, si lo solicitan dentro de los dos (2) meses siguientes a la segunda publicación.

10.7.5 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.

10.8 ESTÁNDARES TÉCNICOS ADMITIDOS

10.8.1 De acuerdo con lo indicado en la Ley 527 de 1999, Artículo 2, literal d), una 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 Ley 019 del 2012, y debe asegurar el debido cumplimiento de los requisitos y estándares técnicos seleccionados o combinados de los siguientes anexos:

i. Actividad 1. Clasificada como: *Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.* Ver anexo A y B.
ii. Actividad 2. Clasificada como: Emitir *certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.* Ver anexo A.
iii. Actividad 3. Clasificada como: *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.* Ver anexo A.
iv. Actividad 4. Clasificada como: *Ofrecer o facilitar los servicios de generación de los datos de creación de las firmas digitales certificadas.* Ver anexo A.
v. Actividad 5. Clasificada como: *Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.* Ver anexo C.
vi. Actividad 6. Clasificada como: *Ofrecer o facilitar los servicios de generación de datos de creación de las firmas electrónicas.* Ver anexo B.
vii. Actividad 7. Clasificada como: *Ofrecer los servicios de registro, custodia y anotación de los documentos electrónicos transferibles.* Ver anexo D.
viii. Actividad 8. Clasificada como: *Ofrecer los servicios de archivo y conservación de mensajes de datos y documentos electrónicos transferibles.* Ver anexo D.
ix. Actividad 9. Clasificada como: *Cualquier otra actividad relacionada con la creación, uso o utilización de firmas digitales y electrónicas.* Ver anexo A y B.
x. Nota: En la definición de los mecanismos de validación del estado del certificado. Ver anexo E.
xi. Nota: Como referencia en dispositivos criptográficos. Ver anexo F.

NOTA 3 Debe entenderse que, si un estándar o un componente se encuentran actualizados por una nueva versión o reemplazado por otro estándar, es obligación de la ECD informar a ONAC sobre las actualizaciones, presentando el plan de actualización para poder implementar los estándares vigentes.

NOTA 4 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.

10.8.2 La ECD debe demostrar que la emisión de certificados en relación con las firmas digitales, cumplen con los requisitos establecidos en este documento.

a) La ECD para certificados centralizados puede utilizar software para el almacenamiento de llaves privadas. Se debe asegurar la llave privada mediante métodos de cifrado robustos en dispositivos criptográficos que cumplan la

certificación en estándares como mínimo FIPS 140-2 Level 3 o superior, o Common Criteria EAL 2 o superior relacionado a seguridad. Así mismo la ECD debe garantizar la protección de las llaves privadas mediante la aplicación de los controles técnicos establecidos en el anexo A de la norma internacional ISO/IEC 27001.

b) 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.

c) La ECD para certificados generados en dispositivos criptográficos como Token, Smartcard o componentes similares, estos deben ostentar las certificaciones en estándares criptográficos como FIPS 140-2 Level 3 o superior, o Common Criteria EAL 2 o superior relacionado a seguridad y almacenamiento de llaves.

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

10.8.3 Cuando el par de llaves sea generado por el suscriptor en software, la ECD debe demostrar la gestión del riesgo para el proceso de emisión de los certificados digitales y la aplicación de los controles correspondientes del Anexo A de la ISO/IEC 27001 vigente, de acuerdo con el formato y las características de la plataforma desatendida que utilice los formatos de los mensajes enviados a una CA para solicitar la certificación de una clave pública. La ECD debe documentar mediante la política de certificación el alcance en la plataforma desatendida, el uso y la responsabilidad del suscriptor en los tipos de certificados emitidos bajo esta modalidad.

10.9 ESTÁNDARES Y PRÁCTICAS TÉCNICAS NO ADMISIBLES PARA LOS SERVICIOS DE CERTIFICADOS CON RELACIÓN A LAS FIRMAS DIGITALES.

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

a) Cualquier estándar que use Criptografía de llave simétrica o asimétrica que se encuentre obsoleto, haya perdido vigencia o la seguridad se vea comprometida. Lo anterior de acuerdo con el listado estipulado en el anexo G.

b) Algoritmo de hash MD5. Algoritmo de reducción criptográfico de 128 bits.

c) No se permite la suspensión de certificados que no conduzca a un estado de revocación inmediato.

d) En el caso de las ECD abiertas, la red donde se encuentra la CA, debe estar aislada. Para las ECD cerradas, la red de la PKI debe estar en una VLAN o VPN exclusiva, con el fin de evitar que la red de la CA sea compartida con otras redes; para cualquiera de los dos casos debe estar aislada para no comprometer la clave de la CA.

e) Para las ECD, todas aquellas operaciones criptográficas relacionadas con la llave privada no pueden ser ejecutadas en un medio no diseñado para tal fin, es decir sólo se admite la operación criptográfica en dispositivos criptográficos certificados. Ver anexo F.

f) Solamente se permite HSM certificado. Ver anexo F.

g) La validez de un certificado digital para persona natural o jurídica no puede ser superior a 2 años.

h) El servicio de validación mediante OCSP, debe estar en línea con la revocación de los certificados digitales conforme al RFC 6960 ó RFC 5019.

i) El servicio de validación mediante CRL, debe estar sincronizado con la revocación de los certificados digitales conforme al RFC 5280.

j) No se permiten Claves RSA con longitud inferior a 2048 para certificados de entidad final.

k) No se permiten Claves inferiores a 4096 para CA Raíz y Subordinada.

l) La plataforma tecnológica de la CA utilizada por la ECD, debe ser de uso exclusivo para las actividades que conforman el alcance de acreditación solicitado.

