REPÚBLICA DE PANAMÁ
REGISTRO PÚBLICO DE PANAMÁ

RESOLUCIÓN No. DG- 039-2026
(De 9 de abril de 2026)

LA DIRECTORA GENERAL DEL REGISTRO PÚBLICO DE PANAMÁ
En uso de sus facultades legales,

CONSIDERANDO:

Que, según el artículo 1 de la Ley No. 82 de 9 de noviembre de 2012, se otorgan al Registro Público de Panamá las atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá;

Que, según numeral 1 del artículo 4 de la Ley No. 82 de 9 de noviembre de 2012 es función de la Dirección Nacional de Firma Electrónica elaborar y recomendar a la Junta Directiva y al Director General los reglamentos, resoluciones y demás documentos técnicos que considere necesarios para el desarrollo de las materias de su competencia;

Que la Ley No. 51 de 22 de julio de 2008, modificada por la Ley No. 82 de 9 de noviembre de 2012, establece el marco jurídico aplicable a las firmas electrónicas y otorga al Registro Público de Panamá, las atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá;

Que el artículo 17, numeral 2, de la Ley No. 51 de 22 de julio de 2008, modificada por la Ley No. 82 de 9 de noviembre de 2012; establece que los certificados emitidos por prestadores de servicios de certificación de firmas electrónicas extranjeros podrán ser reconocidos cuando estos sean emitidos por prestadores debidamente avalados en su país de origen por instituciones homólogas a la Dirección Nacional de Firma Electrónica del Registro Público, que requieran para su reconocimiento estándares que garanticen la seguridad en la creación del certificado, la regularidad de los detalles del certificado, así como su validez y vigencia;

Que el Registro Público de Panamá y el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de la República de Costa Rica suscribieron un Convenio de cooperación sobre la homologación de la firma digital certificada, cuyo objeto es promover la cooperación entre las Partes para el reconocimiento de la firma digital certificada y la firma electrónica calificada, en cumplimiento con las regulaciones de cada una de las Partes y sin contravenir el ordenamiento jurídico interno de cada Estado;

Que, en virtud del citado instrumento de cooperación, las Partes han convenido en homologar y reconocer recíprocamente como legalmente válidos, otorgándoles idéntico valor jurídico y fuerza probatoria, los certificados correspondientes a la firma digital certificada y a la firma electrónica calificada emitidos por las autoridades certificadoras de cada Parte, siempre que estos cumplan con los estándares técnicos internacionalmente aceptados. Asimismo, las Partes acuerdan asegurar la interoperabilidad de los sistemas, así como la compatibilidad de la arquitectura e infraestructura vinculadas al objeto del convenio, condicionadas a su respectiva viabilidad técnica, de modo que la validación de las firmas pueda efectuarse mediante las herramientas disponibles en cada una de ellas.

Que, conforme al Convenio suscrito, la firma electrónica calificada en la República de Panamá y la firma digital certificada en la República de Costa Rica, serán consideradas equivalentes únicamente para los fines de cooperación y reconocimiento recíproco previstos en dicho instrumento, sin perjuicio de las disposiciones legales internas de cada Estado;

Que el reconocimiento recíproco de certificados digitales emitidos en ambos países contribuye al fortalecimiento de la confianza digital, la facilitación de las transacciones electrónicas y la cooperación técnica entre ambas Partes;

RESUELVE:

PRIMERO: Reconocer, para efectos de homologación y de conformidad con las condiciones establecidas en el Convenio de cooperación suscrito, la validez de la firma digital certificada emitida por los certificadores registrados y debidamente autorizados por la Dirección de Gobernanza Digital y Certificadores de Firma Digital del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de la República de Costa Rica, otorgándole igual valor jurídico y fuerza probatoria, siempre que se cumplan los términos y condiciones previstos en dicho instrumento.

SEGUNDO: Establecer que el reconocimiento dispuesto en la presente Resolución estará condicionado al cumplimiento de los requisitos técnicos, operativos y de validación previstos en el Convenio de cooperación, incluyendo la observancia de estándares internacionales aplicables y los mecanismos de verificación de la autenticidad, integridad y vigencia de los certificados digitales.

TERCERO: Disponer que la Dirección Nacional de Firma Electrónica del Registro Público de Panamá coordinará con la autoridad competente de la República de Costa Rica la adopción e implementación progresiva de las medidas técnicas y administrativas necesarias para garantizar el reconocimiento, la interoperabilidad y la adecuada validación de los certificados digitales, conforme a lo establecido en el Convenio.

CUARTO: Advertir que el reconocimiento otorgado mediante la presente Resolución permanecerá vigente mientras se mantenga en vigor el Convenio de cooperación suscrito entre las Partes y subsistan las condiciones técnicas que permitan la validación efectiva de los certificados digitales emitidos por las autoridades certificadoras correspondientes.

QUINTO: Ordenar la publicación de la presente Resolución en la Gaceta Oficial de la República de Panamá, así como en los medios de divulgación institucional del Registro Público de Panamá, para su debida promulgación y conocimiento público.

FUNDAMENTO DE DERECHO: Ley No. 3 de 6 de enero de 1999, Ley No. 51 de 22 de julio de 2008, Ley No. 82 de 9 de noviembre de 2012, Decreto Ejecutivo No. 684 de 18 de octubre de 2013, Decreto Ejecutivo No. 83 de 23 de marzo de 2023, Ley No. 10 de 20 de enero de 2003 y el Convenio entre el Registro Público de Panamá y el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de la República de Costa Rica,

Dado en la ciudad de Panamá, a los nueve (9) días del mes de abril de dos mil veintiséis (2026).

NOTIFÍQUESE, PUBLÍQUESE Y CÚMPLASE.

NAIROBIA ESCRUCERIA
Directora General de Registro Público de Panamá

REGISTRO PÚBLICO DE PANAMÁ
SECRETARÍA GENERAL

ESTE DOCUMENTO ES FIEL COPIA DEL ORIGINAL
9 abril 2026
FECHA
SECRETARIA GENERAL

CONVENIO ENTRE EL REGISTRO PÚBLICO DE LA REPÚBLICA DE PANAMÁ, Y EL MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES DE LA REPÚBLICA DE COSTA RICA, SOBRE COOPERACIÓN EN LA HOMOLOGACIÓN DE LA FIRMA DIGITAL CERTIFICADA.

Entre los suscritos a saber: **NAIROBIA ELIBETH ESCRUCERÍA GONZÁLEZ**, mujer, panameña, mayor de edad, con cédula de identidad personal No. 8-711-362, actuando en su condición de Directora General del **REGISTRO PÚBLICO DE PANAMÁ**, debidamente facultada mediante la Ley No. 3 de 6 de enero de 1999, y designada mediante Decreto Ejecutivo No. 175 de 2 de julio de 2024, por una parte, y por la otra **PAULA BOGANTES ZAMORA**, mujer, costarricense, mayor de edad, , portadora de la cédula de identidad No. 1-858-771, en su condición de **MINISTRA DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES**, nombrada por medio del Acuerdo Presidencial No.194-P, publicado en el Diario Oficial La Gaceta N° 26 de fecha 13 de febrero de 2023, quienes de manera individual se denominarán "la Parte" y de forma conjunta "las Partes", han convenido en celebrar el presente **CONVENIO**, bajo las siguientes condiciones y cláusulas:

CONSIDERANDO:

Que, mediante la Ley No. 3 de 6 de enero de 1999, se creó el **REGISTRO PÚBLICO DE PANAMÁ**, como una entidad autónoma con personería jurídica, patrimonio propio, autonomía en su régimen interno, tanto administrativo y funcional, como presupuestario y financiero, cuya función principal es la inscripción, seguridad y publicidad de los documentos que, de conformidad con la ley, requieran tal formalidad;

Que, mediante la Ley No. 82 de 9 de noviembre de 2012, se otorga al Registro Público de Panamá atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá y se modifica la Ley No. 51 de 22 de julio de 2008, la cual establece el marco regulatorio para la creación de firmas electrónicas, entre otras disposiciones;

Que, el **MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES**, en su calidad de ente rector del sector en Costa Rica, actúa conforme a las atribuciones y competencias establecidas en la Ley N.° 7169, Ley de Promoción del Desarrollo Científico y Tecnológico y creación del Ministerio de Ciencia y Tecnología (MICYT).





MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES
GOBIERNO DE COSTA RICA

Que, la Dirección de Gobernanza Digital y Certificadores de Firma Digital (DGDCFD) de este ministerio, de acuerdo con el artículo 23 de la Ley N.° 8454, Ley de Certificados, Firmas Digitales y Documentos Electrónicos, funge como órgano administrador y supervisor del Sistema Nacional de Certificación Digital. Por lo que, en virtud de lo anterior, la DGDCFD tiene a su cargo todas las funciones relacionadas con la firma digital certificada en Costa Rica, conforme a lo dispuesto en dicho artículo: "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".

Que, el Convenio Básico de Cooperación Técnica y Científica entre el Gobierno de la República de Costa Rica y el Gobierno de la República de Panamá, suscrito en la ciudad de Bambito, Chiriquí, República de Panamá, el 29 de noviembre del 2001 y ratificado por Costa Rica mediante la ley N° 8889, número de gaceta 241, del 13 de diciembre del 2010 y entrado en vigencia el 13 de diciembre 2010, y aprobado por parte de Panamá mediante la Ley No. 10 de 20 de enero de 2003, publicada en la Gaceta Oficial N.º 24726 de 24 de enero de 2003, se establece en su artículo primero lo siguiente:

> *"1. El presente Convenio tiene como objetivo promover la cooperación técnica y científica entre ambos países, a través de la formulación y ejecución, de común acuerdo, de programas y proyectos en dichas áreas.*
> *2. En la elaboración de estos programas y proyectos, las Partes tomarán en consideración las prioridades establecidas en sus respectivos planes de desarrollo y apoyarán la participación, en su ejecución, de organismos y entidades de los sectores público, privado y social, así como de las universidades, instituciones de investigación científica y técnica y organizaciones no gubernamentales.*
> *Asimismo, las Partes deberán tomar en consideración, la importancia de la ejecución de proyectos nacionales de desarrollo y se favorecerá la instrumentalización de proyectos conjuntos de desarrollo tecnológico, que vinculen centros de investigación con entidades industriales de los dos países.*
> *3. Las Partes podrán, con base en el presente Convenio, celebrar Acuerdos complementarios de cooperación técnica y científica, en áreas específicas de interés común, que formarán parte integrante del presente Convenio."*

Que, para efectos del presente Convenio, se entiende que la "firma electrónica calificada" en la República de Panamá y la "firma digital certificada" en la República de Costa Rica serán consideradas como equivalentes, únicamente para los fines de la cooperación y del reconocimiento recíproco previstos en este convenio, sin perjuicio de las disposiciones legales internas de cada Estado;

Que ambas partes reconocen la importancia de la implementación de la firma digital transfronteriza como un instrumento que contribuye a incrementar la eficiencia, la competitividad y a promover el desarrollo de los países que representan;

Que ambas Partes respetan los principios de igualdad y beneficio mutuo;

Que ambas Partes desean profundizar y desarrollar la cooperación en la validación de la firma digital certificada y la firma electrónica calificada, con la visión de agilizar procesos de diversa índole entre ellas;

Que ambas Partes están convencidas de que la cooperación en materia de firma digital certificada, firma electrónica calificada, y procesos de verificación, así como la facilitación de las transacciones electrónicas transfronterizas y la interacción electrónica entre las personas, contribuirá al desarrollo de ambos países;

POR LO TANTO, y en atención a las consideraciones anteriores, LAS PARTES acuerdan lo siguiente:

PRIMERA: OBJETO.

El presente Convenio tiene como objeto promover la cooperación entre las Partes para el reconocimiento de la firma digital certificada y firma electrónica calificada para su homologación, en cumplimiento con las regulaciones de cada una de las Partes, sin contravenir el respectivo ordenamiento jurídico interno.

SEGUNDA: ALCANCE DE LA COOPERACIÓN.

Las áreas de cooperación en virtud del presente convenio podrán incluir:

(a) Equivalencia técnica de las Infraestructuras de Clave Pública;
(b) Reconocimiento de la firma digital certificada o firma electrónica calificada emitidas por las autoridades certificadoras de cada una de las Partes, que cumplan con los estándares técnicos requeridos;
(c) Interoperabilidad, estándares, arquitectura e infraestructura vinculadas al objeto del presente convenio; cuya implementación estará sujeta a la viabilidad técnica de las Partes, de forma que la validación de la firma digital certificada y firma electrónica calificada se pueda realizar sino haciendo uso de las herramientas con que ya dispone cada Parte para tal efecto.
(d) Estrategias de adopción, monitoreo y evaluación;

(e) Colaboración entre los países, intercambiando conocimiento, herramientas e investigación; y
(f) Cualquier otra área que pueda ser determinada en forma conjunta por las Partes.

