El Sistema Nacional de Certificación Digital

Rama del Derecho: Derecho Informático.	**Descriptor: Seguridad informática.**
Palabras Clave: Ley de Certificados, Firmas Digitales y Documentos Electrónicos, Sistema Nacional para la Calidad, Publicaciones en los Diarios Oficiales.	
Fuentes: Normativa.	**Fecha de elaboración: 09/09/2014.**

El presente documento contiene normativa relacionada al Sistema Nacional de Certificación Digital, así como acciones directrices y políticas del Gobierno Digital sobre la implementación de la misma.

Contenido

NORMATIVA

1. LEY DE CERTIFICADOS, FIRMAS DIGITALES Y DOCUMENTOS ELECTRÓNICOS

[Ley 8454 sobre Certificados, Firmas Digitales y documentos Electrónicos][i]

CAPÍTULO I

Disposiciones generales

Artículo 1º-**Ámbito de aplicación.** Esta Ley se aplicará a toda clase de transacciones y actos jurídicos, públicos o privados, salvo disposición legal en contrario, o que la naturaleza o los requisitos particulares del acto o negocio concretos resulten incompatibles.

El Estado y todas las entidades públicas quedan expresamente facultados para utilizar los certificados, las firmas digitales y los documentos electrónicos, dentro de sus respectivos ámbitos de competencia.

Artículo 2º-**Principios.** En materia de certificados, firmas digitales y documentos electrónicos, la implementación, interpretación y aplicación de esta Ley deberán observar los siguientes principios:

a) Regulación legal mínima y desregulación de trámites.

b) Autonomía de la voluntad de los particulares para reglar sus relaciones.

c) Utilización, con las limitaciones legales, de reglamentos autónomos por la Administración Pública para desarrollar la organización y el servicio, interno o externo.

d) Igualdad de tratamiento para las tecnologías de generación, proceso o almacenamiento involucradas.

CAPÍTULO II

Documentos

Artículo 3º-**Reconocimiento de la equivalencia funcional.** Cualquier manifestación con carácter representativo o declarativo,

expresada o transmitida por un medio electrónico o informático, se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos.

En cualquier norma del ordenamiento jurídico en la que se haga referencia a un documento o comunicación, se entenderán de igual manera tanto los electrónicos como los físicos. No obstante, el empleo del soporte electrónico para un documento determinado no dispensa, en ningún caso, el cumplimiento de los requisitos y las formalidades que la ley exija para cada acto o negocio jurídico en particular.

Artículo 4º-**Calificación jurídica y fuerza probatoria.** Los documentos electrónicos se calificarán como públicos o privados, y se les reconocerá fuerza probatoria en las mismas condiciones que a los documentos físicos.

Artículo 5º-**En particular y excepciones.** En particular y sin que conlleve la exclusión de otros actos, contratos o negocios jurídicos, la utilización de documentos electrónicos es válida para lo siguiente:

a) La formación, formalización y ejecución de los contratos.

b) El señalamiento para notificaciones conforme a la Ley de notificaciones, citaciones y otras comunicaciones judiciales.

c) La tramitación, gestión y conservación de expedientes judiciales y administrativos; asimismo, la recepción, práctica y conservación de prueba, incluida la recibida por archivos y medios electrónicos.

De igual manera, los órganos jurisdiccionales que requieran la actualización de certificaciones y, en general, de otras piezas, podrán proceder sobre simples impresiones de los documentos en línea efectuadas por el despacho o aceptar las impresiones de dichos documentos en línea, aportadas por la parte interesada y certificadas notarialmente.

d) La emisión de certificaciones, constancias y otros documentos.

e) La presentación, tramitación e inscripción de documentos en el Registro Nacional.

f) La gestión, conservación y utilización, en general, de protocolos notariales, incluso la manifestación del consentimiento y la firma de las partes.

No se podrán consignar en documentos electrónicos:

a) Los actos o negocios en los que, por mandato legal, la fijación física resulte consustancial.

b) Las disposiciones por causa de muerte.

c) Los actos y convenios relativos al Derecho de familia.

d) Los actos personalísimos en general.

Artículo 6º-**Gestión y conservación de documentos electrónicos.** Cuando legalmente se requiera que un documento sea conservado para futura referencia, se podrá optar por hacerlo en soporte electrónico, siempre que se apliquen las medidas de seguridad necesarias para garantizar su inalterabilidad, se posibilite su acceso o consulta posterior y se preserve, además, la información relativa a su origen y otras características básicas.

La transición o migración a soporte electrónico, cuando se trate de registros, archivos o respaldos que por ley deban ser conservados, deberá contar, previamente, con la autorización de la autoridad competente.

En lo relativo al Estado y sus instituciones, se aplicará la Ley del Sistema Nacional de Archivos, Nº 7202, de 24 de octubre de 1990. La Dirección General del Archivo Nacional dictará las regulaciones necesarias para asegurar la gestión debida y conservación de los documentos, mensajes o archivos electrónicos.

Artículo 7º-**Satisfacción de los requisitos fiscales.** Cuando la emisión de un acto o la celebración de un negocio jurídico en soporte electrónico conlleve el pago de requisitos fiscales, el obligado al pago deberá conservar el comprobante respectivo y exhibirlo cuando una autoridad competente lo requiera.

CAPÍTULO III

Firmas digitales

Artículo 8º-**Alcance del concepto.** Entiéndese por firma digital cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el

documento electrónico.

Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado.

Artículo 9º-**Valor equivalente.** Los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito. En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita.

Los documentos públicos electrónicos deberán llevar la firma digital certificada.

Artículo 10.-**Presunción de autoría y responsabilidad.** Todo documento, mensaje electrónico o archivo digital asociado a una firma digital certificada se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital, vigente en el momento de su emisión.

No obstante, esta presunción no dispensa el cumplimiento de las formalidades adicionales de autenticación, certificación o registro que, desde el punto de vista jurídico, exija la ley para un acto o negocio determinado.

CAPÍTULO IV

Certificación digital

SECCIÓN I

Los certificados

Artículo 11.-**Alcance.** Entiéndese por certificado digital el mecanismo electrónico o digital mediante el que se pueda garantizar, confirmar o validar técnicamente:

a) La vinculación jurídica entre un documento, una firma digital y una persona.

b) La integridad, autenticidad y no alteración en general del documento, así como la firma digital asociada.

c) La autenticación o certificación del documento y la firma digital asociada, únicamente en el supuesto del ejercicio de potestades

públicas certificadoras.

d) Las demás que establezca esta Ley y su Reglamento.

Artículo 12.-**Mecanismos.** Con las limitaciones de este capítulo, el Estado, las instituciones públicas y las empresas públicas y privadas, las personas jurídicas y los particulares, en general, en sus diversas relaciones, estarán facultados para establecer los mecanismos de certificación o validación que convengan a sus intereses.

Para tales efectos podrán:

a) Utilizar mecanismos de certificación o validación máquina a máquina, persona a persona, programa a programa y sus interrelaciones, incluso sistemas de llave pública y llave privada, firma digital y otros mecanismos digitales que ofrezcan una óptima seguridad.

b) Establecer mecanismos de adscripción voluntaria para la emisión, la percepción y el intercambio de documentos electrónicos y firmas asociadas, en función de las competencias, los intereses y el giro comercial.

c) De consuno, instituir mecanismos de certificación para la emisión, la recepción y el intercambio de documentos electrónicos y firmas asociadas, para relaciones jurídicas concretas.

d) Instaurar, en el caso de dependencias públicas, sistemas de certificación por intermedio de particulares, quienes deberán cumplir los trámites de la Ley de contratación administrativa.

e) Fungir como un certificador respecto de sus despachos y funcionarios, o de otras dependencias públicas, en el caso del Estado y las demás instituciones públicas.

f) Ofrecer, en el caso de las empresas públicas cuyo giro lo admita, servicios comerciales de certificación en condiciones de igualdad con las empresas de carácter privado.

g) Implantar mecanismos de certificación para la tramitación, gestión y conservación de expedientes judiciales y administrativos.

Artículo 13.-**Homologación de certificados extranjeros.** Se conferirá pleno valor y eficacia jurídica a un certificado digital emitido en el extranjero, en cualesquiera de los siguientes casos:

a) Cuando esté respaldado por un certificador registrado en el país, en virtud de existir una relación de corresponsalía en los términos del artículo 20 de esta Ley.

b) Cuando cumpla todos los requisitos enunciados en el artículo 19 de esta Ley y exista un acuerdo recíproco en este sentido entre Costa Rica y el país de origen del certificador extranjero.

Artículo 14.-**Suspensión de certificados digitales.** Se podrá suspender un certificado digital en los siguientes casos:

a) Por petición del propio usuario a favor de quien se expidió.

b) Como medida cautelar, cuando el certificador que lo emitió tenga sospechas fundadas de que el propio usuario haya comprometido su confiabilidad, desatendido los lineamientos de seguridad establecidos, suplido información falsa al certificador u omitido cualquier otra información relevante, para obtener o renovar el certificado. En este caso, la suspensión podrá ser recurrida ante la Dirección de Certificadores de Firma Digital regulada en la siguiente sección, con aplicación de lo dispuesto en el artículo 148 de la Ley General de la Administración Pública.

c) Si contra el usuario se ha dictado auto de apertura a juicio, por delitos en cuya comisión se haya utilizado la firma digital.

d) Por orden judicial o de la Dirección de Certificadores de Firma Digital. En este último caso, cuando esta lo determine o cuando el Ente Costarricense de Acreditación (ECA) acredite que el usuario incumple las obligaciones que le imponen esta Ley y su Reglamento.

e) Por no cancelar oportunamente el costo del servicio.

Artículo 15.-**Revocación de certificados digitales.** El certificado digital será revocado en los siguientes supuestos:

a) A petición del usuario, en favor de quien se expidió.

b) Cuando se confirme que el usuario ha comprometido su confiabilidad, desatendido los lineamientos de seguridad establecidos, suplido información falsa al certificador u omitido otra información relevante, con el propósito de obtener o renovar el certificado.

c) Por fallecimiento, ausencia legalmente declarada, interdicción o insolvencia del usuario persona física, o por cese de actividades, quiebra o liquidación, en el caso de las personas jurídicas.

d) Por orden de la autoridad judicial o cuando recaiga condena firme contra el usuario, por delitos en cuya comisión se haya utilizado la firma digital.

Artículo 16.-**Revocación por el cese de actividades del certificador.** El cese de actividades del certificador implicará la revocatoria de todos los certificados que haya expedido, salvo que anteriormente hayan sido traspasados a otro certificador, previo consentimiento del usuario.

Artículo 17.-**Conservación de efectos.** La suspensión o revocación de un certificado digital no producirá, por sí sola, la invalidez de los actos o negocios realizados con anterioridad al amparo de dicho certificado.

SECCIÓN II

Certificadores

Artículo 18.-**Definición y reconocimiento jurídico.** Se entenderá como certificador la persona jurídica pública o privada, nacional o extranjera, que emite certificados digitales y está debidamente autorizada según esta Ley o su Reglamento; asimismo, que haya rendido la debida garantía de fidelidad. El monto de la garantía será fijado por la Dirección de Certificadores de Firma Digital y podrá ser hipoteca, fianza o póliza de fidelidad de un ente asegurador, o bien, un depósito en efectivo.

Sin perjuicio de lo dispuesto en los artículos 3º, 9º y 19 de esta Ley, los certificados digitales expedidos por certificadores registrados ante la Dirección de Certificadores de Firma Digital, solo tendrán pleno efecto legal frente a terceros, así como respecto del Estado y sus instituciones.

Artículo 19.-**Requisitos, trámites y funciones.** La Dirección de Certificadores de Firma Digital será la encargada de establecer, vía reglamento, todos los requisitos, el trámite y las funciones de las personas que soliciten su registro ante esta Dirección; para ello, el ECA, a solicitud del Ministerio de Ciencia y Tecnología, deberá fijar los requerimientos técnicos para el estudio, de acuerdo con la Ley Nº 8279, de 2 de mayo de 2002, y las prácticas y los estándares internacionales.

Artículo 20.-**Corresponsalía.** Los certificadores registrados podrán

concertar relaciones de corresponsalía con entidades similares del extranjero, para efectos de homologar los certificados digitales expedidos por estas entidades o que estas hagan lo propio en el exterior con los emitidos por los certificadores registrados.

Se deberá informar a la Dirección de Certificadores de Firma Digital, acerca del establecimiento de relaciones de esta clase, de previo a ofrecer ese servicio al público.

Artículo 21.-**Auditorías.** Todo certificador registrado estará sujeto a los procedimientos de evaluación y auditoría que acuerde efectuar la Dirección de Certificadores de Firma Digital o el ECA.

Artículo 22.-**Cesación voluntaria de funciones.** Los certificadores registrados de carácter privado podrán cesar en sus funciones, siempre y cuando avisen, a los usuarios, con un mes de anticipación como mínimo, y con dos meses a la Dirección de Certificadores de Firma Digital.

SECCIÓN III

Administración del Sistema de Certificación

Artículo 23.-**Dirección.** La Dirección de Certificadores de Firma Digital, perteneciente al Ministerio de Ciencia y Tecnología, será el órgano administrador y supervisor del Sistema de Certificación.

Artículo 24.-**Funciones.** La Dirección de Certificadores de Firma Digital tendrá las siguientes funciones:

a) Recibir, tramitar y resolver las solicitudes de inscripción de los certificadores.

b) Llevar un registro de los certificadores y certificados digitales.

c) Suspender o revocar la inscripción de los certificadores y de certificados, así como ejercer el régimen disciplinario en los casos y en la forma previstos en esta Ley y su Reglamento.

d) Expedir claves y certificados a favor de los certificadores registrados, y mantener el correspondiente repositorio de acceso público, con las características técnicas que indique el Reglamento.

e) Fiscalizar el funcionamiento de los certificadores registrados, para asegurar su confiabilidad, eficiencia y el cabal cumplimiento de la normativa aplicable, imponiendo, en caso necesario, las

sanciones previstas en esta Ley. La supervisión podrá ser ejercida por medio del ECA, en el ámbito de su competencia.

f) Mantener una página electrónica en la red Internet, a fin de divulgar, permanentemente, información relativa a las actividades de la Dirección de Certificadores de Firma Digital y el registro correspondiente de certificadores.

g) Señalar las medidas que estime necesarias para proteger los derechos, los intereses y la confidencialidad de los usuarios, así como la continuidad y eficiencia del servicio, y velar por la ejecución de tales disposiciones.

h) Dictar el Reglamento respectivo para el registro de certificadores.

i) Las demás funciones que esta Ley o su Reglamento le señalen.

Artículo 25.-**Jefatura.** El superior administrativo de la Dirección de Certificadores de Firma Digital será el director, quien será nombrado por el ministro de Ciencia y Tecnología y será un funcionario de confianza, de conformidad con el inciso g) del artículo 4, del Estatuto de Servicio Civil. El director deberá declarar sus bienes oportunamente, de acuerdo con la Ley contra el enriquecimiento ilícito de los servidores públicos.

CAPÍTULO V

Sanciones

Artículo 26.-**Sanciones a certificadores.** Previa oportunidad de defensa, la Dirección de Certificadores de Firma Digital podrá imponerles, a los certificadores, las siguientes sanciones:

a) Amonestación.

b) Multa hasta por el equivalente a cien salarios base; para la denominación salario base se considerará lo indicado en el artículo 2º de la Ley Nº 7337, de 5 de mayo de 1993.

c) Suspensión hasta por un año.

d) Revocatoria de la inscripción.

El certificador a quien se le haya revocado su inscripción, no podrá volver a registrarse durante los siguientes cinco años, ya sea como tal o por medio de otra persona jurídica en la que figuren las mismas personas

como representantes legales, propietarias o dueñas de más de un veinticinco por ciento (25%) del capital.

Artículo 27.-**Amonestación.** Se aplicará la amonestación, a los certificadores, en los siguientes casos:

a) Por la emisión de certificados digitales que no incluyan la totalidad de los datos requeridos por esta Ley o su Reglamento, cuando la infracción no requiera una sanción mayor.

b) Por no suministrar a tiempo los datos requeridos por la Dirección de Certificadores de Firma Digital, en ejercicio de sus funciones.

c) Por cualquier otra infracción a la presente Ley que no tenga prevista una sanción mayor.

Artículo 28.-**Multa.** Se aplicará la multa, a los certificadores, en los siguientes casos:

a) Cuando se emita un certificado y no se observen las políticas de seguridad o de certificación previamente divulgadas, de modo que cause perjuicio a los usuarios o a terceros.

b) Cuando no se suspenda o revoque, oportunamente, un certificado, estando obligados a hacerlo.

c) Por cualquier impedimento u obstrucción a las inspecciones o auditorias por parte de la Dirección de Certificadores de Firma Digital o del ECA.

d) Por el incumplimiento de los lineamientos técnicos o de seguridad impartidos por la Dirección de Certificadores de Firma Digital.

e) Por la reincidencia en la comisión de infracciones, que hayan dado lugar a la sanción de amonestación, dentro de los dos años siguientes.

Artículo 29º-**Suspensión.** Se suspenderá al certificador que:

a) No renueve oportunamente la caución que respalde su funcionamiento o la rinda en forma indebida.

b) Reincida en cualesquiera de las infracciones que le hayan

merecido una sanción de multa, dentro de los siguientes dos años.

Artículo 30.-**Revocatoria de la inscripción.** Se podrá revocar la inscripción de un certificador cuando:

a) Se compruebe la expedición de certificados falsos.

b) Se compruebe que el certificador suministró información o presentó documentos falsos, con el fin de obtener el registro.

c) Reincida en cualesquiera de las infracciones que le hayan merecido una sanción de suspensión, dentro de los cinco años siguientes.

Artículo 31.-**Procedimiento.** Todas las sanciones serán impuestas mediante el procedimiento administrativo ordinario, previsto en la Ley General de la Administración Pública, salvo en el caso de amonestación, en que podrá aplicarse el procedimiento sumario.

Artículo 32.-**Publicidad.** Excepto el caso de amonestación, todas las sanciones administrativas impuestas serán publicadas por medio de reseña o trascripción íntegra en *La Gaceta*, sin perjuicio de que, en atención al caso concreto, se disponga, además, publicarlas en uno o más medios de circulación o difusión nacional.

Asimismo, la Dirección de Certificadores de Firma Digital dispondrá la publicación electrónica en su página de información en Internet.

CAPÍTULO VI

Disposiciones finales y transitorias

Artículo 33.-**Reglamentación.** El Poder Ejecutivo reglamentará esta Ley dentro de los seis meses siguientes a su publicación.

Además, para el trámite eficiente de sus asuntos, cada dependencia pública podrá adoptar las medidas particulares de aplicación de esta Ley de acuerdo con sus necesidades.

Transitorio único.-Los rubros presupuestarios requeridos para que la Dirección de Certificadores de Firma Digital entre en funcionamiento, deberán ser incluidos por el Ministerio de Hacienda, a propuesta del Ministerio de Ciencia y Tecnología, en el primer presupuesto remitido a la Asamblea Legislativa, después de promulgada esta Ley.

Rige a partir de su publicación.

Dado en la Presidencia de la República.-San José, a los treinta días del mes de agosto del dos mil cinco.

2. SISTEMA NACIONAL PARA LA CALIDAD

[Ley para el Sistema Nacional para la Calidad][ii]

CAPÍTULO I

Disposiciones Generales

Artículo 1º-Propósito de la Ley. La presente Ley tiene como propósito establecer el Sistema Nacional para la Calidad (SNC), como marco estructural para las actividades vinculadas al desarrollo y la demostración de la calidad, que facilite el cumplimiento de los compromisos internacionales en materia de evaluación, de la conformidad, que contribuya a mejorar la competitividad de las empresas nacionales y proporcione confianza en la transacción de bienes y servicios.

El SNC incluye, además, otras actividades de apoyo, difusión y coordinación establecidas en esta Ley y sus Reglamentos.

Artículo 2º-Ámbito de la Ley. Esta Ley se aplicará a todos los bienes y servicios, así como a las actividades de evaluación de la conformidad, incluida la metrología, que se lleven a cabo para demostrar el cumplimiento de los requisitos voluntarios o reglamentarios aplicables a estos bienes, incluidos los procesos de producción o prestación de servicios implicados para generar y comercializar dichos bienes.

Artículo 3º-Fines y Objetivos del Sistema. El fin del SNC será ofrecer un marco estable e integral de confianza que, por medio del fomento de la calidad en la producción y comercialización de bienes y la prestación de servicios, propicie el mejoramiento de la competitividad de las actividades productivas, contribuya a elevar el grado de bienestar general y facilite el cumplimiento efectivo de los compromisos comerciales internacionales suscritos por Costa Rica.

Los objetivos del Sistema serán los siguientes:

a) Orientar, ordenar y articular la participación de la Administración Pública y el sector privado en las actividades de evaluación de la conformidad y de promoción de la calidad, integradas al SNC.

b) Promover la disponibilidad y el uso de los mecanismos de evaluación y demostración de la conformidad.

c) Promover la adopción de prácticas de gestión de la calidad y formación en ellas, en las organizaciones productoras o comercializadoras de bienes en el país.

d) Fomentar la calidad de los bienes disponibles en el mercado y de los destinados a la exportación.

e) Propiciar la inserción cultural de la calidad en todos los planos de la vida nacional, especialmente en el individual y el social.

f) Coordinar la gestión pública y privada que deben realizar las entidades competentes para proteger la salud humana, animal o vegetal, el medio ambiente y los derechos legítimos del consumidor, y para prevenir las prácticas que puedan inducir a error.

g) Articular la gestión pública y privada que realicen las entidades competentes en las actividades de metrología, normalización, reglamentación técnica y evaluación de la conformidad, así como la prevención de prácticas que constituyan barreras técnicas ilegítimas para el comercio.

Artículo 4º-Integración del Sistema. El SNC estará integrado por todos los órganos, organismos, laboratorios y entidades que ofrecen o coordinan servicios relacionados con la evaluación de la conformidad en el ámbito definido en el artículo 3 de esta Ley, independientemente de si operan en el sector público o privado.

Artículo 5º-Principios del Sistema. El SNC podrá incorporar como propios los principios y términos establecidos en las normas, los acuerdos y los códigos internacionales aplicables en su ámbito.

CAPÍTULO II

Consejo Nacional para la Calidad

Artículo 6º-Consejo Nacional para la Calidad. Créase el Consejo Nacional para la Calidad (CONAC), como la entidad responsable de fijar los lineamientos generales del SNC, todo conforme a los lineamientos y las prácticas internacionales reconocidos y a las necesidades nacionales.

El CONAC velará por la adecuada coordinación de las actividades de promoción y difusión de la calidad y elaborará las recomendaciones que considere convenientes. También dará el seguimiento necesario a los lineamientos generales y las recomendaciones que emita.

El CONAC contará con una Secretaría Ejecutiva, adscrita al Ministerio

de Economía, Industria y Comercio (MEIC).

Artículo 7º-Integración. El CONAC estará integrado por los siguientes miembros:

a) El ministro o viceministro de Economía, Industria y Comercio, quien lo presidirá.

b) El ministro o viceministro de Ciencia y Tecnología.

c) El ministro o viceministro de Agricultura y Ganadería.

d) El ministro o viceministro de Salud.

e) El ministro o viceministro del Ambiente y Energía.

f) El ministro o viceministro de Obras Públicas y Transportes.

g) El ministro o viceministro de Educación Pública.

h) El ministro o viceministro de Comercio Exterior.

i) El presidente o vicepresidente de la Cámara de Agricultura y Agroindustria.

j) El presidente o vicepresidente de la Cámara de Comercio.

k) El presidente o vicepresidente de la Cámara Costarricense de la Industria Alimentaria.

l) El presidente o vicepresidente de la Cámara de Industrias.

m) Un representante de las pequeñas y medianas industrias, designado por la Unión Costarricense de Cámaras y Empresas Privadas (UCCAEP) por un plazo de cuatro años.

n) El presidente de la Federación Nacional de Asociaciones de Consumidores (FENASCO) o su representante.

ñ) El presidente o vicepresidente del Consejo Superior de Educación.

o) El presidente o vicepresidente del Consejo Nacional de Rectores.

p) El director del Laboratorio Costarricense de Metrología.

q) El presidente de la Junta Directiva del Ente Costarricense de Acreditación (ECA).

r) El presidente del Ente Nacional de Normalización (ENN).

El CONAC sesionará, en forma ordinaria, una vez por semestre y, en forma extraordinaria, por convocatoria de su presidente o de ocho de sus miembros.

CAPÍTULO III

Laboratorio Costarricense de Metrología

(Reglamentado mediante Decreto Ejecutivo N° 31819 de 30 de abril de 2004)

Artículo 8º—Creación. Créase el Laboratorio Costarricense de Metrología (LACOMET), como órgano de desconcentración máxima, con personalidad jurídica instrumental para el desempeño de sus funciones, adscrito al MEIC. Se regirá por las normas nacionales e internacionales aplicables.

Artículo 9º-Funciones. Las funciones del LACOMET serán las siguientes:

a) Actuar como organismo técnico y coordinador con otros organismos científicos y técnicos, públicos y privados, nacionales e internacionales, en el campo de la metrología.

b) Difundir y fundamentar la metrología nacional y promover el establecimiento de una estructura metrológica nacional.

c) Custodiar los patrones nacionales y garantizar su referencia periódica a patrones de rango superior.

d) Promover el uso, la calibración, la verificación y el ajuste de los instrumentos de medición, así como la trazabilidad a patrones del Sistema Internacional de Unidades, y garantizar la trazabilidad de los instrumentos de medida.

e) Regular y vigilar las características de los instrumentos de medición empleados en las transacciones comerciales nacionales y en la verificación del cumplimiento de los requisitos reglamentarios.

f) Fungir como laboratorio nacional de referencia en metrología y, cuando se le requiera, brindar servicios como laboratorio secundario en las áreas de su competencia.

g) Colaborar con la Secretaría de Reglamentación Técnica en la definición de los asuntos metrológicos, para las especificaciones técnicas de los reglamentos.

h) Reconocer, mediante convenios, a otras instituciones como

laboratorios nacionales en las magnitudes que se considere pertinente y mantener mecanismos de coordinación y vigilancia para el uso de los patrones. El Laboratorio tendrá la responsabilidad de establecer los requisitos necesarios para otorgar y mantener este reconocimiento y verificar su cumplimiento.

i) Reconocer a instituciones públicas o privadas, físicas o jurídicas, como unidades de verificación metrológicas, de acuerdo con los requisitos legales y técnicos que él disponga. Cuando la institución no esté acreditada, el Laboratorio, justificando debidamente la necesidad del reconocimiento, podrá concederlo y le otorgará el plazo máximo de tres años para que obtenga la acreditación correspondiente.

j) Participar en actividades de verificación del cumplimiento de los reglamentos técnicos, en los campos de su competencia.

k) Participar en instancias internacionales de metrología, en particular la Oficina Internacional de Pesas y Medidas (BIPM) y la Organización Internacional de Metrología Legal.

Artículo 10.-Organización. El Laboratorio estará conformado, al menos, por su Dirección, la Comisión de Metrología y los demás órganos que requiera para el desempeño de sus funciones.

Artículo 11.-Creación de la Comisión de Metrología. Créase la Comisión de Metrología como máximo órgano técnico del Laboratorio Costarricense de Metrología. La Comisión estará integrada por las siguientes personas:

a) El director del Laboratorio Costarricense de Metrología, quien la presidirá.

b) Tres representantes del Poder Ejecutivo.

c) Un representante del Consejo Nacional de Rectores.

d) Un representante de los usuarios de los servicios de metrología.

e) Un representante del sector privado, propuesto por la Unión Costarricense de Cámaras y Empresas Privadas (UCCAEP).

Los representantes de las organizaciones serán nombrados por el Consejo de Gobierno, de las ternas que le presentarán las organizaciones mencionadas en los incisos c), d) y e) de este artículo.

Los miembros de la Comisión, excepto el director, permanecerán seis años en sus cargos. Sus nombramientos deberán publicarse en La Gaceta una sola vez.

La Comisión deberá reunirse, al menos, una vez al mes.

Artículo 12.-Funciones de la Comisión de Metrología. Las funciones de la Comisión serán las siguientes:

a) Establecer las políticas generales del LACOMET y velar por su efectivo cumplimiento.

b) Establecer las tarifas y condiciones en que el Laboratorio debe contratar y vender los servicios de metrología. Las tarifas serán efectivas a partir de su publicación en La Gaceta.

c) Adoptar los lineamientos generales en materia de metrología.

d) Conocer los asuntos técnicos que le someta el director del Laboratorio.

e) Conocer y aprobar el plan anual operativo que le presente el director del Laboratorio.

f) Recomendar la incorporación y adopción de instrumentos jurídicos sobre la materia.

g) Promover actividades específicas para el desarrollo de la metrología en el país.

h) Recomendar la política del Laboratorio en materia de equipo, infraestructura y capacitación técnica del personal.

i) Vigilar que el director del Laboratorio cumpla las funciones asignadas en el artículo 9 de esta Ley.

Cuando la Comisión de Metrología deba conocer asuntos relacionados con la labor desempeñada por el director del Laboratorio y exista conflicto de intereses para este funcionario, deberá inhibirse de participar en esa sesión; en tal caso, la Comisión será presidida por uno de los representantes estatales.

Artículo 13.-Director del Laboratorio. El Poder Ejecutivo nombrará al director del LACOMET, quien deberá gozar de reconocida experiencia en el campo de la metrología. El director ostentará la representación extrajudicial para el ejercicio de las potestades otorgadas al Laboratorio en su condición de persona jurídica instrumental, para la negociación y firma de los contratos de venta de servicios que suscriba el Laboratorio, y para la ejecución del presupuesto asignado.

Artículo 14.-Funciones del Director. El director del LACOMET será el responsable del cumplimiento de las funciones asignadas a esa entidad en el artículo 9 de esta Ley. Deberá proponer un plan anual operativo a la Comisión de Metrología, para que lo apruebe. También

deberá presentar al MEIC una propuesta de presupuesto, que deberá contener los objetivos y las metas por cumplir, de conformidad con el plan anual operativo aprobado por dicha Comisión.