10.10 REQUISITOS DE SEGURIDAD

10.10.1 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.

a) La ECD debe mantener, custodiar y proteger los LOG´s de cada uno de los servicios de certificación digital con fines de auditoria. El tiempo de retención de estos registros debe ser como mínimo de tres años o lo definido por el ente de vigilancia y control. (Frecuencia: Permanente).

b) La ECD debe realizar el monitoreo de eventos e incidentes de seguridad computacional (SOC – Security Operation Center) y hacer seguimiento al uso de los recursos y gestionar la capacidad mediante indicadores apropiados y garantizar la disponibilidad de los servicios de certificación digital. (NOC – Network Operation Center) utilizando el modelo PHVA.

c) 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 (**Militarización PKI).**

d) La ECD debe hacer pruebas de Ethical hacking y estas no podrán ser realizadas por la misma organización por más de dos veces consecutivas, y las personas quienes realicen estas pruebas, deben ser certificadas por un organismo de certificación de personas acreditado por un organismo de acreditación reconocido en el marco de los acuerdos de reconocimiento multilateral, garantizando la ejecución de las fases de hacking ético y la implementación eficaz en la evaluación, fortalecimiento y mejoramiento de la seguridad.

e) La ECD debe implementar y mantener un sistema de gestión de seguridad de la información con base en los requisitos de la norma ISO/IEC 27001 vigente para el alcance de las actividades de certificación digital en el marco de la acreditación.

10.11 REQUISITOS RELATIVOS AL PROCESO DEL CICLO DE VIDA DE LA CERTIFICACIÓN DIGITAL

10.11.1 SOLICITUD

La responsabilidad para la gestión de la solicitud debe ser asignada a una función dentro de la RA

La ECD debe obtener toda la información necesaria para gestionar la solicitud del servicio de certificación digital. La información 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 y/o suscriptor busca la certificación digital.
c) Los datos generales del solicitante y/o suscriptor, incluyendo su nombre, domicilio y todos los requisitos legales.
d) Información general respecto al solicitante y/o suscriptor, para el servicio de certificación digital para el cual se presenta la solicitud, de acuerdo con lo establecido en la DPC y la PC.
e) Una declaración de que el solicitante y/o suscriptor acuerda cumplir con los requisitos de la certificación y proporcionar toda información requerida.
f) La ECD debe establecer los medios y mecanismos para recolectar esta información en diversos momentos, a través de un formulario de solicitud en físico o digital.

10.11.2 REVISIÓN DE LA SOLICITUD

La ECD debe asignar la función de la revisión a la RA. La RA debe ejecutar la revisión de la información obtenida con el fin de garantizar que:

a) La revisión de la solicitud debe asegurar la identificación inequívoca de la identidad del suscriptor (persona natural o jurídica), la veracidad y autenticidad de la información, que permita dar una recomendación para la toma de decisión.

b) La ECD debe mantener registros de los procesos de validación de identidad para demostrar el cumplimiento eficaz de la identificación inequívoca del suscriptor y permitir una evaluación de dichos registros.
c) 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.
d) Se define el alcance del servicio de certificación digital solicitado.
e) Se dispone de los medios para realizar todas las actividades de verificación.
f) La ECD tiene la competencia y la capacidad para llevar a cabo la actividad y servicios de certificación digital.
g) 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.
h) La ECD debe documentar los procesos y los resultados relacionados con la revisión de la solicitud, incluyendo la recomendación para la decisión sobre la certificación con base en la revisión.

10.11.3 DECISIÓN DE CERTIFICACIÓN PARA LAS ACTIVIDADES DE EMISIÓN DE CERTIFICADOS

10.11.3.1 La ECD debe ser responsable de sus decisiones relacionadas con la certificación digital y debe conservar su poder de decisión, que no debe ser delegado, incluyendo otorgar, mantener, cancelar o retirar (revocar) la certificación. Las decisiones relativas a la certificación no deben contratase externamente.

10.11.3.2 Para los servicios de certificación digital que incluyan las actividades 1, 2, 3 y 4 del Artículo 161 del Decreto Ley 019 de 2012, la ECD debe asegurar independencia e imparcialidad entre las funciones de revisión y de decisión de la certificación.

10.11.3.3 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) Una entidad bajo el control organizacional de la ECD. 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 5 En el caso de las ECD de naturaleza pública, se puede considerar que otras partes del mismo gobierno están "vinculadas por propiedad" a la ECD.

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

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

10.11.3.5 La información reunida durante el proceso de certificación debe ser suficiente para permitir:

a) Al organismo de certificación tomar una decisión respecto a la certificación.
b) La trazabilidad en el caso, por ejemplo, de una queja.

10.11.3.6 No se debe otorgar la certificación digital o realizar la activación del servicio hasta que no se hayan cumplido todos los requisitos de certificación.

10.11.3.7 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.