TERCERA: FORMAS DE COOPERACIÓN.

Las formas de cooperación contempladas por este Convenio podrán incluir:

(a) Intercambio de especialistas y científicos;
(b) Utilización de equipo e instalaciones;
(c) Intercambio de información, documentación y experiencias;
(d) Transferencia de conocimiento y prestación de asistencia técnica;
(e) Estudio, preparación y ejecución de proyectos técnicos;
(f) Organización de exposiciones, seminarios y conferencias;
(g) Cualquier otra modalidad acordada por las Partes.

Cualquier modalidad de cooperación por implementar en virtud del presente Convenio será determinada de forma conjunta, y estará sujeta a la disponibilidad de fondos y del personal apropiado de cada una de las Partes.

CUARTA: DEL RECONOCIMIENTO

El Registro Público de la República de Panamá, a través de la Dirección Nacional de Firma Electrónica, homologa y reconoce como legalmente válidos y otorga el mismo valor jurídico y probatorio a los certificados de firma digital certificada emitidos por los Certificadores Registrados, debidamente autorizados por la Dirección de Gobernanza Digital y Certificadores de Firma Digital (DGDCFD) del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de la República de Costa Rica.

El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de la República de Costa Rica, a través de la Dirección de Gobernanza Digital y Certificadores de Firma Digital (DGDCFD) homologa y reconoce como legalmente válidos y otorga el mismo valor jurídico y probatorio a los certificados de firma electrónica calificada emitidos por los Prestadores de Servicios de Certificación, debidamente autorizados por la Dirección Nacional de Firma Electrónica del Registro Público de la República de Panamá.

El reconocimiento recíproco se atenderá siempre que se reúnan las siguientes condiciones:

a. Que respondan a estándares reconocidos internacionalmente, conforme lo establezca la autoridad designada por las Partes.

b. Que contengan como mínimo, datos que permitan:

   i. Identificar inequívocamente a su titular y al prestador de servicios de certificación que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;
   ii. Ser susceptible de verificación respecto de su estado de revocación;
   iii. Detallar la información verificada incluida en el certificado digital;
   iv. Contemplar la información necesaria para la verificación de la firma;
   v. Identificar la política de certificación bajo la cual fue emitido.

Las Partes se comprometen a intercambiar en virtud del presente convenio, el listado de los Certificadores Registrados y de los Prestadores de Servicios de Certificación que se encuentren autorizados dentro de los respectivos países, así como a informar cualquier cambio que se produzca en dicho listado.

QUINTO: IMPLEMENTACIÓN

A los efectos de la implementación del presente Convenio, se realizarán las siguientes acciones:

(a) Estudio e intercambio de las Políticas de certificación implementadas por los países para la homologación de los certificados digitales entre las Partes, así como la elaboración de un Informe de equivalencia de dichas políticas.
(b) Evaluación de requerimientos técnicos observados en el ciclo de vida del certificado digital.
(c) Evaluación de requerimientos técnicos para el intercambio de listas de revocación de certificados de firma digital o firmas electrónicas calificadas a los efectos de ser contemplados por las herramientas de validación de firma en los respectivos países.
(d) Intercambio de documentos y herramientas vinculados a la firma digital certificada o firma electrónica calificada.
(e) Publicación de los certificados raíz y subordinados vigentes, en las páginas oficiales de la Dirección de Gobernanza Digital y Certificadores de Firma Digital (DGDCFD) del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de la República de Costa Rica y de la Dirección Nacional de Firma Electrónica del Registro Público de la República de Panamá.

Cualquier actividad por implementarse en virtud del presente Convenio será determinada de manera conjunta y cursada formalmente conforme las direcciones de correo electrónico consignadas en este Convenio y estará sujeta a la disponibilidad de fondos y del personal apropiado.

Para esto, las Partes podrán elaborar un cronograma de trabajo conjunto de las actividades a desarrollar para la homologación de la firma digital certificada o firma electrónica calificada, observando los principios estipulados en el presente convenio. Salvo disposición en contrario, de común acuerdo cada Parte asumirá los gastos en los que incurra por concepto de las actividades de cooperación en virtud del presente instrumento.

El personal asignado por cada una de las Partes para la ejecución de las acciones de cooperación, al amparo del convenio, continuará bajo la dirección y dependencia de la institución a la que pertenezca, por lo que no se crearán relaciones de carácter laboral con la otra Parte.

Las oficinas encargadas de la firma digital certificada o firma electrónica calificada, así como los de asuntos internacionales de las Partes servirán de puntos focales en la ejecución de las actividades de cooperación identificadas en este Convenio.

Las notificaciones que se deriven de este convenio tendrán validez cuando sean remitidas por correo físico o electrónico a las siguientes direcciones:

COSTA RICA

Dirección de Gobernanza Digital y Certificadores de Firma Digital
gobernanzadigital@micitt.go.cr
firmadigital@micitt.go.cr

Unidad de Cooperación Internacional
ucimicit@micitt.go.cr

Dirección física: Costa Rica, San José, Zapote, 400 metros oeste de Casa Presidencial Edificio Mira, piso 1 y 2.

PANAMÁ

Dirección Nacional de Firma Electrónica
servicios@firmaelectronica.gob.pa

Dirección física: Vía España, edificio Registro Público, San Francisco Ciudad de Panamá.

SEXTO: CONFIDENCIALIDAD Y PROPIEDAD INTELECTUAL.

Ninguna de las Partes divulgará a terceros información proporcionada por la otra Parte durante la implementación de este convenio, sin el consentimiento previo y por escrito de la otra Parte.

La propiedad intelectual desarrollada en virtud de este convenio será propiedad conjunta de las Partes y se otorgarán mutuamente una licencia gratuita, ilimitada y perpetua para la producción, publicación y uso de dicha información o productos, otorgando el reconocimiento correspondiente de quienes hayan intervenido en la ejecución de dichos trabajos.

En el curso de la realización de las actividades previstas en este convenio, en caso de que una de las Partes requiera utilizar la propiedad intelectual que pertenece a la otra, deberá obtener previamente su consentimiento formal en las direcciones de correo electrónico que correspondan establecidas en el ordinal quinto, y cumplir con las instrucciones y requisitos razonables para su uso. Todo tratamiento relativo a la propiedad intelectual será regido por la legislación aplicable de las Partes.

SÉPTIMO: SOLUCIÓN DE CONTROVERSIAS.

Cualquier controversia que surja con motivo de la aplicación o interpretación de este convenio, de los acuerdos complementarios o del intercambio de correspondencia oficial vinculada al mismo, deberá resolverse mediante negociación directa y amistosa entre las Partes. Si el asunto no pudiera ser solucionado en un tiempo razonable, deberá ser escalado internamente por las Partes para su resolución. De persistir la controversia, las Partes acuerdan someterla a mediación ante un tercero neutral o a otro mecanismo alternativo de resolución de conflictos que determinen por escrito.

En todo caso, la aplicación, interpretación y ejecución de este Convenio deberá realizarse de buena fe.

OCTAVO: RESPONSABILIDAD DE LAS PARTES.

Atendida la naturaleza del presente Convenio, cuyo propósito es explorar y promover vínculos de cooperación y asistencia entre las Partes, estas acuerdan que actuarán de buena fe en la consecución de dicho propósito. En el evento en que las Partes no logren consensuar actividades de cooperación, o que las mismas resulten insuficientes para alcanzar los objetivos previstos, las Partes acuerdan que no se genera responsabilidad de ningún tipo.

MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES
GOBIERNO DE COSTA RICA

NOVENO. DISPOSICIONES GENERALES.

Este Convenio tiene como base legal el Convenio básico de cooperación técnica y científica entre el Gobierno de la República de Costa Rica y el Gobierno de la República de Panamá, suscrito en la ciudad de Bambito, República de Panamá, el 29 de noviembre del 2001.

Este Convenio entrará en vigor en la fecha de la última firma y continuará en vigencia por un período de cuatro (4) años, prorrogables automáticamente, salvo que una de las Partes notifique por escrito a la otra Parte su solicitud de finalización con al menos tres (3) meses de antelación a la fecha en que se requiere el cierre.

El vencimiento o finalización de este convenio no afectará la validez o duración de cualquier programa y actividad en curso realizados bajo este convenio, salvo decisión conjunta acordada por las Partes.

Este Convenio no crea ninguna obligación legal y no es vinculante bajo la legislación internacional. No obstante, las Partes acuerdan que cualquier controversia será resuelta conforme a lo previsto en el ordinal séptimo, y que toda actuación se realizará de buena fe.

En prueba de conformidad, se firman 2 (dos) ejemplares de un mismo tenor y contenido, a un mismo efecto.

Por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de la República de Costa Rica

Paula Bogantes Zamora
Ministra de Ciencia, Innovación, Tecnología y Telecomunicaciones
En la ciudad de San José, Costa Rica
Fecha: 23-03-2026

Por el Registro Público de Panamá de la República de Panamá

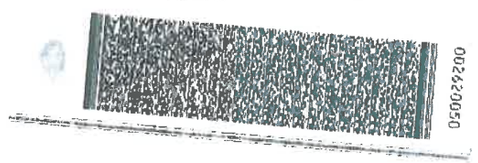
Nairobia E. Escrucería González
Directora General, Registro Público de Panamá
En la ciudad de Panamá, Panamá
Fecha: 11-3-2026


REPÚBLICA DE COSTA RICA
Tribunal Supremo de Elecciones
Cédula de Identidad

1 0858 0771

Nombre: PAULA
1° Apellido: BOGANTES
2° Apellido: ZAMORA
C.C:

Número de Cédula: 1 0858 0771
Fecha de Nacimiento: 24 07 1973
Lugar de Nacimiento: CATEDRAL CENTRAL SAN JOSE
Nombre del Padre: CARLOS LUIS BOGANTES HIDALGO
Nombre de la Madre: NURIA ZAMORA ROJAS
Domicilio Electoral: GUACHIPELIN ESCAZU SAN JOSE
Vencimiento: 04 02 2030



Diario Oficial
LA GACETA
Costa Rica
145 años

JORGE EMILIO CASTRO FONSECA (FIRMA)
Firmado digitalmente por JORGE EMILIO CASTRO FONSECA (FIRMA)
Fecha: 2023.02.10 14:51:16 -06'00'

Imprenta Nacional
Costa Rica

La Uruca, San José, Costa Rica, lunes 13 de febrero del 2023

AÑO CXLV | Nº 26 | 92 páginas

Imprenta Nacional
Costa Rica

INFORMA

Ubicación y horarios de nuestras oficinas

Sucursal la Uruca:
Horario: de 8:00 a.m. a 3:30 p.m., jornada continua.
Dirección: de la Bomba UNO, contiguo a Capris, 100 metros Sur y 100 metros Oeste.

Sucursal Curridabat:
Horario: de 8:00 a.m. a 12:00 p.m. y de 1:00 p.m. a 3:30 p.m. (cerrado de 12:00 p.m. a 1:00 p.m.)
Dirección: en las instalaciones del Registro Nacional.

Le recordamos que puede realizar sus trámites y consultas en línea, sin necesidad de trasladarse a la Imprenta Nacional:

www.imprentanacional.go.cr

Aplicación móvil
Imprenta Nacional

privadas, la producción de programas de radio y televisión que apoyen el plan de estudios en los diferentes ciclos educativos y las actividades culturales a nivel nacional.

Rige a partir de su publicación.

Priscilla Vindas Salazar — Rocío Alfaro Molina

Sofía Alejandra Guillén Pérez — Andrés Ariel Robles Barrantes

Jonathan Jesús Acuña Soto — Antonio José Ortega Gutiérrez

Diputadas y diputados

NOTA: Este proyecto aún no tiene comisión asignada.

1 vez.—Exonerado.—(IN2023715559).

PODER EJECUTIVO

ACUERDOS

PRESIDENCIA DE LA REPÚBLICA

N° 194-P

EL PRESIDENTE DE LA REPÚBLICA

Con fundamento en las facultades que le confiere el artículo 139, inciso 1) de la Constitución Política.

ACUERDA:

Artículo 1º—Nómbrese como Ministro de Gobierno a:

- Paula Bogantes Zamora, cédula de identidad 1 0858 0771, como Ministra de Ciencia, Innovación, Tecnología y Telecomunicaciones.

Artículo 2º—Rige a partir del seis de febrero del dos mil veintitrés.

Dado en San José, a los seis días del mes de febrero del dos mil veintitrés.

RODRIGO CHAVES ROBLES.—1 vez.—O.C. N° 46000 71069.—Solicitud N° MICITT-01.—(IN2023715724).