Artículo 15.-Venta de Servicios. Autorízase al LACOMET para que venda servicios a instituciones públicas o empresas privadas. El producto de la venta de servicios se destinará, en su totalidad, al mejoramiento de los laboratorios, la capacitación técnica de su personal y el desarrollo de la infraestructura metrológica.

Artículo 16.-Presupuesto. Los recursos para el funcionamiento del LACOMET se incluirán en el presupuesto nacional de la República y considerarán, en una partida diferenciada, los ingresos provenientes de la venta de servicios.

Artículo 17.-Asignación de Recursos al LACOMET. Autorízase a las instituciones del Estado y entidades públicas estatales para que efectúen donaciones o aportes al LACOMET y le asignen temporalmente el personal calificado y los recursos financieros necesarios para cumplir sus fines y ejecutar proyectos específicos.

Artículo 18.-Sujeción a la Reglamentación Técnica de Medición. Los entes públicos y privados deberán asegurarse de que los instrumentos de medición empleados se ajustan a los requisitos establecidos en los reglamentos técnicos respectivos.

CAPÍTULO IV

Ente Costarricense de Acreditación

Artículo 19.-Creación. Créase el Ente Costarricense de Acreditación (ECA), como entidad pública de carácter no estatal, con personería jurídica y patrimonio propios. Ejercerá su gestión administrativa y comercial con absoluta independencia y se guiará exclusivamente por las decisiones de su Junta Directiva, basadas en la normativa internacional. La Junta actuará conforme a su criterio, dentro de la Constitución, las leyes y los reglamentos pertinentes en procura del desarrollo y la eficiencia en su función.

El ECA se regirá por las disposiciones de esta Ley y su Reglamento.

Para los efectos de esta Ley, se entenderá como acreditación el procedimiento mediante el cual el ECA reconoce de manera formal que una entidad es competente para ejecutar tareas específicas según los requisitos de las normas internacionales.

Artículo 20.-Misión. La misión del ECA será respaldar la competencia técnica y credibilidad de los entes acreditados, para garantizar la confianza del Sistema Nacional de la Calidad; además, asegurar que los servicios ofrecidos por los entes acreditados mantengan la calidad

bajo la cual fue reconocida la competencia técnica, así como promover y estimular la cooperación entre ellos.

Artículo 21.-Funciones. El ECA será el único competente para realizar los procedimientos de acreditación en lo que respecta a laboratorios de ensayo y calibración, entes de inspección y control, entes de certificación y otros afines. Tendrá las siguientes funciones:

a) Acreditar previo cumplimiento de los requisitos, conforme a las buenas prácticas internacionales.

b) Estimular la acreditación en todos los ámbitos tecnológicos y científicos del país.

c) Garantizar la competencia técnica y credibilidad de los entes acreditados. Para ello, podrá realizar las investigaciones y ordenar las medidas cautelares que considere necesarias, incluso la suspensión temporal de la acreditación.

d) Resolver, previo cumplimiento del debido proceso, las denuncias que, en materia de su competencia, se presenten contra los entes acreditados.

e) Promover la suscripción de convenios de reconocimiento mutuo y otros instrumentos de entendimiento que propicien el reconocimiento de la acreditación otorgada por él ante órganos de acreditación similares.

f) Participar en las instancias internacionales de acreditación.

Artículo 22.-Conformación. El ECA estará conformado por la Junta Directiva, la Comisión de Acreditación y las dependencias que requiera para realizar sus competencias, conforme a la estructura interna que defina el reglamento ejecutivo.

Artículo 23.-Conformación de la Junta Directiva. La Junta Directiva del ECA estará conformada por dieciocho miembros, los cuales deben gozar de reconocida experiencia en la materia:

a) Un representante del Ministerio de Ciencia y Tecnología, quien lo presidirá.

b) Un representante del Ministerio de Economía, Industria y Comercio.

c) Un representante del Ministerio de Salud.

d) Un representante del Ministerio de Agricultura y Ganadería.

e) Un representante del Ministerio del Ambiente y Energía.

f) Un representante del Ministerio de Obras Públicas y Transportes.

g) El director del Laboratorio Costarricense de Metrología (LACOMET).

h) Un representante del Ente Nacional de Normalización.

i) Un representante del Consejo Superior de Educación.

j) Un representante del Consejo Nacional de Rectores.

k) Cuatro representantes del sector privado, designados por la Unión Costarricense de Cámaras y Empresas Privadas (UCCAEP).

l) Un representante de los consumidores, designado por la Federación Nacional de Asociaciones de Consumidores o por otra organización legalmente constituida.

m) Dos representantes de los entes acreditados.

n) Un representante de la Federación de Colegios Profesionales.

Los representantes del sector público serán nombrados por el Consejo de Gobierno, a propuesta del ministro del ramo correspondiente. Los representantes de las organizaciones serán nombrados por el Consejo de Gobierno, de las ternas que le presenten las organizaciones enumeradas en el párrafo anterior.

Los miembros de la Junta Directiva serán nombrados por un período de seis años, podrán ser reelegidos sucesivamente y se renovarán en forma alterna.

En caso de empate en la votación, el presidente de la Junta Directiva ejercerá doble voto.

Artículo 24.-Funciones de la Junta Directiva. La Junta Directiva del ECA tendrá las siguientes funciones:

a) Determinar las políticas generales y los planes estratégicos del ECA.

b) Aprobar el plan de trabajo, el presupuesto anual ordinario, el extraordinario y los informes anuales del ECA.

c) Acordar y reformar el reglamento interno de trabajo del ECA.

d) Resolver las apelaciones presentadas contra los procedimientos y los resultados finales de las acreditaciones, así como los procedimientos de sanción contra los entes acreditados.

e) Publicar, por los medios oficiales, las acreditaciones otorgadas.

f) Velar por el cumplimiento de las normas y los procedimientos de acreditación.

g) Aprobar la conformación de las secretarías de acreditación y los comités técnicos, así como el nombramiento y la remoción de los secretarios de acreditación.

h) Nombrar y destituir al auditor interno.

i) Las demás que se deriven de esta Ley y su Reglamento.

Artículo 25.-Comisión de Acreditación. La Comisión de Acreditación será la encargada de acreditar en las áreas de competencia del ECA. Estará conformada de la siguiente manera:

a) Un representante del sector gubernamental.

b) Un representante del sector empresarial.

c) Un representante del sector de usuarios de los servicios de acreditación.

d) Un representante de los otros sectores involucrados, mencionados en el artículo 23 de esta Ley.

e) Los secretarios de acreditación con que cuente el ECA, según su estructura orgánica.

Los miembros de la Comisión serán nombrados por la Junta Directiva del ECA; deberán poseer experiencia reconocida en el ramo, así como la educación, la destreza, el conocimiento técnico y la experiencia necesarios para las actividades de acreditación por desarrollar.

Artículo 26.-Funciones de la Comisión de Acreditación. La Comisión de Acreditación tendrá las siguientes funciones:

a) Acreditar previa comprobación del cumplimiento de los requisitos correspondientes, conforme a las buenas prácticas internacionales.

b) Instruir los procedimientos de investigación y sancionar a los entes acreditados que incumplan esta Ley y su Reglamento.

c) Nombrar a los comités técnicos ad hoc.

d) Otras que le indiquen esta Ley y su Reglamento.

Artículo 27.-Secretarías de Acreditación. Existirán secretarías de acreditación en las áreas de competencia del ECA según la estructura

interna que se establezca. Serán las encargadas de dar apoyo técnico a la Comisión de Acreditación, de acuerdo con las funciones que se definan en el Reglamento de esta Ley.

Los secretarios de acreditación deberán contar con la educación, la destreza, el conocimiento técnico y la experiencia necesarios para las actividades de acreditación por desarrollar. Asimismo, estarán imposibilitados para desempeñar actividades que puedan generar conflictos de interés.

Artículo 28.-Comités Técnicos de Acreditación. Para analizar las solicitudes de acreditación presentadas, la Comisión de Acreditación podrá nombrar comités técnicos ad hoc, los cuales estarán integrados por profesionales expertos en el ámbito que se acreditará.

Artículo 29.-Nombramiento del Gerente. El ECA tendrá un gerente, nombrado por la Junta Directiva.

Artículo 30.-Funciones del Gerente. El gerente tendrá las siguientes funciones:

a) Ejercer, en nombre y por cuenta del ECA su representación judicial y extrajudicial, con las facultades propias para el ejercicio del cargo.

b) Ejercer las funciones inherentes a su condición de autoridad máxima administrativa, vigilando la organización, el funcionamiento y la coordinación de todas sus dependencias, así como la observancia de la ley y el reglamento interno.

c) Asistir a las sesiones de la Junta Directiva, donde tendrá voz, pero no voto; asimismo, ejecutar los acuerdos y las resoluciones que la Junta decida en las materias de su competencia.

d) Nombrar, promover, suspender y despedir a los empleados del ECA, excepto al auditor interno y los secretarios de acreditación, quienes serán nombrados y destituidos por la Junta Directiva.

e) Proponer a la Junta Directiva la organización interna del ECA.

f) Presentar a la Junta Directiva, para que los apruebe, el presupuesto anual del ECA, acompañado del plan de trabajo y del informe anual de labores

g) Establecer la coordinación necesaria con las instituciones y dependencias del sector público y privado, en cuanto a la colaboración y el apoyo para desarrollar las actividades de acreditación.

Artículo 31.-Deberes de los Entes Acreditados. Los entes acreditados deberán:

a) Respetar y aplicar lo dispuesto en los ámbitos de la acreditación concedida, en el acta de compromiso y en el reglamento de acreditación correspondiente.

b) Facilitar las evaluaciones de seguimiento, anunciadas y no anunciadas, de la acreditación concedida.

c) Respetar los plazos y las condiciones establecidos para la expiración y la posible renovación de la acreditación.

Artículo 32.-Procedimiento Sancionatorio. De conformidad con la Ley General de la Administración Pública, la Comisión de Acreditación del ECA deberá efectuar el procedimiento sancionatorio correspondiente con el fin de verificar, de oficio o por denuncia de cualquier interesado, el incumplimiento, por parte de los entes acreditados, de los deberes referidos en el artículo 31 de esta Ley. Si como resultado de este procedimiento se comprueba que el ente investigado ha incumplido tales deberes, la Comisión de Acreditación deberá retirarle la acreditación.

Artículo 33.-Evaluación y Fiscalización. El ECA deberá realizar evaluaciones a los entes acreditados cumpliendo, en todo momento, lo ordenado en las normas internacionales.

Artículo 34.-Servicios a las Entidades Públicas. Todas las instituciones públicas que, para el cumplimiento de sus funciones, requieren servicios de laboratorios de ensayo, laboratorios de calibración, entes de inspección y entes de certificación, deberán utilizar los acreditados o reconocidos por acuerdos de reconocimiento mutuo entre el ECA y las entidades internacionales equivalentes.

Los laboratorios estatales deberán acreditarse ante el ECA, de conformidad con el reglamento respectivo.

Artículo 35.-Auditoría Interna. El ECA contará con una auditoría interna que dependerá directamente de la Junta Directiva. Su función principal será comprobar el cumplimiento, la suficiencia y la validez del sistema de control interno establecido por la Institución.

Artículo 36.-Financiamiento. El ECA contará con los siguientes recursos:

a) Los ingresos percibidos por concepto de la venta de bienes y servicios compatibles con las actividades de acreditación.

b) Los legados, las donaciones y los aportes de personas físicas o jurídicas, organizaciones nacionales o internacionales, privadas o públicas, y los aportes del Estado o sus instituciones, así como los recursos de cooperación internacional puestos a disposición del Estado para financiar actividades relacionadas con alguna de las

funciones del ECA.

Artículo 37.-Uso de Recursos. Los recursos que se obtengan por lo ordenado en el inciso b) del artículo anterior, serán utilizados para el cumplimiento de los objetivos de esta Ley y para fortalecer, desarrollar, actualizar y mejorar el ECA.

Artículo 38.-Autorización para Asignar Recursos. Autorízase al Estado y sus instituciones para que efectúen donaciones o asignen recursos humanos o financieros al ECA, con el propósito de que alcance sus fines y ejecute proyectos específicos. Esta autorización no incluye los bienes demaniales del Estado, definidos en el inciso 14) del artículo 121 de la Constitución Política.

CAPÍTULO V

Órgano de Reglamentación Técnica (ORT)

Artículo 39.-Creación. Créase el Órgano de Reglamentación Técnica (ORT), como comisión interministerial cuya misión será contribuir a la elaboración de los reglamentos técnicos, mediante el asesoramiento técnico en el procedimiento de emitirlos.

El Órgano será el encargado de coordinar, con los respectivos ministerios, la elaboración de sus reglamentos técnicos, de modo tal que su emisión permita la efectiva y eficiente protección de la salud humana, animal y vegetal, del medio ambiente, de la seguridad, del consumidor y de los demás bienes jurídicos tutelados.

Antes de promulgar cualquier reglamento técnico, deberá darse audiencia a los sectores interesados.

Artículo 40.-Funciones. El ORT tendrá las siguientes funciones:

a) Recomendar la adopción, actualización o derogación de los reglamentos técnicos emitidos por el Poder Ejecutivo.

b) Emitir criterios técnicos con respecto a los anteproyectos de reglamento técnico que desee implementar el Poder Ejecutivo.

Artículo 41.-Integración. El ORT estará compuesto por los siguientes miembros:

a) Un representante del Ministerio de Economía, Industria y Comercio, quien lo presidirá.

b) Un representante del Ministerio de Agricultura y Ganadería.

c) Un representante del Ministerio de Salud.

d) Un representante del Ministerio de Obras Públicas y Transportes.

e) Un representante del Ministerio del Ambiente y Energía.

f) Un representante del Ministerio de Ciencia y Tecnología.

g) Un representante del Ministerio de Comercio Exterior.

Los miembros del ORT serán propuestos por cada ministro al Ministro de Economía, Industria y Comercio.

Serán nombrados por el Poder Ejecutivo por períodos indefinidos y podrán ser sustituidos en cualquier momento. Su nombramiento deberá ser publicado en La Gaceta una sola vez.

Artículo 42.-Secretaría. El ORT deberá contar con una Secretaría Técnica, adscrita al MEIC, la cual será, a la vez, la Secretaría Técnica del Comité Nacional del Codex Alimentarius y el punto de contacto del Comité Nacional del Codex Alimentarius.

La Secretaría tendrá las siguientes funciones:

a) Convocar al ORT.

b) Dar el apoyo administrativo necesario para la gestión del Órgano.

c) Otorgar la audiencia ordenada en el artículo 39 de la presente Ley.

d) Asesorar y capacitar a los entes del Estado con facultades para proponer la emisión de reglamentos técnicos, en cuanto a la conformación de los comités técnicos para elaborar, adoptar y aplicar tales reglamentos.

e) Mantener canales de información regionales e internacionales en el ámbito reglamentario.

f) Establecer los mecanismos de coordinación con instituciones similares en el ámbito nacional e internacional, para facilitar las actividades de integración y armonización de los reglamentos técnicos y las definiciones internacionales.

g) Organizar y administrar el Centro de Información en Obstáculos Técnicos al Comercio.

h) Otras que le correspondan por ley o reglamento.

Artículo 43.-Centro de Información en Obstáculos Técnicos al Comercio. Créase el Centro de Información en Obstáculos Técnicos al

Comercio, el cual será parte de la Secretaría del ORT. Sus funciones serán las definidas en el Acuerdo sobre obstáculos técnicos, integrante del acta final por la que se incorporan los resultados de la Ronda Uruguay de negociaciones comerciales multilaterales, Ley Nº 7475, de 20 de diciembre de 1994, y demás normas conexas.

CAPÍTULO VI

Normalización

Artículo 44.-Reconocimiento de la Normalización. Las normas voluntarias, en tanto facilitadoras del entendimiento entre proveedores y consumidores o usuarios, y promotoras del desarrollo tecnológico y productivo del país, serán reconocidas como de interés público. Por eso, la Administración Pública promoverá su uso y participará activamente en su desarrollo y financiamiento.

Artículo 45.-Ente Nacional de Normalización (ENN). Cada cinco años, previa recomendación del Consejo Nacional para la Calidad, el Poder Ejecutivo concederá el reconocimiento como Ente Nacional de Normalización (ENN) a la entidad privada sin fines de lucro que haya adoptado los requisitos internacionales y los cumpla. En virtud de este reconocimiento, dicho Ente podrá participar en actividades realizadas por otros organismos de normalización internacionales.

El reconocimiento podrá ser retirado en forma anticipada si el citado Consejo comprueba que el ente que ostenta la condición de ENN ha incumplido las disposiciones de esta Ley y las buenas prácticas de normalización.

Artículo 46.-Funciones del ENN. Las funciones del ENN serán las siguientes:

a) Encauzar y dirigir la elaboración de las normas convenientes para el desarrollo socieconómico nacional, incluso la adopción de normas internacionales y la armonización en ámbitos supranacionales.

b) Promover la participación nacional ante las organizaciones internacionales y regionales de normalización.

c) Difundir la aplicación adecuada de las normas a las actividades productivas y comerciales, tanto en el sector público como en el privado.

d) Promover el establecimiento de acuerdos y convenios de colaboración con entidades nacionales, extranjeras o internacionales.

e) Organizar actividades de formación y difusión y colaborar en ellas.

f) Comercializar las normas nacionales e internacionales y las

publicaciones técnicas.

g) Promover la agrupación de los interesados en el desarrollo de la normalización nacional y coordinarlos.

h) Cualquier otra actividad compatible con las actividades de normalización.

Artículo 47.-Vigilancia de la Gestión del ENN. El Consejo Nacional para la Calidad vigilará la adhesión del ENN a los códigos internacionales de normalización y recomendará al Poder Ejecutivo el reconocimiento o la pérdida del reconocimiento como ENN. Asimismo, recomendará las condiciones y la cuantía de la participación del Estado en el presupuesto de dicho Ente, mientras esta contribución se considere necesaria.

Capítulo VII

Disposiciones Finales

Artículo 48.-Auditorías Internacionales. El LACOMET, el ENN y el ECA deberán someterse a auditorías internacionales periódicas ante los entes internacionales competentes, para asegurar que los servicios que brinden se ajusten a los estándares internacionales.

Artículo 49.-Modificaciones. Modifícase el inciso c) del artículo 4 de la Ley Orgánica del Ministerio de Economía, Industria y Comercio, Nº 6054, de 14 de junio de 1977, y sus reformas. El texto dirá:

"Artículo 4.- (...]

c) Promover en el país el uso de la normalización y participar activamente en su desarrollo."

Artículo 50.-Derogaciones. Deróganse las siguientes normas:

a) Los artículos 7º , 8º , 9º y 10 de la Ley del Sistema Internacional de Unidades, Nº 5292, de 9 de agosto de 1973.

b) El artículo 8 de la Ley de promoción de la competencia y defensa efectiva del consumidor, Nº 7472, de 29 de diciembre de 1994.

CAPÍTULO VIII

Disposiciones Transitorias

Transitorio I.-Sobre el LACOMET. Mientras no existan organizaciones de usuarios de los servicios de metrología, el representante de los

usuarios ante la Comisión de Metrología será propuesto por el Consejo Nacional para la Calidad.

Transitorio II.-Sobre el ECA. El gerente del ECA será nombrado en los seis meses siguientes a la entrada en vigencia de esta Ley. Mientras no sea nombrado ese gerente, el presidente de la Junta Directiva ostentará la representación de la entidad, con las mismas facultades del gerente y en forma ad honórem.

El Poder Ejecutivo está autorizado para otorgar la ayuda financiera necesaria al ECA en forma tal que su actividad de acreditación pueda ser subvencionada, por el período necesario hasta que disponga de los recursos propios suficientes para realizar su gestión. Esta ayuda financiera deberá otorgarse de manera gradual y por el plazo máximo de cinco años.

Solamente para el primer período, los miembros de la Junta Directiva del ECA serán nombrados así: por un período de tres años, el representante del Ministerio de Salud, el del Ministerio de Agricultura y Ganadería, el del Ministerio del Ambiente y Energía, el del Ministerio de Obras Públicas y Transportes, el del Consejo Superior de Educación, los dos del sector privado, el de los consumidores y el de la Federación de Colegios Profesionales; el resto de los miembros serán nombrados por todo el período de seis años.

Las instituciones y los entes del Estado que realizaban actividades de acreditación conforme a la definición dada en esta Ley, deberán trasladar sus funciones al ECA.

Los laboratorios oficiales, estatales o privados, que brindan servicio al Estado y hayan operado antes de la entrada en vigencia de la presente Ley, deberán acreditarse ante el ECA dentro del plazo máximo de tres años y de acuerdo con el procedimiento que defina dicho Ente.

Mientras no existan organizaciones de entes acreditados, los representantes referidos en el artículo 23 de esta Ley serán propuestos por el Consejo Nacional para la Calidad.

Transitorio III.-Sobre el ENN. Reconócese al Instituto de Normas Técnicas de Costa Rica (INTECO) como ENN, de conformidad con los artículos 44, 45, 46 y 47 de esta Ley.

Transitorio IV.-Traspaso de activos. Los recursos financieros, derechos y activos en general, asignados a la gestión del Ente Nacional de Acreditación, serán traspasados al ECA conforme a la disposición que emitirá el Poder Ejecutivo. Para este efecto, los bienes que deberán traspasarse son: el manual de calidad del Ente Nacional de Acreditación, los procedimientos de acreditación para entes de inspección, los procedimientos de acreditación para entes de certificación, los procedimientos de acreditación para laboratorios de

ensayo y calibración, las normas internacionales, dos computadoras y una impresora.

El ECA iniciará sus funciones en el plazo máximo de seis meses. Durante este lapso, podrá planificar y organizar su estructura interna, celebrar convenios y coordinar todo lo necesario con otras entidades públicas o privadas, para garantizar su funcionamiento óptimo. El Poder Ejecutivo podrá disponer todo lo necesario para trasladar a dicha entidad los recursos humanos, financieros, presupuestarios y los demás activos destinados a otras entidades públicas, para el cumplimiento de las funciones reguladas en esta Ley.

Transitorio V.-Derechos Laborales. A los funcionarios que laboran actualmente en la Oficina Nacional de Normas y Unidades de Medida (ONNUM) se les garantizan todos sus derechos laborales, conforme al inciso f) del artículo 37 del Estatuto del Servicio Civil. Los funcionarios que no deseen continuar laborando con el LACOMET, deberán manifestarlo ante la Comisión de Metrología, sin perjuicio de que puedan ser contratados en el sector público, bajo una nueva relación laboral. A los funcionarios que no deseen continuar laborando con el LACOMET, pero sí con otra entidad pública, manteniendo su relación laboral, se les permitirá la movilidad horizontal.

Rige a partir de su publicación.

3. PUBLICACIONES EN LOS DIARIOS OFICIALES EN LA IMPRENTA NACIONAL, MEDIANTE FIRMA DIGITAL CERTIFICADA, A PARTIR DEL 1º DE SETIEMBRE DE 2012

[Circular número 003-2012. Imprenta Nacional][iii]

CIRCULAR Nº 003-2012

ASUNTO: Publicaciones en los Diarios Oficiales en la Imprenta Nacional, mediante Firma Digital certificada, a partir del 1º de setiembre de 2012.

LA DIRECCIÓN GENERAL DE LA IMPRENTA NACIONAL

En uso de las facultades y atribuciones que confieren el artículo 4 de la Ley Nº 5394 del 5 de noviembre de 1973, el artículo 14 inciso a) del Decreto Ejecutivo Nº 3937 del 1º de julio de 1974, los artículos 2, 3 y 10 del Decreto Ejecutivo Nº 26651 del 19 de

diciembre de 1997, y de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, Ley Nº 8454 publicada en el Diario Oficial La Gaceta N° 197 del 13 de octubre del 2005,

Considerando:

I. - Que nuestro país ha venido promoviendo desde hace varios años el aprovechamiento de las nuevas tecnologías de la información y las telecomunicaciones, para una mejor prestación de los servicios públicos.

II. - Que como parte de este proceso evolutivo, resalta la promulgación de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, Ley Nº 8454 publicada en el Diario Oficial La Gaceta N° 197 del 13 de octubre del 2005, que proclama la equivalencia funcional, validez, eficacia y valor probatorio del documento electrónico, respecto al documento físico. En tal sentido, el artículo 9 de dicha Ley reza: "Valor equivalente. Los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito. En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita. Los documentos públicos electrónicos deberán llevar la firma digital certificada."

III. - Que el artículo 1º de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, dispone en lo conducente: "El Estado y todas las entidades públicas quedan expresamente facultados para utilizar los certificados, las firmas digitales y los documentos electrónicos, dentro de sus respectivos ámbitos de competencia."

IV. - Que particularmente el actual Gobierno ha propiciado políticas de digitalización y simplificación de los servicios, y en este proceso la Imprenta Nacional emerge como decidida impulsora hacia un auténtico Gobierno Digital.

V. - Que el aprovechamiento de las nuevas tecnologías de esta era digital, genera invaluables beneficios: una mayor eficiencia, eficacia y valor agregado en la prestación de los servicios públicos, simplificación de trámites, reducción de tiempos y costos, protección del medio ambiente a través de la reducción del papel, mejor acceso a la información, mayor transparencia, etc.

VI. - Que la Imprenta Nacional es conciente de que la culturización en este proceso de digitalización, está en manos esencialmente de las instituciones públicas, o eventualmente algunos notarios públicos, como emisores de los documentos a publicar en los Diarios Oficiales. Por tanto:

LA DIRECCIÓN GENERAL DE LA IMPRENTA NACIONAL

HACE SABER A LAS INSTITUCIONES ESTATALES

Y AL PÚBLICO EN GENERAL QUE:

A partir de esta fecha se otorga un período de seis meses, es decir, al 1º de setiembre de 2012, a las instituciones estatales, para que adopten las medidas necesarias para que los documentos a publicar en los Diarios Oficiales, tanto internos institucionales, como los externos dirigidos a los particulares, sean emitidos con Firma Digital

certificada, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos.

Jorge Luis Vargas Espinoza

Director General

[i] 30/08/2005.Ley de Certificados, Firmas Digitales y Documentos Electrónicos. Fecha de vigencia desde:13/10/2005 Publicación: Nº Gaceta: 197 del: 13/10/2005

[ii] Asamblea Legislativa. Ley : 8279 del 02/05/2002. Sistema Nacional para la Calidad .Fecha de vigencia desde:21/05/2002 Publicación: Nº Gaceta: 96 del: 21/05/2002

[iii] Imprenta Nacional. Circular : 003 del 01/03/2012.Publicaciones en los Diarios Oficiales en la Imprenta Nacional, mediante Firma Digital certificada, a partir del 1º de setiembre de 2012.Fecha de vigencia desde:01/09/2012.Publicación: Nº Gaceta: 44 del: 01/03/2012

Directrices para las Autoridades de Registro. Características de cumplimiento de Autoridades de Registro (RA) de la jerarquía nacional de certificadores registrados de Costa Rica

Dirección de Certificadores de Firma Digital
Ministerio de Ciencia y Tecnología

OID 2.16.188.1.1.1.1
Versión: 1.00
4 de setiembre, 2008


MICIT
Ministerio de
Ciencia y Tecnología

Control de versiones

Fecha	Versión	Autor(es)	Aprobado	Descripción
03-12-07	Borrador	Comité de Políticas	Lic.Oscar Solís Director DCFD	Se incorporan las observaciones de la consulta pública, de acuerdo al edicto publicado el día lunes 19 de noviembre del 2007 en el diario oficial "La Gaceta", número Nº 222
04-09-08	1.00	Comité de Políticas	Lic.Oscar Solís Director DCFD	Oficialización y entrada en vigencia de las políticas.

Índice

1. Disposiciones Generales

Este documento regula la operación y procedimientos mínimos adoptados por las Autoridades de Registro (en adelante RA) que gestionan los certificados dentro de la jerarquía nacional de certificadores registrados de Costa Rica, y es un complemento de la "Política de Certificados para la jerarquía nacional de certificadores registrados"

La Autoridad de Registro (RA) es la entidad responsable por la comunicación entre el usuario y la autoridad certificadora (CA). Está vinculada a una CA y tiene por objetivo recibir, validar, verificar y gestionar las solicitudes de emisión o revocación de los certificados digitales, cumpliendo con lo establecido en la política de certificación nacional y en concordancia con las políticas y procedimientos definidos por la CA correspondiente

Para el presente documento se aplican las definiciones del "Reglamento a la Ley de certificados, firma digitales y documentos electrónicos (Decreto No. 33018-MICIT)" y de la "Política de Certificados para la jerarquía nacional de certificadores registrados". Sin embargo, para ampliar la reglamentación de la RA se deben aclarar los siguientes conceptos:

a. Agente de registro: Persona responsable de la ejecución de las actividades propias de la RA. Esta persona debe realizar las validaciones y verificaciones definidas en la política del certificado que corresponda.

b. Confirmar la identidad del solicitante: proceso para comprobar que el solicitante es la persona con autoridad para solicitar el certificado, de acuerdo a la política asociada al certificado.

c. Suspensión de un agente de registro: Es cuando un funcionario que tiene el rol de agente de registro deja de ejercer sus labores temporalmente, alterándosele sus permisos dentro del sistema de la CA.

d. Desvincular a un Agente de Registro: Es el proceso de separar a un agente de registro de sus funciones, eliminándole los permisos dentro del sistema de la CA. Este proceso ocurre cuando:

    1. El funcionario ha renunciado a su cargo en la organización

    2. El funcionario es cesado de sus funciones o de su organización

    3. El funcionario que ha recibido la función de agente de registro la deja de ejercer, aunque continúa trabajando en otros puestos de la organización.

    4. El funcionario sancionado mediante un proceso administrativo, o por un procedimiento disciplinario, que impidan continuar en su cargo.

e. Encargado de la RA: Persona responsable de la supervisión de las funciones de los agentes de registro, y la coordinación con la CA.

f. Expediente del agente de registro: Es el conjunto de documentos relativos a un agente de registro.

g. Expediente de instalación: Es el conjunto de documentos relativo a las instalaciones de la RA, tales como plan de continuidad de negocio, análisis de riesgos, reglamento de sanciones, inventario de activos y un plan de terminación de la RA (de acuerdo con el punto "5.8 Terminación de una CA o RA" del documento de Política de certificados para la jerarquía nacional de certificadores registrados).

h. Instalaciones: Es el ambiente físico de una RA, cuyo funcionamiento es debidamente autorizado para realizar las actividades de validación y verificación de las solicitudes de certificado.

i. Validación del solicitante del certificado: Es la verificación de la identidad del individuo o la organización que se presente ante una RA para solicitar un certificado. Esta validación requiere de la presencia física del solicitante y de la evidencia que permita determinar su autoridad para la solicitud de su certificado respectivo.