10.11.4 DOCUMENTACIÓN DE LA CERTIFICACIÓN DIGITAL

10.11.4.1 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 o las características del servicio adquirido como lo ha establecido en la DPC y PC.

10.11.4.2 La documentación de los servicios de certificación digital suministrada al suscriptor debe incluir como mínimo:

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

10.11.4.3 La documentación formal de los servicios de certificación digital debe incluir la firma de a quienes la ECD le ha asignado la responsabilidad y autoridad para la toma de decisión y/o la activación del servicio

10.11.4.4 La documentación formal de los servicios de 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 los servicios de certificación digital.
b) Se ha firmado el acuerdo de los servicios de certificación digital.

10.11.4.5 La documentación formal de los servicios de certificación digital debe dar cumplimiento a lo establecido en el RAC-3.03 Reglamento de uso de los símbolos de acreditado y/o asociado.

10.11.5 REVOCACIÓN O CANCELACIÓN DE LA CERTIFICACIÓN DIGITAL

10.11.5.1 En la DPC debe tener una regla para revocar o cancelar un certificado digital ya sea por solicitud del suscriptor, o cuando la ECD conoce, tiene indicios o confirmación de alguna de las siguientes situaciones:

a) Por compromiso de la seguridad en cualquier motivo, modo, situación o circunstancia.
b) Por muerte o incapacidad sobrevenida del suscriptor.
c) Por liquidación de la persona jurídica representada que consta en el servicio de certificación digital.
d) Por la confirmación de que alguna información o hecho contenido en el certificado digital es falso.
e) Por la ocurrencia de hechos nuevos que provoquen que los datos originales no correspondan a la realidad.
f) Por orden judicial o de entidad administrativa competente.
g) Por pérdida, inutilización del certificado digital que haya sido informado a la ECD.
h) Por la terminación del contrato de suscripción, de conformidad con las causales establecidas en el contrato.
i) Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto de que se ponga en duda la confiabilidad del servicio.
j) Por el manejo indebido por parte del suscriptor del certificado digital.
k) 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.

10.11.5.2 En caso de que se revoque un certificado con relación a las firmas electrónicas o digitales, posteriormente el mismo NO podrá ser rehabilitado por la ECD.

10.11.5.3 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.

10.11.5.4 Cuando las acciones a seguir respecto al cambio de estado de un certificado digital incluyen la revisión o decisión sobre la certificación digital.

10.12 QUEJAS Y RECLAMOS

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

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

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

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

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

10.12.6 La ECD debe emprender las acciones posteriores necesarias para resolver el reclamo.

10.13 REQUISITOS DEL SISTEMA DE GESTIÓN

La ECD debe tener un sistema de gestión en seguridad de la información y calidad que garantice la emisión y creación de firmas digitales, la conservación y archivo de certificados y documentos en soporte de mensaje de datos, dando conformidad con el capítulo 48 del DURSCIT, Artículo 2.2.2.48.3.2. Infraestructura y recursos, que 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 (…).*

Adicionalmente, la ECD debe demostrar la implementación del modelo de gestión de calidad PHVA (Planear, Hacer, Verificar y Actuar), para para el sistema de gestión y sus procesos.

La ECD debe determinar los riesgos y oportunidades que es necesario tratar, relacionadas con sus actividades y procesos de certificación digital con el fin de:

- Asegurare de que el sistema de gestión pueda lograr los resultados previstos
- Prevenir o reducir efectos indeseados
- Lograr la mejora continua

10.13.1 La caracterización de los procesos que cubran los servicios de certificación digital debe contener como mínimo:

a. Nomenclatura, versión y fecha de última actualización
b. Objeto
c. Roles y responsables.
d. Proveedores e insumos, o entradas y productos, o salidas y usuarios o clientes.
e. Recursos asociados a la gestión del proceso.
f. Riesgos y controles asociados e indicadores del proceso.
g. Requisitos relacionados con el proceso, documentos y registros del mismo.
h. Flujograma del proceso.

10.13.2 La ECD debe implementar y mantener un procedimiento de seguridad para el manejo y la gestión de incidentes conforme a lo descrito en el capítulo 48 del DURSCIT, Artículo 2.2.2.48.3.1 numeral 9, en el cual se definen entre otros eventos e incidentes que se deben registrar.

10.13.3 La ECD debe establecer, documentar, implementar, mantener y mejorar continuamente un sistema de gestión capaz de demostrar el cumplimiento coherente de los requisitos de los Criterios Específicos de Acreditación. Además de cumplir los criterios definidos en el presente documento, relacionados al sistema de gestión; la ECD debe implementar un sistema de gestión de acuerdo con la opción A o la opción B.

10.13.3.1 OPCIÓN A

Un sistema general de gestión que dé cumplimiento a los siguientes aspectos:

a) Documentación del sistema de gestión.

La ECD debe garantizar el cumplimiento de los requisitos sobre la documentación del sistema de gestión, establecidos en mantener y documentar los requisitos aplicables de la ISO 9001 o ISO/IEC 20000-1.

La ECD debe documentar los requisitos aplicables de estos Criterios Específicos de Acreditación. La ECD debe asegurarse de que la documentación del sistema de gestión es accesible a todo el personal pertinente.

b) Control de la información documentada.