MINISTERIO DE EDUCACIÓN PÚBLICA

N° 0002-2023-AC-MEP

EL PRESIDENTE DE LA REPÚBLICA
Y LA MINISTRA DE EDUCACIÓN PÚBLICA

En ejercicio de las atribuciones conferidas por los artículos 140 inciso 3), 8) y 18), 146 de la Constitución Política; los artículos 25 inciso 1), 27 inciso 1), 28 inciso 2) acápite b, de la Ley General de la Administración Pública, Ley N° 6227 del 2 de mayo de 1978; los artículos 5° y el 6° inciso a) del Decreto Ejecutivo N° 34276, Reglamento de la Organización y funcionamiento de la Comisión Costarricense de Cooperación con la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO).

Considerando:

I.—Que de conformidad con el artículo 5° del Decreto Ejecutivo N° 34276 del 5 de noviembre de 2007, denominado: Reglamento de la Organización y funcionamiento de la Comisión Costarricense de Cooperación con la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), establece que el Comité Ejecutivo es el órgano gubernativo superior de la Comisión, quien dictará los parámetros de acción de la Secretaría General de la entidad.

II.—Que de conformidad con el artículo 6° inciso a) del Decreto Ejecutivo N° 34276 del 5 de noviembre de 2007, denominado: Reglamento de la Organización y funcionamiento de la Comisión Costarricense de Cooperación con la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), establece que para la elección de las representaciones de los Integrantes del Comité Ejecutivo se seguirán las siguientes reglas: a) Las representaciones de los Jerarcas Ministeriales, se designarán mediante acuerdo del Poder Ejecutivo.

III.—Que de conformidad, con lo indicado en la Ley de Adhesión a la UNESCO, número 758 del 11 de octubre de 1949, se establece en su artículo 2° que *"El Estado integrará,* ***por medio del Ministerio de Educación Pública****, una Comisión Nacional encargada de asociar al trabajo de la Organización los principales cuerpos e institutos del país, cuyas actividades comprendan materias educativas, científicas o culturales"*.

IV.—Que mediante oficios C.C.C.U.02-2022 al Ministerio de Cultura y Juventud; C.C.C.U.031-2022 al Ministerio Ciencia, Innovación, Tecnología y Telecomunicaciones; C.C.C.U.033-2022 al Ministerio de Ambiente y Energía y al Ministerio de Relaciones Exteriores y Culto, la Secretaria General de la Comisión Costarricense de Cooperación con la UNESCO, solicita la designación de las representaciones de los Jerarcas Ministeriales ante el Comité Ejecutivo de la Comisión Costarricense de Cooperación con la UNESCO.

V.—Que mediante oficio DM-2154-2022 de fecha 19 de julio de 2022, el señor Arnoldo André Tinoco, Ministro de Relaciones Exteriores y Culto, informa que se mantiene la designación como representante del Ministerio de Relaciones Exteriores y Culto ante el Comité Ejecutivo de la Comisión Costarricense de Cooperación con la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), a la señora María Gabriela Castillo García, cédula de identidad número 9-0078-0850.

VI.—Que mediante oficio MICIT-DM-OF-412-2022 de fecha 06 de junio de 2022, el señor Carlos Enrique Alvarado Briceño, Ministro Ciencia, Innovación, Tecnología y Telecomunicaciones, informa que se mantiene la designación como representante del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, ante el Comité Ejecutivo de la Comisión Costarricense de Cooperación con la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), a la señora Eliana Ulate Brenes, cédula de identidad número 110910596.

VII.—Que mediante oficio MCJ-DM-0991-2022 de fecha 02 de setiembre de 2022, la señora Nayuribe Guadamuz Rosales, Ministra de Cultura y Juventud, informa la designación como representante del Ministerio de Cultura y Juventud, ante el Comité Ejecutivo de la Comisión Costarricense de Cooperación con la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), a la señora Patricia Soto Ramos, cédula de identidad número 502910005, en sustitución del señor Javier Carvajal Molina.

LEY Nº 10
(De 20 de enero de 2003)

Por la cual se aprueba el **CONVENIO BASICO DE COOPERACION TECNICA Y CIENTIFICA ENTRE EL GOBIERNO DE LA REPUBLICA DE PANAMA Y EL GOBIERNO DE LA REPUBLICA DE COSTA RICA**, suscrito en Bambito, República de Panamá, el 29 de noviembre de 2001

LA ASAMBLEA LEGISLATIVA
DECRETA:

Artículo 1. Se aprueba, en todas sus partes, el **CONVENIO BASICO DE COOPERACION TECNICA Y CIENTIFICA ENTRE EL GOBIERNO DE LA REPUBLICA DE PANAMA Y EL GOBIERNO DE LA REPUBLICA DE COSTA RICA**, que a la letra dice:

CONVENIO BASICO DE COOPERACION TECNICA Y CIENTIFICA ENTRE EL GOBIERNO DE LA REPUBLICA DE PANAMA Y EL GOBIERNO DE LA REPUBLICA DE COSTA RICA

El Gobierno de la República de Panamá y el Gobierno de la República de Costa Rica, en adelante denominados "las Partes",

ANIMADOS por el deseo de fortalecer los tradicionales lazos de amistad existentes entre ambos países;

CONSCIENTES de su interés común por promover y fomentar el progreso técnico y científico y de las ventajas recíprocas que resultarían de una cooperación en campos de interés mutuo;

CONVENCIDOS de la importancia de establecer mecanismos que contribuyan al desarrollo de ese proceso y de la necesidad de ejecutar programas de cooperación técnica y científica, que tengan efectiva incidencia en el avance económico y social de sus respectivos países;

Ambas Partes han convenido lo siguiente:

ARTICULO I

1. El presente Convenio tiene como objetivo promover la cooperación técnica y científica entre ambos países, a través de la formación y ejecución, de común acuerdo, de programas y proyectos en dichas áreas.

2. En la elaboración de estos programas y proyectos, las Partes tomarán en consideración las prioridades establecidas en sus respectivos planes de desarrollo y apoyarán la participación, en su ejecución, de organismos y entidades de los sectores público, privado y social, así como de las universidades, instituciones de investigación científica y técnica y organizaciones no gubernamentales.

Asimismo, las Partes deberán tomar en consideración, la importancia de la ejecución de proyectos nacionales de desarrollo y se favorecerá la instrumentalización de proyectos conjuntos de desarrollo tecnológico, que vinculen centros de investigación con entidades industriales de los dos países.

3. Las Partes podrán, con base en el presente Convenio, celebrar Acuerdos complementarios de cooperación técnica y científica, en áreas específicas de interés común, que formarán parte integrante del presente Convenio.

ARTICULO II

1. Para los fines del presente Convenio, las Partes elaborarán conjuntamente Programas Bienales, de acuerdo con las prioridades de ambos países en el ámbito de sus respectivos planes y estrategias de desarrollo económico y social.

2. Cada programa deberá especificar objetivos, recursos financieros y técnicos, cronogramas de trabajo, así como las tareas en que serán ejecutados los proyectos. Deberán igualmente especificar las obligaciones operativas y financieras de cada una de las Partes.

3. Cada programa será evaluado anualmente por las entidades coordinadoras, mencionadas en el Artículo V.

ARTICULO III

En la ejecución de los programas se incentivará e incluirá, cuando las Partes así lo consideren necesario, la participación de organismos multilaterales y regionales de cooperación técnica, así como de las instituciones de terceros países.

Las Partes podrán, siempre que lo estimen necesario y por acuerdo mutuo, solicitar el financiamiento y la participación de organismos internacionales y de otros países en la ejecución de programas y proyectos que se acuerden de conformidad con el presente Convenio.

ARTICULO IV

1. Para los fines del presente Convenio, la cooperación técnica y científica entre las Partes podrá asumir las siguientes modalidades:

a) intercambio de especialistas, investigadores y profesores universitarios;

b) elaboración de programas de pasantía para entrenamiento profesional y capacitación;

c) realización conjunta o coordinada de programas y proyectos de investigación y/o desarrollo tecnológico que vinculen centros de investigación e industria;

d) intercambio de información sobre investigación científica y tecnológica;

e) desarrollo de actividades conjuntas de cooperación en terceros países;

f) otorgamiento de becas para estudios de especialización profesional y estudios intermedios de capacitación técnica;

g) organización de seminarios, talleres y conferencias;

h) prestación de servicios de consultoría;

i) envío de equipo y material necesario para la ejecución de proyectos específicos; y

j) cualquier otra modalidad acordada por las Partes.

ARTICULO V

Con el fin de contar con un adecuado mecanismo de seguimiento de las acciones de cooperación previstas en el presente Convenio y de lograr las mejores condiciones para su ejecución, las Partes establecerán una Comisión Mixta Panameño - Costarricense, integrada por representantes de ambos Gobiernos, así como de aquellas instituciones cuyas actividades incidan directamente en el ámbito de la cooperación técnica y científica de ambos países.

Esta Comisión Mixta será presidida por el Ministerio de Relaciones Exteriores, por parte de Panamá y por el Ministerio de Relaciones Exteriores y Culto, por parte de Costa Rica, la cual tendrá las siguientes funciones:

a) evaluar y delimitar áreas prioritarias en que sería factible la realización de proyectos específicos de cooperación técnica y científica;

b) estudiar y recomendar los programas y proyectos a ejecutar;

c) revisar, analizar y aprobar los Programas Bienales de cooperación técnica y científica; y

d) supervisar la adecuada observancia y cumplimiento del presente Convenio y formular a las Partes las recomendaciones que consideren pertinentes.

El órgano ejecutor responsable de coordinar las acciones que se desprendan del presente Convenio, es el Ministerio de Economía y Finanzas,

por parte de Panamá y el Ministerio de Relaciones Exteriores y Culto, por parte de Costa Rica.

ARTICULO VI

La Comisión Mixta se reunirá alternativamente cada dos años en Panamá y en Costa Rica, en las fechas acordadas previamente a través de la vía diplomática.

Sin perjuicio de lo previsto en el párrafo precedente, cada una de las Partes podrá someter a consideración de la otra, en cualquier momento, proyectos específicos de cooperación técnica y científica, para su debido análisis y, en su caso, aprobación. Asimismo, las Partes podrán convocar, de común acuerdo y cuando lo consideren necesario, reuniones extraordinarias de la Comisión Mixta.

ARTICULO VII

Ambas Partes tomarán las medidas necesarias para que las técnicas y los conocimientos adquiridos por los nacionales de las Partes, como resultado de la cooperación a que se refiere el Artículo IV, contribuyan al desarrollo económico y social de sus países.

ARTICULO VIII

En el envío de personal a que se refiere el Artículo IV, los costos de transporte internacional de una de las Partes al territorio de la otra, se sufragarán por la Parte que lo envíe. El costo de hospedaje, alimentación y transporte local, se cubrirá por la Parte receptora, a menos que expresamente se especifique de otra manera o sea objeto de los acuerdos complementarios a que se refiere el numeral 3 del Artículo I del presente Convenio.

ARTICULO IX

Cada Parte otorgará todas las facilidades necesarias para la entrada, permanencia y salida de los participantes, que en forma oficial intervengan en los proyectos de cooperación. Estos participantes se someterán a las disposiciones nacionales vigentes en el país receptor y no podrán dedicarse a ninguna actividad ajena a sus funciones, ni recibir ninguna remuneración fuera de las estipuladas, sin la previa autorización de ambas Partes.

ARTICULO X

Las Partes Contratantes tendrán derecho a:

1. la exención de todo tributo que afecte la importación y compra local de los bienes necesarios que se requieran para la realización de los proyectos, siempre que queden incorporados al proyecto o que sean necesarios para prestar los servicios.

2. La exención temporal de todo tributo para la importación de los equipos directamente requeridos en la ejecución de los proyectos. Los equipos deberán permanecer en el país únicamente mientras se ejecuta el proyecto, según el caso.

Los bienes internados bajo la modalidad de importación temporal, una vez finalizado el proyecto deberán ser exportados o nacionalizados, previo pago de los impuestos correspondientes.

ARTICULO XI

1. El presente Convenio entrará en vigor a partir de la fecha de recepción de la segunda de las Notas mediante las cuales, las Partes se comuniquen, a través de la vía diplomática, haber cumplido con los requisitos exigidos por su legislación nacional para tal efecto y tendrá una vigencia inicial de cinco años, renovable por períodos de igual duración, previa evaluación de las Partes.

2. El presente Convenio podrá ser modificado por mutuo consentimiento y las modificaciones acordadas entrarán en vigor en la fecha en que las Partes, mediante un Canje de Notas diplomáticas, se comuniquen el cumplimiento de los requisitos exigidos por la legislación nacional.

3. Cualquiera de las Partes podrá, en todo momento, dar por terminado el presente Convenio, mediante notificación escrita, dirigida a la Otra a través de la vía diplomática, con seis meses de antelación.

La terminación del presente Convenio no afectará la conclusión de los programas y proyectos que hubieren sido formalizados durante su vigencia.

Hecho en Bambito, República de Panamá, a los 29 días del mes de noviembre de 2001, en dos ejemplares originales, siendo ambos textos igualmente válidos.