Las áreas y actividades ejecutadas por la RA incluyen, entre otras:

- Verificar y validar los documentos de identidad
- Registrar y enrolar a los suscriptores
- Entregar certificados digitales
- Gestionar la aceptación del certificado por parte del suscriptor
- Gestionar revocaciones de certificados
- Registrar los eventos en las bitácoras
- Controlar y supervisar a los agentes de registro
- Almacenar y custodiar la documentación
- Controlar los reportes de incidentes
- La RA debe establecer los procedimientos y guías para asegurar el cumplimiento de la política de certificados de la jerarquía nacional y de este documento, además de tomar las acciones que prevengan alguna deficiencia de la RA, incluyendo la terminación o suspensión de sus deberes.

1.1 Administración del documento

1.1.1 Organización que administra el documento

Dirección de Certificadores de Firma Digital

Ministerio de Ciencia y Tecnología, dirección: San José, 50 metros Este del Museo Nacional. Apartado Postal: 5589-1000 San José, Costa Rica. Correo Electrónico: informacion@firmadigital.go.cr

1.1.2 Persona de contacto

Jefatura de la Dirección de Certificadores de Firma Digital Director de Certificadores de Firma Digital, Correo Electrónico: informacion@firmadigital.go.cr. Tel. (506) 2248-1515

2. Controles del Personal

2.1 Disposiciones generales

La autoridad de registro es la responsable administrativa de su operación y debe enviar a la CA la información actualizada de los agentes de registros activos, sus perfiles, cualidades y necesidades de acceso a la información Esta información es actualizada y consolidada por la CA, ejecutando los más estrictos procedimientos de custodia y fiscalización indicados en la sección 5.5.3 “protección de archivos”, de la Política de Certificados para la jerarquía nacional de certificadores registrados.

Los agentes de registro deben ser funcionarios de la organización que opera como Autoridad de Registro.

2.2 Requerimientos de documentación del Agente de Registro

Para cada agente de registro, en concordancia con los requisitos de personal ejecutando roles de confianza en la sección 5.3 de la política de certificados para la jerarquía nacional de certificadores registrados, la RA correspondiente debe poseer un expediente con:

a. Un contrato de trabajo o documento que permita comprobar su situación laboral

b. Comprobante de verificación de antecedentes criminales

c. Comprobante de verificación de situación crediticia

d. Comprobante de verificación de empleos anteriores. Incluyendo empleos en otras RA y las sanciones aplicadas, en caso de que existan.

e. Comprobante de escolaridad y residencia

f. Comprobante de aprobación de las capacitaciones recibidas referentes a las actividades propias de un Agente de Registro.

g. Declaración en que afirma conocer las atribuciones que asume y el deber de cumplir con la política nacional de certificación, y de mantener confidencialidad y privacidad de los datos disponibles en la CA o RA

h. Resultados de las evaluaciones periódicas

i. Registro que lo compromete a ejecutar labores de agente de registro en la RA

j. Registro en la CA o RA del momento en que fue incluido el rol de agente en el sistema de certificación

Cuando un Agente de Registro es desvinculado o suspendido de sus actividades en la RA entonces el expediente de la persona debe indicar:

- Registro de la solicitud para deshabilitar al agente de registro del sistema de certificación
- Registro en la CA del momento en que el agente de registro es deshabilitado o suspendido del sistema de certificación

2.3 Requerimientos Capacitación

Todo agente de registro, y personal involucrado de su administración, debe recibir capacitación y documentación en los siguientes temas:

a. Concepto básico de certificados digitales, Tokens y Smart Card

b. Principios y mecanismos de seguridad de la RA

c. Uso del Sistema de Certificación de la CA

d. Procedimientos de recuperación de desastres y de continuidad del negocio

e. Procedimientos para la validación y verificación de identidad

Esto deberá constar en el expediente de agente de registro. Cuando se presenten cambios significativos en las operaciones de la RA, el personal involucrado debe recibir capacitación al respecto.

2.4 Procedimiento de suspensión o desvinculación

Cuando un Agente de Registro sea suspendido o desvinculado de sus actividades, el encargado de la RA debe gestionar inmediatamente con la CA la suspensión o revocación de sus permisos de acceso a los sistemas de la CA y de las labores inherentes a las actividades de la RA. Estos procesos deben ser documentados.

3. Controles físicos

3.1 Exigencias mínimas de seguridad física

Todas las Autoridades de Registro deben cumplir con las siguientes exigencias mínimas de seguridad:

a. Dispositivos para la detección de incendios

b. Gabinetes o armarios con llave, de uso exclusivo de la RA

c. Los equipos de la RA deben estar protegidos contra fallas del fluido eléctrico y otras anomalías en la energía

d. Vigilancia y monitoreo del ambiente de la RA durante su horario de operación

e. Un perímetro de seguridad en el edificio donde se encuentran las instalaciones de la RA, con un guarda asignado durante el horario de operación.

f. Controles contra coacción para cada agente de registro

g. Iluminación de emergencia

3.2 Procedimientos de monitoreo

Mantener monitoreo por Circuito Cerrado de Televisión (CCTV), o cualquier otra tecnología de video-vigilancia, para la supervisión de las actividades de la RA. Las imágenes deben ser mantenidas en un ambiente seguro por al menos 60 días.

4. Controles lógicos

4.1 Controles de seguridad de las estaciones de trabajo

Las estaciones de trabajo de la RA, incluyendo los equipos portátiles, deben estar protegidas contra amenazas y acciones no autorizadas.

Las estaciones de trabajo de la RA, deben cumplir las siguientes directivas de seguridad:

a. Control de acceso lógico al sistema operacional

b. Autenticación robusta (por ejemplo, utilizando certificados digitales) para hacer uso de las estaciones de trabajo

c. Directivas bloqueo de la sesión de usuario

d. Bitácoras de auditoría del sistema operativo activadas, registrando:

    1. Inicio y terminación de las sesiones del sistema operativo

2. Intentos de crear, remover, definir contraseñas o modificar los privilegios del sistema operativo

3. Modificaciones en la configuración de las estaciones

4. Accesos (login) y de salidas (logoff) del sistema operativo

5. Intentos de acceso no autorizado al sistema operativo

e. Antivirus instalados, actualizados y habilitados

f. Permisos de acceso mínimos que le permitan ejecutar las actividades estrictamente necesarias.

g. Protector de pantalla activado como máximo dos minutos después de estar en inactividad el equipo y exigiendo un mecanismo de autenticación del usuario para desbloquearlo.

h. Sistema operativo actualizado y con la aplicación de las correcciones necesarias (parches, hotfix, etc.)

i. Endurecimiento de Estación (Hardening[1)]

j. Instalar únicamente aplicaciones autorizadas y concernientes a la función.

k. Utilización de software licenciado en las estaciones de la RA

l. Limitar el acceso remoto a la estación de trabajo de la RA, vía otro equipo ligado a una red de computadores utilizada por la RA, excepto para actividades de soporte remoto de la CA

m. Sincronización con la hora UTC en Costa Rica

Las bitácoras deben permanecer almacenadas localmente por un periodo de al menos 60 días y posteriormente pueden ser eliminadas.

En las estaciones de la RA debe contarse con un perfil de administrador de los equipos, que sea el responsable de administrar la configuración de la máquina y esta labor debe ser segregada de las funciones del agente de registro de la RA.

4.2 Controles de la aplicación de la RA

La aplicación de la RA es la conexión entre la RA y el sistema de certificados de la CA y debe cumplir al menos con las siguientes funcionalidades:

a. Autenticar robustamente (por ejemplo utilizando un certificado digital) al funcionario que funge en el rol de agente de registro

[1] **El Hardening es una técnica compuesta por un conjunto de actividades llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo posible la seguridad de este.**

b. Permitir acceso solamente a través de equipos autenticados

c. Almacenar el historial de las inclusiones y exclusiones de los agentes de registro y los permisos o revocatorias aplicadas

d. Proveer mecanismo de revocación automática de los certificados por parte del suscriptor o dueño del certificado

e. Almacenar información que evidencie los procesos de identificación y autenticación de los solicitantes

f. Implementar controles para verificar la información incluida en el certificado digital, en particular validarlos con las fuentes oficiales de información definidas en política de Certificados para la jerarquía nacional de certificadores registrados

g. Remitir la solicitud de certificado digital a la CA emisora, firmada digitalmente

h. Proveer métodos de activación de los dispositivos criptográficos a través de esquemas seguros, que evite divulgar información acerca de la activación de los dispositivos.

i. Evidenciar que el proceso de generación e instalación del certificado se realizó dentro del tiempo definido en la sección "4.2.3 Tiempo para procesar solicitudes de certificado" de las políticas de certificación o con base en el acuerdo del suscriptor.

j. Implementar controles para la preservación de la privacidad de la información

k. Dejar evidencia para los certificados de persona física de la aceptación de los deberes y responsabilidades por parte del suscriptor acerca del uso del certificado, firmando digitalmente el comprobante de aceptación con el certificado entregado y validando que funciona correctamente

l. Registrar en la bitácoras de auditoría las operaciones del ciclo de vida del certificado

m. Reportar cualquier incidente a la CA

5. Controles de seguridad de la RED

Cada instalación de la RA debe mantener los componentes de su red local en un ambiente físicamente seguro y sus configuraciones deben ser revisadas periódicamente. Además, deben protegerse la privacidad e integridad de los datos sensibles.

6. Controles de seguridad de la información

6.1 Directrices generales

Toda la información y documentos relacionados con la instalación y puesta en operación de la RA deben ser clasificados y almacenados de acuerdo a los requisitos de seguridad definidos en la sección "5.5 Archivado de registros" de Política de certificados para la jerarquía nacional de certificadores registrados; y que garantizan privacidad y confidencialidad de la información.

El "Expediente de Instalación" es un documento clasificado como privado y confidencial, por mantener información sensible de la instalación técnica de la RA, y está constituido por los siguientes documentos actualizados:

a. Plan de continuidad del negocio

b. Análisis de riesgos

c. Reglamento de sanciones

d. Plan de terminación de una RA

e. Inventario de Activos de la RA

Adicionalmente, debe tener disponible los siguientes documentos para uso de los agentes de registro:

- Copia de las políticas de certificación
- Manual de operación para los agentes de registro

6.2 Procedimientos de almacenamiento, manipulación y destrucción de documentos

Los documentos en papel que componen los expedientes de los solicitantes de certificado deben ser guardados obligatoriamente en archivos donde únicamente tengan acceso los agentes de registro. Una RA puede sustituir los documentos físicos por digitales, siempre y cuando estén firmados digitalmente con un certificado emitido por la jerarquía nacional de certificación digital.

Los documentos que contengan información confidencial o privada deben ser almacenados en los gabinetes o armarios con llave de uso exclusivo de la RA y cuando se dejen de utilizar deberán ser destruidos, de tal forma que no se pueda recuperar la información contenida en ellos.

7. Controles del ciclo de vida del certificado

La RA debe respetar el ciclo de vida del certificado definido en el capítulo 4 "Requerimientos operacionales del ciclo de vida del certificado", del documento de "Política de certificados para la jerarquía nacional de certificadores registrados".

8. Acuerdos operacionales

La CA debe celebrar un acuerdo operacional para que la RA ejecute las actividades de validación y verificación de las solicitudes de certificado. Este acuerdo debe contener al menos:

a. La identificación y calidades de los celebrantes del acuerdo de la RA

b. La identificación de los deberes que competen a la RA en función del acuerdo

c. La identificación de los responsables de la RA

d. Compromiso de la RA de cumplir con las normas y procedimientos definidos

e. Plazo por medio del cual el acuerdo es celebrado

f. Obligaciones de la RA para verificar los procesos que ejecuta

Política de Certificados para la jerarquía nacional de certificadores registrados

Dirección de Certificadores de Firma Digital
Ministerio de Ciencia y Tecnología

OID 2.16.188.1.1.1.1
Versión: 1.00
04 de setiembre, 2008


MICIT
Ministerio de
Ciencia y Tecnología

Control de versiones

Fecha	Versión	Autor(es)	Aprobado	Descripción
26-10-07	**Consulta pública**	**Comité de Políticas Comité Técnico**	**Lic.Oscar Solís Director DCFD**	**Se presenta la versión para discusión final del comité de políticas y aprobación del Director de la DCFD.**
03-12-07	**Borrador**	**Comité de Políticas**	**Lic.Oscar Solís Director DCFD**	**Se incorporan las observaciones de la consulta pública, de acuerdo al edicto publicado el día lunes 19 de noviembre del 2007 en el diario oficial "La Gaceta", número Nº 222**
04-09-08	**1.00**	**Comité de Políticas**	**Lic.Oscar Solís Director DCFD**	**Oficialización y entrada en vigencia de las políticas.**

Índice

1. Introducción

Este documento define las Políticas de Certificado (en adelante CP) dictadas por la Dirección de Certificadores de Firma Digital (en adelante DCFD) para el Sistema Nacional de Certificación Digital.

La autoridad certificadora registrada debe implementar las políticas en los servicios de certificación que incluyen: la emisión, gestión, suspensión y revocación de los certificados.

Las siguientes secciones describen las políticas de acatamiento obligatorio que deben ser implementadas por la Autoridad Certificadora Raíz (en adelante CA Raíz) y por cualquier otra Autoridad Certificadora Registrada (en adelante CA) en los niveles inferiores de la jerarquía nacional de certificadores registrados. Sin embargo, este documento no pretende ser una guía exhaustiva para la evaluación del cumplimiento de los requisitos necesarios para un proceso de acreditación. La guía detallada para la evaluación de una autoridad certificadora que desea incorporarse al sistema de certificación nacional, debe solicitarse a la DCFD, y la misma se adhiere a los lineamientos establecidos en: la norma INTE-ISO-21188:2007 “Infraestructura de llave pública para servicios financieros — Estructura de prácticas y políticas”.

Este CP se ha desarrollado conforme a lo estipulado en el RFC 3647” Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework”.

1.1 Resumen

Estas Políticas de Certificación (CP) son específicamente aplicables a:

- Autoridad Certificadora Raíz (CA Raíz).
- Autoridades Certificadoras de Políticas (CA de Políticas) dentro de la jerarquía nacional de certificadores registrados.
- Autoridades Certificadoras emisoras (CA emisoras) que se registren ante la DCFD, y que emitan los certificados a las entidades finales.
- Suscriptores y partes que confían.

Las políticas nacionales contemplan los siguientes tipos de certificados, definidos en este documento como:

- Certificados para CA emisoras.
- Certificados de autenticación de persona física.
- Certificados de firma digital de persona física.
- Certificados de autenticación y firma digital de agente electrónico.
- Certificados de autoridades de sellado de tiempo (TSA).

Los diferentes tipos de certificados están definidos en la política y se implementan a través de una jerarquía de tres niveles: el primero corresponde a la raíz nacional, el segundo nivel corresponde a las autoridades certificadoras de políticas y el tercer nivel a las CA emisoras de certificados.

El siguiente diagrama detalla la estructura de la jerarquía nacional de certificadores registrados:

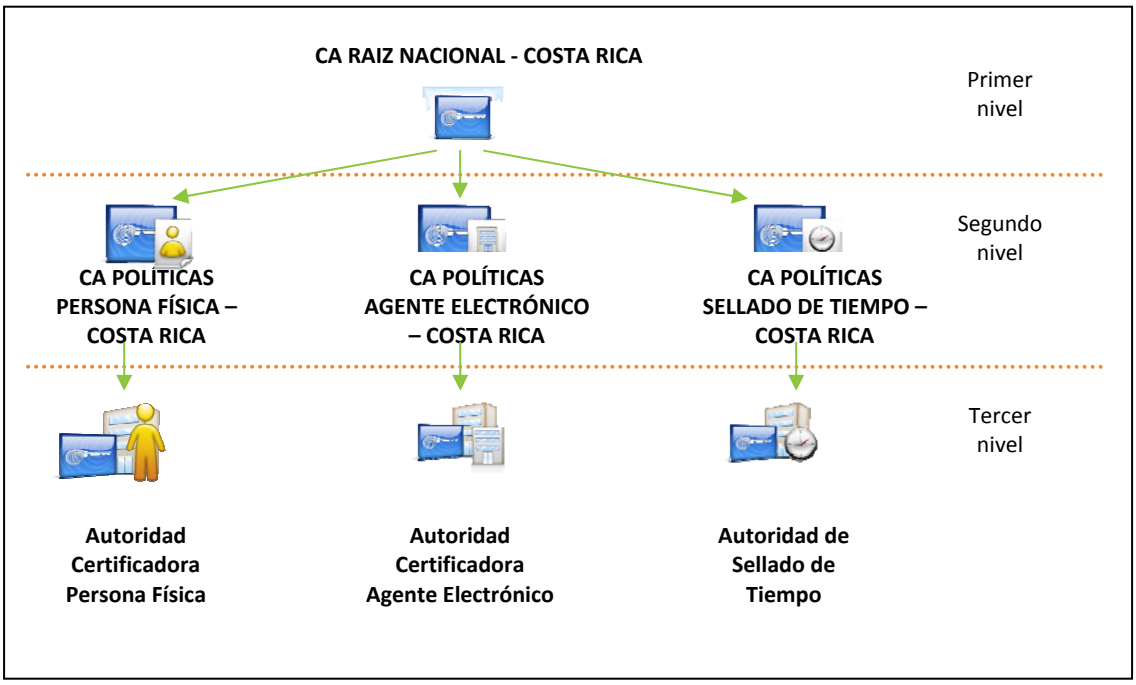


Diagrama de la jerarquía nacional de certificadores registrados

1.2 Nombre e identificación del documento

Este documento es la "Política de Certificados para la jerarquía nacional de certificadores registrados" y se referencia mediante el identificador de objeto (OID): 2.16.188.1.1.1.1

Sección	Descripción
2	**joint-iso-itu-t**
16	**Country**
188	**Costa Rica**
1	**Organización**
1	**Dirección de Certificadores de Firma Digital**
1	**Políticas**
1	**Política de Certificados para la jerarquía nacional de certificadores registrados**

Las políticas derivadas para la jerarquía nacional de certificadores registrados son:

Política para certificados generados por la jerarquía nacional de certificadores registrados	OID
Certificados de CA emisora	**2.16.188.1.1.1.1.1**
Certificados de persona Física • **Firma digital** • **Autenticación**	 **2.16.188.1.1.1.1.2** **2.16.188.1.1.1.1.3**
Certificados de firma digital y autenticación de agente electrónico	**2.16.188.1.1.1.1.4**
Política de sellado de tiempo del sistema nacional de certificación digital	**2.16.188.1.1.1.1.5**

1.3 Participantes en la PKI

1.3.1 Autoridades certificadoras

Las autoridades certificadoras (CA) son todas las entidades autorizadas a emitir certificados de llave pública dentro de la **jerarquía nacional de certificadores registrados**. Esto incluye:

- CA Raíz.
- CA de Políticas.
- CA emisoras.

La CA Raíz y las CAs de Políticas son parte de la jerarquía nacional administrada por el Ministerio de Ciencia y Tecnología (MICIT). Ambas se regulan a través de la Dirección de Certificadores de Firma Digital (DCFD) y del Comité Asesor de Políticas (CAP). Las CAs emisoras deben implementar esta política, para formar parte de la **jerarquía nacional de certificadores registrados.**

1.3.2 Autoridades de Registro

Una Autoridad de Registro (RA) es una entidad que ejecuta labores de identificación y autenticación de los solicitantes que aplican por un certificado. La RA debe validar los requisitos de identificación del solicitante, dependiendo del tipo de certificado y de la especificación de la política pertinente. Además, tramita las solicitudes de revocación para los certificados y valida la información contenida en las solicitudes de certificados. Las Autoridades de Registro se regulan en el documento de "Directrices para las Autoridades de Registro. Características de cumplimiento de Autoridades de Registro (RA) de la jerarquía nacional de certificadores registrados de Costa Rica" emitido por la DCFD para este propósito.

1.3.3 Suscriptores

Se define como suscriptor a todos los usuarios finales a quienes se les ha emitido un certificado por una CA, dentro de la jerarquía nacional de certificadores registrados. El suscriptor puede ser un individuo o una organización representada por el agente electrónico.

1.3.4 Partes que confían

Una parte que confía es un individuo o entidad que actúa confiando en un certificado y/o firmas digitales emitidas bajo la **jerarquía nacional de certificadores registrados**. Una parte que confía puede o no ser también un suscriptor.

1.3.5 Otros participantes

Sin estipulaciones

1.4 Uso del certificado

1.4.1 Usos apropiados del certificado

Tipo	Descripción de uso apropiado
Certificados de CA emisora	• **Operar la infraestructura PKI (por ejemplo: Firma de listas de revocación)** • **Emitir certificados a suscriptores dentro de la cadena de confianza.**
Certificados de firma digital de persona física	• **Firma digital y no repudio.**
Certificados de autenticación de persona física	• **Autenticación.**
Certificados de firma digital y autenticación de agente electrónico	• **Firma digital de documentos electrónicos actuando en nombre de la empresa o institución.** • **Autenticación.**
Certificados de Autoridad de Sellado de Tiempo (TSA)	• **Sellado de Tiempo.**

1.4.2 Usos prohibidos del certificado

Los certificados emitidos deben ser utilizados dentro del marco de la ley 8454 “Ley de certificados, firmas digitales y documentos electrónicos” y su reglamento. Cualquier otro uso del certificado no especificado en esta CP está fuera del alcance y responsabilidad de estas políticas.

1.5 Administración de la Política

1.5.1 Organización que administra el documento

Dirección de Certificadores de Firma Digital

Ministerio de Ciencia y Tecnología, dirección: San José, 50 metros Este del Museo Nacional. Apartado Postal: 5589-1000 San José, Costa Rica. Correo Electrónico: informacion@firmadigital.go.cr

1.5.2 Persona de contacto

Jefatura de la Dirección de Certificadores de Firma Digital Director de Certificadores de Firma Digital, Correo Electrónico: informacion@firmadigital.go.cr. Tel. (506) 2248-1515, ext. 189.

1.5.3 Persona que determina la adecuación de la CPS a la Política

El director de la Dirección de Certificadores de Firma Digital será el encargado de determinar la adecuación de la declaración de prácticas de certificación (CPS) de todas las autoridades certificadoras que desean pertenecer a la **jerarquía nacional de certificadores registrados**.

1.5.4 Procedimientos de aprobación de la CP

La política y las subsecuentes enmiendas o modificaciones deben ser propuestas por el Comité Asesor de Políticas y presentadas al Director de la DCFD, quien posterior a su análisis y correcciones, las somete a consulta pública (salvo casos de urgencia) en la que se invitará a las entidades públicas y privadas, organizaciones representativas y público en general a ofrecer comentarios y sugerencias pertinentes; todo conforme a los artículo 361 [1] y 362 [2] de la Ley General de Administración Pública (LGAP). La encargada de la aprobación final de la CP, es la DCFD.

1.6 Definiciones y acrónimos

Ver Anexo A: Definiciones y acrónimos

---

1 **Artículo 361.-**

1. **Se concederá audiencia a las entidades descentralizadas sobre los proyectos de disposiciones generales que puedan afectarlas.**
2. **Se concederá a las entidades representativas de intereses de carácter general o corporativo afectados por la disposición la oportunidad de exponer su parecer, dentro del plazo de diez días, salvo cuando se opongan a ello razones de interés público o de urgencia debidamente consignadas en el anteproyecto.**
3. **Cuando, a juicio del Poder Ejecutivo o del Ministerio, la naturaleza de la disposición lo aconseje, el anteproyecto será sometido a la información pública, durante el plazo que en cada caso se señale.**

2 **Artículo 362.- En la disposición general se han de consignar expresamente las anteriores que quedan total o parcialmente reformadas o derogadas.**

2. Responsabilidades de publicación y del repositorio

2.1 Repositorios

Las autoridades emisoras son responsables de las funciones de repositorio para su propia CA. Las listas de los certificados emitidos a usuarios finales no se deben hacer públicas.

Sobre la revocación de certificados de suscriptores, las autoridades emisoras deben publicar el aviso de revocación de los certificados de sus suscriptores.

2.2 Publicación de información de certificación

La CA emisora debe mantener un repositorio basado en Web que permita a las partes que confían verificar en línea la revocación y cualquier otra información necesaria para validar el estado del certificado. La CA emisora debe proporcionar a las partes que confían la información de cómo encontrar el repositorio adecuado para verificar el estado del certificado y los servicios de validación de certificados en línea (OCSP) para la verificación en línea.

La CA emisora debe mantener publicada, entre otros aspectos, la versión actualizada de:

- La Política de los certificados que implementa.
- La plantilla del contrato de suscriptor.
- Los certificados en la cadena de confianza.
- Las listas de revocación.

La información de la CA Raíz está publicada en el sitio Web del MICIT, en las siguientes direcciones:

- Sitio primario:
  - http://www.firmadigital.go.cr
- Sitio alterno:
  - http://www.micit.go.cr/firmadigital

2.3 Tiempo o frecuencia de publicación

Las actualizaciones de las políticas de certificado se publicarán de acuerdo con lo establecido en la sección 9.12 de este documento. Las actualizaciones de acuerdos de suscriptores serán publicadas, cuando sufran modificaciones. La información de estados de certificado es publicado de acuerdo con las disposiciones de esta política, de acuerdo a la sección 4.9.7 de "Frecuencia de emisión de CRL".

2.4 Controles de acceso a los repositorios

La información publicada en el repositorio es información accesible únicamente para consulta. La CA emisora debe establecer controles para prevenir que personas no autorizadas agreguen, eliminen o modifiquen información de los repositorios

3. Identificación y autenticación

3.1 Nombres

3.1.1 Tipos de nombres

En la sección 3.1.4 se explican las reglas para interpretación del código de identificación, la que, en el caso de las personas físicas nacionales corresponde al número de cédula, para personas extranjeras, al número de único de permanencia y para las empresas o instituciones corresponde al número de cédula de persona jurídica. El uso del campo número de serie (serial number OID 2.5.4.5) se establece de acuerdo al RFC 3039 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile" como un atributo del nombre distintivo del sujeto.

A continuación se presentan los formatos de los nombres para el suscriptor del certificado dependiendo de su tipo. Cuando los datos se encuentran en *itálica* significan que son valores de ejemplo.

En el caso de la CA Raíz:

Atributo	Valor	Descripción
Country (C)	**CR**	**El código de país es asignado de acuerdo al estándar ISO 3166[3]**
Organization (O)	**MICIT**	**El Ministerio de Ciencia y Tecnología es el responsable de la Raíz Nacional**
Organization Unit (OU)	**DCFD**	**La Dirección de Certificadores de Firma Digital**
Common Name	**CA RAIZ NACIONAL –**	**Nombre de la CA Raíz**

3 Norma ISO 3166 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países". Esta norma establece los códigos de dos caracteres para la asignación del país

	COSTA RICA	
Serial Number {OID:2.5.4.5}	**CPJ-2-100-098311**	**Número de cédula de persona jurídica en el Registro Nacional. El prefijo CPJ es Cédula Persona Jurídica**

En el caso de la CA de Políticas:

En el caso de la CA de Políticas:

Atributo	Valor	Descripción
Country (C)	**CR**	**El código de país es asignado de acuerdo al estándar ISO 3166**
Organization (O)	**MICIT**	**El Ministerio de Ciencia y Tecnología es el responsable de la Raíz Nacional**
Organization Unit (OU)	**DCFD**	**La Dirección de Certificadores de Firma Digital**
Common Name	**CA POLITICA *PERSONA FISICA – COSTA RICA***	**CA POLÍTICA + *Nombre de la política – COSTA RICA***
Serial Number {OID:2.5.4.5}	**CPJ-2-100-098311**	**Número de cédula de persona jurídica en el Registro Nacional. El prefijo CPJ es Cédula Persona Jurídica**

En el caso de la CA emisoras:

Atributo	Valor	Descripción
Country (C)	**CR**	**El código de país es asignado de acuerdo al estándar ISO 3166**
Organization (O)	***CORP. EJEMPLO S.A***[4]	**Nombre de la empresa o institución definido en la certificación de personería jurídica**
Organization Unit (OU)	***CA EJEMPLO***	**Unidad organizacional de la empresa o institución**
Common Name	**CA *EJEMPLO* - *PERSONA FISICA***	**CA + Nombre CA - Política. La Política puede ser: PERSONA FISICA, AGENTE ELECTRONICO, SELLADO DE TIEMPO, u otra definida por la CA Raíz**
Serial Number {OID:2.5.4.5}	**CPJ-*9-999-999999***	**Número de cédula de persona jurídica en el Registro Nacional, debe ser validada durante el proceso de registro.**

4 Los valores en itálica son colocados a manera de ejemplo.

En el caso de suscriptor persona física:

Atributo	Valor	Descripción
Country (C)	**CR**	**El código de país es asignado de acuerdo al estándar ISO 3166**
Organization (O)	***PERSONA FISICA***	**La política identifica si se trata de un certificado para: Persona Física, Agente Electrónico o Sellado de tiempo o bien otra definida por la jerarquía nacional de certificadores registrados**
Organization Unit (OU)	***CIUDADANO***	**La clase de certificado es: CIUDADANO, EXTRANJERO.**
Common Name	***JUAN PEREZ PEREZ (FIRMA)***	**Nombre del suscriptor, según documento de identificación, en mayúsculas y sin tildes El propósito puede ser FIRMA o AUTENTICACION**
Serial Number {OID:2.5.4.5}	**CPF-*01-0449-0161***	**El formato del documento de identificación se especifica en la sección 3.1.4 "Reglas para la interpretación de varias formas de nombres"**
Surname (SN) {OID:2.5.4.4}	***PEREZ PEREZ***	**Se registran los dos apellidos del suscriptor, en mayúsculas y sin tildes.**
GivenName (G) {OID:2.5.4.42}	***JUAN***	**Se registra el nombre del suscriptor, en mayúsculas y sin tildes**

En el caso de suscriptor para agente electrónico:

Atributo	Valor	Descripción
Country (C)	**CR**	**El código de país es asignado de acuerdo al estándar ISO 3166**
Organization (O)	***CORTE SUPREMA DE JUSTICIA***	**Razón social/Nombre de la empresa o institución que solicita el certificado, según la información del Registro Mercantil.**
Organization Unit (OU)	***0001***	**Identificador consecutivo de Agente asociado a una organización. Este campo es responsabilidad de la empresa o institución proporcionarlo.**
Common Name	***CORTE SUPREMA DE JUSTICIA***	**Razón social/Nombre de la empresa o institución que solicita el certificado, según la información del Registro Mercantil.**
Serial Number {OID:2.5.4.5}	**CPJ-*2-300-042155***	**El formato de la cédula de persona jurídica se especifica en la sección 3.1.4 "Reglas para la interpretación de varias formas de nombres"**
Subject Alternative Name {OID:2.5.29.17}	**Dns=www.poder-judicial.go.cr**	**Este es un valor opcional donde se coloca el nombre del dominio.**

En el caso de suscriptor para autoridad de sellado de tiempo:

Atributo	Valor	Descripción
Country (C)	**CR**	**El código de país es asignado de acuerdo al estándar ISO 3166**
Organization (O)	***LABORATORIO COSTARRICENSE DE METROLOGIA***	**Nombre de la empresa o institución que solicita el certificado**
Organization Unit (OU)	***0001***	**Identificador consecutivo para la autoridad de sellado de tiempo. Este campo es responsabilidad de la empresa o institución proporcionarlo, y es utilizado para mantener la continuidad del negocio**
Common Name	**TSA *LABORATORIO COSTARRICENSE DE METROLOGIA***	**TSA + Nombre de la empresa o institución, según documento de expedido como el Registro Mercantil. Se concatena el propósito de TSA (Time Stamping Authority) para indicar que es una autoridad de sellado de tiempo.**
Serial Number {OID:2.5.4.5}	**CPJ-3-007-351220**	**El formato de la cédula de persona jurídica se especifica en la sección 3.1.4 "Reglas para la interpretación de varias formas de nombres"**

3.1.2 Necesidad de nombres significativos

El nombre significativo corresponde al nombre especificado en el documento oficial presentado por el solicitante en el momento de registro. Además para evitar errores de interpretación en el nombre de personas físicas, se registra el nombre y los apellidos en atributos separados (GivenName y SurName, respectivamente).