La ECD debe establecer procedimientos para controlar los documentos (internos y externos) que se refieren al cumplimiento de estos Criterios Específicos de Acreditación. Los procedimientos deben definir los controles necesarios para:

1. Aprobar los documentos en cuanto a su adecuación antes de su emisión.
2. Revisar y actualizar los documentos cuando sea necesario, y aprobarlos nuevamente.
3. Asegurarse de que se identifican los cambios y el estado de revisión en vigor de los documentos.
4. Asegurarse de que las versiones pertinentes de los documentos aplicables se encuentran disponibles en los lugares de uso.
5. Asegurarse de que los documentos permanezcan legibles y fácilmente identificables.
6. Asegurarse de que se identifican los documentos de origen externo y se controla su distribución
7. La ECD debe establecer procedimientos para definir los controles necesarios para la identificación, el almacenamiento, la protección, la recuperación, el tiempo de retención y la disposición de los registros relacionados con el cumplimiento de los requisitos de estos Criterios Específicos de Acreditación.
8. La ECD debe establecer procedimientos para la retención de registros por un periodo que sea coherente con sus obligaciones contractuales y legales. El acceso a estos registros debe ser compatible con los acuerdos de confidencialidad

NOTA 6 La documentación puede estar en cualquier forma o tipo de medio.

c) Revisión por la dirección

La ECD debe garantizar el compromiso de la alta dirección, para llevar a cabo la implementación y mantener la estructura en el tiempo, conforme al numeral "Revisión por la dirección" de la ISO/IEC 27001.

La alta dirección de la ECD debe establecer procedimientos para revisar su sistema de gestión a intervalos planificados para asegurar su continua conveniencia, adecuación y eficacia, incluyendo las políticas y los objetivos declarados, relativos al cumplimiento de estos Criterios Específicos de Acreditación. Estas revisiones deben llevarse a cabo al menos cada doce meses y deben estar documentadas.

La información de entrada para la revisión por la dirección debe incluir información relativa a:

1. Los resultados de las auditorías internas y externas (por ejemplo, evaluación del organismo de acreditación).
2. La retroalimentación de los solicitantes y suscriptores.
3. La salvaguardia de la imparcialidad.
4. La eficacia de las acciones tomadas para abordar los riesgos y las oportunidades.
5. Seguimiento a las acciones correctivas y de mejora.
6. Las acciones de seguimiento provenientes de revisiones por la dirección previas.
7. El cumplimiento de los objetivos.
8. Los cambios que podrían afectar al sistema de gestión.
9. Las quejas y reclamos.

Los resultados de la revisión por la dirección deben incluir como mínimo decisiones y acciones relativas a lo siguiente:

1. La mejora de la eficacia del sistema de gestión y de sus procesos.

2. Las mejoras de los servicios de certificación en relación con el cumplimiento de esta Norma Internacional.

3. La necesidad de recursos.

d) Auditoría de Tercera Parte

En cumplimiento del capítulo 48 del DURSCIT, Artículo 2.2.2.48.3.5. Auditorías, la ECD debe subcontratar la realización de una auditoria de Tercera Parte, que incluya la evaluación de los requisitos establecidos en Ley 527 de 1999, los reglamentos que lo modifican y/o complementen, la norma ISO/IEC 27001 para el alcance de los servicios dentro del alcance de acreditación y el CEA-3.0-07 de ONAC. La auditoría de tercera parte, se debe realizar al menos una vez cada 12 meses. La frecuencia de la auditoría de tercera parte se puede aumentar en función de la eficacia demostrada del sistema de gestión y su estabilidad probada.

El proveedor de los servicios de auditoría de tercera parte debe cumplir los criterios del numeral 10.3 del presente CEA-3.0-07 y adicionalmente asegurar los siguientes criterios:

I. Las competencias del grupo auditor deberán demostrarse respecto a los criterios específicos de acreditación, los requisitos de la norma internacional ISO/IEC 27001 en cuanto a seguridad de la información, en relación con el servicio ISO 9001 o ISO/IEC 20000-1, en caso de que el auditor no tenga competencia en PKI, debe estar en compañía de un experto técnico conocedor de la gestión relacionada a infraestructura de llave pública PKI.

II. Los auditores no deben tener conflicto de interés.

III. El personal responsable del área auditada sea informado del resultado de la auditoria.

IV. Cualquier acción resultante de las auditorías de tercera parte se realice sin demora no justificada.

V. Cualquier oportunidad de mejora sea identificada.

VI. Debe ser una empresa de auditoría legalmente constituida cuyo objeto social esté incluido: servicios de auditoría de sistemas, seguridad de la información e infraestructura de llave pública PKI.

VII. Personal auditor debe contar con tarjeta profesional vigente en Ingeniería.

La auditoría de tercera parte deberá demostrar en el Informe final que se auditaron todos los requisitos del presente CEA-3.0-07, con resultados en cuanto a la conformidad.

e) Mejora

La ECD debe garantizar la idoneidad, adecuación y eficacia del sistema de gestión.

f) No conformidades, acciones correctivas y acciones de mejora.