POR EL GOBIERNO DE LA REPUBLICA DE PANAMA
(Fdo.)
JOSE MIGUEL ALEMAN
Ministro de Relaciones Exteriores

POR EL GOBIERNO DE LA REPUBLICA DE COSTA RICA
(Fdo.)
ROBERTO ROJAS
Ministro de Relaciones Exteriores y Culto

Artículo 2. Esta Ley comenzará a regir desde su promulgación.

COMUNIQUESE Y CUMPLASE.

Aprobada en tercer debate, en el Palacio Justo Arosemena, ciudad de Panamá, a los 26 días del mes de diciembre del año dos mil dos.

El Presidente,

CARLOS R. ALVARADO A.

El Secretario General,

JOSE GOMEZ NUÑEZ

ORGANO EJECUTIVO NACIONAL.- PRESIDENCIA DE LA REPUBLICA.- PANAMA, REPUBLICA DE PANAMA, 20 DE ENERO DE 2003.

MIREYA MOSCOSO
Presidenta de la República

HARMODIO ARIAS CERJACK
Ministro de Relaciones Exteriores

MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES | GOBIERNO DE COSTA RICA

MINUTA: DIAGNÓSTICO PARA LA IMPLEMENTACIÓN DEL CONVENIO DE RECONOCIMIENTO MUTUO DE CERTIFICADOS DE FIRMA DIGITAL ENTRE LA REPÚBLICA DE PANAMÁ Y LA REPÚBLICA DE COSTA RICA.

Se ha requerido a la Asesoría Jurídica de la Dirección Nacional de Firma Electrónica del Registro Público de la República de Panamá, y a la Asesoría Jurídica de la Dirección de Gobernanza Digital y Certificadores de Firma Digital (DGDCFD) del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) de la República de Costa Rica, analizar la existencia de eventuales incompatibilidades normativas para la implementación práctica de la firma digital transfronteriza en el marco del Convenio de reconocimiento mutuo de certificados de Firma Digital entre ambos países, según lo establecido en el Convenio Básico de Cooperación Técnica y Científica entre el Gobierno de la República de Costa Rica y el Gobierno de la República de Panamá, suscrito en la ciudad de Bambito, Chiriquí, República de Panamá, el 29 de noviembre del 2001 y ratificado por Costa Rica mediante la ley N° 8889, número de gaceta 241, del 13 de diciembre del 2010 y entrado en vigencia el 13 de diciembre 2010, y aprobado por parte de Panamá mediante la Ley No. 10 de 20 de enero de 2003, publicada en la Gaceta Oficial N.º 24726 de 24 de enero de 2003, establece en su artículo primero lo siguiente:

> *"1. El presente Convenio tiene como objetivo promover la cooperación técnica y científica entre ambos países, a través de la formulación y ejecución, de común acuerdo, de programas y proyectos en dichas áreas.*
> *2. En la elaboración de estos programas y proyectos, las Partes tomarán en consideración las prioridades establecidas en sus respectivos planes de desarrollo y apoyarán la participación, en su ejecución, de organismos y entidades de los sectores público, privado y social, así como de las universidades, instituciones de investigación científica y técnica y organizaciones no gubernamentales.*
> *Asimismo, las Partes deberán tomar en consideración, la importancia de la ejecución de proyectos nacionales de desarrollo y se favorecerá la instrumentalización de proyectos conjuntos de desarrollo tecnológico, que vinculen centros de investigación con entidades industriales de los dos países.*
> *3. Las Partes podrán, con base en el presente Convenio, celebrar Acuerdos complementarios de cooperación técnica y científica, en áreas específicas de interés común, que formarán parte integrante del presente Convenio."*

MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES | GOBIERNO DE COSTA RICA

I. SOBRE EL ACUERDO

El Convenio de reconocimiento mutuo de certificados de Firma Digital, que busca ser suscrito entre la República de Panamá y la República de Costa Rica tiene como objeto promover la cooperación entre las Partes para el reconocimiento de la firma digital certificada y firma electrónica calificada para su homologación, en cumplimiento con las regulaciones de cada una de las Partes, sin contravenir el respectivo ordenamiento jurídico interno de cada estado.

Para efectos del Convenio, se entiende que la "firma electrónica calificada" en la República de Panamá y la "firma digital certificada" en la República de Costa Rica serán consideradas como equivalentes, únicamente para los fines de la cooperación y del reconocimiento recíproco previstos en este convenio, sin perjuicio de las disposiciones legales internas de cada Estado.

En relación con los mecanismos previstos para resguardar la compatibilidad y fiabilidad reciproca de los sistemas de certificación de firma digital certificada/ calificada de cada país firmante, se deben tener en cuenta las siguientes disposiciones del Convenio:

> *"**4. DEL RECONOCIMIENTO:***
>
> *"El Registro Público de la República de Panamá, a través de la Dirección Nacional de Firma Electrónica, homologa y reconoce como legalmente válidos y otorga el mismo valor jurídico y probatorio a los certificados de firma digital certificada emitidos por los Certificadores Registrados, debidamente autorizados por la Dirección de Gobernanza Digital y Certificadores de Firma Digital (DGDCFD) del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) de la República de Costa Rica.*
>
> *El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de la República de Costa Rica, a través de la Dirección de Gobernanza Digital y Certificadores de Firma Digital (DGDCFD) homologa y reconoce como legalmente válidos y otorga el mismo valor jurídico y probatorio a los certificados de firma electrónica calificada emitidos por los Prestadores de Servicios de Certificación, debidamente autorizados por la Dirección Nacional de Firma Electrónica del Registro Público de la República de Panamá.*
>
> *El reconocimiento recíproco se atenderá siempre que se reúnan las siguientes condiciones:*
>
> *a) Que respondan a estándares reconocidos internacionalmente, conforme lo establezca la autoridad designada por las Partes.*
> *b) Que contengan como mínimo, datos que permitan:*
> *I. Identificar inequívocamente a su titular y al prestador de servicios de certificación que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;*

II. *Ser susceptible de verificación respecto de su estado de revocación;*
III. *Detallar la información verificada incluida en el certificado digital;*
IV. *Contemplar la información necesaria para la verificación de la firma;*
V. *Identificar la política de certificación bajo la cual fue emitido.*

Las Partes se comprometen a intercambiar en virtud del presente convenio, el listado de los Certificadores Registrados y de los Prestadores de Servicios de Certificación que se encuentren autorizados dentro de los respectivos países, así como a informar cualquier cambio que se produzca en dicho listado.

5. IMPLEMENTACIÓN:

A los efectos de la implementación del presente Convenio, se realizarán las siguientes acciones:

a) *Estudio e intercambio de las Políticas de certificación implementadas por los países para la homologación de los certificados digitales entre las Partes, así como la elaboración de un Informe de equivalencia de dichas políticas.*
b) *Evaluación de requerimientos técnicos observados en el ciclo de vida del certificado digital.*
c) *Evaluación de requerimientos técnicos para el intercambio de listas de revocación de certificados de firma digital o firmas electrónicas calificadas a los efectos de ser contemplados por las herramientas de validación de firma en los respectivos países.*
d) *Intercambio de documentos y herramientas vinculados a la firma digital certificada o firma electrónica calificada.*
e) *Publicación de los certificados raíz y subordinados vigentes, en las páginas oficiales de la Dirección de Gobernanza Digital y Certificadores de Firma Digital (DGDCFD) del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) de la República de Costa Rica y de la Dirección Nacional de Firma Electrónica del Registro Público de la República de Panamá.*

Cualquier actividad por implementarse en virtud del presente convenio será determinada de manera conjunta y cursada formalmente conforme las direcciones de correo electrónico consignadas en este Convenio y estará sujeta a la disponibilidad de fondos y del personal apropiado.

Para esto, las Partes podrán elaborar un cronograma de trabajo conjunto de las actividades a desarrollar para la homologación de la firma digital certificada o firma electrónica calificada, observando los principios estipulados en el presente convenio. Salvo disposición en contrario, de común acuerdo cada Parte asumirá los gastos en los que incurra por concepto de las actividades de cooperación en virtud del presente instrumento.

El personal asignado por cada una de las Partes para la ejecución de las acciones de cooperación, al amparo del convenio, continuará bajo la dirección y dependencia de la institución a la que pertenezca, por lo que no se crearán relaciones de carácter laboral con la otra Parte.

Las oficinas encargadas de la firma digital certificada o firma electrónica calificada, así como los de asuntos internacionales de las Partes servirán de puntos focales en la ejecución de las actividades de cooperación identificadas en este Convenio.

Las notificaciones que se deriven de este convenio tendrán validez cuando sean remitidas por correo físico o electrónico a las siguientes direcciones:
(...)"

II. SOBRE LA REGULACIÓN DE LA REPÚBLICA DE PANAMÁ EN LA MATERIA:

1. Ley N° 51 de 22 de julio de 2008: "Que define y regula los documentos electrónicos y las firmas electrónicas y la prestación de servicios de almacenamiento tecnológico de documentos y de certificación de firmas electrónicas y adopta otras disposiciones para el desarrollo del comercio electrónico."
   https://www.gacetaoficial.gob.pa/pdfTemp/26090/12199.pdf
2. Ley N° 82 de 9 de noviembre de 2012: "Que otorga al Registro Público de Panamá atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá, modifica la Ley 51 de 2008 y adopta otras disposiciones".
   https://www.gacetaoficial.gob.pa/pdfTemp/27160/39632.pdf
3. Decreto Ejecutivo N° 684 de 18 de octubre de 2013: "Que reglamenta la Ley 51 de 22 de julio de 2008 y la Ley 82 de 9 de noviembre de 2012 en materia de firma electrónica."
   https://www.gacetaoficial.gob.pa/pdfTemp/27401/44155.pdf
4. Decreto Ejecutivo N° 83 de 23 de marzo de 2023: "Que modifica artículos del Decreto Ejecutivo N° 684 de 18 de octubre de 2013: "Que reglamenta la Ley 51 de 22 de julio de 2008 y la Ley 82 de 9 de noviembre de 2012, en materia de firma electrónica."
   https://www.gacetaoficial.gob.pa/pdfTemp/29746_B/97527.pdf

Estos son los principales cuerpos legales que regulan los documentos electrónicos, sus efectos legales y la utilización de la firma electrónica en Panamá.

III. SOBRE LA REGULACIÓN DE LA REPÚBLICA DE COSTA RICA EN LA MATERIA:

La Ley N° 8454: *"Ley de Certificados, Firmas Digitales y Documentos Electrónicos"* del 13 de octubre de 2005 y el Decreto Ejecutivo N° 33.108: *"Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos"* de fecha 20 de marzo de 2006, son los principales cuerpos legales que regulan los documentos electrónicos y sus efectos legales,

junto con la utilización de firma digital. Para analizar la compatibilidad de la regulación nacional sobre firma electrónica con la normativa costarricense y el texto del acuerdo, es necesario considerar las siguientes normas:

***Artículo 1º de la Ley N° 8454 - 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 13º de la Ley N° 8454 - 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 18º de la Ley N° 8454 - 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 19º de la Ley N° 8454 - 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, Tecnología y Telecomunicaciones (*), 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.*
(*)(Así modificada su denominación por el artículo 11 de la Ley "Traslado del sector Telecomunicaciones del Ministerio de Ambiente, Energía y Telecomunicaciones al Ministerio de Ciencia y Tecnología, N° 9046 del 25 de junio de 2012).
(**) (Nota de Sinalevi: La ley N° 8279 a la que hace referencia el presente artículo fue derogada por el numeral 83 de la Ley del Sistema Nacional para la Calidad, N° 10473 del 24 de abril de 2024).

***Artículo 20º de la Ley N° 8454 - Corresponsal:** 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 1º del Decreto Ejecutivo N° 33.108 – Propósito: *El presente texto servirá para reglamentar y dar cumplida ejecución a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, número 8454 del 30 de agosto del 2005. Tendrá el carácter y la jerarquía de reglamento general, en los términos del artículo 6.1.d) de la Ley General de la Administración Pública, frente a los demás reglamentos particulares o autónomos en la materia.*

Artículo 10º del Decreto Ejecutivo N° 33.108 - Reconocimiento jurídico*: Solo tendrán pleno efecto legal frente a terceros, así como respecto del Estado y sus instituciones, los certificados digitales expedidos por certificadores registrados ante la Dirección de Certificadores de Firma Digital. Las firmas y certificados emitidos dentro o fuera del país que no cumplan con esa exigencia no surtirán efectos por sí solos, pero podrán ser empleados como elemento de convicción complementario para establecer la existencia y alcances de un determinado acto o negocio.*

IV. MATRIZ COMPARATIVA ENTRE LA REGULACIÓN DE LA REPÚBLICA DE PANAMÁ Y LA REGULACIÓN DE LA REPÚBLICA DE COSTA RICA:

En atención a lo expuesto en los párrafos precedentes, incluyendo las normas transcritas del Convenio, como también las normas relevantes de la Ley N° 51 de 22 de julio de 2008, Ley N° 82 de 9 de noviembre de 2012, Decreto Ejecutivo N° 684 de 18 de octubre de 2013, Decreto Ejecutivo N° 83 de 23 de mayo de 2023 de la República de Panamá, así como lo referente a la ley Ley N° 8454 "Ley de Certificados, Firmas Digitales y Documentos Electrónicos" del 13 de octubre de 2005 y el Decreto Ejecutivo N° 33.108 "Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos" de fecha 20 de marzo de 2006, es posible identificar una serie de principios y/o mecanismos regulatorios que determinan la compatibilidad normativa entre los regímenes aplicables a los certificados de firma electrónica calificada o firma digital certificada en Panamá y Costa Rica respectivamente.