3.1.3 Anonimato o pseudónimos de los suscriptores

De acuerdo con la ley 8454, "Ley de certificados, firmas digitales y documentos electrónicos" y su reglamento, los certificados de firma digital no admiten anonimato para cumplir con el requisito de **"No Repudio".** El pseudónimo no se considera un nombre significativo del solicitante y no se utilizará como parte del certificado.

3.1.4 Reglas para la interpretación de varias formas de nombres

Certificados de CA emisora

La cédula de persona jurídica es definida por el Registro Nacional de la Propiedad y debe cumplir el siguiente formato.

Tipo de documento	Prefijo	Formato
Cédula de persona jurídica	**CPJ**	**CPJ-9-999-999999**

Certificados de firma digital y autenticación de persona física

El nombre común tiene concatenado el propósito del certificado entre paréntesis, el cual puede ser únicamente uno de los siguientes:

- (FIRMA)
- (AUTENTICACION)

La cédula y el documento único de permanencia deben cumplir el siguiente formato:

Tipo de documento	Prefijo	Formato
Cédula de persona física	**CPF**	**CPF-99-9999-9999**
Número único de permanencia	**NUP**	**NUP-9XXX99999999**[5]

Certificados de firma digital y autenticación de agente electrónico y de Autoridad de Sellado de Tiempo

La cédula de persona jurídica debe cumplir el siguiente formato:

Tipo de documento	Prefijo	Formato
Cédula de persona jurídica	**CPJ**	**CPJ-9-999-999999**

3.1.5 Unicidad de los nombres

La CA emisora debe asegurar que el "nombre distintivo del suscriptor" (***subject distinguished name***) es único dentro de la jerarquía nacional de certificadores registrados, a través de una verificación dentro del proceso de inscripción.

5 El número único de permanencia (NUP) está conformado por los siguientes elementos:

- Código de No Nacional, es un dígito, y siempre se asigna el número 1
- Código de país, es un código alfanumérico de acuerdo con el ISO-3166 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países." con formato de 3 letras, por ejemplo: NIC = Nicaragua, CRI = Costa Rica, USA = Estados Unidos de América, COL= Colombia, etc.
- Consecutivo por país, corresponde a la numeración de seis dígitos, que representa la cantidad de personas que han ingresado con estatus migratorio al país en el momento de la inscripción
- Dígitos de verificación, son dos dígitos que verifican la consistencia de la notación para ese extranjero

La CA emisora debe garantizar que solamente existe un certificado vigente con el mismo propósito para cada suscriptor, en caso de persona física.

3.1.6 Reconocimiento, autenticación y rol de las marcas registradas

La jerarquía nacional de certificadores registrados no arbitrará, mediará o resolverá ninguna disputa concerniente a la propiedad de nombres de dominio, nombres de empresas o instituciones y marcas registradas.

3.2 Validación inicial de identidad

3.2.1 Método para probar posesión de la llave privada

El solicitante del certificado debe demostrar que posee la llave privada correspondiente a la llave pública que estará listada en el certificado. El método de prueba de posesión de la llave privada puede ser el PKCS#10, u otras demostraciones criptográficas equivalentes, aprobadas por la DCFD.

3.2.2 Autenticación de identidad de organización

La identidad de la organización solicitante debe ser confirmada por la CA emisora, o por la RA, donde aplique, de acuerdo con los procedimientos establecidos. Como mínimo, se debe verificar el nombre o razón social, la cédula de persona jurídica y representante legal debidamente acreditado.

La CA emisora, o donde aplique, la RA, debe verificar la información suministrada por el solicitante contra los datos oficiales correspondientes.

En el caso de certificados de agente electrónico, si el solicitante requiere incluir uno o más nombres DNS en el campo “nombre alternativo del sujeto” (Subject Alternative Name, o también conocido como SAN por sus siglas en inglés), la CA emisora, o donde aplique, la RA, debe verificar la información de DNS suministrada por el solicitante, contra los datos oficiales correspondientes.

3.2.3 Autenticación de identidad individual

Para la identificación de la persona física la CA emisora o RA verifica la validez y vigencia del documento legalmente aceptado, presentado por el solicitante. Este proceso debe realizarse en forma presencial (cara a cara).

La CA emisora, o donde aplique, la RA, debe verificar la información suministrada por el solicitante contra los datos oficiales correspondientes.

3.2.4 Información del suscriptor no verificada

No aplica, la información incluida en el certificado es verificada durante el proceso de autenticación de la identidad.

3.2.5 Validación de la Autoridad

La CA emisora, o donde aplique, la RA debe validar la autoridad que posee el solicitante para gestionar un tipo de certificado específico. Además, debe validar que el solicitante no posea impedimentos legales, de acuerdo a la información oficial vigente para tales efectos.

En el caso de certificados de persona física, debe validar que sea mayor de edad.

En el caso de una organización debe verificar:

- Nombre o razón social y cédula de persona jurídica.
- Nombre del representante legal y documento de identidad legalmente aceptado.

La CA emisora, o donde aplique, la RA, debe verificar la información suministrada por el solicitante contra los datos oficiales correspondientes.

3.2.6 Criterios para interoperabilidad

Se permitirá la interoperabilidad de los certificados emitidos, siempre y cuando la CA emisora cumpla con la política de la raíz y estén adscritas a la **jerarquía nacional de certificadores registrados**. La homologación de certificados extranjeros se hará de acuerdo con la legislación aplicable y los procedimientos establecidos por la DCFD para tales casos.

3.3 Identificación y autenticación para solicitudes de re-emisión de llaves

3.3.1 Identificación y autenticación para re-emisión de llaves rutinaria

No se permite la re-emisión de certificados. En dado caso, se debe optar por un nuevo certificado.

3.3.2 Identificación y autenticación para la re-emisión de llaves después de una revocación

Bajo estas circunstancias la re-emisión de llaves no aplica.

3.4 Identificación y autenticación para solicitudes de revocación

Los procedimientos de revocación deben asegurar, previo a cualquier revocación, que la solicitud de revocación ha sido generada por el suscriptor del certificado o por una entidad autorizada para tales propósitos.

Los procedimientos aceptados para la autenticación de solicitudes de revocación presentadas por el suscriptor incluyen alguno de los siguientes medios:

- La recepción de un mensaje firmado digitalmente por el suscriptor del certificado.

- Mediante la validación de una “frase de desafío” (challenge phrase).
- Presencialmente, a través de los procesos de autenticación de identidad (secciones 3.2.2 y 3.2.3).
- Cualquier otro medio aprobado por la DCFD que permita una autenticación robusta.

Los procedimientos aceptados para la autenticación de solicitudes de revocación presentadas por una entidad autorizada para tales efectos (ver sección 4.9.2), incluye la recepción de un mensaje firmado por una autoridad competente.

4. Requerimientos operacionales del ciclo de vida del certificado

4.1 Solicitud de certificado

4.1.1 Quién puede presentar una solicitud de certificado

En la siguiente lista se detallan las personas que pueden presentar una solicitud de certificado:

- Para el caso de certificados de CA de políticas, el Director de Certificadores de Firma Digital.
- Para el caso de certificados de CA emisoras, el representante legal o apoderado con poderes suficientes de la entidad a ser registrada.
- Para el caso de certificados de firma digital y autenticación de persona física, cualquier persona mayor de edad con un documento de identidad legalmente aceptado, que será el sujeto a cuyo nombre se emita el certificado.
- Para el caso de certificados de firma digital y autenticación de agente electrónico, el representante legal o apoderado con poderes suficientes de la entidad a ser certificada.
- Para los certificados de Autoridad de Sellado de Tiempo, el representante legal o apoderado con poderes suficientes de la entidad de sellado de tiempo (TSA).

4.1.2 Proceso de inscripción y responsabilidades

Durante el proceso de inscripción, el solicitante debe firmar un acuerdo de suscriptor, donde se establecen las responsabilidades y deberes asumidos con el uso del certificado.

La DCFD tiene la responsabilidad de:

- Ejecutar el proceso de registro y verificación de identidad de las CA emisoras.
- Velar porque la entidad solicitante cumpla los requisitos establecidos en la Ley 8454, Ley de certificados, firmas digitales y documentos electrónicos y su reglamento.
- Informar al suscriptor de sus deberes y responsabilidades con respecto al uso del certificado.

- Emitir el certificado de acuerdo con la información suministrada en la solicitud de certificado.

La CA emisora tiene la responsabilidad de:

- Validar la identidad de la RA que remite las solicitudes.
- Validar la información suministrada en la solicitud.
- Emitir el certificado de acuerdo con la información suministrada en la solicitud.
- Enviar el certificado a la RA para que sea entregado al suscriptor.

La RA tiene la responsabilidad de:

- Ejecutar el proceso de registro y verificación de identidad del solicitante.
- Remitir la solicitud de certificado digital a la CA emisora, firmada digitalmente.
- Informar al suscriptor de sus deberes y responsabilidades con respecto al uso del certificado.

El solicitante tiene las siguientes responsabilidades dependiendo del tipo de certificado:

Certificados de CA emisora

- Completar el formulario de inscripción de certificado y proveer información correcta y verdadera. Esta información debe presentarse ante la RA, para este caso la DCFD.
- Presentar un documento de identificación legalmente aceptado y vigente, así como una personería jurídica vigente (con menos de un mes de emitida) donde se establezca su relación como representante legal o apoderado con poderes suficientes de la empresa o institución a certificar.
- Generar la solicitud de certificado de forma que se demuestre la posesión de la llave privada correspondiente a la llave pública entregada, cumpliendo lo estipulado en el apartado 3.2.1.
- Firmar el acuerdo de suscriptor.

Certificados de firma digital y autenticación de persona física

- Completar el formulario de inscripción de certificado y proveer información correcta y verdadera.
- Presentar un documento de identificación legalmente aceptado y vigente.
- Ingresar confidencialmente la “frase de desafío” (“challenge phrase”), que será requerida en el proceso de revocación del certificado.
- Generar la solicitud de certificado de forma que se demuestre la posesión de la llave privada correspondiente a la llave pública entregada, cumpliendo con lo dispuesto en el apartado 3.2.1.
- Firmar el acuerdo de suscriptor.

Certificados de firma digital y autenticación de agente electrónico

- Completar el formulario de inscripción de certificado y proveer información correcta y verdadera.
- Presentar un documento de identificación legalmente aceptado y vigente, así como una personería jurídica con menos de un mes de emitida, donde se establezca su relación como el representante legal o apoderado con poderes suficientes de la empresa o institución.
- En el caso, de requerir que uno o varios nombres DNS formen parte del campo nombre alternativo del sujeto (Subject Alternative Name o SAN por sus siglas en inglés) es necesario que el representante legal presente evidencia de que el nombre de dominio solicitado está registrado a nombre de la organización que representa (ver sección 7.1.2.3). Generar la solicitud de certificado cumpliendo con el apartado 3.2.1 de este CP y presentarla ante la CA, con lo que se demuestra la posesión de la llave privada correspondiente a la llave pública entregada.
- Firmar el acuerdo de suscriptor.

Certificados de Autoridad de Sellado de Tiempo (TSA)

- Completar el formulario de inscripción de certificado y proveer información correcta y verdadera ante la DCFD.
- Cumplir con todas las responsabilidades señaladas anteriormente para solicitante de certificado de Agente Electrónico.

4.2 Procesamiento de la solicitud de certificado

4.2.1 Ejecución de las funciones de identificación y autenticación

Certificados de CA emisora y de autoridad de sellado de tiempo

La encargada de estas funciones es la DCFD, entidad que debe velar por el cumplimiento de la identificación y la autenticación de acuerdo con las disposiciones establecidas en la sección 3.2.

Certificados de firma digital y autenticación de persona física o de agente electrónico

La encargada de estas funciones es la autoridad de registro (RA), o donde aplique la CA, que debe velar por el cumplimiento de la identificación y la autenticación de acuerdo con las disposiciones establecidas en la sección 3.2.

4.2.2 Aprobación o rechazo de solicitudes de certificado

Certificados de CA emisora y de autoridad de sellado de tiempo (TSA)

La DCFD debe administrar y supervisar el proceso de certificación, en particular lo concerniente a la aceptación o rechazo de las aplicaciones para certificados de autoridad certificadora.

Para optar por un certificado de autoridad certificadora, la CA solicitante debe cumplir con todos los requisitos establecidos en la Ley 8454, su Reglamento y demás lineamientos establecidos por la DCFD.

Certificados de firma digital y autenticación de persona física o de agente electrónico

La RA debe rechazar cualquier solicitud de certificado que no cumpla con la Ley, su Reglamento y demás lineamientos establecidos por la DCFD. Asimismo, la CA emisora debe rechazar cualquier solicitud proveniente de una RA que no cumpla con los requisitos para la emisión del certificado.

4.2.3 Tiempo para procesar solicitudes de certificado

El tiempo de procesamiento de solicitudes de certificados (tiempo entre la solicitud emitida a la CA y la emisión del certificado al suscriptor) de persona física, cuando el proceso se realice en forma automática, no debe ser mayor a diez minutos.

En cualquier otro caso, las CA y RA procesarán las solicitudes de certificados dentro de un tiempo razonable, a menos que se especifiquen otros parámetros en el acuerdo de suscriptor, en la CPS o en otros acuerdos entre los participantes.

4.3 Emisión de certificado

4.3.1 Acciones de la CA durante la emisión de certificados

Certificados de CA y certificados de autoridad de sellado de tiempo (TSA)

La CA debe verificar que el solicitante cumple con los requisitos de esta política, con las normas técnicas y con la legislación aplicable.

Certificados de firma digital y autenticación de persona física o de agente electrónico

La CA debe verificar que las solicitudes de certificado provengan de RAs autorizadas. Una vez creado el certificado, la CA debe remitirlo a la RA desde la cual ingresó la solicitud.

4.3.2 Notificación al suscriptor por parte de la CA sobre la emisión del certificado

Certificados de CA emisora y certificados de autoridad de sellado de tiempo (TSA)

La DCFD debe notificar a la CA emisora o la TSA solicitante sobre la emisión del certificado, de acuerdo a los procedimientos definidos para tales efectos.

Certificados de firma digital y autenticación de persona física

En este caso, la entrega del certificado es presencial por lo tanto la notificación es inmediata.

Certificado de agente electrónico

Cuando las circunstancias lo permitan, la RA, o donde aplique la CA, entregará el certificado en forma presencial, en cuyo caso la notificación será inmediata.

En cualquier otro caso, la notificación se realizará de acuerdo a los procedimientos definidos para tales efectos.

4.4 Aceptación de certificado

4.4.1 Conducta constitutiva de aceptación de certificado

Certificados de CA emisora y certificados de autoridad de sellado de tiempo (TSA)

El proceso de descarga o instalación del certificado respectivo por parte de la CA emisora o TSA solicitante, constituirá la aceptación del certificado.

Certificados de firma digital y autenticación de persona física

El certificado se da por aceptado cuando la persona firma digitalmente un comprobante de aceptación del certificado entregado, esta es la primera vez que se usa y permite al suscriptor verificar que el certificado está funcionando correctamente.

Certificados de firma digital y autenticación de agente electrónico

El proceso de descarga o instalación del certificado respectivo por parte de la empresa o institución que utiliza el certificado de agente electrónico, constituirá la aceptación del certificado.

4.4.2 Publicación del certificado por la CA

La CA no debe publicar información de los certificados emitidos en los repositorios de acceso público.

4.4.3 Notificación de la emisión del certificado por la CA a otras entidades

No se definen entidades externas que necesiten o requieran ser notificadas acerca de los certificados emitidos por las CA.

4.5 Uso del par de llaves y del certificado

4.5.1 Uso de la llave privada y del certificado por el suscriptor

El uso de la llave privada correspondiente a la llave pública contenida en el certificado solamente debe ser permitido una vez que el suscriptor haya aceptado el certificado

emitido. Dicho uso debe realizarse en concordancia con la normativa aplicable, lo estipulado en este CP, y los contratos de suscriptor respectivos.

Los suscriptores deben proteger sus llaves privadas del uso no autorizado y deben descontinuar su uso después de la expiración o revocación del certificado.

Certificados de CA

1. CA raíz: la llave privada sólo puede ser utilizada para firmar certificados de CA de políticas.

2. CA políticas: Las CA de políticas son CA emisoras cuya llave privada únicamente puede ser utilizada para firmar certificados de CA emisoras subordinarios (SubCa) y autoridades certificadoras de sellado de tiempo.

3. CA emisora de persona física o agente electrónico: la llave privada solo debe ser utilizada para firmar certificados de autenticación y firma digital de personas físicas o de agente electrónico.

Certificados de firma digital y autenticación de persona física

El uso que se le dé a los certificados de persona física debe ser acorde con lo dispuesto en la sección 6.1.7.

Certificados de firma de digital y autenticación de agente electrónico

El uso que se le dé a los certificados de agente electrónico debe ser acorde con lo dispuesto la sección 6.1.7.

Certificados autoridad de sellado de tiempo (TSA)

La llave privada solo debe ser utilizada para prestar el servicio de sellado de tiempo.

4.5.2 Uso de la llave pública y del certificado por la parte que confía

Las partes que confían deben aceptar las estipulaciones establecidas en este CP, en lo que les resulte aplicable, como condición indispensable para confiar en el certificado.

La confianza en un certificado debe ser razonable, de acuerdo con las circunstancias. Si las circunstancias indican la necesidad de verificaciones adicionales, la parte que confía debe obtener tales verificaciones para que la confianza sea considerada razonable.

Antes de cualquier acto de confianza las partes que confían deben evaluar en forma independientemente:

- La pertinencia del uso del certificado para cualquier propósito dado y determinar que la voluntad del certificado, de hecho, sea utilizada para un propósito apropiado que no está prohibido o de otra forma restringido por

este CP. Las CA o RA no son responsables por la evaluación de la pertinencia en el uso de un certificado.

- Que el certificado sea utilizado de acuerdo con las disposiciones de esta CP (por ejemplo: Si en el certificado faltan los propósitos de firma y no repudio en el atributo de KeyUsage, entonces el certificado no puede ser confiable para validar la firma de un suscriptor).
- El estado del certificado y el estado de todos los certificados de las CA en la cadena que emitieron el certificado. Si cualquiera de los certificados en la cadena del certificado ha sido revocado, la parte que confía es la única responsable de investigar si la confianza en una firma digital efectuada por un suscriptor antes de la revocación de un certificado en la cadena es razonable. Cualquier confianza de este tipo es asumida únicamente bajo el riesgo de la parte que confía.

Si se determina que el uso del certificado es apropiado, las partes que confían deben utilizar el hardware y software necesario para ejecutar la verificación de la firma digital u otra operación criptográfica que ellos deseen efectuar, como una condición para confiar en los certificados relacionados con tales operaciones.

4.6 Renovación de certificado

La renovación del certificado no está permitida por esta CP, cuando un certificado requiera ser renovado debe solicitarse un nuevo certificado, de acuerdo con la sección 4.1 de este CP.

4.6.1 Circunstancias para renovación de certificado

No aplica.

4.6.2 Quién puede solicitar renovación

No aplica.

4.6.3 Procesamiento de solicitudes de renovación de certificado

No aplica.

4.6.4 Notificación al suscriptor sobre la emisión de un nuevo certificado

No aplica.

4.6.5 Conducta constitutiva de aceptación de un certificado renovado

No aplica.

4.6.6 Publicación por la CA del certificado renovado

No aplica.

4.6.7 Notificación por la CA de la emisión de un certificado a otras entidades

No aplica.

4.7 Re-emisión de llaves de certificado

La re-emisión del certificado no está permitida por esta CP, cuando un certificado requiera ser re-emitido debe solicitarse un nuevo certificado, de acuerdo con la sección 4.1 de este CP.

4.7.1 Circunstancia para re-emisión de llaves de certificado

No aplica.

4.7.2 Quién puede solicitar la certificación de una nueva llave pública

No aplica.

4.7.3 Procesamiento de solicitudes de re-emisión de llaves de certificado

No aplica.

4.7.4 Notificación al suscriptor sobre la reemisión de un nuevo certificado

No aplica.

4.7.5 Conducta constitutiva de aceptación de un certificado reemitido

No aplica.

4.7.6 Publicación por la CA de los certificados reemitidos

No aplica.

4.7.7 Notificación por la CA de la reemisión de un certificado a otras entidades

No aplica.

4.8 Modificación de certificados

4.8.1 Circunstancias para modificación del certificado

Cuando se requiera la modificación de la información contenida en un certificado debe revocarse y realizar una solicitud para un nuevo certificado, de acuerdo con la sección 4.1.

4.8.2 Quién puede solicitar modificación del certificado

No aplica.

4.8.3 Procesamiento de solicitudes de modificación del certificado

No aplica.

4.8.4 Notificación al suscriptor de la emisión de un nuevo certificado

No aplica.

4.8.5 Conducta constitutiva de aceptación del certificado modificado

No aplica.

4.8.6 Publicación por la CA de los certificados modificados

No aplica.

4.8.7 Notificación por la CA de emisión de certificado a otras entidades

No aplica.

4.9 Revocación y suspensión de certificado

4.9.1 Circunstancias para la revocación

Certificados de CA:

- A petición de la CA que considera o sospecha que su llave privada fue comprometida.
- Identificación o componentes de afiliación inválidos.
- Violación del acuerdo de suscriptor.
- Insolvencia, cese de actividades, quiebra o liquidación de la CA.
- Se comprueba la expedición de certificados falsos.
- Reincidencia en cualquiera de las infracciones que le hayan merecido una sanción de suspensión, dentro de los cinco años siguientes.
- Cuando se tienen razones para creer que el certificado no fue emitido de acuerdo a los lineamientos de la CP aplicable.
- Cuando se determina que los pre-requisitos para la emisión del certificado no fueron satisfechos.

Certificados de firma digital y autenticación de persona física, de agente electrónico y de sellado de tiempo:

- A petición del suscriptor, a favor de quién se expidió, quién tiene razones o sospechas para creer que su llave privada ha sido comprometida.
- Cuando se confirme que el suscriptor ha comprometido su confiabilidad, desatendiendo los lineamientos de seguridad establecidos, suplido información falsa al certificador u omitido otra información relevante, con el propósito de obtener o re-emitir el certificado.
- Por fallecimiento (en el caso de persona física), ausencia legalmente declarada, interdicción o insolvencia.
- Cuando el suscriptor finaliza el contrato por voluntad propia.
- Por errores de información del certificado, por ejemplo el nombre del suscriptor o alguno de los atributos.
- El acuerdo entre el suscriptor y la CA emisora se ha terminado.
- Cuando se tienen razones para creer que el certificado no fue emitido de acuerdo a los lineamientos de la CP aplicable.
- Cuando se determina que los pre-requisitos para la emisión del certificado no fueron satisfechos.
- Cuando la información incluida dentro del certificado es incorrecta o ha cambiado.

Adicionalmente, cuando se determine que el uso del certificado atenta contra la seguridad del Sistema Nacional de Certificación Digital. Esto se determinará con base en la legislación aplicable, la naturaleza y el número de denuncias recibidas, la identidad del denunciante, y cualquier otra que la DCFD determine.

4.9.2 Quién puede solicitar revocación

De pleno derecho el suscriptor del certificado puede solicitar la revocación de su certificado, ya sea por voluntad propia o por compromiso de su llave privada. En caso de sospecha o compromiso de su llave privada, la notificación debe realizarla en forma inmediata a la CA correspondiente.

Para todos los casos, la CA emisora del certificado y la autoridad judicial competente pueden solicitar la revocación del certificado.

Asimismo, pueden solicitar la revocación los siguientes participantes según el tipo de certificado:

Para certificados de CA emisora o TSA

- El representante legal o apoderado con poderes suficientes de la CA emisora o TSA.
- La DCFD.

Para certificados de firma digital y autenticación de persona física

- El Tribunal Supremo de Elecciones, en caso de fallecimiento.

Para certificados de firma digital y autenticación de agente electrónico

- El representante legal o apoderado con poderes suficientes de la empresa o institución suscriptora del certificado.
- El Registro Nacional, por medio de su registro de personas jurídicas.

Además, cualquier persona puede solicitar la revocación de un certificado ante la CA correspondiente presentando evidencia contundente que revele el compromiso de la llave privada del suscriptor.

4.9.3 Procedimiento para la solicitud de revocación

Verificar que la solicitud de revocación ha sido presentada por el suscriptor del certificado o por una autoridad competente, de acuerdo con la sección 3.4.

Las solicitudes para la revocación de certificados de CA emisoras deben ser autenticadas por sus entidades superiores dentro de la jerarquía nacional de certificadores registrados, para asegurar que la revocación de una CA emisora ha sido solicitada por una entidad autorizada para tales efectos.

4.9.4 Periodo de gracia para solicitud de revocación

No se estipulan periodos de gracia para revocación de certificados, salvo los impuestos por la ley para realizar apelaciones.

4.9.5 Tiempo dentro del cual la CA debe procesar la solicitud de revocación

Las solicitudes de revocación deben ser procesadas en un rango de tiempo razonable, de acuerdo con el procedimiento para la solicitud de revocación (ver sección 4.9.3). Cuando la solicitud provenga del suscriptor y se utilicen mecanismos electrónicos automatizados, la revocación debe realizarse en forma inmediata.

4.9.6 Requerimientos de verificación de revocación para las partes que confían

Las partes que confían deben evaluar el estado del certificado y el estado de todos los certificados de las CA en la cadena a la que pertenece el certificado, antes de confiar en él.

En caso de que cualquiera de los certificados en la cadena del certificado haya sido revocado, la parte que confía es la única responsable de investigar si la confianza en una firma digital efectuada por un suscriptor antes de la revocación de un certificado en la cadena es razonable. Cualquier confianza de este tipo es asumida únicamente bajo el riesgo de la parte que confía. Para estos propósitos las partes que confían pueden verificar el estado del certificado mediante el servicio de OCSP o la lista de revocación más reciente, de acuerdo el riesgo.

4.9.7 Frecuencia de emisión de CRL

CA Raíz

La CA Raíz debe actualizar su lista de revocación cada cuatro meses y cada vez que se presente una revocación del certificado de una CA de Políticas, en cuyo caso se debe notificar a las CA subsecuentes.

CA de Políticas

La CA de Políticas debe actualizar su lista de revocación cada dos meses y cada vez que se presente una revocación del certificado de una CA emisora, en cuyo caso se debe notificar a todas las CA emisoras.

CA emisora

La CA emisora debe actualizar y publicar las listas de revocación al menos una vez a la semana. Además deberá publicar los Delta CRL una vez al día.

4.9.8 Latencia máxima para CRLs

La CA o TSA debe publicar la CRL en el repositorio en un plazo no mayor a dos horas posterior a su generación.

4.9.9 Disponibilidad de verificación de revocación/estado en línea

Todas las CA o TSA deben mantener disponible un repositorio con información del estado de los certificados emitidos por ésta, el cual puede ser accedido vía Web. Adicionalmente, para la CA emisora registrada es obligatorio implementar el servicio de validación en línea OCSP.

4.9.10 Requerimientos para verificar la revocación en línea

La parte que confía debe verificar el estado de un certificado en el cual desea confiar, utilizando los mecanismos de verificación del estado de certificados establecidos en la sección anterior.

4.9.11 Otras formas de advertencias de revocación disponibles

No se estipulan.

4.9.12 Requerimientos especiales por compromiso de llaves reemitidas

La DCFD debe notificar en el menor tiempo posible a todos los participantes de la jerarquía nacional de certificadores registrados acerca del compromiso de la llave privada de alguna de las CA.

4.9.13 Circunstancias para suspensión

4.9.13.1 Suspensión de certificados de firma digital para personas físicas o agente electrónico

De conformidad con el artículo 14 de la ley 8454 de certificados digitales, las circunstancias de suspensión son:

a. Por petición del propio usuario a favor de quién se expidió el certificado.

b. Como medida cautelar, cuando el certificador que lo emitió tenga sospechas fundadas de que el propio usuario haya comprometido su confiabilidad, para obtener el certificado.

c. Si contra el usuario se ha dictado auto de apertura a juicio, por delitos en cuya comisión se haya utilizado la firma digital.

d. Por no cancelar oportunamente el costo del servicio.