La ECD debe establecer e implementar procedimientos para gestionar las no conformidades, definir las correcciones y acciones correctivas para prevenir su recurrencia y verificar su eficacia. La ECD debe mejorar continuamente la eficacia del sistema de gestión, con base en los resultados de:

- Gestión de No conformidades.
- Gestión de Incidentes de seguridad de la información.
- Atención de PQRS.
- Indicadores de desempeño.
- Gestión de la continuidad del negocio.
- Auditorías.

- Revisión por la dirección.

10.13.3.2 OPCIÓN B

Un sistema de gestión certificado en el cumplimiento de los requisitos de las normas ISO9001 o ISO/IEC 20000-1, y que es capaz de sustentar y demostrar el cumplimiento constante de los requisitos del presente CEA-3.0-07.

NOTA 7 En esta opción también se debe hacer la Auditoria de tercera parte como lo indica el criterio numeral 10.13.3.1 literal (d) del presente CEA-3.0-07.

11. DOCUMENTOS RELACIONADOS

- RAC-3.0-01 REGLAS DEL SERVICIO DE ACREDITACIÓN
- LEY 527 DE 1999
- DECRETO LEY 019 DE 2012
- DECRETO ÚNICO DEL SECTOR COMERCIO, INDUSTRIA Y TURISMO - DURSCIT, 1074 DE 2015
- DECRETO 1595 DE 2015

12. CONTROL DE CAMBIOS

Versión	Fecha de emisión	Resumen de cambios
1	2015-08-11	Versión Inicial del documento
2	2021-07-02	Actualización general del documento, alineando los requisitos técnicos establecidos con el desarrollo y transformación de nuevas tecnologías.

13. ANEXOS

Anexo A: Actividades del artículo 161 que hacen referencia al Decreto Ley 019 del 2012, estas actividades están clasificadas como EMISIÓN DE CERTIFICADOS DIGITALES (firmas digitales).

Anexo B: Actividades del artículo 161 que hacen referencia al Decreto Ley 019 del 2012, estas actividades están clasificadas servicios de firma electrónica.

Anexo C: Actividades del artículo 161 que hacen referencia al Decreto Ley 019 del 2012, estas actividades están clasificadas como SERVICIOS ESTAMPADO CRONOLÓGICO, (estampado de tiempo).

Anexo D: Actividades del artículo 161 que hacen referencia al Decreto Ley 019 del 2012, estas actividades están clasificadas como ARCHIVO, REGISTRO, CONSERVACIÓN CUSTODIA Y ANOTACIÓN PARA LOS DOCUMENTOS ELECTRÓNICOS TRANSFERIBLES Y MENSAJES DE DATOS

Anexo E: MECANISMOS DE VALIDACIÓN DEL ESTADO DEL CERTIFICADO

Anexo F: DISPOSITIVOS CRIPTOGRÁFICOS

Anexo G: ANEXOS INFORMATIVOS

ESTÁNDARES TÉCNICOS PARA LOS SERVICIOS DE LAS ECD

Anexo A: Actividades del artículo 161 que hacen referencia al Decreto Ley 019 del 2012, estas actividades están clasificadas como EMISIÓN DE CERTIFICADOS DIGITALES (firmas digitales).

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
9. Cualquier otra actividad relacionada con la creación, uso o utilización de firmas digitales y electrónicas

Los siguientes, son los estándares técnicos vigentes aplicables a las anteriores actividades:

ID	ARTÍCULO 161. ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACIÓN	REQUISITO	ESTÁNDARES TÉCNICOS VIGENTES
A1	1,2,3,4,9	**Algoritmo de firma**	Función hash y RSA SHA256 con RSA Encryption RSA con tamaño o longitud de clave no inferior a 2048 para entidad final. RSA con tamaño o longitud de clave no inferior a 4096 para CA Raíz y Subordinadas. 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.
A2	1,2,3,4,9	**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.
A3	1,2,3,4,9	**Ciclo de vida de los certificados**	RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Estandar ETSI EN 319 411 V 1.1.1 febrero 2016 Estandar ETSI EN 319 412 V 1.1.1 febrero 2016
A4	1,2,3,4,9	**LDAP repositorio de certificados (LDAP)**	RFC 4523 - Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates
A5	1,2,3,4,9	**Generación de claves**	Dispositivos criptográficos certificados.

ID	ARTÍCULO 161. ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACIÓN	REQUISITO	ESTÁNDARES TÉCNICOS VIGENTES
A6	1,2,3,4,9	**Dispositivo Criptográfico**	Ver Anexo F
A7	1,2,3,4,9	**Validación del estado del certificado**	Ver Anexo E
A8	1,2,3,4,9	**Formatos de Firma digital**	RFC 5126 CMS Advanced Electronic Signatures (CAdES) ISO/IEC 14533-1 (CAdES) RFC 5652 Cryptographic Message Syntax (CMS). ETSI TS 101 733 CMS Advanced Electronic Signatures (CAdES) W3C XML Advanced Electronic Signatures (XAdES) NTC-ISO/IEC 14533-2 (XAdES) ETSI TS (EN) 101 903 XML Advanced Electronic Signatures (XAdES) ETSI TS(EN) 102 778 PDF Advanced Electronic Signature Profiles (PAdES) RFC 2630 "Cryptographic Message Syntax" RFC 3852 "Cryptographic Message Syntax" (deja obsoletos los RFC3369, RFC 3211, RFC 2630, RFC 2315-PKCS #7 version 1.5) RFC 4853 – (Actualización Marzo 2008) "Cryptographic Message Syntax – Multiple Signer Clarification" ISO/IEC 32001 Pend (PDF) 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.