Para dicho efecto, a continuación se presenta una matriz que compara las normativas de ambos países, en atención a: (i) los principios legales consagrados en la materia; (ii) la existencia de diferentes niveles de firma electrónica; (iii) el valor que se reconoce a los documentos suscritos con firma electrónica; (iv) el valor probatorio de los documentos suscritos con firma electrónica; (v) el requisito de comprobación de identidad de los solicitantes de certificados; (vi) el régimen de responsabilidad aplicable a los prestadores de servicios de certificación; (vii) el requisito de acreditación de los prestadores de servicios de certificación; (viii) el régimen de inspecciones al que se someten los prestadores de servicios de certificación; (ix) las causales de cese de actividades de los prestadores de servicios de certificación; (x) el régimen de sanciones administrativas aplicable, y; (xi) los derechos de los titulares de los certificados emitidos en cada país.

MATRIZ COMPARATIVA

PRINCIPIOS / DISPOSICIONES LEGALES		NORMATIVA DE CADA PAÍS	
1	**Leyes y normativa relevante**	**PANAMÁ** Ley N° 51 de 22 de julio de 2008: "Que define y regula los documentos electrónicos y las firmas electrónicas y la prestación de servicios de almacenamiento tecnológico de documentos y de certificación de firmas electrónicas y adopta otras disposiciones para el desarrollo del comercio electrónico." https://www.gacetaoficial.gob.pa/pdfTemp/26090/12199.pdf Ley N° 82 de 9 de noviembre de 2012: "Que otorga al Registro Público de Panamá atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá, modifica la Ley N° 51 de 2008 y adopta otras disposiciones".	**COSTA RICA** Ley N° 8454: "Ley de Certificados, Firmas Digitales y Documentos Electrónicos" del 13 de octubre de 2005: https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=55666 Decreto Ejecutivo N° 33.108: "Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos" de fecha 20 de marzo de 2006: https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=56884

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
26

		https://www.gacetaoficial.gob.pa/pdfTemp/27160/39632.pdf Decreto Ejecutivo N° 684 de 18 de octubre de 2013: "Que reglamenta la Ley 51 de 22 de julio de 2008 y la Ley 82 de 9 de noviembre de 2012 en materia de firma electrónica." https://www.gacetaoficial.gob.pa/pdfTemp/27401/44155.pdf Decreto Ejecutivo N° 83 de 23 de marzo de 2023: "Que modifica artículos del Decreto Ejecutivo N° 684 de 18 de octubre de 2013: Que reglamenta la Ley 51 de 22 de julio de 2008 y la Ley N° 82 de 9 de noviembre de 2012, en materia de firma electrónica." https://www.gacetaoficial.gob.pa/pdfTemp/29746_B/97527.pdf Declaración de Prácticas de Certificación (DPC) y Políticas de Certificación (PC) https://www.firmaelectronica.gob.pa/politicas-certificacion.html	Política de Certificados para la Jerarquía Nacional de Certificadores Registrados: https://www.mifirmadigital.go.cr/wp-content/uploads/2022/08/DCFD-Politica-de-certificados-v2.0.pdf

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
27

2	**Principios legales**	**PANAMÁ** Libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia funcional. (Artículo N° 3 de la Ley N° 51 de 2008). Artículo 3. Interpretación, ámbito de aplicación y régimen de la prestación de servicios. Las actividades reguladas por esta Ley se someterán a los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia funcional y se aplicarán sin perjuicio de lo dispuesto en otras normas que tengan como finalidad la protección de la salud, de la seguridad pública, de datos personales, de los intereses del consumidor, de la libre competencia y del régimen tributario aplicable a las actividades comerciales e industriales. Toda interpretación de los preceptos de esta Ley deberá guardar armonía con los principios señalados. La prestación de servicios de almacenamiento tecnológico de documentos, de certificación de firmas electrónicas y de servicios de comercio a	**COSTA RICA** 1. Equivalencia funcional (Art. 3 Ley N° 8454). 2. Regulación legal mínima y desregulación de trámites (Art. 2 Ley N° 8454) 3. Autonomía de la voluntad de los particulares para reglar sus relaciones (Art. 2 Ley N° 8454). 4. Utilización con las limitaciones legales, de reglamentos autónomos por la Administración Pública para desarrollar la organización y el servicio, interno o externo (Art. 2 Ley N° 8454) 5. Igualdad de tratamiento para las tecnologías de generación, proceso o almacenamiento involucradas (Art. 2 Ley N° 8454) 6. Principio de No repudio (Art. 4 Ley N° 8454 y Art. 11 de Decreto Ejecutivo N° 33.018) 7. Principio de vinculación jurídica,

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
28

		través de Internet se regirá por los mismos principios expresados en el párrafo anterior, no estará sujeta a autorización previa y se realizará en régimen de libre competencia. Sin embargo, las personas naturales o jurídicas que se dediquen a la prestación de estos servicios deberán cumplir las condiciones y los requisitos establecidos en esta Ley y sus reglamentos.	identificación unívoca y presunción de autoría (Art. 4 y 10 Ley N° 8454 y Art. 11 de Decreto Ejecutivo N° 33.018) 8. Principio de validez y eficacia probatoria (Art. 4 Ley N° 8454 y Art. 11 de Decreto Ejecutivo N° 33.018).
3	**Diferentes niveles de firma electrónica**	**PANAMÁ** 1. **FIRMA ELECTRÓNICA.** Método técnico para identificar a una persona y para indicar que esa persona aprueba la información que figura en un mensaje de datos o documento electrónico. (Artículo 2, numeral 20 de la Ley 51 de 2008, modificado por el artículo 7 de la Ley 82 de 2012). 2. **FIRMA ELECTRÓNICA CALIFICADA.** Firma electrónica cuya validez es respaldada por un certificado electrónico calificado que: a) Permite identificar al firmante y	**COSTA RICA** 1. **FIRMA DIGITAL**: 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. 2. **FIRMA DIGITAL CERTIFICADA**: Una firma digital que haya sido emitida al amparo de un certificado digital válido y vigente, expedido por un certificador registrado.

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
29

		detectar cualquier cambio posterior de los datos firmados. b) Está vinculada al firmante de manera única y a los datos a que se refiere. c) Ha sido creada utilizando dispositivos seguros de creación de firmas electrónicas, los cuales mantiene el firmante bajo su control exclusivo. d) Ha sido creada a través de la infraestructura de un prestador de servicios de certificación registrado ante la Dirección Nacional de Firma Electrónica. (Artículo 2, numeral 21 de la Ley 51 de 2008, modificado por el artículo 7 de la Ley 82 de 2012).	3. **SELLO ELECTRÓNICO**: Firma digital certificada generada a partir de un certificado digital de sello electrónico de persona jurídica; se utilizan como parte de procesos automáticos de sellado electrónico sin que se requiera intervención humana al momento de sellar los documentos o archivos electrónicos.
4	**Valor de documentos suscritos con firma electrónica**	**PANAMÁ** Artículo 4 de la Ley N° 51 de 2008, modificado por el artículo 10 de la Ley 82 de 2012: Valor legal de los documentos electrónicos. Cuando la ley requiera que la información conste en un documento escrito, se le reconocerá validez, efectos jurídicos y fuerza obligatoria a los actos,	**COSTA RICA** **Artículo 3º de la Ley N° 8454 - Reconocimiento de la equivalencia funcional.** Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, se tendrá por

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
30

		poderes y contratos y a todo documento que haya sido otorgado o recibido a través de mensajes de datos, de conformidad con esta Ley y sus reglamentos, siempre que la información que este contiene sea accesible para su posterior consulta. Artículo 35-A de la Ley N° 51 de 2008, adicionado por el artículo 34 de la Ley N° 82 de 2012: Responsabilidad por alteración, modificación o adulteración de firmas o certificados electrónicos calificados. Las personas que se apoderen, destruyan, modifiquen o adulteren indebidamente los datos de una firma o certificado electrónico durante o después de la fecha de creación del certificado electrónico respectivo responderán penalmente por su actuación y quedarán sujetas a las sanciones tipificadas en el Código Penal, sin perjuicio de la responsabilidad civil o administrativa que pudiera corresponderles.	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. El documento electrónico con firma digital es jurídicamente equivalente a los documentos que se otorgue o transmitan por medios físicos. **Artículo 4º de la Ley N° 8454 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. El documento electrónico con firma digital

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
31

			tiene el mismo valor probatorio que los documentos físicos.
5	**Valor probatorio de documentos suscritos con firma electrónica**	**PANAMÁ** Artículo 7 de la Ley N° 51 de 2008, modificado por el artículo 12 de la Ley N° 82 de 2012: Admisibilidad y fuerza probatoria de documentos electrónicos. Los documentos electrónicos serán admisibles como medios de prueba y tendrán la misma fuerza probatoria otorgada a los documentos en el Libro Segundo, Procedimiento Civil, del Código Judicial. En todo caso, al valorar la fuerza probatoria de un documento electrónico se tendrá presente la confiabilidad de la forma en la que se haya generado, archivado o comunicado, la confiabilidad de la forma en la que se haya conservado la integridad de la información, la forma en que se identifique a su iniciador y cualquier otro factor pertinente. Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta Ley, se tendrán en cuenta las reglas de la sana crítica y	**COSTA RICA** **Artículo 4º de la Ley N° 8454 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. El documento electrónico con firma digital tiene el mismo valor probatorio que los documentos físicos.

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
32

		demás criterios reconocidos legalmente para la apreciación de las pruebas. Artículo 9 de la Ley 51 de 2008, modificado por el artículo 15 de la Ley 82 de 2012: Fe pública. Si una disposición legal requiere que una firma relacionada a un documento o a una transacción sea reconocida o hecha bajo la gravedad del juramento, dicho requisito será satisfecho en un documento electrónico si el otorgante utiliza la firma electrónica calificada. Si una disposición legal requiere que una firma relacionada a un documento o a una transacción sea notariada, refrendada o hecha bajo la gravedad del juramento ante un notario o funcionario público, dicho requisito será satisfecho en un documento electrónico si a la firma electrónica calificada del otorgante se adiciona la firma electrónica calificada del funcionario autorizado para dar fe pública. No obstante, dicho documento electrónico no conferirá fe pública con respecto a su fecha, a menos que esta conste a través de un sellado de tiempo, otorgado por un prestador de servicios de certificación registrado. En el ámbito de documentos electrónicos,	

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
33

		corresponderá al prestador de servicios de certificación acreditar la existencia de los servicios prestados en el ejercicio de su actividad, a solicitud del usuario o de una autoridad judicial o administrativa competente.	
6	**Comprobación de la identidad de los solicitantes de certificados**	**PANAMÁ** Artículo 26 de la Ley N° 51 de 2008, modificado por el artículo 28 de la Ley N° 82 de 2012: Comprobación de identidad y otras circunstancias personales de los solicitantes de un certificado calificado. La persona que solicite un certificado comprobará su identidad a través de cualquiera de los siguientes procedimientos de verificación: 1. Su comparecencia física ante los encargados de verificarla, que se acreditará mediante la cédula de identidad personal o el pasaporte e incluirá identificación y verificación plena de la identificación del firmante. 2. En el caso de personas jurídicas, se deberán comprobar los datos relativos a la constitución y personalidad jurídica, así como el nombre, la extensión y la vigencia de las facultades de representación legal del solicitante mediante	**COSTA RICA** **Artículo 8° de la Ley N° 8454 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. La firma digital está asociada a un documento electrónico que identifica de manera unívoca, al autor del documento electrónico.