Para los efectos prácticos se puede implementar la suspensión de certificados de personas físicas o de agentes electrónicos, como la anulación técnica del certificado, que evite que pueda seguir siendo utilizado para el propósito de firma por parte del suscriptor. Además, ninguna CA emisora podrá expedirle un certificado de firma mientras el estado de suspensión se encuentre vigente. Aspecto que será determinado por las declaración de prácticas de certificación o el acuerdo de suscriptor definido por la CA que emita los certificados.

4.9.13.2 Suspensión de una CA

Se puede suspender una CA emisora, si existe una orden judicial o por decisión de la DCFD, o cuando el ECA acredite que la CA emisora incumple las obligaciones que le impone la ley 8454 y su reglamento. Para este caso en particular el reglamento define la suspensión de la CA emisora en el artículo 32, como la imposibilidad para el certificador sancionado de expedir nuevos certificados digitales o de renovar los que expiren durante el plazo de suspensión. Esta suspensión no afectará a los certificados emitidos previamente.

4.9.14 Quién puede solicitar la suspensión

De pleno derecho, el suscriptor del certificado puede solicitar la suspensión de su propio certificado.

Asimismo, pueden solicitar la suspensión otros participantes según el tipo de certificado:

Certificados de CA y certificados de autoridad de sellado de tiempo (TSA)

- El representante legal o apoderado con poderes suficientes de la CA emisora o TSA.
- El Ente Costarricense de Acreditación.
- La autoridad judicial competente.
- La DCFD.

Certificados de firma digital y autenticación de persona física

- La autoridad judicial competente.
- La CA emisora.

Certificados de firma de digital y autenticación de agente electrónico

- El representante legal o apoderado con poderes suficientes de la empresa. o institución suscriptora del certificado.
- La autoridad judicial competente.
- La CA emisora.

4.9.15 Procedimiento para la solicitud suspensión

El procedimiento de suspensión depende del tipo de certificado y del solicitante de la suspensión, de acuerdo con:

Certificados de CA emisora

- El representante legal o apoderado con poderes suficientes de la CA emisora debe:
    - Presentar un documento de identificación legalmente aceptado y vigente, así como la personería jurídica vigente (con menos de un mes de emitida) donde se establezca su relación como representante legal o apoderado con poderes suficientes de la empresa o institución suscriptora del certificado.
    - Implementar los controles y procedimientos para no expedir nuevos certificados digitales o de renovar los que expiren durante el plazo de suspensión.
- Ente Costarricense de Acreditación (ECA)
    - Comunicar a la DCFD el incumplimiento de la acreditación o de las obligaciones que imponen la ley 8454, Ley de certificados, firmas digitales y documentos electrónicos y su reglamento.
- La autoridad judicial competente

- Remitir a la DCFD la resolución en la que se ordena la suspensión, los alcances y los plazos de la misma.

- La DCFD
  - Notificar a la CA correspondiente las razones por las cuales se le va a suspender.
  - Recibir las pruebas de descargo correspondientes, en caso de que las hubieran.
  - Comunicar a las CA emisoras la resolución correspondiente.

Certificados de firma digital y autenticación de persona física

- Suscriptor del certificado
  - Puede presentarse ante una RA de la CA que emitió el certificado y solicitar la suspensión.
  - Puede solicitar la suspensión vía web, proporcionando la respuesta a la "frase desafío" (challenge phrase) que suministró durante el proceso de aplicación del certificado.
  - Puede solicitar la suspensión a través del centro de atención al cliente de la CA que emitió el certificado.
  - Por cualquier otro medio autorizado por la DCFD y que cumpla con un mecanismo de autenticación robusto.
- La autoridad judicial competente
  - Remitir a la DCFD la resolución en la que se ordena la suspensión, los alcances y los plazos de la misma.
  - La DCFD comunica a la CA emisora respectiva, la resolución judicial para suspender el certificado de firma digital emitido para el suscriptor en cuestión.
- La CA emisora
  - Contar con las justificaciones para emitir la suspensión.
  - Si la suspensión es recurrida ante la Dirección de Certificadores de Firma Digital, la CA emisora debe esperar la resolución de la DCFD para suspender el certificado.
  - Si fuera el caso, se procede con la suspensión (o revocación) del certificado.

Certificados de firma digital y autenticación de agente electrónico o TSA

- El representante legal o apoderado con poderes suficientes de la empresa o institución suscriptora del certificado debe:

- Presentar ante la autoridad de registro correspondiente, la documentación que lo acredita como representante legal.
- Solicitar la suspensión del certificado.

- La autoridad judicial competente:
  - Remitir a la DCFD la resolución en la que se ordena la suspensión, los alcances y los plazos de la misma.
- La CA emisora:
  - Contar con las justificaciones para emitir la suspensión.
  - Si la suspensión es recurrida ante la Dirección de Certificadores de Firma Digital, la CA emisora debe esperar la resolución de la DCFD para suspender el certificado.
  - Si fuera el caso, se procede con la suspensión (o revocación) del certificado.

4.9.16 Límites del periodo de suspensión

De acuerdo con el artículo 8 del reglamento de la Ley 8454 de certificados, firmas digitales y documentos electrónicos, la suspensión (o revocación) se mantendrá por todo el plazo en que subsista la causal que le dio origen.

4.10 Servicios de estado de certificado

4.10.1 Características operacionales

El estado de los certificados debe estar disponible a través de los CRL publicados en un sitio Web (en el URL especificado en el CP) y para las CA emisoras de certificados de firma digital de personas físicas, es obligatorio implementar un servicio OCSP.

4.10.2 Disponibilidad del servicio

La CA debe mantener los servicios de verificación del estado de los certificados disponibles 24 x 7 x 365.

4.10.3 Características opcionales

El servicio OCSP, que permite consultar el estado de certificados es una característica opcional para la CA de la Raíz y las CAs de políticas. Sin embargo, para las CA emisoras constituye una característica obligatoria.

4.11 Finalización de la suscripción

Un suscriptor puede finalizar su suscripción de las siguientes formas:

- Revocando su certificado antes del vencimiento (fecha de expiración).
- Cuando expira el certificado.

4.12 Custodia y recuperación de llave

4.12.1 Política y prácticas de custodia y recuperación de llave

La CA no debe custodiar llaves de suscriptores para ningún certificado cuyo propósito sea de firma digital, únicamente se mantienen respaldos de sus propias llaves privadas de acuerdo con el Plan de Continuidad de Negocio.

Para los efectos de Plan de Continuidad de Negocio, las llaves privadas de las CA deben estar en custodia y respaldadas bajo estrictas normas de seguridad, y almacenadas en dispositivos criptográficos FIPS 140-2 nivel 3, que garantizan la no divulgación de las llaves.

4.12.2 Políticas y prácticas de recuperación y encapsulación de llave de sesión

Sin estipulaciones para esta sección.

5. Controles operacionales, de gestión y de instalaciones

La Autoridad Certificadora Raíz mantiene controles de seguridad no-técnicos (esto es, controles físicos, procedimientos y de personal) para asegurar la ejecución de las funciones de generación de llave, autenticación de los sujetos, emisión del certificado, revocación del certificado, auditoría y almacenamiento.

5.1 Controles físicos

5.1.1 Localización y construcción del sitio

Las operaciones de la CA deben estar dentro de un ambiente de protección física que impida y prevenga usos o accesos no autorizados o divulgación de información sensible.

Las instalaciones de la CA deben contar con al menos cuatro perímetros de seguridad física (área de recepción, área de servicios de soporte - climatización, energía, comunicaciones, etc.-, área de operación de la CA, área de custodia de material criptográfico). Un perímetro es una barrera o entrada que provee un control de acceso para individuos y requiere una respuesta positiva para proceder a ingresar a la siguiente área. Cada perímetro sucesivo se encuentra más restringido, con controles de acceso más estrictos.

Las instalaciones donde se crean los certificados de la CA se deben proteger con su propio y único perímetro físico, y las barreras físicas (paredes, barrotes) deben ser sólidas, extendiéndose desde el piso real al cielo raso real. Asimismo, estas barreras deben prevenir las emisiones de radiación electromagnética.

5.1.2 Acceso físico

Los controles de acceso físico deben evitar el acceso no autorizado a las instalaciones de la CA. Adicionalmente, el acceso al recinto donde se encuentran las operaciones de la autoridad certificadora debe utilizar controles con 2 factores de autenticación como mínimo (al menos uno de ellos debe ser biométrico).

Cuando las instalaciones operacionales de la CA estén desocupadas, deben estar cerradas con llave y con las alarmas debidamente activadas.

Los perímetros deben ser auditados y controlados para verificar que solo puede tener acceso el personal autorizado debidamente identificado.

Los derechos de acceso a las instalaciones de la CA deben revisarse y actualizarse regularmente, al menos cada seis meses o cuando se presente movimiento en el personal relacionado con labores de operación de la CA.

Los visitantes o personal de servicio de soporte tercerizado que requiera acceso a las instalaciones operacionales de la CA, deben ser escoltados y registrarse el responsable de autorizar el acceso, la fecha y hora de entrada y salida.

5.1.3 Energía y aire acondicionado

El equipo de la autoridad certificadora debe protegerse contra fallas en el fluido eléctrico corriente y otras anomalías en la energía.

Las instalaciones de la CA deben estar equipadas con sistemas de energía primario y de respaldo para asegurar continuidad del fluido eléctrico.

Las instalaciones deben contar con sistemas de aire acondicionado redundantes. El equipo instalado para climatizar el recinto, debe ser capaz de controlar la humedad relativa del mismo.

5.1.4 Exposiciones al agua

Las instalaciones de la CA deben ser construidas y equipadas, y contar con procedimientos implementados para prevenir inundaciones y otros daños por exposición al agua.

5.1.5 Prevención y protección contra fuego

Las instalaciones de la CA deberán contar con procedimientos implementados para la prevención y protección al fuego. Además de ser construidas y equipadas para prevenir, detectar y suprimir incendios o daños producidos por la exposición a llamas o humo.

5.1.6 Almacenamiento de medios

La CA debe asegurar el adecuado manejo y protección de los medios de almacenamiento de información, que contengan datos críticos o sensitivos del sistema, contra daños accidentales (agua, fuego, electromagnetismo) y debe impedir, detectar y prevenir su uso no autorizado, acceso o su divulgación.

5.1.7 Eliminación de residuos

La CA debe implementar controles para la eliminación de residuos (papel, medios, equipos y cualquier otro desecho) con el fin de prevenir el uso no autorizado, el acceso o divulgación de información privada y confidencial contenida en los desechos.

5.1.8 Respaldo fuera de sitio

La CA debe mantener respaldos de los datos críticos del sistema y de cualquier otra información sensitiva, incluyendo los datos de auditoría, en una instalación segura fuera del sitio principal.

5.2 Controles procedimentales

5.2.1 Roles de confianza

Los empleados, contratistas y consultores designados para gestionar la infraestructura de confianza deben ser considerados “personas de confianza” sirviendo en “roles de confianza”.

Los roles de confianza deben incluir, al menos, roles que contemplen las siguientes responsabilidades:

a. responsabilidad general de administrar la implementación de las prácticas de seguridad de la CA;

b. aprobación de la generación, revocación y suspensión de los certificados;

c. instalación, configuración y mantenimiento de los sistemas de la CA;

d. operación diaria de los sistemas de la CA, respaldo y recuperación de sistemas;

e. funciones de auditoria interna para ejecutar la inspección y mantenimiento de las bitácoras del sistema de la CA y de los registros de auditoría;

f. funciones de gestión del ciclo de vida de llaves criptográficas (ejemplo, custodios de componentes de llaves);

g. desarrollo de sistemas de la CA.

5.2.2 Número de personas requeridas por tarea

La CA debe establecer, mantener y ejecutar procedimientos de control rigurosos para asegurar la segregación de funciones, basados en las responsabilidades del trabajo y la cantidad de personas de confianza que ejecutan las tareas sensitivas.

5.2.3 Identificación y autenticación para cada rol

La CA debe confirmar la identidad y autorización de todo el personal que intente iniciar labores de confianza. La autenticación de la identidad debe incluir la presencia física de la persona y una verificación por medio de documentos vigentes de identificación legalmente reconocidos, tales como la cédula de identidad para los ciudadanos costarricenses, o el documento único de permanencia, en caso de extranjeros.

5.2.4 Roles que requieren separación de funciones

Los roles que requieren separación de los deberes incluyen (pero no está limitado) a los encargados de ejecutar las siguientes responsabilidades:

- La validación de información en aplicaciones de certificado y de solicitudes o información del suscriptor.

- La aceptación, rechazo, otros procesamientos de la aplicación de certificado, solicitud de revocación, información de afiliación.
- La emisión, o revocación de los certificados, incluyendo personal con acceso a porciones restringidas del repositorio.
- La generación, emisión o destrucción de los certificados de la CA.
- La puesta en operación de la CA en producción.
- La auditoría interna de la operación de la CA y RA debe ser ejecutada por un rol particular.

5.3 Controles de personal

5.3.1 Requerimientos de experiencia, capacidades y autorización

Las personas seleccionadas para laborar en roles de confianza deben contar con un contrato y deben:

- Haber aprobado exitosamente el programa de entrenamiento apropiado.
- Haber demostrado capacidad para ejecutar sus deberes.
- Haber aceptado las cláusulas de confidencialidad.
- No poseer otros deberes que puedan interferir o causar conflicto con los de la CA.
- No tener antecedentes de negligencia o incumplimiento de labores.
- No tener antecedentes penales.

5.3.2 Procedimientos de verificación de antecedentes

La CA debe contar con procedimientos para verificar la experiencia y los antecedentes del personal que intenta obtener un rol de confianza. Algunos aspectos de la investigación de antecedentes incluyen:

- Confirmación de empleos anteriores.
- Verificación de referencias profesionales.
- Título académico obtenido.
- Búsqueda de antecedentes criminales.
- Verificación de registros financieros y crediticios.

La verificación de registros financieros y crediticios debe ser repetida para el personal de confianza al menos una vez cada tres años.

Los antecedentes deben ser evaluados por la CA para tomar las acciones que sean razonables, de acuerdo al tipo, magnitud y frecuencia del comportamiento descubierto por la investigación respectiva. Los factores revelados en el proceso de verificación

pueden ser considerados como motivos para retirar al funcionario del puesto de confianza.

5.3.3 Requerimientos de capacitación

Todo el personal involucrado en las operaciones de la CA debe estar capacitado apropiadamente, en aspectos tales como: operación del software y hardware, políticas y procedimientos organizacionales, procedimientos de seguridad y operacionales, y las estipulaciones legales.

5.3.4 Requerimientos y frecuencia de re-capacitación

La CA debe capacitar al personal cuando se presenten cambios significativos en las operaciones de la CA, por ejemplo cuando se producen actualizaciones de hardware o software, cambios en los sistemas de seguridad, etc.

La CA debe proveer los programas de entrenamiento y actualización a su personal para asegurar que el personal mantiene el nivel requerido de eficiencia para ejecutar sus labores satisfactoriamente.

5.3.5 Frecuencia y secuencia en la rotación de las funciones

La CA debe efectuar una rotación de sus roles de trabajo. La frecuencia de la rotación del personal debe ser al menos:

- una vez cada tres años, para la CA emisora.
- una vez cada cinco años, para la CA Raíz.

Antes de asumir las nuevas labores, el personal debe recibir a una actualización de la capacitación que le permita asumir las tareas satisfactoriamente.

5.3.6 Sanciones para acciones no autorizadas

La CA debe ejecutar las acciones administrativas y disciplinarias apropiadas contra el personal que violente las normas de seguridad establecidas en esta política o su CPS, de acuerdo a lo estipulado en el contrato de trabajo definido para los roles de confianza. Además debe llevar un registro de la frecuencia y severidad de las acciones, con el fin de determinar la sanción que debe ser aplicada.

5.3.7 Requerimientos para contratistas independientes

La CA puede contratar personal externo o consultores solamente si existe una relación claramente definida con el contratista y bajo las siguientes condiciones:

- existe un contrato con cláusulas propias de los roles de confianza y estipula sanciones para las acciones no autorizadas.
- no se posee personal disponible para llenar los roles de confianza contratados.

- los contratistas o consultores cumplen con los mismos requisitos del punto 5.3.1.
- una vez finalizado el servicio contratado se revocan los derechos de acceso.

5.3.8 Documentación suministrada al personal

La CA debe suministrar suficiente documentación al personal para que ejecute un rol, donde se definen los deberes y procedimientos para el correcto desempeño de su función.

5.4 Procedimientos de bitácora de auditoría

La CA debe mantener controles para proveer una seguridad razonable de que:

- los eventos relacionados con el ambiente de operación de la CA, la gestión de las llaves y los certificados, son registrados exacta y apropiadamente;
- se mantiene la confidencialidad y la integridad de los registros de auditoría vigentes y archivados;
- los registros de auditoría son archivados completa y confidencialmente;
- los registros de auditoría son revisados periódicamente por personal autorizado.

5.4.1 Tipos de eventos registrados

La CA debe registrar los tipos de eventos que se presentan en sus operaciones. La CA debe mantener las bitácoras manuales o automáticas, indicando para cada evento la entidad que lo causa, la fecha y hora del mismo. La CA debe registrar los eventos relacionados con:

- la gestión del ciclo de vida de las llaves de la CA;
- la gestión del ciclo de vida del dispositivo criptográfico;
- la gestión del ciclo de vida del sujeto de certificado;
- la información de solicitud de certificados;
- la gestión del ciclo de vida del certificado;
- los eventos sensibles de seguridad;

Las bitácoras de auditoría no deben registrar las llaves privadas de ninguna forma y los relojes del sistema de cómputo de la CA deben estar sincronizados con el servicio de tiempo UTC-6 para un registro exacto de los eventos.

5.4.2 Frecuencia de procesamiento de la bitácora

El personal de la CA emisora con el rol de auditor debe realizar al menos tres revisiones por año de las bitácoras de auditoría, sin necesidad de ser avisadas; mientras que la CA de la Raíz debe realizar al menos una revisión anual de las bitácoras.

Además de las revisiones oficiales, las bitácoras de auditoría deben ser revisadas en respuesta a una alerta, por irregularidades o incidentes dentro de los sistemas de la CA.

El procesamiento de la bitácora de auditoría consiste en una revisión de las bitácoras y la documentación de los motivos para los eventos significativos, y todas las acciones deben ser documentadas.

Las bitácoras de auditorías actuales y archivadas deben ser recuperadas solamente por personal autorizado, ya sea por razones válidas del negocio o por seguridad.

5.4.3 Periodo de retención para la bitácora de auditoría

Las bitácoras de auditoría deben ser mantenidas en el sistema por al menos dos meses posterior a su procesamiento y deber ser archivadas de acuerdo a la sección 5.5.2.

5.4.4 Protección de bitácora de auditoría

Las bitácoras de auditorías actuales o archivadas deben mantenerse de forma que se prevenga su revelación, modificación, destrucción no autorizada o cualquier otra intromisión.

5.4.5 Procedimientos de respaldo de bitácora de auditoría

La CA debe mantener copias de respaldo de todos los registros auditados.

5.4.6 Sistema de recolección de auditoría (interno vs. Externo)

Los procesos de auditoría de seguridad deben ejecutarse independientemente y no deben, de ninguna forma, estar bajo el control de la CA, los procesos de auditoría deben ser invocados al iniciar el equipo y terminarlos solo cuando el sistema es apagado.

En caso de que el sistema automatizado de auditoría falle, la operación de la CA debe cesar hasta que las capacidades de auditoría puedan ser reestablecidas.

5.4.7 Notificación al sujeto que causa el evento

Cuando un evento es almacenado por la bitácora, no se requiere notificar al causante de dicho evento.

5.4.8 Evaluación de Vulnerabilidades

La CA y el personal operativo deben estar vigilantes de intentos para violar la integridad del sistema de generación de certificados, incluyendo equipo, localización física y personal. Las bitácoras deben ser revisadas por un auditor de seguridad para los eventos que poseen acciones repetitivas, solicitudes para información privilegiada, intentos de acceso al sistema de archivos y respuestas no autenticadas.

Los equipos donde se ejecutan las operaciones de la CA emisora deben someterse a análisis semestrales de vulnerabilidades.

5.5 Archivado de registros

5.5.1 Tipos de registros archivados

La CA debe almacenar los registros para establecer la validez de una firma y de la operación propia de la infraestructura PKI. Se deben archivar los siguientes datos:

Durante la inicialización del sistema de la CA:

- la acreditación de la CA (si es necesaria);
- el CP y el CPS;
- cualquier acuerdo contractual para establecer los límites de la CA;
- la configuración del sistema.

Durante la operación de la CA:

- modificaciones o actualizaciones de cualquiera de los ítems anteriores;
- solicitudes de certificados o de revocación;
- documentación para autenticar la identidad del suscriptor;
- documentación de recepción y aceptación del certificado;
- documentación de recepción de dispositivos de almacenamiento de llaves;
- todos los certificados y CRLs (información de revocación) tanto emitidos o publicados;
- bitácoras de auditoría;
- otros datos o aplicaciones para verificar el contenido de los archivos;
- todos los trabajos comunicados o relacionados a políticas, otras CA y cumplimiento de auditoría.

5.5.2 Periodos de retención para archivo

Todos los archivos deben mantenerse por un periodo de al menos diez años. Además de mantener los controles para que los archivos puedan ser leídos durante el periodo de retención definido.

5.5.3 Protección de archivo

Los archivos no deben modificarse o eliminarse por alguna operación no autorizada del equipo de la CA. La CA debe mantener la lista de personas autorizadas a mover los registros a otros medios.

Los medios de almacenamientos deben estar guardados en instalaciones seguras, los registros deben ser etiquetados con un nombre distintivo, la fecha y hora de almacenamiento y la clasificación del tipo de información.

5.5.4 Procedimientos de respaldo de archivo

La CA debe mantener procedimientos adecuados de respaldo de archivos (físicos y electrónicos), tanto en el sitio principal como en el alterno, que aseguren la disponibilidad de los mismos, de acuerdo a un análisis de riesgos determinado por los factores de operación de la CA.

5.5.5 Requerimientos para sellado de tiempo de registros

Los certificados, las listas de revocación (CRL) y otras entradas en la bases de datos de revocación debe contener información de fecha y hora. Esta información de fecha y hora no necesita tener una base criptográfica, pero si debe estar sincronizada con el servicio de tiempo de la UTC-6.

5.5.6 Sistema de recolección de archivo (interno o externo)

Los sistemas de archivos de la CA son internos al ámbito de sus operaciones y deben conservar las pistas de auditoría.

5.5.7 Procedimientos para obtener y verificar la información archivada

Solamente el personal de confianza autorizado está habilitado para obtener acceso al archivo. La CA debe realizar pruebas de restauración de la información archivada al menos una vez al año. La integridad de la información debe ser verificada cuando es restaurada.

5.6 Cambio de llave

La CA debe cambiar periódicamente sus llaves de firma, de acuerdo con los años de validez de sus certificados en la jerarquía nacional de certificadores registrados (tiempo de uso) y considerando que el último certificado otorgado debe poder ser verificado durante su vigencia (tiempo operacional). Tal como se muestra en el siguiente cuadro:

Nivel de jerarquía	Tiempo de uso en años	Tiempo operacional en años	Descripción
Certificado de suscriptores	**2**	**2**	**El certificado emitido al usuario es otorgado por dos años, al finalizar ese periodo pierde su validez.**

Nivel de jerarquía	Tiempo de uso en años	Tiempo operacional en años	Descripción
CA emisoras	**5**	**7**	**La CA emisora se le otorga un certificado con una validez de 5 años, durante ese periodo puede emitir certificados a los usuarios o suscriptores. Sin embargo el último certificado emitido antes de vencer su validez, debe tener la misma efectividad, es decir, dos años para el usuario o suscriptor. Entonces su tiempo de uso es 5 años (con capacidad para emitir certificados de suscriptor), pero dura dos años más en operación para validar las listas de revocación, de ahí que el tiempo operacional es por 7 años.**
CA Políticas	**10**	**17**	**La CA de políticas tiene una validez de 10 años, y el último certificado otorgado a una CA emisora debe garantizar la operación por siete años más. Por estos motivos el periodo operacional de la CA de Políticas debe ser de al menos 17 años.**
CA Raíz	**20**	**37**	**Siguiendo el mismo criterio la validez de la CA Raíz es 20 años, más 17 años que pueda operar la CA de Política, da como resultado los 37 años de tiempo operacional para el certificado de la CA Raíz.**

Del cuadro anterior, se deduce que en determinado momento puede haber dos certificados activos, uno que finalizó el periodo de uso y que por lo tanto no puede seguir firmando certificados, pero que posee certificados que están vigentes en uno de los sub niveles de la jerarquía nacional de certificadores registrados. En estos casos, la última llave (vigente) es usada para propósitos de firma de certificados. La llave anterior todavía estará disponible para verificar las firmas y para firmar CRLs. El tiempo de traslape de las llaves es al menos el tiempo operacional del certificado de un suscriptor.

5.7 Recuperación de desastre y compromiso

5.7.1 Procedimientos para el manejo de incidente y compromiso

La CA debe contar con políticas y procedimientos formales para el reporte y atención de incidentes.

La funcionarios ejecutando roles de confianza deben velar por la seguridad de las instalaciones y la CA debe mantener procedimientos para que estos funcionarios reporten los incidentes.

La CA debe mantener un plan de recuperación de desastres, si el equipo de la CA es dañado entonces las operaciones de la CA deben reestablecerse lo más pronto posible, dando prioridad a la capacidad de revocar certificados de suscriptor.

Si la CA no puede ser reestablecida dentro de una semana, entonces su llave se reporta como comprometida y todos sus certificados son revocados. En casos excepcionales, la DCFD puede otorgar extensiones para la CA.

5.7.2 Corrupción de datos, software y/o recursos computacionales

Posterior a una corrupción de recursos computacionales, software o datos, la CA afectada debe realizar, en forma oportuna, un reporte del incidente y una respuesta al evento.

5.7.3 Procedimientos de compromiso de llave privada de la entidad

La CA debe mantener controles para brindar una seguridad razonable de que la continuidad de las operaciones se mantenga en caso de compromiso de las llaves privadas de la CA.

Los planes de continuidad del negocio de la CA deben referirse al compromiso o sospecha de compromiso de las llaves privadas de la CA como un desastre.

En caso de que la llave de la CA se haya comprometido, el superior de la CA deberá revocar el certificado de CA, y la información de la revocación debe publicarse inmediatamente.

5.7.4 Capacidad de continuidad del negocio después de un desastre

La CA debe contar con un proceso administrativo para desarrollar, probar, implementar y mantener sus planes de continuidad del negocio.

La CA debe desarrollar, probar, mantener e implementar un plan de recuperación de desastres destinado a mitigar los efectos de cualquier desastre natural o producido por el hombre. Los planes de recuperación de desastres se enfocan en la restauración de los servicios de sistemas de información y de las funciones esenciales del negocio.

El sitio alterno debe contar con protecciones de seguridad física equivalentes al sitio principal.

El sitio alterno, deben tener la capacidad de restaurar o recobrar operaciones esenciales dentro de las veinticuatro horas siguientes al desastre, con al menos soporte para las siguientes funciones: revocación de certificados y publicación de información de revocación.

5.8 Terminación de una CA o RA

En caso de que la terminación de la CA se de por conveniencia, reorganización, o por otras razones que no estén relacionadas con la seguridad, entonces se deben tomar las previsiones antes de terminar la CA para evitar el compromiso de toda la infraestructura. En este caso, puede ser que ningún certificado firmado por la CA deba ser revocado.

En caso de que la terminación de la CA esté relacionada con eventos de seguridad, entonces la CA debe considerarse como una CA comprometida.

Antes de la terminación de la CA, toda la información relacionada con la operación de la CA deben ser enviados a la DCFD para su custodia.

Cuando se presenta la terminación de una RA, todos los archivos de datos deben ser enviados a la CA respectiva para su custodia.

Si se presenta un compromiso de la llave de la CA o un desastre donde las instalaciones de la CA están físicamente dañadas y todas las copias de las llaves de firma de la CA están destruidos, entonces la CA debe solicitar que se revoque su certificado.

Cada CA o RA debe desarrollar un plan de terminación que minimice el impacto y la interrupción del servicio provisto a los clientes, suscriptores y partes que confían. Dicho plan debe darle tratamiento al menos a los siguientes puntos:

- Notificación a las partes afectadas asumiendo el costo de la misma.
- Procedimiento de revocación del certificados (de la CA, CA subordinadas, los utilizados en RA para sus operaciones, suscriptores, etc. según sea el caso).
- La preservación de toda la información en concordancia con este CP y la normativa aplicable.
- La continuación de los servicios de validación de los certificados y de soporte a los suscriptores.
- Procedimientos para la eliminación de las llaves privadas y del hardware que las contiene.
- Disposiciones para la transición de los servicios a una CA sucesora.

6. Controles técnicos de seguridad

En esta sección se definen las medidas de seguridad tomadas por la CA para proteger sus llaves criptográficas y los datos de activación. La gestión de las llaves es un factor crítico que permite asegurar que todas las llaves privadas están protegidas y solamente pueden ser activadas por personal autorizado.

6.1 Generación e instalación del par de llaves

La CA mantendrá controles para brindar seguridad razonable de que los pares de llaves de la CA, se generan e instalan de acuerdo con el protocolo definido para la generación de llaves.

6.1.1 Generación del par de llaves

El proceso de generación de llaves ejecutado por la CA previene la pérdida, divulgación, modificación o acceso no autorizado a las llaves privadas que son generadas. Este requerimiento aplica para toda la jerarquía nacional de certificadores registrados hasta llegar a los suscriptores.

Certificados de CA emisora

La CA debe generar las llaves mediante un proceso seguro por medio del módulo criptográfico de hardware, que cumple como mínimo el estándar Fips 140-2 nivel 3 y a un procedimiento acorde con la "ceremonia de generación de llaves" definida en el anexo D de la norma INTE/ISO 21188 "Infraestructura de llave pública para servicios financieros — Estructura de prácticas y políticas.". La CA garantiza que la llave privada de firma nunca permanecerá fuera del módulo donde fue generada, a menos que se almacene en un mecanismo de recuperación de llaves.