Anexo B: Actividades del artículo 161 que hacen referencia al Decreto Ley 019 del 2012, estas actividades están clasificadas servicios de firma electrónica.

5. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.
6. Ofrecer o facilitar los servicios de generación de datos de creación de las firmas electrónicas.
9. Cualquier otra actividad relacionada con la creación, uso o utilización de firmas digitales y electrónicas.

Los siguientes, son los estándares técnicos vigentes aplicables a las anteriores actividades:

ID	ARTÍCULO 161. ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACIÓN	REQUISITO	ESTÁNDARES TÉCNICOS VIGENTES

ID	ARTÍCULO 161. ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACIÓN	REQUISITO	ESTÁNDARES TÉCNICOS VIGENTES
B1	1,6,9	**Formatos de Firma electrónica**	CAdES (CMS Advanced Electronic Signatures). ETSI TS 101 733 CAdES version 1.7.4 from Jul, 2008 XAdES (XML Advanced Electronic Signatures). ETSI TS 101 903 XAdES version 1.4.1 from 2009-06-15 PAdES (PDF Advanced Electronic Signatures). ETSI TS 102778 (PAdES FAQ) RFC 3126 "Electronic Signature Formats for long term electronic signatures" RFC 2634 "Enhanced Security Services for S/MIME" RFC 5126 "CMS Advanced Electronic Signatures (CAdES)" RFC 3275 "(Extensible Markup Language) XML-Signature Syntax and Processing " RFC 2797 "Certificate Management Messages over CMS" RFC 2585 "Operational Protocols: FTP and HTTP" RFC 3029 "Data Validation and Certification Server Protocols" CWA 15579 E-invoices and digital signatures ETSI TS 102 042 Policy requirements for CA issuing PKC ETSI TS 102 023 Policy Requirements for Time Stamping Authorities Certificates for Electronic Signatures – Part 1: System Security Requirements ETSI TS 102 231 Provision of harmonized Trust Service Provider status information (TSL) ETSI TS 102 280 X.509 V.3 Certificate Profile for Certificates Issued to

ID	ARTÍCULO 161. ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACIÓN	REQUISITO	ESTÁNDARES TÉCNICOS VIGENTES
			Natural Persons ETSI TS 102 158 Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates CEN / ISSS CWA 14167-2 Cryptographic module for CSP signing operations with backup – Protection profile – CMCSOB PP CEN / ISSS CWA 14167-3 Cryptographic module for CSP key generation services protection profile CMCKG-PP CEN / ISSS CWA 14167-4 Cryptographic module for CSP signing operations – Protection profile – CMCSO PP CEN / ISSS CWA 14169 Secure signature-creation devices "EAL 4+" CEN / ISSS CWA 14170 Security requirements for signature creation applications CEN / ISSS CWA 14171 General Guidelines for Electronic Signature Verification CEN / ISSS CWA 14172 EESSI Conformity Assessment Guidance (8 parts) CEN / ISSS CWA 14355 Guidelines for the implementation of Secure Signature-Creation Devices CEN / ISSS CWA 14365-1 Guide on the Use of Electronic Signatures – Part 1: Legal and Technical Aspects CEN / ISSS CWA 14365-2 Guide on the Use of Electronic Signatures – Part 2: Protection Profile for Software Signature Creation Devices CEN / ISSS CWA 14167-1 Security Requirements for Trustworthy

ID	ARTÍCULO 161. ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACIÓN	REQUISITO	ESTÁNDARES TÉCNICOS VIGENTES
			Systems Managing CEN / ISSS CWA 14890-1 Application Interface for smart cards used as Secure Signature Creation Devices – Part 1: Basic requirements CEN / ISSS CWA 14890-2 Application Interface for smart cards used as Secure Signature Creation Devices – Part 2: Additional Services TR 102 047 (International Harmonization of Electronic Signature Formats) FIPS PUB 180-1 (Secure Hash Standard) ISO/IEC 32000 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.
B2	1,6,9	**Biometría**	ISO/IEC 19794-1: 2006 Information Technology. Formato de datos biométricos para el intercambio entre aplicaciones. Marco general que resume los demás trabajos. ISO/IEC 19794-10: 2007 Information Technology. Formato de los datos para sistemas biométricos basados en la geometría de la mano. ISO/IEC 19794-2: 2005 Information Technology. Formato de los datos para sistemas biométricos basados en minucias de los dedos. ISO/IEC 19794-3: 2005 Information Technology. Formato de los datos para sistemas biométricos basados en patrones de dedo. ISO/IEC 19794-4: 2005 Information Technology. Formato de los datos para sistemas biométricos basados en imágenes de dedo. ISO/IEC 19794-5: 2005 + A2: 2009 Information Technology. Formato de los datos para sistemas biométricos