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
34

		certificación del Registro Público de Panamá en la que consten de forma clara y precisa todos estos datos. 3. Cualquier mecanismo técnico autorizado por la Dirección Nacional de Firma Electrónica que garantice validar de manera inequívoca la identidad de quien se encuentra realizando la solicitud o descarga del certificado de firma electrónica calificada. 4. Otros mecanismos establecidos en la reglamentación de esta Ley de forma complementaria, adicionales o distintos a los ya exigidos en el presente artículo. Cuando el certificado calificado contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional, idoneidad o su título profesional, estos deberán comprobarse mediante los documentos oficiales que los acrediten de conformidad con su normativa específica. Lo dispuesto en los párrafos anteriores podrá omitirse en los siguientes casos: a. Cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados	**Artículo 6° del Decreto Ejecutivo N° 33.018 Tipos de certificados**. La DCFD establecerá los tipos de certificados que podrán emitir los certificadores, con estricto apego a las normas técnicas y estándares internacionales aplicables que promuevan la interoperabilidad con otros sistemas. En el caso de los certificados digitales que vayan a ser utilizados en procesos de firma digital y de autenticación de la identidad, los certificadores necesariamente deberán: 1) Utilizar al menos un proceso de verificación y registro presencial (cara a cara) de sus suscriptores. (Así reformado el inciso anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008) 2) Guardar copia de la documentación utilizada para verificar la identidad de la persona. 3) Registrar de forma biométrica (fotografía, huellas digitales, etc.) al suscriptor a quién le

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
35

		constaran ya para el prestador de servicios de certificación en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubieran empleado los medios señalados en este artículo y el periodo de tiempo transcurrido desde la identificación no sea mayor de un año, siempre que dichos datos de identificación sigan siendo los mismos. b. Cuando para solicitar un certificado se utilice otro vigente para cuya expedición se hubiera identificado al firmante en la forma prescrita en este artículo. Los prestadores de servicios de certificación podrán realizar las actuaciones de comprobación previstas en este artículo por sí mismos o por medio de otras personas naturales o jurídicas, públicas o privadas, siendo responsable, en todo caso, el prestador de servicios de certificación. El presente artículo será objeto de reglamentación. POLITICA DE CERTIFICACIÓN CERTIFICADO DE PERSONA NATURAL 1.1. Solicitud de certificados	será emitido un certificado. 4) Requerir el uso de módulos seguros de creación de firma, con certificación de seguridad que se indique conforme a las normas internacionales y a las Políticas establecidas por la DCFD. (Así reformado el inciso anterior por el artículo 1° del Decreto Ejecutivo N° 34890 del 27 de octubre de 2008) 5) Establecer un contrato de suscripción detallando el nivel de servicio que ofrece y los deberes y responsabilidades de las partes. 6) La DCFD podrá establecer cualquier otro requisito que considere pertinente, en tanto emisor y gestor de políticas del sistema de firma digital. Se establecen los requisitos que deben solicitar los entes certificadores para identificar de manera unívoca al autor con el documento electrónico.

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
36

		4.1.1. Quién puede efectuar una solicitud La solicitud de certificado de persona natural será efectuada por la persona natural que vaya a ser titular del mismo. 4.1.2. Registro de las solicitudes de certificados y responsabilidades de los solicitantes El procedimiento de solicitud de certificados de persona natural es el siguiente: 1. La persona natural que será titular del certificado electrónico realiza la preinscripción completando el formulario en la página web www.firmaelectronica.gob.pa. 2. En el formulario de prescripción deberá colocar su número de identificación o cédula (de ser panameño), que será validado automáticamente por el Sistema de Verificación de Identidad del Tribunal Electoral de Panamá (nombre, número de cédula, fecha de nacimiento); adicionalmente, debe colocar los datos adicionales, según el perfil del certificado electrónico solicitado, que para el caso de la presente política de certificación, será la dirección de correo electrónico.	

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
37

		Para la validación de nacionales el operador de registro de la DNFE coteja la cédula de identidad personal contra el Sistema de Verificación de Identidad (SVI) del Tribunal Electoral. https://www.firmaelectronica.gob.pa/normativa/P-12-Politica-de-Certificacion-de-Certificados-de-Persona-Natural.pdf	
7	**Responsabilidad**	**PANAMÁ** Artículo 33 de la Ley N° 51 de 2008: Responsabilidad del prestador de servicios de certificación de firmas electrónicas. El prestador de servicios de certificación responderá por los daños y perjuicios que cause a cualquier persona en el ejercicio de su actividad cuando incumpla las obligaciones que le impone esta Ley. En todo caso, corresponderá al prestador de servicios de certificación demostrar que actuó con la diligencia profesional que le es exigible. De manera particular, el prestador de servicios de certificación responderá de los perjuicios que se causen al firmante o a terceros de buena fe, por la falta o el retraso en la actualización de su repositorio, sobre	**COSTA RICA** **Artículo 18° de la Ley N° 8454 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

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
38

		la vigencia, la extinción, la revocación o la suspensión de los certificados electrónicos. Los prestadores de servicios de certificación asumirán toda la responsabilidad frente a terceros, por la actuación de las personas en las que deleguen la ejecución de alguna de las funciones necesarias para la prestación de servicios de certificación. Artículo 23 de la Ley N° 51 de 2008: Obligaciones del prestador de servicios de certificación público y privado que expida certificados electrónicos calificados. Todo prestador de servicio de certificación que expida certificados electrónicos calificados deberá cumplir con las siguientes obligaciones: ..... 17. Contratar una póliza de responsabilidad civil contractual y extracontractual, para afrontar el riesgo de la responsabilidad por daños y perjuicios que pueda ocasionar el uso de los certificados que expidan. El monto de esta póliza será fijada por reglamento.	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 13 del Decreto Ejecutivo N° 33.018 Caución.** Los sujetos privados deberán rendir una caución que será utilizada para responder por las eventuales consecuencias civiles, contractuales y extracontractuales de su actividad. Esta caución será rendida preferiblemente por medio de una póliza de fidelidad expedida por el Instituto Nacional de Seguros. El monto -de acuerdo con la Ley- será fijado por la DCFD en consulta con el Instituto Nacional de Seguros, tomando en consideración los riesgos y responsabilidades inherentes en la labor de certificación digital. (Así reformado el párrafo anterior por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008) Cuando la caución esté sujeta a vencimiento, necesariamente deberá ser renovada por el interesado al menos dos meses antes de la fecha de expiración.

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
39

		Artículo 21 del Decreto Ejecutivo N. 684 de 18 de octubre de 2013, modificado por el artículo 4 del Decreto Ejecutivo 83 de 23 de marzo de 2023. El prestador de servicios de certificación deberá contar con póliza de seguros vigente, expedida por una entidad aseguradora autorizada para operar en Panamá en los términos señalados en el numeral 17 del artículo 23 de la Ley 51 de 2008 por un total asegurado hasta la suma de ciento cincuenta mil balboas con 00/100 (B/150,000.00).	Los entes certificadores deben rendir garantía de fidelidad o seguro de caución por los daños y perjuicios o las eventuales consecuencias civiles, contractuales y extracontractuales de su actividad. El monto de la póliza es definida por la Dirección de Gobernanza Digital y Certificadores de Firma Digital.
8	**Acreditación**	**PANAMÁ** Artículo 20-B y 20-C de la Ley 51 de 2008, adicionados por el artículo 22 de Ley 82 de 2012: Artículo 20-B. Atribuciones. La Dirección Nacional de Firma Electrónica tendrá la facultad para reglamentar, supervisar y sancionar todas las actividades de los prestadores de servicios de certificación concernientes al registro, comprobación y otorgamiento de firmas electrónicas y firmas electrónicas calificadas a particulares y entidades gubernamentales, así como registrar y/o suspender el registro de dichos	**COSTA RICA** **Artículo 19 de la Ley N° 8454 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, Tecnología y Telecomunicaciones (*), 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

No. 30509 D

Gaceta Oficial Digital, miércoles 22 de abril de 2026

		prestadores de servicio. Artículo 20-C. Funciones. Además de las funciones establecidas por ley para la Dirección Nacional de Firma Electrónica, se establecen las siguientes funciones en materia de certificación de firma electrónica: 1.Dictar y emitir los reglamentos, resoluciones y demás documentos técnicos que considere necesarios para el desarrollo de las materias de su competencia. 2.Realizar la función de Registro de los Prestadores de Servicios de Certificación y de Certificación de Firmas Electrónicas. 3.Velar por el adecuado funcionamiento y la eficiente prestación de los servicios de registro de los prestadores de servicios de certificación y certificación de firmas electrónicas, por parte de todo prestador de servicios registrados, así como por el cabal cumplimiento de las disposiciones legales y reglamentarias de la actividad.	internacionales. (*)(Así modificada su denominación por el artículo 11 de la Ley "Traslado del sector Telecomunicaciones del Ministerio de Ambiente, Energía y Telecomunicaciones al Ministerio de Ciencia y Tecnología, N° 9046 del 25 de junio de 2012) (**) (Nota de Sinalevi: La ley N° 8279 a la que hace referencia el presente artículo fue de rogada por el numeral 83 de la Ley del Sistema Nacional para la Calidad, N° 10473 del 24 de abril de 2024). **Artículo 11 del Decreto Ejecutivo N° 33.018 Comprobación de idoneidad técnica y administrativa**. Para obtener la condición de certificador registrado, se requiere poseer idoneidad técnica y administrativa, que serán valoradas por el ECA, de conformidad con los lineamientos técnicos establecidos en las Normas INTE-ISO/IEC 17021 e INTE/ISO 21188 versión vigente, las políticas fijadas por la DCFD y los restantes requisitos que esa dependencia establezca, de acuerdo con su normativa específica.

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
41

		4.Revocar o suspender el Registro de los Prestadores de Servicios de Certificación o de Certificación de Firmas Electrónicas, en los casos que determinen la ley y sus reglamentos. 5.Requerir a los prestadores de servicios registrados que suministren información relacionada con sus actividades, pero únicamente cuando se refieran a los procesos que afecten la seguridad e integridad de datos. Esta función no permitirá el acceso al contenido de documentos y mensajes, a las firmas o a los procesos utilizados, excepto mediante orden judicial. 6.Ordenar la revocación o suspensión de firmas y certificados electrónicos, cuando el prestador de servicios de certificación de firmas electrónicas los emita sin el cumplimiento de las formalidades legales. 7.Imponer sanciones a los prestadores de servicios de certificación de firmas electrónicas por el incumplimiento de los requerimientos técnicos establecidos en las disposiciones legales y	A fin de cumplir con lo establecido en el párrafo anterior, el certificador contará con el plazo de un año contado a partir de la fecha en que se le otorgó el registro por parte de la DCFD , con el propósito de lograr la acreditación respectiva por parte del ECA. Si en el plazo señalado no lograra obtener la acreditación, se le cancelará su registro por parte de la DCFD y no podrá ser registrado nuevamente hasta tanto no presente la acreditación del ECA. (Así reformado por el artículo 1° del decreto ejecutivo N° 34890 del 27 de octubre de 2008). Los entes certificadores deben acreditarse con el Ente de Costarricense de Acreditación (ECA), según lo dispuesto en la Ley del Sistema Nacional para la Calidad, N° 10473 del 24 de abril de 2024.

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026

		reglamentarias vigentes. 8.Designar los repositorios en los eventos previstos en la ley y sus reglamentos. 9.Ejercer las demás funciones que determine esta Ley y sus reglamentos. Comentario adicional: El artículo 4 de la Ley Nº 82 de 9 de noviembre de 2012 y el artículo 3 del Decreto Ejecutivo Nº 684 de 18 de octubre de 2013, establecen funciones complementarias de la Dirección Nacional de Firma Electrónica, lo cual refuerza y amplía las atribuciones previstas en los artículos 20-B y 20-C de la Ley 51 de 2008.	
9	**Auditorias**	**PANAMÁ** Artículo 4 de la Ley Nº 82 de 9 de noviembre de 2012: La Dirección Nacional de Firma Electrónica tendrá las siguientes funciones: 1.Elaborar y recomendar a la Junta Directiva y al director general los reglamentos, resoluciones y	**COSTA RICA** **Artículo 21 de la Ley N° 8454 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.

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
43

		demás documentos técnicos que considere necesarios para el desarrollo de las materias de su competencia. 2.Remitir a la Comisión Técnica Independiente las solicitudes de los prestadores de servicio de certificación, revisadas de acuerdo con la reglamentación para tal fin, dentro de un término de sesenta días, contado a partir de su presentación. 3.Registrar a los prestadores de servicio de certificación que hayan sido recomendados por la Comisión Técnica Independiente, dentro de un término máximo de treinta días, contado a partir de la fecha de recibida la documentación por parte de la Comisión Técnica Independiente para tal fin, de acuerdo con su reglamentación. De no efectuar ningún pronunciamiento dentro del término señalado, se entenderá que ha emitido criterio favorable y deberá procederse con el registro solicitado. 4.Auditar o requerirles auditorías a los prestadores de servicio de certificación. 5.Registrar y auditar a los prestadores de servicio de certificación que así lo soliciten, dentro de un término de noventa días, contado a partir de la	**Artículo 24 Decreto Ejecutivo N° 33.018 Funciones.** La Dirección de Certificadores de Firma Digital tendrá las siguientes funciones: (...) 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. La Dirección de Certificadores de Firma Digital tiene la obligación de supervisar y fiscalizar el funcionamiento de los entes certificadores registrados, con la finalidad de que cumplan con la normativa correspondiente.