El proceso de generación de llaves de CA debe producir llaves que:

a. sean apropiadas para la aplicación o propósito destinado y que sean proporcionales a los riesgos identificados;

b. usen un algoritmo aprobado en este CP, de acuerdo a la sección 7.1.3;

c. tengan una longitud de llave que sea apropiada para el algoritmo y para el período de validez del certificado de la CA, de acuerdo con la sección 6.1.5 de tamaños de llave;

d. tomen en cuenta los requisitos del tamaño de llave de la CA padre (la CA que le emitió el certificado) y subordinada (la CA que recibe el certificado);

Certificados de firma digital y autenticación de persona física

La generación de las llaves de los suscriptores requiere que los módulos de criptografía cumplan al menos con el estándar Fips 140-2 nivel 2.

Certificados de firma digital y autenticación de agente electrónico

La generación de las llaves de agentes electrónicos cumple al menos con módulos de criptografía Fips 140-2 nivel 3.

Certificados de autoridad de sellado de tiempo (TSA)

La TSA debe generar las llaves mediante un proceso seguro, con un módulo criptográfico de hardware, que cumpla al menos con el estándar Fips 140-2 nivel 3.

6.1.2 Entrega de la llave privada al suscriptor

Se debe generar y mantener la llave privada dentro de los límites del módulo criptográfico, es decir el módulo criptográfico debe generar la llave privada localmente.

6.1.3 Entrega de la llave pública al emisor del certificado

Las llaves públicas transferidas deben ser entregadas a través de mecanismos que aseguren que la llave pública no se altera durante el tránsito.

Certificados de CA emisora

La llave pública debe ser entregada mediante un método fuera de banda, tal como:

- almacenado en un módulo criptográfico de la entidad;
- otros medios seguros que garanticen autenticidad e integridad.

Certificados de firma digital y autenticación de persona física

La llave pública debe ser entregada por la RA a través de medios legibles por computadoras desde una fuente autenticada;

Certificados de firma digital y autenticación de agente electrónico

La llave pública debe ser distribuida utilizando uno de los siguientes métodos:

- medios legibles por computadoras desde una fuente autenticada;
- almacenado en un módulo criptográfico de la entidad;
- otros medios seguros que garanticen autenticidad e integridad.

Certificados de autoridad de sellado de tiempo (TSA)

La llave pública debe ser entregada mediante un método fuera de banda, tal como:

- almacenado en un módulo criptográfico de la entidad;
- otros medios seguros que garanticen autenticidad e integridad.

6.1.4 Entrega de la llave pública de la CA a las partes que confían

La distribución de la llave pública se realiza a través del certificado digital y del repositorio público respectivo.

6.1.5 Tamaños de llave

El tamaño de las llaves debe ser suficientemente largo para prevenir que otros puedan determinar la llave privada utilizando cripto-análisis durante el periodo de uso del par de llaves.

Certificados de CA emisora

La llave de la CA raíz debe tener un tamaño mínimo de 4096 bits. La CA de Políticas debe mantener llaves con un tamaño mínimo de 2048 bits. Para las CA emisoras debe tener un tamaño de 2048 bits.

Certificados de firma digital y autenticación de persona física y de agente electrónico y de TSA

El tamaño de las llaves para el suscriptor debe ser de 2048 bits. La longitud de la llave pública que será certificada por la CA, debe ser menor o igual al tamaño de la llave privada de firma de la CA.

6.1.6 Generación de parámetros de llave pública y verificación de calidad

La CA genera y verifica los parámetros de llave pública de acuerdo con el estándar FIPS 186-2 (Digital Signature Standard-DSS) que define el cripto-algoritmo utilizado en la generación.

6.1.7 Propósitos de uso de llave (Campo "keyusage" de X.509 v3)

Certificados de CA emisora

La CA Raíz únicamente podrá emitir certificados de firma para las Autoridades de Políticas y para las CRL respectivas. Las CAs de políticas únicamente podrán emitir certificados de firma a las CA emisoras y para sus CRLs.

La CA emisora **no** puede emitir certificados con el uso de encripción.

Certificados de firma digital y autenticación de persona física y de agente electrónico

Los suscriptores tendrán dos certificados emitidos uno con el uso de firma digital y el otro con el uso de autenticación.

- Para firmar: digitalSignature + nonRepudiation
- Para autenticarse a servidores: digitalSignature + KeyEncipherment

6.2 Controles de ingeniería del módulo criptográfico y protección de la llave privada

6.2.1 Estándares y controles del módulo criptográfico

Certificados de CA emisora

La CA debe mantener controles para asegurar que las llaves privadas de la CA permanecen confidenciales y mantienen su integridad y el acceso al hardware criptográfico de la CA está limitado a individuos autorizados.

Las llaves privadas de la CA deben ser respaldadas, guardadas y recuperadas por personal autorizado con roles de confianza, utilizando controles múltiples en un ambiente físicamente seguro.

Las copias de respaldo de las llaves privadas de la CA Raíz deben estar sujetas al mismo o mayor nivel de controles de seguridad que las llaves que actualmente están en uso. La recuperación de las llaves de la CA debe llevarse a cabo de una forma tan segura como el proceso de respaldo.

El estándar de módulos criptográficos es el "**Security Requirements for Cryptographics Modules**" (actualmente FIPS140). Los módulos criptográficos para las CAs Emisoras deben certificarse como mínimo con el FIPS 140-2 nivel 3.

Certificados de firma digital y autenticación de persona física

El suscriptor debe cumplir con los controles definidos en el acuerdo de suscriptor y utilizar módulos criptográficos basados como mínimo en el estándar FIPS 140-2 nivel 2

Certificados de firma digital y autenticación de agente electrónico

El certificado de agente electrónico debe cumplir con los controles definidos en el acuerdo de suscriptor y utilizar un módulo criptográfico basado como mínimo en el estándar FIPS 140-2 nivel 3

Certificados de autoridad de sellado de tiempo (TSA)

El certificado de TSA debe cumplir con los controles definidos en el acuerdo de suscriptor y utilizar un módulo criptográfico basado como mínimo en el estándar FIPS 140-2 nivel 3.

6.2.2 Control multi-persona de llave privada (m de n)

Certificados de CA emisora

Para la activación de la llave privada de firma de la CA se debe utilizar controles de acceso de múltiples partes (es decir, "m" de "n") con un valor mínimo de 3 para "m".

Si las llaves privadas de la CA son respaldadas, estas deben ser respaldadas, guardadas y recuperadas por personal autorizado con roles de confianza, utilizando controles múltiples en un ambiente físicamente seguro. La cantidad de personal autorizado para llevar a cabo esta función debe mantenerse al mínimo.

Certificados de firma digital y autenticación de persona física

Sin estipulaciones.

Certificados de firma digital y autenticación de agente electrónico

Para la activación de la llave privada de firma del agente electrónico se debe utilizar controles de acceso que resguarden la llave privada. Una vez activado el dispositivo de

firma se debe mantener resguardado físicamente y monitoreado, para evitar otros usos.

Certificados de autoridad de sellado de tiempo (TSA)

Para la activación de la llave privada de firma del TSA se debe utilizar controles de acceso de múltiples partes (es decir, “m” de “n”) con un valor mínimo de 3 para “m”. Una vez activado el dispositivo de firma se debe mantener resguardado físicamente y monitoreado, para evitar otros usos

6.2.3 Custodia de llave privada

No se deben implementar servicios de custodia de llaves de firmas emitidas a terceros.

6.2.4 Respaldo de llave privada

Los respaldos de llaves privadas de la CA son únicamente para propósitos de recuperación en caso de una contingencia o desastre. Los planes de continuidad del negocio de la CA deben incluir procesos de recuperación de desastres para todos los componentes críticos del sistema de la CA, incluyendo el hardware, software y llaves, en el caso de falla de uno o más de estos componentes.

Las copias de respaldo de las llaves privadas de la CA deberían estar sujetas al mismo o mayor nivel de controles de seguridad que las llaves que actualmente están en uso. La recuperación de las llaves de la CA debe llevarse a cabo de una forma tan segura como el proceso de respaldo.

Las llaves privadas de certificados de firma digital de los suscriptores no son respaldadas por ningún motivo en la CA, y estas permanecen dentro de los límites de los dispositivos criptográficos donde fueron generadas.

6.2.5 Archivado de llave privada

La CA no archiva la llave privada de ninguno de los suscriptores. En el caso de de la CA, ésta debe archivar su par de llaves (pública y privada) en forma encriptada en concordancia con las disposiciones de protección de llaves definidas en este CP, por un plazo acorde con la legislación aplicable.

6.2.6 Transferencia de llave privada hacia o desde un módulo criptográfico

Las llaves privadas de la CA son generadas por un módulo criptográfico seguro. En el evento que una llave privada es transportada desde un módulo criptográfico a otro, la llave privada debe estar encriptada durante su transporte.

La llave privada usada para encriptar el transporte de la llave privada debe estar protegida contra divulgación no autorizada.

6.2.7 Almacenamiento de la llave privada en el módulo criptográfico

Los dispositivos criptográficos utilizados para el almacenamiento del respaldo de las llaves privadas de la CA deben ser guardados de forma segura, en un sitio alterno, para que sean recuperados en el caso de un desastre en el sitio primario

Las partes de la clave secreta o los componentes necesarios para usar y gestionar los dispositivos criptográficos de recuperación de desastres, deberían estar también guardados con seguridad en una ubicación fuera del sitio primario.

Las llaves privadas de la CA deben ser almacenadas y utilizadas dentro de un dispositivo criptográfico seguro que cumpla como mínimo con el perfil de protección apropiado de los requisitos del estándar FIPS 140-2 nivel 3

6.2.8 Método de activación de llave privada

Certificados de CA emisora

Los métodos de activación de llaves de la CA están protegidos y para accederlos se deben contar con mecanismos de autenticación de al menos dos factores de seguridad, por ejemplo: tarjetas inteligentes, más "frases de paso" o PINs. Los datos de activación deben estar distribuidos en roles de confianza que ejecutan diversas personas.

Certificados de firma digital y autenticación de persona física

Los métodos de activación de llaves para un usuario deben contar con al menos uno de los siguientes factores de seguridad: "frases de paso", PINs, o datos biométricos.

Certificados de firma digital y autenticación de agente electrónico

Los métodos de activación de llaves de agente electrónico están protegidos mediante una combinación de al menos dos de los siguientes factores de seguridad: tarjetas inteligentes, "frases de paso", PINs, o datos biométricos.

Certificados de autoridad de sellado de tiempo (TSA)

Los métodos de activación de llaves de autoridades de sellado de tiempo están protegidos mediante una combinación de al menos dos de los siguientes factores de seguridad: tarjetas inteligentes, "frases de paso", PINs, o datos biométricos. Los datos de activación deben estar distribuidos en roles de confianza que ejecutan diversas personas.

6.2.9 Método de desactivación de llave privada

Certificados de CA emisora

Para la CA Raíz y de Políticas es obligatorio que los módulos criptográficos, los cuales han sido activados, no estén desatendidos o abiertos al acceso no autorizado. Después de usarlos, estos deben ser desactivados manualmente o por un tiempo de expiración

por estado pasivo. Los módulos de hardware criptográfico deben ser removidos y almacenados cuando no estén en uso.

En el caso de las CA emisoras los equipos se mantienen en línea, para dichos efectos una vez activados los dispositivos criptográficos, estos se deben mantener monitoreados y protegidos contra accesos no autorizados.

Certificados de firma digital y autenticación de persona física

Sin estipulaciones

Certificados de firma digital y autenticación de agente electrónico

Cuando los equipos que hospedan los certificados de agente electrónico se encuentran en línea, estos se deben mantener monitoreados y protegidos contra accesos no autorizados. Cuando los equipos no estén en uso entonces los módulos de hardware criptográfico deben ser removidos y almacenados.

Certificados de autoridad de sellado de tiempo (TSA)

Cuando los equipos que hospedan el certificado sellado de tiempo se encuentran en línea, estos se deben mantener monitoreados y protegidos contra accesos no autorizados. Cuando los equipos no estén en uso entonces los módulos de hardware criptográfico deben ser removidos y almacenados.

6.2.10 Método de destrucción de llave privada

El procedimiento para la destrucción de llaves privadas debe incluir la autorización para destruirla.

Certificados de CA emisora

La CA raíz, las CA de políticas y la CA emisora deben destruir los respaldos de las llaves privadas que han expirado. Para los módulos criptográficos de hardware, estos deben ser limpiados por medio de inicialización de ceros (Zeroize Command).

Certificados de firma digital y autenticación de persona física

Los módulos criptográficos de hardware que hospedan la llave privada deben ser limpiados por medio de inicialización de ceros (Zeroize Command).

Certificados de firma digital y autenticación de agente electrónico

Los módulos criptográficos de hardware que hospedan la llave privada deben ser limpiados por medio de inicialización de ceros (Zeroize Command).

Certificados de autoridad de sellado de tiempo (TSA)

La TSA debe destruir los respaldos de las llaves privadas que han expirado. Para los módulos criptográficos de hardware, estos deben ser limpiados por medio de inicialización de ceros (Zeroize Command).

6.2.11 Clasificación del módulo criptográfico

Certificados de CA emisora

La capacidad del módulo criptográfico de la CA emisora es expresada en cumplimiento como mínimo del estándar Fips 140-2, nivel 3

Certificados de firma digital y autenticación de persona física

El módulo criptográfico para los suscriptores de certificados de firma digital y autenticación debe cumplir como mínimo con el estándar Fips 140-2, nivel 2

Certificados de firma digital y autenticación de agente electrónico

El módulo criptográfico para los certificados de agentes electrónicos debe cumplir como mínimo con el estándar Fips 140-2, nivel 3

Certificados de autoridad de sellado de tiempo (TSA)

La TSA debe cumplir como mínimo con el estándar Fips 140-2, nivel 3

6.3 Otros aspectos de gestión del par de llaves

Las CA de la jerarquía nacional de certificadores registrados deben establecer los medios necesarios para gestionar en forma segura las llaves de los suscriptores durante el ciclo de vida de las mismas.

6.3.1 Archivado de la llave pública

La CA debe mantener controles para sus propias llaves, de acuerdo a lo estipulado en la sección 5.5. Las llaves archivadas de la CA deberían estar sujetas al mismo o mayor nivel de control de seguridad que las llaves que están en uso actualmente.

6.3.2 Periodo operacional del certificado y periodo de uso del par de llaves

Los periodos de uso de la llave son descritos en la sección 5.6, de acuerdo a la siguiente tabla:

Nivel de jerarquía	Tiempo de uso en años	Tiempo operacional en años
Certificado de usuario	**2**	**2**
CA emisoras	**5**	**7**
CA Políticas	**10**	**17**
CA Raíz	**20**	**37**

6.4 Datos de activación

La CA mantiene estrictos controles en los datos de activación para operar los módulos criptográficos y que necesitan ser protegidos (ejemplo un PIN, una frase de paso o "password", una medida biométrica o una parte de llave mantenida manualmente).

6.4.1 Generación e instalación de los datos de activación

Certificados de CA emisora

Se debe contar con datos de activación de múltiples factores para protección de los accesos al uso de llaves privadas y su activación requiere de un control de múltiples partes (es decir, "m" de "n") con un valor mínimo de tres para "m".

Certificados de firma digital y autenticación de persona física

Se deben generar e instalar sus propios datos de activación para proteger y prevenir perdidas, robos, modificación, divulgación o uso no autorizado de sus llaves privadas.

Certificados de firma digital y autenticación de agente electrónico

Se debe contar con controles para protección de los accesos al uso de llaves privadas. En particular, se requiere generar sus propios datos de activación para prevenir uso no autorizado de la llave privada.

Certificados de autoridad de sellado de tiempo (TSA)

Se debe generar e instalar sus propios datos de activación para proteger y prevenir perdidas, robos, modificación, divulgación o uso no autorizado de sus llaves privadas. Adicionalmente, como parte de los datos de activación se requiere de un control de múltiples partes (es decir, "m" de "n") con un valor mínimo de tres para "m".

6.4.2 Protección de los datos de activación

Los datos de activación deberían ser memorizados, sin mantener respaldo escrito. Si se escriben, estos deberían de estar almacenados en un nivel de seguridad semejante al de los módulos criptográficos para protegerlos, y en una localización diferente a la de los módulos criptográficos. Los datos de activación de la CA deben incluir dispositivos biométricos.

6.4.3 Otros aspectos de los datos de activación

Los datos de activación de los módulos criptográficos de la CA Raíz y CA de Políticas deben ser cambiados al menos una vez cada año. Y en el caso de las CA emisoras o TSA la frecuencia debe ser al menos una vez cada dos meses.

6.5 Controles de seguridad del computador

El equipo de la CA debe usar sistemas operativos que:

- Requieran autenticación para poder ser accedidos
- Provean capacidad para mantener bitácoras y registros de seguridad con fines de auditoría
- Cumplan con requerimientos y controles de seguridad, al menos tan estrictos como los definidos en este CP.

Luego de que la plataforma donde opera el equipo de la CA ha sido aprobada, debe continuar operando bajo los mismos parámetros aprobados.

6.5.1 Requerimientos técnicos de seguridad de computador específicos

Los equipos donde operan los sistemas de la CA, que requieran acceso remoto deben poseer autenticación mutua y los sistemas operativos deberían estar configurados de acuerdo con los estándares del sistema operativo de la CA y ser revisados periódicamente.

Las actualizaciones y parches de los sistemas operativos deberían ser aplicados de manera oportuna y la utilización de programas utilitarios del sistema debería ser restringida al personal autorizado, y debe estar estrictamente controlado.

6.5.2 Clasificación de la seguridad del computador

Los sistemas sensibles de la CA requieren un ambiente informático dedicado y aislado, que implemente el concepto de sede computacional confiable con procesos de auditoria que ejecuten pruebas de seguridad al menos dos veces al año.

6.6 Controles técnicos del ciclo de vida

La CA debe mantener controles en los equipos de seguridad (hardware y software) requeridos para operar en una infraestructura PKI desde el momento de la compra

hasta su instalación, de forma que reduzcan la probabilidad que cualquiera de sus componentes sea violentado.

Todo el hardware y software que ha sido identificado para operar las CA debe ser enviado y entregado con métodos que provean una adecuada cadena de custodia.

6.6.1 Controles para el desarrollo de sistemas

La CA debe mantener controles que proporcionen una seguridad razonable de las actividades de desarrollo y mantenimiento de los sistemas de la CA.

Los nuevos sistemas o para la expansión de los sistemas existentes, deben especificar los requisitos de control, seguir procedimientos de prueba de software y control de cambios para la implementación de software.

La CA debe mantener controles sobre el acceso a las bibliotecas fuente de programas.

6.6.2 Controles de gestión de seguridad

Los Administradores de la CA son los responsables de garantizar que se cumplan los procedimientos de seguridad correctamente. Además de ejecutar revisiones periódicas para asegurar el cumplimiento de los estándares de implementación de seguridad

6.6.3 Controles de seguridad del ciclo de vida

La CA debe incluir controles en la gestión de seguridad por medio de herramientas y procedimientos que verifiquen la adherencia a la configuración de seguridad de los sistemas operativos y redes.

6.7 Controles de seguridad de red

El equipo de la CA debe estar dentro de los límites de la red interna, operando bajo un nivel de seguridad de red crítico. La red de la CA debe estar protegida contra ataques. Los puertos y servicios que no se requieran deben estar apagados.

En el caso de la CA Raíz debe estar off-line y aislada de la red organizacional.

Los niveles críticos de seguridad de red, deben incluir:

- La encripción de las conexiones involucradas con las operaciones de la CA.
- Los sitios Web están provistos de certificados SSL.
- La red está protegida por firewalls y sistemas de detección de intrusos.
- Los accesos externos a información de bases de datos de la CA están prohibidos.
- La CA debe controlar la ruta de acceso del usuario desde la Terminal hasta los servicios.

- Los componentes de la red local deben mantenerse en un ambiente físicamente seguro y sus configuraciones deben ser auditadas periódicamente.
- Los datos sensibles deben encriptarse cuando se intercambian sobre redes públicas o no confiables.

La CA debe definir los procedimientos de control del cambio para el hardware, los componentes de la red y los cambios de configuración del sistema.

6.8 Sellado de tiempo ("Time-Stamping")

Los certificados, CRL y otras entradas en la base de datos de revocaciones deben contener la fecha y hora, sincronizadas utilizando los servicios UTC-6. El sellado de tiempo es una característica opcional.

7. Perfiles de Certificados, CRL y OCSP

Este capítulo especifica el formato de las CRL y OCSP, tales como información del perfil, versión y extensiones utilizadas. En el caso de la jerarquía nacional de certificadores registrados, los OCSP son un mecanismo opcional para la CA Raíz y las CA de Políticas, debido a que son pocos los certificados emitidos y por tanto revocados por ellas. La verificación del estado de los certificados para las CA emisoras constituye un factor crítico de seguridad para diversas aplicaciones, por lo tanto deben obligatoriamente implementar los dos métodos de validación: OCSP y CRL.

7.1 Perfil del Certificado

Los certificados digitales deben cumplir con:

- Estándar X.509 versión 3.
- RFC3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- RFC 3039 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile.
- ISO 3166-1 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países".

Cómo mínimo el certificado contiene:

Campo	Valor o restricciones
Versión	**V3, los certificados deben ser X.509 versión 3.**
Número de serie	**Valor único emitido dentro del ámbito de cada CA emisora.**
Algoritmo de firma	**El Algoritmo de firma debe ser como mínimo SHA1RSA.**
Emisor	**Nombre de la CA Emisora.Ver sección 7.1.4.**

Campo	Valor o restricciones
Valido desde	**Este campo especifica la fecha y hora a partir de la cual el certificado es válido. Las fechas establecidas para el periodo de validez deben ser sincronizadas con respecto al servicio de tiempo UTC-6.**
Valido hasta	**Este campo especifica la fecha y hora a partir de la cual el certificado deja de ser válido. Las fechas para la validez del certificado deben ser sincronizadas con el servicio de tiempo UTC-6.**
Sujeto	**Nombre del suscriptor.Ver sección 7.1.4.**
Llave pública del sujeto	**Codificado de acuerdo con el RFC 3280. Con un largo de llave mínima de 2048 bits y algoritmo RSA.**
Identificador de llave de la autoridad	**Este campo es usado por los diversos software de validación para ayudar a identificar a la autoridad certificadora registrada que emitió el certificado en la cadena de confianza. Referencia el campo "Subject Key Identifier" de la CA emisora del certificado.**
Identificador de la llave del sujeto	**Este campo es usado por software de validación para ayudar a identificar un certificado que contiene una determinada llave pública.**
Política del certificado	**Describe las políticas aplicables al certificado, especifica el OID y la dirección URL donde se encuentra disponible el CP respectivo.**
Uso de la llave	**Debe indicar los usos permitidos de la llave. Este campo debe ser marcado como un CAMPO CRÍTICO. Ver sección 1.4.1 Usos apropiados del certificado**
Punto de distribución del CRL	**Este campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no. En el caso del certificado de la CA Raíz, este atributo no debe especificarse.**
Acceso a la información de la autoridad	**Este campo es usado para indicar las direcciones donde puede ser encontrado el certificado de la CA emisora. Además, para indicar la dirección donde puede accederse el servicio de OCSP, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no. En el caso del certificado de la CA Raíz, este atributo no debe especificarse.**
Usos extendidos de la llave	**Referencia otros propósitos de la llave, adicionales al uso. De acuerdo con la sección 7.1.2.5.**
Restricciones básicas	**Para el caso de la CA emisora la extensión PathLenConstraint debe ser igual a cero. Ver sección 7.1.2.4 Restricciones básicas.**

7.1.1 Número(s) de versión

Todos los certificados emitidos dentro de la jerarquía nacional de certificadores registrados deben ser X.509 versión 3 o superior.

7.1.2 Extensiones del certificado

7.1.2.1 Key Usage

El “key usage” es una extensión crítica que indica el uso del certificado de acuerdo con el RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”. Ver sección 1.4.1 Usos apropiados del certificado.

7.1.2.2 Extensión de política de certificados

La extensión de “certificatepolicies” del X.509 versión 3 es el identificador del objeto de este CP de acuerdo con la sección 7.1.6. La extensión no es considerada como crítica.

7.1.2.3 Nombre alternativo del sujeto

La extensión “sujectAltName” es opcional y solamente se puede usar para certificados de agente electrónico. En caso de ser utilizada, el uso de esta extensión debe ser “NO critico” y únicamente está permitido el uso del nombre DNS, en concordancia con la sección 4.1.2.

7.1.2.4 Restricciones básicas

Para el caso de las CAs emisoras se debe colocar el campo “PathLenghtConstraint” con un valor de 0, para indicar que la CA no permite más sub-niveles en la ruta del certificado. **Es un campo crítico.**

7.1.2.5 Uso extendido de la llave

La extensión permite configurar los propósitos de la llave, y no es considerada crítica. A continuación se presenta el cuadro con los propósitos comunes:

OID	Descripción	Tipos de certificado
1.3.6.1.5.5.7.3.1	**Autenticación de servidor**	**Autenticación agente electrónico**
1.3.6.1.5.5.7.3.2	**Autenticación del cliente**	**Autenticación persona física** **Firma digital (para no repudio)** **Agente electrónico**
1.3.6.1.5.5.7.3.4	**Protección del correo**	**Firma Digital de persona física y agente electrónico**
1.3.6.1.5.5.7.3.8	**Sellado de tiempo**	**Sellado de tiempo**
1.3.6.1.4.1.311.20.2.2	**Smart Card Logon**	**Autenticación persona física**

7.1.2.6 Puntos de distribución de los CRL

La extensión “CRL Distribution Points” contiene las direcciones URL de la localización donde las partes que confían pueden obtener el CRL para verificar el estado del certificado. La extensión NO es crítica.

7.1.2.7 Identificador de llave de Autoridad

El método para la generación del identificador está basado en la llave pública de la CA emisora del certificado, de acuerdo a lo descrito por el RFC 3280 “Internet X.509 Public Key Infraestructura Certificate and CRL Profile”. La extensión NO es crítica.

7.1.2.8 Identificador de la llave del sujeto

La extensión no es crítica, y el método para la generación del identificador de llave está basado en la llave pública del sujeto del certificado y es calculado de acuerdo con uno de los métodos descritos en el RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”.

7.1.3 Identificadores de objeto de algoritmos

Los certificados generados dentro de la jerarquía nacional de certificadores registrados deben usar uno de los siguientes algoritmos:

- sha-1WithRSAEncryption OID ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
- sha256WithRSAEncryption OID::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

7.1.4 Formas del nombre

Los nombres dentro de la jerarquía nacional de certificadores registrados deben cumplir las regulaciones de la sección 3.1.1. Adicionalmente, los certificados de suscriptores generalmente deben incluir el URL donde se encuentran los términos del uso de los certificados y los acuerdos entre las partes.

7.1.5 Restricciones del nombre

Los nombres se escriben en mayúsculas y sin tildes, únicamente se debe aceptar el carácter Ñ como un caso especial para los nombres de personas físicas y jurídicas.

El código de país es de dos caracteres y se asigna de acuerdo al estándar ISO 3166-1 “Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países”.

7.1.6 Identificador de objeto de Política de Certificado

El OID de la política de certificado correspondiente a cada clase de certificado es definido acorde a la sección 1.2. El director de la DCFD le corresponde la administración de los “Identificadores de Objetos” (OID) para el Sistema Nacional de Certificación Digital.

7.1.7 Uso de la extensión “Restricciones de Política” (*Policy Constraints*)

Sin estipulaciones.

7.1.8 Semántica y sintaxis de los "Calificadores de Política" (*Policy Qualifiers*)

El calificador de la política está incluido en la extensión de "certificate policies" y contiene una referencia al URL con el CP aplicable y a los acuerdos de partes que confían.

7.1.9 Semántica de procesamiento para la extensión crítica de "Políticas de Certificado" (*Certificate Policies*)

Sin estipulaciones.

7.2 Perfil de la CRL

Las listas de revocación de certificados cumplen con el RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile"y contienen los elementos básicos especificados en el siguiente cuadro:

Campo	Valor o restricciones
Versión	**Ver sección 7.2.1**
Algoritmo de firma	**Algoritmo usado para la firma del CRL, puede ser:** • **sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)** • **sha256WithRSAEncryption (OID:1.2.840.113549.1.1.11)**
Emisor	**Entidad que emite y firma la CRL**
Fecha efectiva	**Fecha de emisión del CRL**
Siguiente actualización	**Fecha para la cual es emitida la siguiente CRL. La frecuencia de emisión del CRL está acorde con lo requerido en la sección 4.9.7**
Certificados revocados	**Lista de certificados revocados, incluyendo el número de serie del certificado revocado y la fecha de revocación**

7.2.1 Número(s) de versión

La jerarquía nacional de certificadores registrados de certificación soporta las CRLs X.509 versión 2.

7.2.2 *CRL y extensiones de entradas de CRL*

Sin estipulación.

7.3 Perfil de OCSP

El servicio de validación de certificados en línea OCSP (Online Certificate Status Protocol) es una forma para obtener información reciente sobre el estado de un certificado.

El servicio OCSP que se implemente debe cumplir lo estipulado en el RFC2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”.

7.3.1 Número(s) de versión

Debe cumplir al menos con la versión 1 del RFC2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”.

7.3.2 Extensiones de OCSP

Sin estipulaciones.

8. Auditoría de cumplimiento y otras evaluaciones

De acuerdo con el artículo 21 de la Ley de firma digital, “Todo certificador registrado estará sujeto a los procedimientos de evaluación y auditoría que acuerde efectuar la DCFD o el ECA”.

Adicionalmente, el artículo 24 inciso e) de ese cuerpo normativo, dispone como una función de la DCFD el “fiscalizar el funcionamiento de los certificadores registrados, para asegurar su confiabilidad, eficiencia y el cabal cumplimiento de la normativa aplicable, imponiendo, en caso necesario, las sanciones previstas en esta Ley. La supervisión podrá ser ejercida por medio del ECA, en el ámbito de su competencia”.

Todas las autoridades emisoras de certificados deben ajustarse al cumplimiento de las auditorías realizadas por el ECA, las cuales permiten establecer una confianza razonable en el sistema de firma digital.