ID	ARTÍCULO 161. ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACIÓN	REQUISITO	ESTÁNDARES TÉCNICOS VIGENTES
			basados en imágenes del rostro. ISO/IEC 19794-6: 2005 Information Technology. Formato de los datos para sistemas biométricos basados en imágenes de iris. ISO/IEC 19794-7: 2007 Information Technology. Formato de los datos para sistemas biométricos basados en la firma manuscrita. ISO/IEC 19794-8: 2008 Information Technology. Formato de los datos para sistemas biométricos basados en el esqueleto del dedo. ISO/IEC 19794-9: 2007 Information Technology. Formato de los datos para sistemas biométricos basados en imágenes vasculares ISO/IEC 19794-11, Information Technology. Formato de los datos para sistemas biométricos basados en firmas dinámicas ISO/IEC 19794-13, Information Technology. Formato de los datos para sistemas biométricos basados en la voz ISO/IEC 19794-14, Information Technology. Formato de los datos para sistemas biométricos basados en el ADN
B3	1,6,9	**Credenciales**	Nivel Medio equivalente al nivel de Garantía 2 (NdG2) Nivel muy Alto equivalente a nivel de Garantía 4 (NdG4) ITU X.1254 ISO/IEC 29115:2013. ITU X.1251 ITU X 1253 NIST: 800-63-3 Digital Identity Guidelines NITS:800-63A Enrollment and Identity Proofing NITS:800-63B Authentication and

ID	ARTÍCULO 161. ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACIÓN	REQUISITO	ESTÁNDARES TÉCNICOS VIGENTES
			Lifecycle Management NITS:800-53 Revisión 5, Security and Privacy Controls for Information Systems and Organizations

Anexo C: Actividades del artículo 161 que hacen referencia al Decreto Ley 019 del 2012, estas actividades están clasificadas como SERVICIOS ESTAMPADO CRONOLÓGICO, (estampado de tiempo).

5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.

Los siguientes, son los estándares técnicos vigentes aplicables a las anteriores actividades

ID	ARTÍCULO 161. ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACIÓN	REQUISITO	ESTÁNDARES TÉCNICOS VIGENTES
C1	5	**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 ETSI TS 101 861 V1.2.1 Time stamping profile
C2	5	**Fuente de tiempo**	Hora oficial de país, provista por el Instituto Nacional de Metrología. Los servidores se mantienen actualizados con la escala de tiempo internacional UTC, mediante sincronización a través del protocolo NTP v4, conforme al Instituto nacional de metrología (INM), y debe tener otro punto de sincronización ya sea por coordenadas establecidas en la plataforma. RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification
C3	5	**HSM para TSA**	Anexo F
C4	5	**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 del artículo 161 que hacen referencia al Decreto Ley 019 del 2012, estas actividades están clasificadas como ARCHIVO, REGISTRO, CONSERVACIÓN CUSTODIA Y ANOTACIÓN PARA LOS DOCUMENTOS ELECTRÓNICOS TRANSFERIBLES Y MENSAJES DE DATOS:

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.

Los siguientes, son los estándares técnicos vigentes aplicables a las anteriores actividades:

ID	ARTÍCULO 161. ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACIÓN	REQUISITO	ESTÁNDARES TÉCNICOS VIGENTES
D1	7,8	**Archivos y conservación de mensajes de datos y documentos electrónicos transferibles**	NTC-ISO/IEC 14641-1 Noviembre 2014 GTC-ISO-TR 18492:2013 ISO/IEC 15489-1:2001 ISO/IEC 14721:2012 NTC 4095 Septiembre 2013
D2	7,8	**Registro, custodia, y anotación, de los documentos transferibles.**	NTC-ISO/IEC 14641-1 Noviembre 2014 ISO/IEC 17068 versión vigente. ISO/IEC 15489-1:2001 ISO/IEC 14721:2012
D3	7,8	**Archivo, custodia y conservación**	ISO/IEC 639. Establecer códigos internacionalmente reconocidos NTC 4095. NORMA GENERAL PARA LA DESCRIPCION ARCHIVISTICA ISO/IEC TR/17068. Information and documentation. Trusted third party repository for digital records GTC-ISO-TR 18492. Preservación a largo plazo de la información basada en documentos electrónicos NTC-ISO/IEC 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 NTC-ISO/IEC 23081-1. Información y documentación. Procesos para la gestión de registros. Metadatos para los registros. Parte 1: principios ISO/IEC 23081-2. Information and documentation. Managing metadata for record. Part 2: Conceptual and implementation issues.

ID	ARTÍCULO 161. ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACIÓN	REQUISITO	ESTÁNDARES TÉCNICOS VIGENTES
			ISO/IEC 23081-3. Information and documentation. Managing metadata for records. Part 3: Self-assessment method ISO/IEC 11179-3. los registros de metadatos (MDR) – meta modelo Registro y atributos básicos GTC-ISO-TR 26122. Información y documentación. Análisis de procesos de trabajo para registros. ISO-TR 18128. Information and documentation. Risk assessment for records processes and systems. GTC-ISO-TR 15801. Gestión de documentos. Información almacenada electrónicamente. Recomendaciones para la integridad y la fiabilidad. ISO/IEC 14721. Space data and information transfer systems. Open archival information system (OAIS). Reference model. NTC-ISO/IEC 30301. Información y documentación. Sistemas de gestión de registros. Requisitos. NTC-ISO/IEC 30300. Información y documentación. Sistemas de gestión para registros. Fundamentos y vocabulario. NTC-ISO/IEC 15489-1. Información y documentación. Gestión de documentos. Parte 1. Generalidades. GTC-ISO-TR 15489-2. Información y documentación. Gestión de documentos. Parte 2. Guía ISO/IEC 15836. Information and documentation. The Dublin Core metadata element set ANSI/ARMA 19. Policy Design for Managing Electronic Messages ARMA TR 24. Best Practices for Managing Electronic Messages ARMA TR 23. Developing Electronic File Structures BS 10008. Evidential weight and legal admissibility of electronic information. Specification