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
44

		presentación de toda la documentación solicitada para tal fin, de acuerdo con su reglamentación. De no efectuar ningún pronunciamiento dentro del término señalado, se entenderá que ha emitido criterio favorable y deberá procederse con el registro solicitado. 6.Velar por el adecuado funcionamiento y la eficiente prestación de servicios, por parte de todo prestador de servicios de certificación, así como por el cabal cumplimiento de las disposiciones legales y reglamentarias de la actividad. 7.Revocar o suspender el registro de prestadores de servicio de certificación en los casos que determinen la ley y sus reglamentos. Artículo 23-A de la Ley N° 51 de 2008, adicionado por el artículo 26 de Ley N° 82 de 2012: Auditorías y evaluaciones técnicas. La Dirección Nacional de Firma Electrónica tendrá la facultad de efectuar o requerir, por lo menos una vez al año, auditorías e inspecciones técnicas, o autorizar a otras entidades públicas o privadas a realizarlas, con el propósito de verificar el fiel cumplimiento de las obligaciones de los prestadores de certificación. Del resultado de estas diligencias, la Dirección	

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
45

		Nacional de Firma Electrónica podrá, de ser necesario, aplicar las sanciones o medidas correctivas necesarias para garantizar los estándares de calidad internacional, de conformidad con las exigencias legales y reglamentarias. Artículo 16 del Decreto Ejecutivo N° 684 de 18 de octubre de 2013. Para la renovación del registro cada dos (2) años el prestador de servicios de certificación deberá presentar a la Dirección los siguientes documentos: 1. Los dos (2) informes favorables de auditoria anuales respectivos. 2. La documentación que acredite la contratación de la póliza de responsabilidad civil y extracontractual. Artículo No. 5 de la Resolución No. DG-075-2025 de 14 de agosto de 2025 (Estándares de cumplimiento). Los prestadores de servicios de certificación privados, dependiendo de los servicios de certificación u otros servicios y actividades	

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
46

		complementarias que la Dirección Nacional de Firma Electrónica les autorice a brindar, para garantizar que mantienen sistemas confiables deberán cumplir con mínimamente con los siguientes estándares de referencia o su equivalente en el estándar WebTrust:	
10	**Cese de la actividad**	**PANAMÁ** Artículo 4 de la Ley Nº 82 de 9 de noviembre de 2012: La Dirección Nacional de Firma Electrónica tendrá las siguientes funciones: ..... Artículo 32 Ley N° 51 de 2008, modificado por el artículo 30 de la Ley N° 82 de 2012: Cese de actividades por parte de un prestador de servicios de certificación de firmas electrónicas. Todo prestador de servicios de certificación que vaya a cesar en su actividad deberá comunicarlo a la Dirección Nacional de Firma Electrónica y a cada firmante, con un mínimo de noventa días de anticipación, con la siguiente información:	**COSTA RICA** **Artículo 22 de la Ley N° 8454 - 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. **Artículo 24 del Decreto Ejecutivo N° 33.018 - Funciones.** La Dirección de Certificadores de Firma Digital tendrá las siguientes funciones: (...) c) Suspender o revocar la inscripción de los

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
47

		1. La fecha de la cesación efectiva de actividades, y 2. Los motivos por los cuales se procede a tal cese. Los certificados que continúen vigentes podrán ser transferidos a otro prestador de servicios de certificación, previo consentimiento del firmante y por cuenta del prestador de servicios de certificación o, en caso contrario, suprimir su vigencia. El prestador de servicios de certificación deberá comunicar a la Dirección Nacional de Firma Electrónica, con un mínimo de cuarenta y cinco días de anticipación al cese de su actividad, el destino que vaya a dar a los certificados, especificando, en su caso, si va a transferir los certificados a otro prestador registrado o si va a extinguir su vigencia. Sin perjuicio de ello, la Dirección Nacional de Firma Electrónica publicará un aviso a costa del prestador de servicio de certificación, informando del cese de actividades y estableciendo la fecha a partir de la cual los certificados que no hayan sido transferidos a otro prestador de servicios de certificación perderán su vigencia.	certificadores y de certificados, así como ejercer el régimen disciplinario en los casos y en la forma previstos en esta Ley y su Reglamento. (...) El cese de la actividad de los entes certificadores puede ser de manera voluntaria, y deberán avisar a los usuarios con un mes de anticipación y 2 meses a la DCFD; pero además, esta Dirección puede suspender o revocar la inscripción de dichos entes y aplicar el régimen disciplinario que corresponda. **Artículo 12 del Decreto Ejecutivo N° 33.018 - Formalidades de la solicitud.** La solicitud de inscripción del certificador se presentará debidamente autenticada ante la DCFD y deberá incluir la siguiente información: 1) Nombre o razón social de la solicitante, número de cédula de persona jurídica, domicilio y dirección postal, así como los correspondientes números telefónicos y de fax (si lo tuviera), su sitio Web en Internet y al

No. 30509 D Gaceta Oficial Digital, miércoles 22 de abril de 2026 48

		Si al momento del cese de actividades por parte del prestador de servicios de certificación, el certificado electrónico calificado de un firmante tiene una vigencia pendiente de uso superior a seis meses, el prestador de servicios de certificación deberá reembolsarle el importe de la tarifa proporcional a la vigencia no utilizada, a menos que el prestador que cese en sus actividades haya transferido los certificados a otro prestador de servicios de certificación. Artículo 20-A de la Ley N° 51 de 2008, adicionado por el artículo 22 de Ley N° 82 de 2012: Registro y certificación electrónica. El Registro Público de Panamá a través de la Dirección Nacional de Firma Electrónica se constituirá en la autoridad certificadora raíz de la República de Panamá, y tendrá a su cargo el Registro de los Prestadores de Servicios de Certificación Electrónica y de Certificación de Firmas Electrónicas. Artículo 21 de la Ley N° 51 de 2008, modificado por el artículo 23 de Ley N° 82 de 2012: Registro de prestadores de servicios de certificación de firmas	menos una dirección de correo electrónico para la recepción de comunicaciones de la DCFD. En el caso de los sujetos privados, deberá adjuntar además una certificación de personería jurídica con no menos de un mes de expedida, o el acuerdo de nombramiento debidamente certificado, en el caso de los funcionarios públicos. Dicho documento deberá acreditar, en el primer supuesto, que la persona jurídica se encuentra debidamente constituida de acuerdo con la ley y en pleno goce y ejercicio de su capacidad jurídica. (Así reformado el inciso el anterior por el artículo 1° del Decreto Ejecutivo N° 34890 del 27 de octubre de 2008). 2) Identificación completa de la persona o personas que fungirán como responsables administrativos del certificador ante la DCFD. Ésta o éstas necesariamente serán los firmantes de la gestión y ostentarán la representación legal u oficial de la solicitante. (Así reformado el inciso el anterior por el artículo 1° del Decreto Ejecutivo N° 34890 del 27 de octubre de 2008). 3) Identificación completa de la persona o

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
49

		electrónicas calificadas. Toda persona natural o jurídica, nacional o extranjera, que ofrezca el servicio de certificación de firmas electrónicas calificadas a terceros deberá registrarse ante la Dirección Nacional de Firma Electrónica. Para solicitar el registro, el prestador de servicios de certificación deberá pagar una tasa cuyo monto y procedimiento de pago será determinado por reglamento. Mientras no haya sido reglamentada la tasa, se establece que la tasa de registro será de cinco mil balboas (B/.5,000.00). Cumplidos todos los requisitos, el prestador de servicios de certificación será inscrito en un registro que llevará la Dirección Nacional de Firma Electrónica, el cual será de carácter público. El prestador de servicios de certificación tendrá la obligación de informar a la Dirección Nacional de Firma Electrónica de cualquiera modificación de las condiciones que permitieron su registro. Artículo 4 del Decreto Ejecutivo N° 684 de 18 de octubre de 2013: La Dirección, mantendrá un registro de prestadores de servicios de certificación, el que deberá contener: El número de la resolución que concede el registro, el nombre o	personas que fungirán como responsables técnicos del certificador, si no fueren las mismas del punto anterior. Se entenderá por tales a la persona o personas que recibirán y custodiarán las claves, contraseñas y/o mecanismos de identificación asignados al certificador y que podrán firmar digitalmente en su nombre. 4) La dirección física precisa del establecimiento o local desde el cual se realizará la actividad de certificación digital. 5) Documentación en la cual se demuestre a juicio de la DCFD , que cuenta con los requisitos para brindar el servicio de certificación digital (con personal calificado, con los conocimientos y experiencia necesarios para las labores que realizan, procedimientos de seguridad y de gestión apropiados, así como la infraestructura adecuada para realizar las actividades de certificación digital, todo acorde a los requerimientos de las normas INTE/ISO 21188 versión vigente, INTE-ISO/IEC 17021 versión vigente, así como a las políticas dictadas por la DCFD). Así reformado el inciso el anterior

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
50

		razón social del prestador de servicios de certificación, el domicilio, el número de Registro Único de Contribuyente (RUC) si se trata de un prestador de servicios de certificación del sector privado, el nombre de su representante legal, el número de teléfono, su sitio de dominio electrónico y correo electrónico así como la compañía de seguros con que ha contratado la póliza de seguros que exige la Ley y su número, y cualquier otro documento que acredite identificación que crea pertinente la Dirección. Artículo 5. Para registrarse, quienes pretendan realizar las actividades propias de los prestadores de servicios de certificación deberán presentar ante la Dirección: 1. Poder y solicitud mediante abogado. 2. Señalar su nombre o denominación social, su Registro Único de Contribuyente (RUC), el nombre del representante legal, su domicilio, número telefónico y dirección de correo electrónico, aceptando expresamente dicho medio electrónico como forma de comunicación,	por el artículo 1° del Decreto Ejecutivo N° 34890 del 27 de octubre de 2008) 6) Certificación de composición y propiedad del capital social, si la solicitante fuera una sociedad mercantil. 7) (Derogado este inciso por el artículo 3° del Decreto Ejecutivo N° 34890 del 27 de octubre de 2008). Los entes certificadores deben cumplir con lo indicado en este artículo, sino también podrá la DCFD, proceder con la suspensión o revocación de la inscripción de estos entes.

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
51

		3. Certificación del Registro Público, en la cual conste el nombre de la sociedad, representación legal, directores, dignatarios, apoderados, capital social y vigencia, si el solicitante es una persona jurídica; 4. Resultado final satisfactorio de una auditoria de sistemas y procedimientos realizada por un auditor autorizado por la Dirección. 5. Documentación que acredite que el prestador de servicio de certificación cumple con los requisitos mininos de una infraestructura de clave pública, equipo de personas, una infraestructura física, tecnológica, procedimientos y sistemas de seguridad establecidas en las obligaciones de los prestadores de servicios de certificación y cualquier reglamentación técnica emitida por la Dirección para tal efecto. 6. Presentar las certificaciones obtenidas para sus actividades o servicios y las certificaciones de los dispositivos que utilicen que demuestren conformidad con estándares internacionales	

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
52

		reconocidos. 7. Declaración de prácticas de certificación, de acuerdo con los requisitos establecidos en el artículo 24 de la Ley N° 51 de 2008, en este Decreto Ejecutivo y por la Dirección. 8. Los datos que permitan establecer comunicación con el prestador, incluidos el nombre de dominio de Internet y los datos de atención al público. 9. Documentación que acredite la contratación de una póliza de responsabilidad civil contractual y extracontractual con una compañía de seguros autorizada por la Superintendencia de Seguros y Reaseguros de Panamá para afrontar el riesgo de la responsabilidad por daños y perjuicios que pueda ocasionar el uso de los certificados que expidan. Esta póliza deberá mantenerse siempre vigente. 10. Comprobante del pago de la tasa de registro ante la Dirección. En caso de tratarse de prestadores de servicios de certificación que utilicen infraestructura o servicios	

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
53

		tecnológicos prestados desde el extranjero, se deberá presentar la documentación y certificaciones requeridas traducidas al idioma español y debidamente apostillada o legalizada por la vía consular. La Dirección tendrá la facultad de solicitar ampliación o aclaración sobre los puntos que estime conveniente. El registro deberá ser actualizado permanentemente y es obligación de todo prestador de servicios de certificación informar en cinco (5) días hábiles a la Dirección de todo cambio a la información requerida. Cuando el prestador de servicios de certificación sea una entidad pública, la responsabilidad extracontractual a que se refiere el numeral 9 de este artículo será reclamada a través de la vía gubernativa, y una vez agotada esta, a través de la jurisdicción contencioso administrativa. Artículo 6. Admitida a trámite la solicitud de registro, la Dirección procederá a realizar un examen sobre el cumplimiento de los requisitos y obligaciones exigidas por la Ley, este Decreto	