Se pueden ejecutar investigaciones y revisiones para asegurar la confianza de la jerarquía nacional de certificadores registrados, las cuales incluyen, pero no se limitan a:

- Revisión de seguridad y de prácticas, las cuales incluyen instalaciones, documentos de seguridad, declaración de prácticas de certificación, acuerdos entre las partes, política de privacidad y validación de los planes para asegurar el cumplimiento de estándares.
- El ECA es la entidad responsable de ejecutar las auditorias, de acuerdo a lo estipulado en la ley.
- La DCFD puede solicitar al ECA auditorías especiales cuando tenga sospecha de un incidente o compromiso de la CA, que ponga en riesgo la integridad del sistema.

Adicionalmente, cada CA debe implementar un programa de auditorías internas para la verificación de su sistema de gestión. Dicho programa de auditorías debe estar basado en la INTE-ISO/IEC 19011 “Directrices para la auditoría de sistemas de gestión de la calidad y/o ambiental”.

8.1 Frecuencia o circunstancias de evaluación

El cumplimiento de la evaluación externa del ECA se debe ejecutar al menos una vez al año y los costos deben ser asumidos por la entidad evaluada. El ECA puede realizar evaluaciones extraordinarias de acuerdo con sus procedimientos.

El programa de auditorías internas establecerá la frecuencia o circunstancias para su realización, pero en términos generales se espera que las CA ejecuten al menos una auditoría al año.

8.2 Identidad/calidades del evaluador

El personal que ejecuta las evaluaciones para el ECA incluye:

- Experto Técnico: Persona asignada por el ECA para aportar conocimientos técnicos específicos o pericia respecto al alcance de acreditación a ser evaluado.
- Evaluador: Persona designada para ejecutar como parte de un equipo evaluador, la evaluación de un Organismo de Evaluación de la Conformidad OEC.
- Evaluador Líder: Evaluador al que le es dada la completa responsabilidad por actividades de evaluación específicas.

El ECA tiene procedimientos establecidos para determinar la competencia de cada uno de estos.

Para las auditorías internas la CA debe establecer los requisitos de competencia de sus auditores según los lineamientos de la INTE-ISO/IEC 19011 “Directrices para la auditoría de sistemas de gestión de la calidad y/o ambiental”.

8.3 Relación del evaluador con la entidad evaluada

Por ley, el ECA constituye un ente independiente e imparcial, el cual ejecutará las evaluaciones acorde a sus procedimientos.

Para las auditorías internas la CA debe seguir lo establecido en la INTE-ISO/IEC 19011 “Directrices para la auditoría de sistemas de gestión de la calidad y/o ambiental”.

8.4 Aspectos cubiertos por la evaluación

Los puntos de evaluación para cada entidad son detallados a continuación:

Auditorias de la autoridad de registro

Es obligatorio que la autoridad certificadora registrada (CA emisora) supervise las autoridades de registro y notifique cualquier excepción o irregularidad de las políticas

de la jerarquía nacional de certificadores registrados, y además tome las medidas para remediarlas.

Auditorias de las CA emisoras

Las CA emisoras dentro de la jerarquía nacional de certificadores registrados deben cumplir con las políticas nacionales y con los estándares determinados, a saber:

- Ley y reglamento de firma digital,
- Políticas de la raíz para los certificados de:
- Firma digital y autenticación de persona física.
- Firma digital y autenticación de agente electrónico.
- INTE/ISO 21188: “Infraestructura de llave pública para servicios financieros. Estructura de prácticas y políticas”.
- RFC 3647: “Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework”.

Autoridades de sellado de tiempo

- Ley y reglamento de firma digital.
- Políticas de la raíz para los certificados de:
- Autoridad de sellado de tiempo.
- RFC 3161: “Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)”.
- RFC 3628: “Policy Requirements for Time-Stamping Authorities (TSAs)”.
- Política de sellado de tiempo del sistema nacional de certificación digital

8.5 Acciones tomadas como resultado de una deficiencia

La CA debe tener procedimientos para ejecutar acciones correctivas para las deficiencias identificadas tanto en las evaluaciones externas como en las auditorías internas.

8.6 Comunicación de resultados

El ECA tiene procedimientos para la ejecución de la acreditación que incluyen la comunicación de los resultados y los procedimientos de apelación.

9. Otros asuntos legales y comerciales

9.1 Tarifas

9.1.1 *Tarifas de emisión o renovación de certificados*

La tarifa para la emisión y administración de los certificados será determinada por la CA emisora del certificado.

9.1.2 Tarifas de acceso a certificados

Las CA emisoras dentro de la jerarquía nacional de certificadores registrados no pueden cobrar por el mantenimiento de los repositorios de certificados a las partes que confían.

9.1.3 Tarifas de acceso a información del estado o revocación

Las CA emisoras dentro de la jerarquía nacional de certificadores registrados no pueden cobrar por el mantenimiento de las listas de revocación de certificados a las partes que confían. Sin embargo, se pueden establecer tarifas para otros servicios especializados de revocación, OCSP o sellado de tiempo.

9.1.4 Tarifas por otros servicios

Las CA emisoras dentro de la jerarquía nacional de certificadores registrados no pueden establecer tarifas para acceder información del CP o su respectivo CPS.

9.1.5 Política de reembolso

La CA que implemente una política de reembolso debe documentarla como parte de sus políticas y publicarlas dentro de su sitio Web.

9.2 Responsabilidad financiera

9.2.1 Cobertura de seguro

De acuerdo con los artículos 12 y 13 del reglamento de firma digital, es obligatorio para los sujetos privados, mantener una caución rendida preferiblemente por medio de póliza de fidelidad, y cuyo monto será fijado por la DCFD. Cuando la caución esté sujeta a vencimiento, esta debe ser renovada al menos dos meses antes de la fecha de expiración.

9.2.2 Otros activos

La CA emisora debe poseer suficientes recursos financieros para mantener sus operaciones y ejecutar sus deberes. La CA emisora debe ser razonablemente capaz de administrar el riesgo de responsabilidad para los suscriptores y partes que confían.

9.2.3 Cobertura de Seguro o garantía para entidades finales

Sin estipulaciones.

9.3 Confidencialidad de la información comercial

9.3.1 Alcance de la información confidencial

Los siguientes registros del suscriptor deben ser mantenidos confidenciales:

- Registros de solicitudes de la Autoridad Certificadora, tanto aprobados como rechazados.
- Registros de solicitud de certificados de sujeto.
- Registros de las transacciones.
- Registros de pistas de auditorías.
- Planes de contingencias y recuperación de desastres.
- Medidas de seguridad controlando las operaciones de certificados (Hardware/Software).
- Servicios de administración de certificados y servicios de enrolamiento.

9.3.2 Información no contenida en el alcance de información confidencial

No se considera información confidencial las listas de revocación ni la información del estado de los certificados.

9.3.3 Responsabilidad para proteger la información confidencial

Las CA emisoras participantes dentro de la jerarquía nacional de certificadores registrados deben asegurar a los participantes que su información no será comprometida ni divulgada a terceras partes y deben cumplir con las leyes aplicables de privacidad.

9.4 Privacidad de información personal

9.4.1 Plan de privacidad

Las CA emisoras dentro de la jerarquía nacional de certificadores registrados deben implementar las políticas de privacidad de información, de acuerdo con las leyes vigentes. No se puede divulgar o vender información de los suscriptores a certificados o información de identificación de éstos.

9.4.2 Información tratada como privada

Cualquier información acerca de los suscriptores que no esté públicamente disponible a través del contenido del certificado emitido y servicios de CRL’s debe ser tratada como información privada.

9.4.3 Información que no es considerada como privada

El tratamiento de la información que no es considerada como privada, estará sujeto a lo que dispone la normativa nacional al efecto. Únicamente se considera pública la información contenida en el certificado.

9.4.4 *Responsabilidad para proteger información privada*

Las CA emisoras dentro de la jerarquía nacional de certificadores registrados deben asegurar que la información privada no puede ser comprometida o divulgada a terceras partes.

9.4.5 Notificación y consentimiento para usar información privada

La información privada no puede ser usada sin el consentimiento de las partes. En este sentido, la CA no requiere notificar a los suscriptores para usar información privada.

9.4.6 Divulgación de acuerdo con un proceso judicial o administrativo

Para divulgar información privada se requiere de una orden judicial que así lo determine y se divulga estrictamente la información solicitada por los jueces.

9.4.7 Otras circunstancias de divulgación de información

La información privada podrá ser divulgada en otras circunstancias, siempre que ésta resulte expresamente prevista por la legislación aplicable.

9.5 Derechos de propiedad intelectual

Sin estipulaciones.

9.6 Representaciones y garantías

9.6.1 Representaciones y garantías de la CA

Las CA de la jerarquía nacional de certificadores registrados deben garantizar que:

- No se presentan distorsiones en la información contenida en los certificados o en la emisión del mismo.
- No haya errores en la información que fue introducida por la entidad que aprueba la emisión del certificado.
- Los certificados reúnen los requerimientos expuestos en esta CP.
- Los servicios de revocación y el uso de los repositorios cumplen lo estipulado en este CP.

9.6.2 Representaciones y garantías de la RA

Las Autoridades de Registro (RA) deben garantizar que:

- No se presentan distorsiones en la información contenida en los certificados o en la emisión del mismo.
- No se presentan errores en la información del certificado que fue introducida por las entidades de registro.
- Que los dispositivos y materiales requeridos cumplen con lo dispuesto en este CP.

9.6.3 Representaciones y garantías del suscriptor

El suscriptor debe garantizar que:

- Cada firma digital creada usando la llave privada corresponde a la llave pública listada en el certificado.
- La llave privada está protegida y que no autoriza a personas a tener acceso a la llave privada del suscriptor.
- Toda la información suplida por el suscriptor y contenida en el certificado es verdadera.
- El certificado es utilizado exclusivamente para los propósitos autorizados.

9.6.4 Representaciones y garantías de las partes que confían

Los acuerdos de partes que confían requieren que los actores conozcan suficiente información para tomar las decisiones de aceptar el certificado.

9.6.5 Representaciones y garantías de otros participantes

Sin estipulaciones.

9.7 Renuncia de garantías

Cualquier tipo de cláusula relativa a la renuncia de garantías debe estar prevista en los acuerdos de suscriptor y de partes que confían.

9.8 Limitaciones de responsabilidad legal

Las limitaciones de responsabilidad legal deben estar previstas en forma expresa en los acuerdos de suscriptor y de partes que confían.

9.9 Indemnizaciones

La CA dentro de la jerarquía nacional de certificadores registrados debe indemnizar a los suscriptores por cualquier causa legalmente establecida, incluyendo:

- Falsedad en la información suministrada.
- Por fallas en la protección del sistema de la CA, o por el uso de sistemas no confiables.

En ambos casos, se deberá demostrar ante las autoridades correspondientes los daños y perjuicios causado por la CA.

9.10 Plazo y Finalización

9.10.1 Plazo

El CP empieza a ser efectivo después de la publicación en el repositorio y los nuevos certificados deben ser emitidos cumpliendo las políticas determinadas en la nueva versión del CP.

9.10.2 Finalización

La vigencia del CP se debe mantener hasta que todos los certificados emitidos bajo esta política hayan finalizado o hayan sido reemplazados por otros certificados emitidos bajo la nueva política.

9.10.3 Efectos de la finalización y supervivencia

Después de finalizada la vigencia del CP, la cual puede ser por cambios o modificaciones en las políticas, esta se mantendrá válida mientras existan certificados activos.

9.11 Notificación individual y comunicaciones con participantes

Se permiten las comunicaciones comerciales con los participantes, a menos de que el contrato entre las partes especifique otras cláusulas.

9.12 Enmiendas

9.12.1 Procedimiento para enmiendas

De oficio el Comité Asesor de Políticas tendrá al menos una reunión anual para evaluar los atributos del certificado, determinando la conveniencia de seguir utilizando los mismos algoritmos, longitudes de las llaves y parámetros para la generación de los certificados.

Los cambios en las políticas nacionales deben ser sometidos a consulta pública, y una vez aprobadas deben comunicarse a los participantes dentro de la jerarquía nacional de certificadores registrados.

Las modificaciones o enmiendas de las políticas deben documentarse y mantenerse actualizadas a través de versiones. Las enmiendas deben publicarse en el sitio Web de la CA emisora.

9.12.2 Mecanismo y periodo de notificación

La DCFD es la responsable de realizar los comunicados a las CA emisoras para implementar las modificaciones. Al menos treinta días naturales antes de cualquier cambio mayor en las políticas, estas se deben publicar en el sitio Web y realizar una comunicación en los medios escritos.

9.12.3 Circunstancias bajo las cuales los OID deben ser cambiados

Los cambios en los OIDs corresponden a nuevas políticas que contengan otros objetos con OID adicionales. Si la estructura del certificado se mantiene entonces no es necesario cambiar los OIDs.

9.13 Disposiciones para resolución de disputas

De acuerdo con la ley de firma digital, le compete a la DCFD la resolución de las disputas, como órgano administrador y supervisor del sistema de certificación digital. Las resoluciones dictadas por la DCFD agotan la vía administrativa.

9.14 Ley gobernante

Las CA emisoras dentro de la jerarquía nacional de certificadores registrados están sujetas a las leyes de la República de Costa Rica, en particular de la ley 8454 “Ley de certificados, firmas digitales y documentos electrónicos” y su reglamento.

9.15 Cumplimiento con la ley aplicable

Las políticas descritas cumplen con las regulaciones nacionales.

9.16 Disposiciones varias

9.16.1 Acuerdo completo

No aplicable.

9.16.2 Asignación

No aplicable.

9.16.3 Separabilidad

En el eventual caso que una cláusula de la política sea declarada inconstitucional por los tribunales de justicia o las leyes, el resto de las cláusulas de estas políticas se mantendrán vigentes.

9.16.4 Aplicación (Honorarios de abogado y renuncia de derechos)

No aplicable.

9.16.5 Fuerza mayor

Los acuerdos de suscriptores y partes que confían deben incluir cláusulas de fuerza mayor para proteger a la CA emisora.

9.17 Otras disposiciones

No aplicable.

10. Anexo A: Definiciones y acrónimos

10.1 Definiciones

Términos	Definición
Acuerdo de parte que confía, RPA (por sus siglas en inglés Relying party agreement)	**Es un acuerdo entre la autoridad certificadora y las partes que confían que típicamente establece los derechos y responsabilidades entre estas partes con respecto a la verificación de las firmas digitales y otros usos del certificado. Este acuerdo no requiere la aceptación explícita de la parte que confía.**
Acuerdo de suscriptor	**Es un acuerdo entre la CA raíz o la CA emisora y el suscriptor que establece los derechos y responsabilidades de las partes con respecto a la emisión y gestión de los certificados. Este acuerdo sí requiere la aceptación explícita del suscriptor.**
Agente Electrónico	**Sistema informático u otro medio automático que realiza transacciones electrónicas con relevancia jurídica, en forma automática, sin intervención humana. Las obligaciones y responsabilidades que se derivan de su accionar automático, obligan a su propietario o responsable.**
Apoderado	**Persona que tiene la capacidad jurídica para actuar en nombre de una empresa o institución y que tiene la potestad legal para cumplir con las responsabilidades asignadas en este CP.**
Autenticación	**Verificación de la identidad afirmada por el individuo:** **a) en el momento de registro, el acto de evaluar las credenciales de las entidades finales (esto es, suscriptores) como evidencia de la identidad afirmada;** **b) durante su uso, el acto de comparar electrónicamente la identidad y las credenciales presentadas contra los valores almacenados, para probar identidad.**
Autoridad certificadora CA (por sus siglas en inglés)	**Entidad en la cual una o más entidades confían para crear, asignar, revocar o suspender certificados de llave pública.**
Autoridad certificadora registrada	**El certificador inscrito y autorizado por la Dirección de Certificadores de Firma Digital.**
Autoridad de políticas PA (por sus siglas en inglés)	**Parte o cuerpo con autoridad y responsabilidad final de especificar las** políticas de certificado **y asegurar que las prácticas y controles de la** CA**, cumplen totalmente las** políticas de certificado **respectivas. (Ver definición ampliada en el artículo 28 del Reglamento de la ley 8454).**
Autoridad de registro RA (por sus siglas en inglés)	**Entidad responsable de la identificación y autenticación de sujetos de certificados, que no es la** CA **y por lo tanto no firma ni emite certificados.** Nota: **Una RA puede ayudar en el proceso de solicitud del certificado, en el proceso de revocación o en ambos. La RA no necesita ser un organismo separado, sino que puede ser parte de la CA.**

Términos	Definición
CA emisora	**Autoridad certificadora registrada que forma parte de la jerarquía nacional de certificadores registrados, y que implementa una o varias políticas para emisión de certificados de usuario final.**
CA de Políticas	**Autoridad certificadora que forma parte de la raíz nacional, utilizada para segmentar el riesgo de acuerdo a la política de emisión para un tipo de certificado.**
CA raíz	**Autoridad certificadora registrada que se ubica en el ápice de la jerarquía nacional de certificadores registrados.**
CA subordinada o Sub-CA	**Autoridad certificadora registrada que está más abajo en relación a otra** CA **en la jerarquía nacional de certificadores registrados.**
Calificador de la política	**Información dependiente de la política, que acompaña un identificador de** política de certificado **en un certificado de la norma X.509.**
Certificación	**Proceso de creación de un certificado de llave pública para una** entidad.
Certificado	**La llave pública y la identidad de un suscriptor, junto con otra información, que se torna infalsificable al ser firmada con la llave privada de la autoridad certificadora que emitió ese certificado de llave pública.**
Certificado suspendido	**Suspensión de la validez de un certificado**.
Compromiso	**Violación de la seguridad de un sistema tal que pueda haber ocurrido una divulgación no autorizada de información sensible.**
Comité asesor de políticas (CAP)	**Ver "Autoridad de políticas (PA)".**
Control múltiple	**Condición bajo la cuál dos o más partes, mantienen por separado y confidencialmente, la custodia de componentes de una sola llave que, individualmente, no conlleva al conocimiento de la llave criptográfica resultante.**
Datos de autenticación	**Información utilizada para verificar la identidad afirmada de una entidad, tal como la de un individuo, un rol definido, una corporación o una institución.**
Datos de activación	**Valores de los datos, distintos a las llaves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos (por ejemplo: por un PIN, una frase de paso o una llave mancomunada).**
Declaración de divulgación PKI o PDS (por sus siglas en inglés)	**Documento suplementario de una** CP **o una** CPS **que divulga la información crítica sobre las políticas y prácticas de una** CA **/**PKI. Nota: **Una declaración de divulgación PKI es un medio para divulgar y enfatizar la información normalmente cubierta en detalle por la CP y/o la CPS asociados. Por lo tanto, un PDS no tiene la intención de sustituir una CP o una CPS.**
Declaración de prácticas de certificación o CPS (por sus siglas en inglés)	**Declaración de las prácticas que emplea una** autoridad certificadora **al emitir certificados y que define el equipo, políticas y procedimientos que utiliza la** CA **para satisfacer los requisitos especificados en las políticas del certificado que son soportadas por esta.**

Términos	Definición
Delta CRL	**Partición del CRL dentro de una unidad de tiempo, que contiene los cambios realizados al CRL base desde su última actualización.**
Diario de eventos o bitácora de auditoría	**Registro cronológico de las actividades del sistema, el cual es suficiente para permitir la reconstrucción, revisión e inspección de la secuencia de los ambientes y de las actividades que rodean o que conducen a cada acontecimiento en la ruta de una transacción desde su inicio hasta la salida de los resultados finales.**
Documento de identidad legalmente aceptado	**Es el documento formal que según el ordenamiento jurídico costarricense, sirve para identificar legalmente a un suscriptor. En el caso de las personas físicas costarricenses, es la cédula de identidad, para las personas físicas extranjeras, es el documento único de permanencia, según sea su estatus migratorio y para las personas jurídicas nacionales, la cédula de persona jurídica.** **En el caso de la cédula de persona jurídica el documento debe ser acompañado por una certificación de personería jurídica vigente (con menos de un mes de emitida), y el documento de identidad del personero.**
Emisor del certificado	**Organización cuyo nombre aparece en el campo del emisor de un** certificado**.**
Encripción	**Proceso para convertir la información a un formato más seguro. En otras palabras, los datos que están en un formato claro, o sea entendible, se convierten mediante un proceso matemático a un formato encriptado o codificado, o sea ininteligible.**
Entidad	CA**,** RA **o** entidad final**.**
Entidad final	**Sujeto de certificado que utiliza su llave privada para otros propósitos diferentes al de firmar certificados. En este caso, puede tratarse de una persona física, un agente electrónico o una autoridad de sellado de tiempo.**
Firma digital	**Transformación criptográfica que, cuando está asociada a una unidad de datos, proporciona los servicios de autenticación del origen, integridad de los datos y no-repudio del firmante.**
Firma digital certificada	**Firma digital generada utilizando la llave privada correspondiente de un certificado de llave pública, emitido por una CA registrada.**
Dispositivo criptográfico o módulo de seguridad de hardware (HSM por sus siglas en inglés)	**Es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas.**
Identificador de objeto u OID (por sus siglas en inglés)	**Serie única de números enteros que identifica inequívocamente un objeto de información.**

Términos	Definición
Infraestructura de llave pública o PKI (por sus siglas en inglés)	**Estructura de *hardware*, *software*, recurso humano, procesos y políticas que utiliza tecnología de firma digital para facilitar una asociación comprobable entre el componente público de un par de llaves asimétricas con un suscriptor específico que posee la llave privada correspondiente.** Nota **La llave pública puede ser provista para verificación de firma digital, autenticación del sujeto en diálogos de comunicación, y/o para el intercambio o la negociación de llaves de encripción de mensajes.**
Lista de revocación de certificados o CRL (por sus siglas en inglés)	**Es una lista con los números de serie de los** certificados que han sido **revocados.**
Parte que confía RP (por sus siglas en inglés)	**Receptor de un certificado quien actúa confiando en ese certificado, en las firmas digitales verificadas usando ese certificado, o ambos.**
Perfil del certificado	**Especificación del formato requerido para un tipo particular de** certificado **(incluyendo requisitos para el uso de los campos estándar y extensiones).**
Período de operación	**Período de vigencia de un certificado que comienza en la fecha y la hora en que es emitido por una** CA **(o una fecha y una hora posterior, si se indica en el certificado) y termina en la fecha y la hora en que expira o se revoca el mismo.**
Política de certificado o CP (por sus siglas en inglés)	**Conjunto de reglas establecidas que indican la aplicabilidad de un certificado a una comunidad particular y/o una clase de aplicaciones con requisitos comunes de seguridad.**
Protocolo de consulta en línea del estado del certificado u OCSP (por sus siglas en inglés)	**Protocolo para determinar el estado actual de un certificado en lugar de o como suplemento a la comprobación contra una** CRL **periódica, y que especifica los datos que necesitan ser intercambiados entre una aplicación que comprueba el estado de un certificado y el servidor que proporciona ese estado.**
Re-emisión de llaves del certificado	**Proceso por medio del cual una entidad con un par de llaves y un** certificado **recibe un nuevo** certificado **para una nueva llave pública, siguiendo la generación de un nuevo par de llaves.**
Renovación del certificado	**Proceso por medio del cual a una entidad le es emitida una nueva instancia de un certificado existente con un nuevo período de validez, conservando el mismo par de llaves.**
Repositorio	**Sistema para el almacenamiento y la distribución de los certificados y de la información relacionada (esto es, almacenamiento y recuperación de la** política de certificado**, estado del certificado, etc.).**
Rol de confianza	**Puesto de trabajo que realiza funciones críticas que, si se realiza insatisfactoriamente, puede tener un impacto adverso sobre el grado de confianza proporcionado por la** CA**.**

Términos	Definición
Ruta de certificación	**Secuencia ordenada de certificados de entidades que, junto con la llave pública de la entidad inicial en la ruta, pueden ser procesadas para obtener la llave pública de la entidad final en la ruta.**
Servicios de validación del certificado	**Servicios proporcionados por la** CA **o su agente quien realiza la tarea de confirmar la validez de un** certificado **a una** parte que confía**.**
Solicitud de certificado	**Presentación a una** CA **por una** RA (o a la CA raíz por una CA)**, su agente o un sujeto, de una solicitud de registro validada para registrar la llave pública del sujeto que se colocará en un** certificado**.**
Solicitud de registro	**Presentación por parte de una entidad a una** RA **(o** CA**) para registrar la llave pública de la entidad en un certificado.**
Solicitud de servicio de validación	**Petición realizada por la** parte que confía **a un servicio de validación para comprobar la validez de un** certificado**.**
Sujeto	**Entidad cuya llave pública es certificada en un certificado de llave pública.**
Suscriptor	**Entidad que se suscribe con una** autoridad certificadora **a nombre de uno o más sujetos.**
Validez del certificado	**Aplicabilidad (apto para el uso previsto) y estado (activo, suspendido, revocado o expirado) de un** certificado**.**
Verificación de la firma	**Determinación y validación de:** **a) que la firma digital fue creada durante el período operacional de un certificado válido por la llave privada correspondiente a la llave pública que se encuentra en el** certificado**;** **b) que el mensaje no ha sido alterado desde que su firma digital fue creada.**

10.2 Abreviaturas:

Abreviatura	Descripción
CA	Autoridad Certificadora (CA por sus siglas en inglés Certificate Authority).
CAP	Comité Asesor de Políticas.
CP	Políticas de Certificado (CP por sus siglas en inglés Certificate Policy).
CPS	Declaración de prácticas de Certificación (CPS por sus siglas en inglés Certifcation Practice Statement).
CRL	Listas de revocación de Certificados (CRL por sus siglas en inglés Certificate Revocation List).
DCFD	Dirección de Certificadores de Firma Digital.
DNS	Sistema de nombres de dominio (Domain name system).
ECA	Ente Costarricense de Acreditación.
FIPS	Estándar para los dispositivos criptográficos (FIPS por sus siglas en inglés Federal Information Processing Standard).
HSM	Dispositivo criptográfico (HSM por sus siglas en inglés Hardware Security Module).
ISO	Organización Internacional para la Estandarización (ISO por sus siglas en inglés International Standards Organization).
LGAP	Ley General de Administración Pública.
MICIT	Ministerio de Ciencia y Tecnología.
NIC	Centro de información de redes de Internet en Costa Rica (NIC por sus siglas en inglés Network Information Center).
OCSP	Servicios de validación de certificados en línea (OCSP por sus siglas en inglés Online Certificate Status Protocol).
OEC	Organismo de Evaluación de la Conformidad.
OID	Identificador de Objeto (OID por sus siglas en inglés Object Identifier).
PDS	Declaración de divulgación PKI (PDS por sus siglas en inglés PKI Disclosure Statement).
PIN	Número de identificación Personal (PIN por sus siglas en inglés Personal Identification Number).
PKI	Infraestructura de llave pública (PKI por sus siglas en inglés Public Key Infraestructura).
RA	Autoridad de registro (RA por sus siglas en inglés Registration Authority).
RFC	Documento técnico aplicable que aún no es un estándar internacional (RFC por sus siglas en inglés Request for Comments).
RNP	Registro nacional de la propiedad.
TSA	Autoridad de sellado de tiempo (TSA por sus siglas en inglés Time Stamping Authority).
TSE	Tribunal Supremo de Elecciones.
URL	Localizador Uniforme de Recurso que permite asignar nombres a recursos en Internet (URL por sus siglas en inglés Uniform Resource Locutor).

Abreviatura	Descripción
UTC	**Tiempo Universal Coordinado (UTC por sus siglas en inglés (Universal Time Coordinated).**
X.509	**Estándar utilizado para estructuras de datos y algoritmos de validación en las infraestructuras de llave pública.**

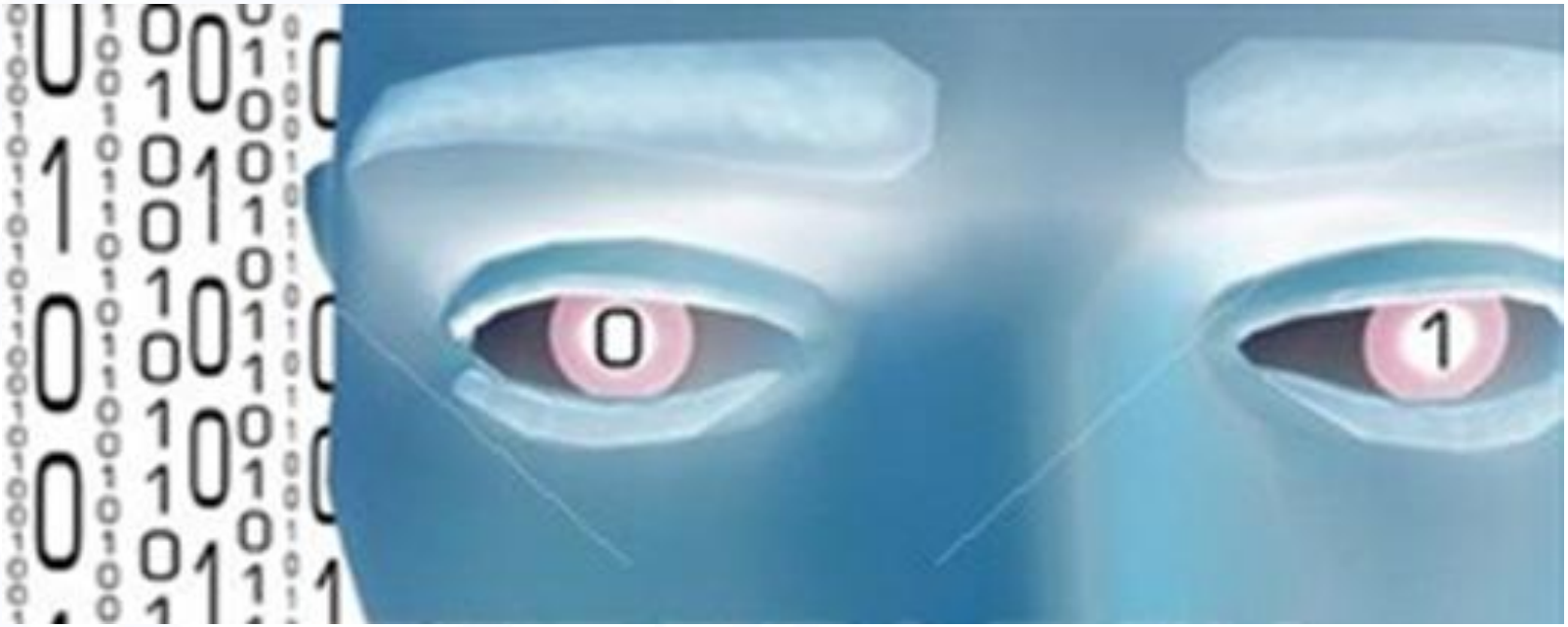
11. Anexo B: Documentos de referencia

Los siguientes documentos referenciados son aplicados para la confección de las políticas de certificación.