ID	ARTÍCULO 161. ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACIÓN	REQUISITO	ESTÁNDARES TÉCNICOS VIGENTES
			ISO/IEC 27005. Information technology -- Security techniques -- Information security risk management ISO/IEC 27037. Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence
D4	7,8	**Servicios de digitalización y migración**	NTC 5985. Información y documentación. Directrices de implementación para digitalización de documentos ISO/TR 15801: Gestión de documentos. Información almacenada electrónicamente. Recomendaciones para la integridad y la fiabilidad. NTC-ISO/IEC 13008. Información y documentación. Proceso de conversión y migración de registros digitales ISO/TR 13028. Directrices de aplicación para la digitalización de los registros
D5	7,8	**Transferencia**	NTC-ISO/IEC 12639. Tecnología gráfica - el intercambio de datos digitales de pre impresión - Tag formato de archivo de imagen para la tecnología de imagen (TIFF / IT) ISO/IEC 32000 a gestión de documentos - Formato de Documento Portátil ISO/IEC 19005 (PDF/A-2): Document Management - Electronic document file format for long term preservation (en caso de utilizarlos) ISO/IEC 15444-1:2004 (JPEG). ISO/IEC 13008. Información y documentación. Proceso de conversión y migración de registros digitales ISO/IEC 9660. Procesamiento de la información - Volumen y estructura de archivos de CD-ROM para el intercambio de información ISO/IEC 16363: Space data and information transfer systems -- Audit and certification of trustworthy digital repositories
D6	7,8	**Servicios Asociados a Sistemas de Información**	NTC-ISO/IEC 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.

ID	ARTÍCULO 161. ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACIÓN	REQUISITO	ESTÁNDARES TÉCNICOS VIGENTES
			NTC-ISO/IEC 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. ISO/IEC 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 ISO/IEC 22957. Document management. Analysis, selection and implementation of electronic document management systems (EDMS). AIIM/ARMA TR48. Revised Framework for Integration of EDMS & ERMS Systems.
D7	7,8	**Blockchain**	ISO/IEC /CD 22739 Tecnologías de blockchain y ledger distribuido – Terminología ISO/IEC / NP TR 23244 descripción general de la privacidad y la protección de la información de identificación personal (PII) ISO/IEC / NP TR 23245 Riesgos y vulnerabilidades de seguridad ISO/IEC / NP TR 23246 descripción general de la gestión de identidades utilizando las tecnologías blockchain y libro mayor distribuido. ISO/IEC / AWI 23257 Arquitectura de referencia ISO/IEC / AWI TS 23258 Taxonomía y Ontología ISO/IEC / AWI TS 23259 contratos inteligentes vinculantes legalmente. ISO/IEC / CD TR 23455 descripción general e interacciones entre contratos inteligentes en sistemas de blockchain y sistemas de tecnología de ledger distribuido. ISO/IEC / NP TR 23576 Seguridad de custodios de activos digitales ISO/IEC / NP TR 23578 problemas de

ID	ARTÍCULO 161. ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACIÓN	REQUISITO	ESTÁNDARES TÉCNICOS VIGENTES
			descubrimiento relacionados con la interoperabilidad. ISO/IEC / NP TS 23635 Pautas para la gobernabilidad

Anexo E: MECANISMOS DE VALIDACIÓN DEL ESTADO DEL CERTIFICADO

ESTÁNDARES TÉCNICOS PARA LOS SERVICIOS DE LAS ECD

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.
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, disponible, 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 CRIPTOGRÁFICO	REQUISITO
Dispositivos criptográficos para el almacenamiento de certificados digitales y llave privada de los suscriptores.	Certificado FIPS 140-2 Level 3 o superior o, Common Criteria relacionado a seguridad y almacenamiento de llaves. 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 o, Common Criteria relacionado a seguridad y almacenamiento de llaves. Longitud de Clave RSA 2048 o superior, exigible 4096 cuando se declare inseguro RSA 2048.

Anexo G: ANEXOS INFORMATIVOS

G.1 RESUMEN DE LOS ESTÁNDARES PKCS

PKCS	Versión	Nombre	Comentarios	Estado
PKCS#1	2.1	Estándar criptográfico RSA	Ver RFC 3447. Define el formato del cifrado RSA.	
PKCS#2	-	RSA Cryptography Standard	Definía el cifrado RSA de resúmenes de mensajes, pero fue absorbido por el PKCS#1.	Obsoleto
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	-	RSA Cryptography Standard	Definía la sintaxis de la clave RSA, pero fue absorbido por el PKCS#1.	Obsoleto
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	Versión	Nombre	Comentarios	Estado
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.	No admisible
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.	