- RFC 3039 “Internet X.509 Public Key Infrastructure Qualified Certificates Profile.
- RFC 3280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- RFC2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”.
- RFC 3647: “Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework”.
- RFC 3161: “Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)”.
- RFC 3628: “Policy Requirements for Time-Stamping Authorities (TSAs)”.
- INTE-ISO-21188:2007 “Infraestructura de llave pública para servicios financieros — Estructura de prácticas y políticas.
- INTE-ISO/IEC 19011 “Directrices para la auditoría de sistemas de gestión de la calidad y/o ambiental”.
- ISO 3166 “Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países.
- INTE-ISO/IEC 17021 Evaluación de la conformidad — Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión.
- Ley 8454 “Ley de certificados, firmas digitales y documentos electrónicos” y su reglamento.

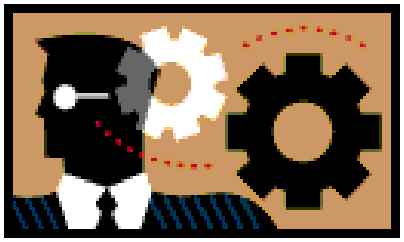
Documentos anexos:

- Política de sellado de tiempo del sistema nacional de certificación digital
- Directrices para las Autoridades de Registro. Características de cumplimiento de Autoridades de Registro (RA) de la jerarquía nacional de certificadores registrados de Costa Rica
- Guía para la autorización de una Autoridad Certificadora Emisora de la jerarquía nacional de certificadores registrados de Costa Rica



Sistema Nacional de Certificación Digital

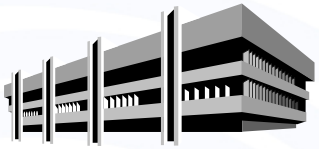
Temario



- El Sistema Nacional de Pagos - SINPE
- Aspectos legales relevantes
- Autoridad Certificadora Raíz y del Banco Central
- Certificación del ciudadano utilizando el Sistema Financiero
- Estrategia de masificación del uso de Certificados Digitales
- Certificación de usuarios y empleados de las Entidades Públicas
- Documento Nacional de Identidad Electrónica (DNIE)
- Equipamiento sugerido para firmar transacciones
- Tipos de certificados digitales
- Autenticando y Firmando transacciones en los sitios Web Institucionales
- Ejemplos del uso de la firma en diferentes aplicaciones
- Otros temas relacionados

Componentes del sistema de pagos de Costa Rica

Clientes:
- **Personas**
- **Empresas**



Cliente Origen

Relación privada

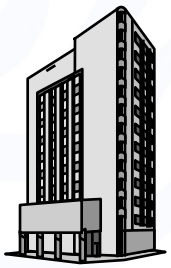
Clientes Destino

Clientes:
- **Personas**
- **Empresas**

Medios:
Sitios Web
Sucursales
Otros

Cuenta Cliente

- **Bancos**
- **Financieras**
- **Mutuales**
- **Cooperativas**
- **Casas de Cambio**
- **Puestos de Bolsa**
- **Fondos de Inversión**
- **Fondos de Pensiones**
- **Operadores de Tarjetas**
- **Instituciones Públicas**



Entidad Origen

sinpe

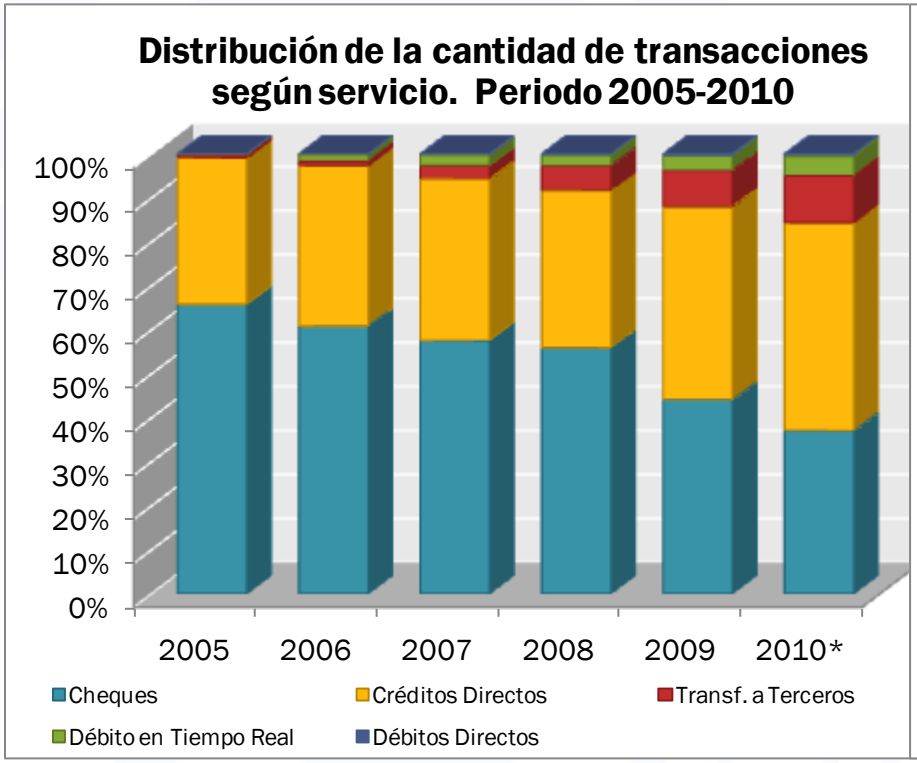
Entidades Destino

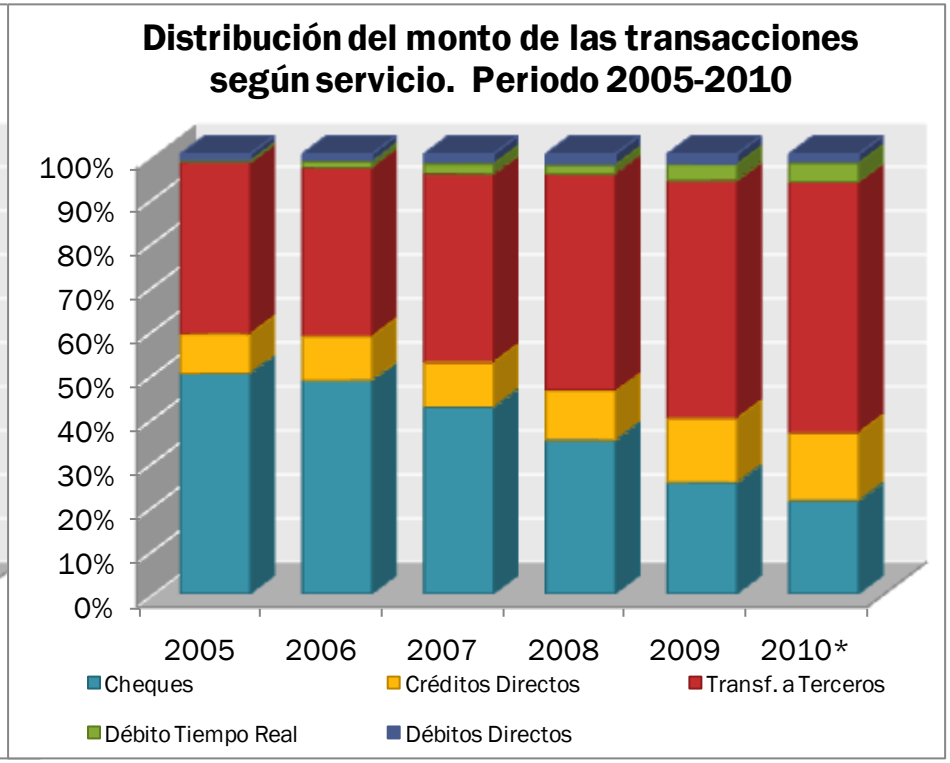
- **Bancos**
- **Mutuales**
- **Cooperativas**

Servicios:
- **Cámara de Cheques (Cobro)**
- **Transferencias en Tiempo Real (Pago)**
- **Débito en Tiempo Real (Cobro)**
- **Créditos Directos (Pago)**
- **Débito Directo (Cobro)**
- **MONEX**
- **Emisión de Certificados Digitales**

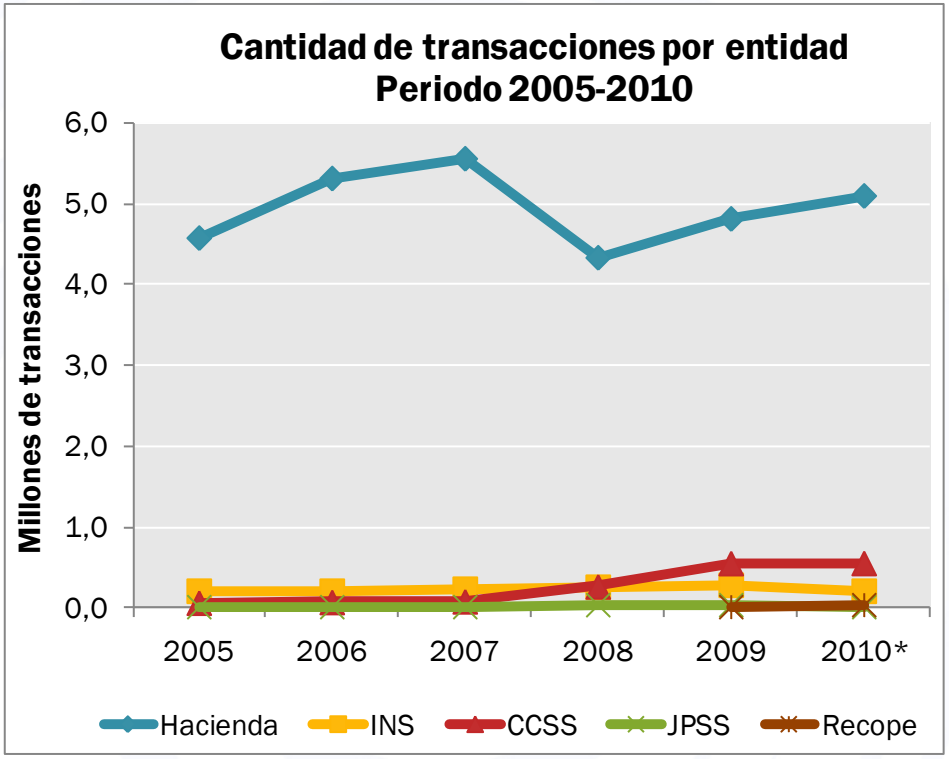
firmadigital

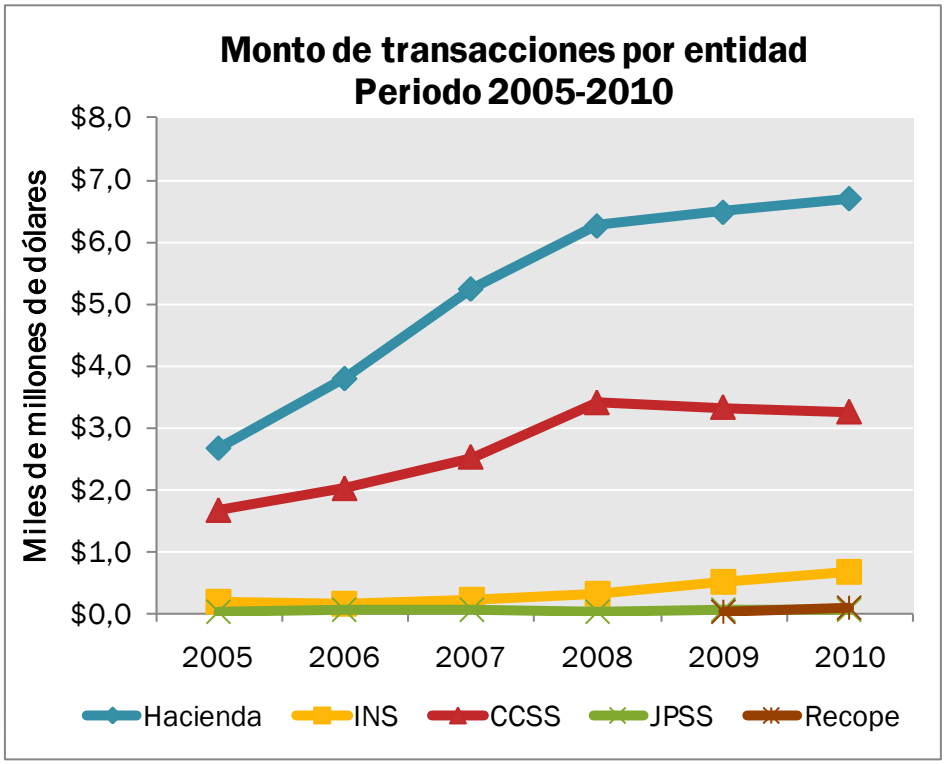
Evolución del SINPE:
Periodo 2005-2010





Entidades Públicas asociadas al SINPE





*Proyección 2010

Ley: Alcance de la Firma Digital

Valor Equivalente (art. 9):

"Los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito."

Presunción de autoría (art. 10)

"Todo documento […] asociado a una firma digital **certificada** se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital […]"

- ✓ **Identificación unívoca**
- ✓ **Vinculación jurídica**
- ✓ **Validez y eficacia probatoria**
- ✓ **Presunción de autoría**
- ✓ **No Repudio**

Sistema Nacional de Certificacion Digital

Estrategia: Certificados emitidos con la más alta calidad a un costo que permita su masificación

Oficinas de Registro

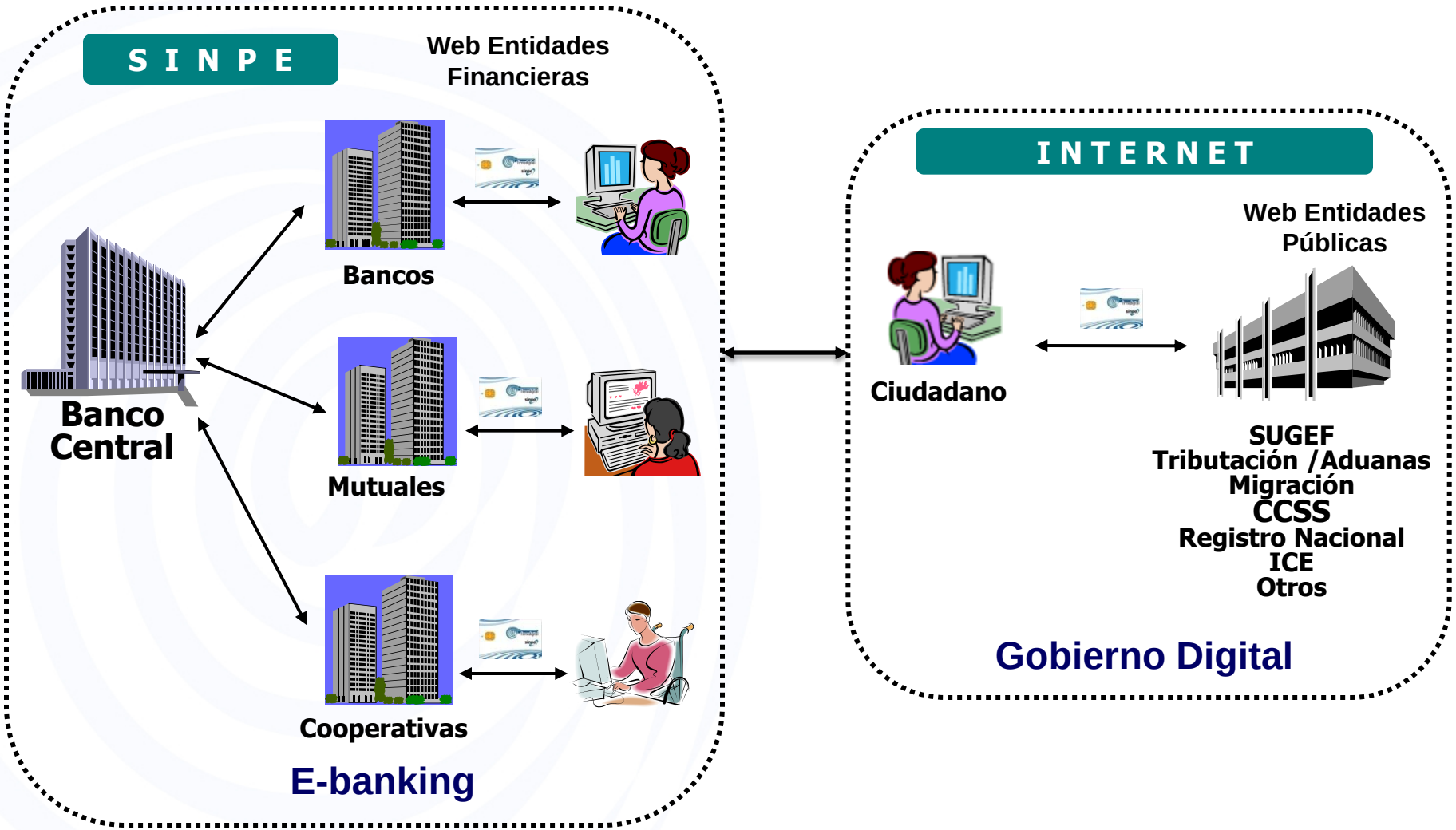
Activas: 16

- **Banco Popular: 4**
  - Oficina Central
  - Sucursal Oreamuno Cartago
  - Plaza Cristal
  - Cinco Esquinas de Tibás
- **Banco Nacional: 7**
  - Oficina Central
  - Gobierno Digital (4)
  - Cartago
  - Alajuela
- **Banco BCT: 1**
  - Oficina Central
- **Banco BAC SJ: 2**
  - Sucursal La Bandera
  - Guachipilín Escazú
- **Banco BCR: 1**
  - Oficina Central
- **BCCR: 1**
  - Edificio Principal

En proceso: 13

- **Banco Popular: 2**
  - Alajuela Este
  - Plaza Heredia
- **Banco Nacional: 5**
  - Heredia
  - Limón
  - Liberia
  - Puntarenas
  - Ciudad Quesada
- **Mutual Alajuela: 1**
  - Oficina Central
- **INS: 1**
  - Oficina Central
- **Banco Crédito Agrícola: 1**
  - Oficina San José
- **Coopenae: 1**
  - Oficina Central
- **Banco Lafise: 1**
  - Oficina Central
- **ATH: 1**
- Oficina Central

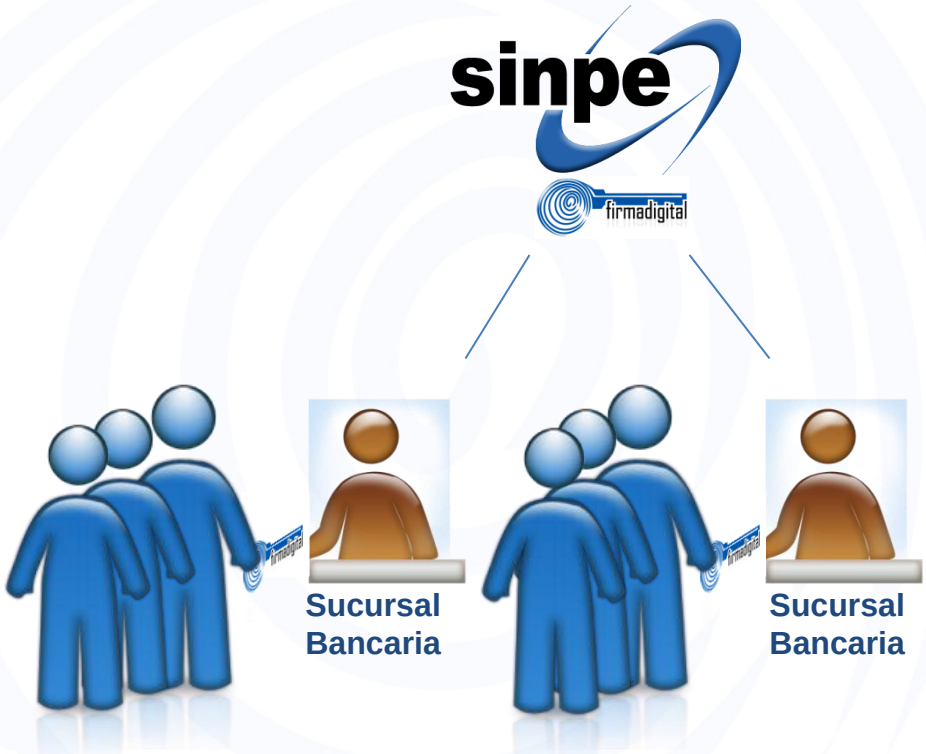
Estrategia Nacional de Certificación



¿Qué impulsa el uso de la firma?

Oferta

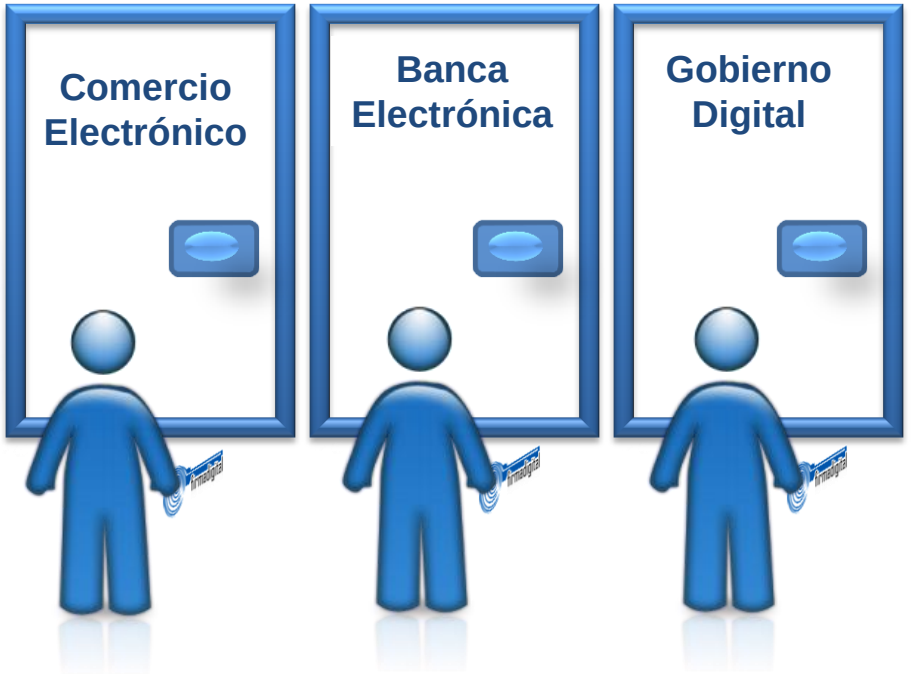
Capacidad de Entrega



Oficinas de Registro en Sucursales Bancarias

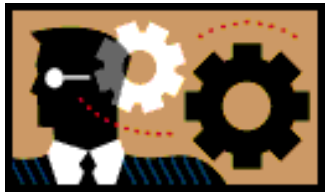
Demanda

- ✓ Nuevas Funcionalidades
- ✓ Seguridad Jurídica



Servicios que soportan certificados y firma digital

Utilización de la Firma Digital Certificada



En operación:

- Superintendencia de Valores (SUGEVAL)
- Banco Popular
- Municipalidad de San José
- Poder Judicial - Expedientes Judicial
- Hacienda – Compra Red
- ICE: Merlink
- Compañía Nacional de Fuerza y Luz: CNFL
- Banco Central – Central Directo

En construcción:

- Bancos y Superintendencias
- ICE: Sitios Web Institucionales
- Contraloría – Declaración de bienes, Presupuestos
- Comercio Exterior – Certificación de origen
- Hacienda: Tributación Digital, Tesoro Virtual, otros
- Colegio de Ingenieros y Arquitectos
- Otros

Sistema de solicitudes de Certificación

Solicitudes

1-222-111	C1
1-222-112	C2
1-333-111	C1
1-333-112	C3

Registro de Clientes
Entidad Asociada al SINPE
(Bancos. M.Hacienda, ICE, CCSS, INS, Otros Bancos…)

Oficina de Registro Banco X

Oficina de Registro Banco Y

Reglamento del SINPE:
- **Emisión c1.000**
- **Tarjeta c7.000**
- **Lector c10.000**

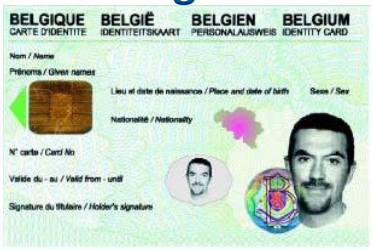
Estrategia de uso de tarjetas inteligentes como dispositivo contenedor del Certificado Digital

Tendencias en el mundo de las tarjetas

Documento de Identidad Electrónico

España

Bélgica



Finlandia

Estonia

Italia

Suecia

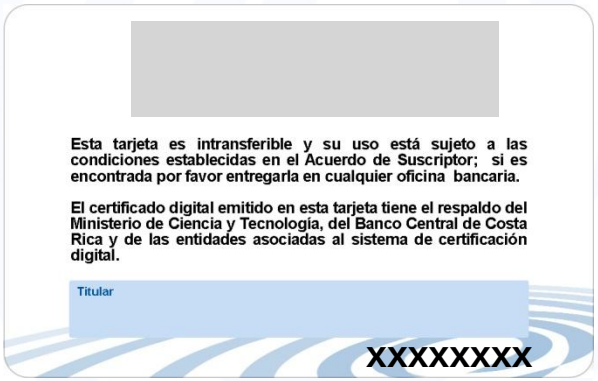
Costa Rica

(mediano plazo)

Estrategia de Corto Plazo

(TFD: Tarjeta de Firma Digital)

Anverso



Reverso

Dispositivos de Lectura

Beneficios de la Firma Digital para el ciudadano

Mayor confianza en las transacciones en línea:

- Provee alta seguridad jurídica y tecnológica
- Eliminación del riesgo de Phishing y cualquier otra técnica de robo electrónico de identidad

Comodidad o facilidad de uso:

- Una única clave para accesar cualquier Sitio Web Nacional

Disponibilidad de nuevos servicios ofrecidos por internet:

- Nuevas funcionalidades en Banca en línea, Gobierno digital y Comercio Electrónico
- Permite digitalizar cualquier trámite que requiera la firma manuscrita y ofrecerlo a través de Internet

Tipos de Certificados Digitales

Tipos de Certificados Digitales

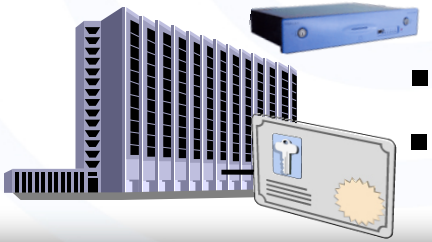
Certificado de Persona Física ✓

- Firma Digital y Autenticación de Personas Físicas
- Implementa Equivalencia Funcional con Firma Autógrafa

Certificado de Estampado de Tiempo (TimeStamping) ✓

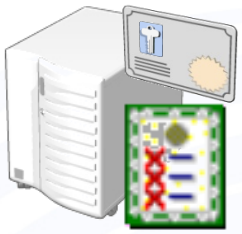
- Garantizar la existencia de una firma o un documento en el tiempo

Certificado de Agente Electrónico (en construcción)



- Firma Digital y Autenticación de Entidades
- Implementa Servicios Electrónicos Automatizados

Funcionamiento
Atributos de las personas (roles)

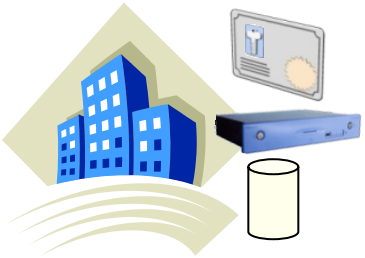


Servicio de listas de revocación

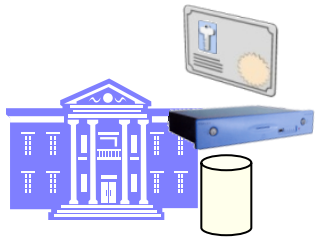
Servicio Sellado de Tiempo

Registro Nacional

...

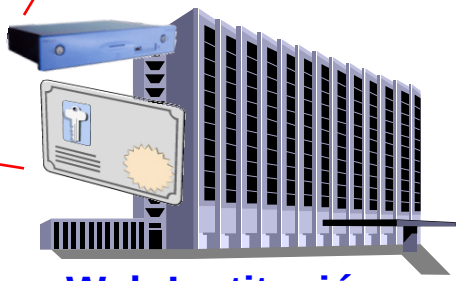


Colegio de Ingenieros



Dirección de Notariado

Internet



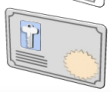
Web Institución Pública

Sitio Web

Ciudadano

Persona Física

Estampado de Tiempo



Agente Electrónico

Ejemplos de aplicación de la Firma Digital

Pagina Principal - Windows Internet Explorer

https://www.centraldirecto.fi.cr/sitio/cd/paginaprincipal.aspx

Live Search

File Edit View Favorites Tools Help

Pagina Principal

Page

CENTRAL DIRECTO

BANCO CENTRAL DE COSTA RICA

Ingrese con certificado digital

Suscríbase en Central Directo

Usuario

Clave de acceso

Ingresar

Problemas con su clave

VeriSign Secured VERIFICAR

BIENVENIDOS

a Central Directo, el portal Web de servicios financieros y de seguridad del Banco Central de Costa Rica

Inversiones

Consulte aquí las opciones de inversión disponibles.

Monex

Consulte aquí noticias y comunicados sobre el mercado cambiario costarricense.

Guías

Consulte aquí las guías sobre los servicios y funcionalidades de Central Directo

Noticias

Versiones de explorador compatibles con Central Di

Publicada: 13/10/2009

¡Muchas Gracias!