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
54

		Ejecutivo y las normas técnicas para obtener el registro.	
11	**Sanciones**	**PANAMÁ** Artículo 20-B de la Ley N° 51 de 2008, adicionado por el artículo 22 de Ley N° 82 de 2012: Atribuciones. La Dirección Nacional de Firma Electrónica tendrá la facultad para reglamentar, supervisar y sancionar todas las actividades de los prestadores de servicios de certificación concernientes al registro, comprobación y otorgamiento de firmas electrónicas y firmas electrónicas calificadas a particulares y entidades gubernamentales, así como registrar y/o suspender el registro de dichos prestadores de servicio. Artículo 35 de la Ley N° 51 de 2008, modificado por el artículo 22 de Ley N° 82 de 2012. Responsables. Los prestadores de servicios de certificación de firmas electrónicas registrados ante la Dirección Nacional de Firma Electrónica están sujetos al régimen sancionador establecido en este Título y deberán cumplir las disposiciones establecidas en la presente Ley y sus reglamentos para sus	**COSTA RICA** **Artículo 26 Ley N° 8454 - 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

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
55

		respectivas actividades. Artículo 35-A de la Ley N° 51 de 2008, adicionado por el artículo 22 de Ley N° 82 de 2012: Responsabilidad por alteración, modificación o adulteración de firmas o certificados electrónicos calificados. Las personas que se apoderen, destruyan, modifiquen o adulteren indebidamente los datos de una firma o certificado electrónico durante o después de la fecha de creación del certificado electrónico respectivo responderán penalmente por su actuación y quedarán sujetas a las sanciones tipificadas en el Código Penal, sin perjuicio de la responsabilidad civil o administrativa que pudiera corresponderles. Artículo 38 de la Ley N° 51 de 2008: Sanciones. Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones: 1. Por la comisión de infracciones leves, multa de cien balboas (B/.100.00) hasta mil balboas (B/.1,000.00). 2. Por la comisión de infracciones graves, multa de mil balboas (B/.1,000.00) hasta cien mil balboas (B/.100,000.00).	capital. **Artículo 27 de la Ley N° 8454 - 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 de la Ley N° 8454 - 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,

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
56

		3. Por la comisión de infracciones muy graves, multa de cien mil balboas (B/.100,000.00) hasta quinientos mil balboas (B/.500,000.00). La reiteración en el plazo de cinco años, de dos o más infracciones muy graves, sancionadas con carácter firme, dará lugar a la prohibición de la prestación de servicios de certificación de firmas electrónicas calificadas en la República de Panamá, durante un plazo máximo de dos años. La comisión de una infracción muy grave, una vez levantada la prohibición a que hace referencia este artículo, conllevará la prohibición definitiva de la prestación de servicios de certificación de firmas electrónicas.	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 29 de la Ley N° 8454 - 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 de la Ley N° 8454 - Revocatoria de la inscripción.** Se podrá revocar la inscripción de un certificador cuando:

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
57

			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 de la Ley N° 8454 - 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 de la Ley N° 8454 - 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.
12	**Derechos de los titulares**	**PANAMÁ** Artículo 19 de la Ley N° 51 de 2008, modificado por el artículo 20 de Ley N° 82 de 2012. Solicitud de revocación de la vigencia del certificado electrónico. El firmante podrá voluntariamente solicitar al prestador de servicios de certificación la revocación del certificado de firma electrónica calificada, pero estará obligado a hacerlo en los siguientes casos: ..... Artículo 20 de la Ley 51 N° de 2008: Solicitud de información. El firmante podrá solicitar información al prestador de servicios de certificación, sobre todo asunto relacionado con su certificado o su firma electrónica.	**COSTA RICA** **Artículo 24 de la Ley N° 8454 - Funciones.** La Dirección de Certificadores de Firma Digital tendrá las siguientes funciones: (...) 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. (...) Mediante políticas y resoluciones anexas al tema, se establecen de manera taxativa, los

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
59

		Artículo 23 de la Ley 51 de 2008 . Obligaciones del prestador de servicios de certificación público y privado que expida certificados electrónicos calificados. Todo prestador de servicio de certificación que expida certificados electrónicos calificados deberá cumplir con las siguientes obligaciones: 1. No almacenar, ni copiar los datos de creación de firma de la persona a la que haya prestado sus servicios. 2. Proporcionar al solicitante antes de la expedición del certificado la siguiente información mínima que deberá transmitirse de forma gratuita, por escrito o por vía electrónica:	derechos de los usuarios de los certificados digitales.
13	**Acuerdos de reconocimiento transfronterizo**	**PANAMÁ** Artículo 17 de la Ley N° 51 de 2008, modificado por el artículo 20 de Ley N° 82 de 2012: Reconocimiento de certificados extranjeros. Los certificados emitidos por prestadores de servicios de certificación de firmas electrónicas extranjeros	**COSTA RICA** Ley N° 8454, artículo 13: -Homologación de certificados extranjeros. Se conferirá pleno valor y eficacia jurídica a un certificado digital emitido en el extranjero, en cualesquiera de

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
60

		podrán ser reconocidos en los mismos términos y condiciones establecidos por esta Ley para los certificados calificados en cualquiera de los siguientes casos: 1. Cuando tales certificados sean reconocidos en virtud de acuerdos con otros países, ya sean bilaterales o multilaterales, o efectuados en el marco de organizaciones internacionales de las que Panamá sea parte. 2. Cuando tales certificados sean emitidos por prestadores de servicios de certificación debidamente avalados en su país de origen por instituciones homólogas a la Dirección Nacional de Firma Electrónica del Registro Público, que requieren para su reconocimiento estándares que garanticen la seguridad en la creación del certificado y la regularidad de los detalles del certificado, así como su validez y vigencia. 3. Cuando se acredite que tales certificados fueron emitidos por un prestador de servicios de certificación que cumple con los estándares mínimos requeridos para un prestador de servicios de certificación de firmas electrónicas registrado ante la Dirección Nacional de Firma Electrónica del Registro Público.	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.

No. 30509 D
Gaceta Oficial Digital, miércoles 22 de abril de 2026
61

V. CONCLUSIÓN

Mediante el Convenio, la República de Panamá y la República de Costa Rica han convenido que los certificados de firma electrónica calificada (Panamá) o firma digital certificada (Costa Rica) de persona física emitidos en cada país tendrán la misma validez jurídica para la otra parte, siempre que sean emitidos por una prestadora de servicios de certificación, y que se cumpla con las condiciones establecidas en esta minuta y en la minuta técnica.

Unido a lo anterior, se puede afirmar que las partes reconocen en el Convenio una asimetría en los marcos jurídicos nacionales sobre la materia, respecto de la cual es fundamental garantizar la seguridad jurídica, en un marco que asegure la compatibilidad y fiabilidad reciproca de los sistemas tecnológicos y la regulación aplicable de cada país.

En este orden de ideas, cabe señalar que los artículos citados del Convenio plasman la compatibilidad tecnológica, estableciendo parámetros comunes para el reconocimiento de validez de las firmas electrónica calificadas o firmas digital certificada, y promulgando la creación de mecanismos de control sobre los Certificadores Registrados y los Prestadores de Servicios de Certificación. Así las cosas, es dable entender que las partes cuentan con medios tecnológicos homologables para llevar a cabo los objetivos del Acuerdo, o bien, estos pueden ser implementados con relativa facilidad, conclusión que ha sido respaldado por las partes.

Así, en atención al análisis expuesto en las páginas precedentes, estas divisiones jurídicas no han identificado incompatibilidades normativas para la suscripción e implementación práctica del Acuerdo.

MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES | GOBIERNO DE COSTA RICA

Minuta: Dirección de Certificadores de Firma Digital (DCFD)
Tema: Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital entre la República de Costa Rica y la República de Panamá

Basado en el constante desarrollo de las tecnologías de la información y en las relaciones comerciales que tiene la República de Costa Rica y la República de Panamá, se ha llegado a la convicción que las firmas digitales, basados en certificados electrónicos, permiten una mayor fluidez para las transacciones económicas de cada país.

Es por lo anterior que la Dirección de Gobernanza Digital y Certificadores de Firma Digital, analizará las condiciones que se deben cumplir para que dicho acto permita garantizar que los certificados de firma digital emitidos en una de las partes tengan la misma validez jurídica para la otra.

Para sustentar la validez jurídica (desde el punto de vista técnico), el Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital establecerá las bases y principios que se deben tener para que este sea implementado, donde las principales consideraciones son:

a) Qué, los certificados electrónicos sean entregados por un prestador de servicios de certificación.
b) Qué, estos respondan a formatos reconocidos internacionalmente, conforme lo establezca la autoridad designada por cada parte.
c) Qué, contengan como mínimo, datos que permitan identificar fehacientemente a su titular y al prestador de servicios de certificación que lo emitió.
d) Qué, en el certificado se debe indicar el periodo de vigencia y los datos que permitan la identificación única de este.
e) Qué, permita la verificación respecto de su estado de revocación y se establezcan la política de certificación bajo la cual fue emitido.

Adicionalmente a lo definido en la estructura del certificado, las partes deben prever la evaluación y armonización de los aspectos normativos, los cuales aseguren la existencia de estándares, que permitan establecer las prácticas de certificación, el marco regulatorio referente a la Firma Digital Certificada/ Firma Electrónica Calificada respectivamente.

MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES | GOBIERNO DE COSTA RICA

Teniendo en consideración lo expuesto en los párrafos anteriores, se desarrolló por los encargados técnicos de cada país, una matriz comparativa que unifica las normas y principios, que permiten establecer las bases para la emisión de certificados electrónicos. Donde esta da como resultado que ambos países trabajan bajo estándares similares, los cuales se ajustan al cumplimiento de las disposiciones de la Ley N°8454 del 15 de octubre del 2005 y su reglamento, de la República de Costa Rica y la Ley Nº 82 del 9 de noviembre de 2012, de la República de Panamá.

PRINCIPIOS / DISPOSICIONES TECNICAS		NORMATIVA DE CADA PAÍS	
1	Prácticas de Certificación	**COSTA RICA** • RFC 3647: "Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework". • La Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v.2, se adhiere a los lineamientos establecidos en: la norma INTE-ISO-21188 "Infraestructura de llave pública para servicios financieros — Estructura de prácticas y políticas" versión vigente o el estándar Trust Service Principles and Criteria for Certification Authorities Versión vigente – Webtrust. • La Política de Formato Oficial v2.0, establece que los documentos electrónicos firmados digitalmente, están construidos con base en los formatos avanzados emitidos como normas técnicas y estándares ETSI.	**PANAMÁ** • RFC 3647-Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. • Política de Certificación de Certificados de Persona Natural (v0.4). https://www.firmaelectronica.gob.pa/normativa/P-12-Politica-de-Certificacion-de-Certificados-de-Persona-Natural.pdf • Política de Certificación de Firma Electrónica Calificada en la Nube (v0.0). https://www.firmaelectronica.gob.pa/normativa/P-27-PC-Firma-Electronica-en-la-Nube.pdf
2	Seguridad de la Información	**COSTA RICA** • La evaluación de una autoridad certificadora que desea incorporarse al Sistema de Certificación Nacional se adhiere a los lineamientos establecidos en: la norma INTE-ISO-21188 "Infraestructura de llave pública para servicios financieros — Estructura de	**PANAMÁ** • Los documentos de los certificadores licenciados en Panamá se fundamentan en el marco legal nacional (Ley N.º 51 de 2008 y Ley N.º 82 de 2012) y en el estándar internacional RFC 3647, que establece la

		prácticas y políticas" versión vigente o el estándar Trust Service Principles and Criteria for Certification Authorities Version vigente – Webtrust. • FIPS 140 (Federal Information Processing Standards) nivel 3.	estructura de la Declaración de Prácticas de Certificación y Políticas de Certificación. • FIPS 140 (Federal Information Processing Standards) nivel 3.
3	Estructura de Certificados / Certificados de Claves Publicas y Atributos	**Costa Rica** Los certificados digitales deben cumplir con: • Estándar X.509 versión 3. • RFC 3280: 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"	**PANAMÁ** Los certificados digitales deben cumplir con: • RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
4	Repositorio de Información	**Costa Rica** • Establecido en el artículo 19 del Reglamento de la Ley No.8454 "Ley de Certificados, Firmas Digitales y Documentos Electrónicos", que define las atribuciones y responsabilidades de los certificadores registrados.	**PANAMÁ** • Se mantiene según un repositorio donde se publican los certificados emitidos, las listas de revocación (CRL) y la documentación de las prácticas y políticas de certificación, conforme al marco de la Declaración de Prácticas de Certificación aprobado por la Dirección Nacional de Firma Electrónica.
5	Sellado de Tiempo/Time Stamping	**Costa Rica** A continuación se señalan los estándares incluidos en la Política de sellado de tiempo del sistema nacional de certificación digital: • RFC 3161: "Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)".	**PANAMÁ** Estándares incluidos en la política de sellado de tiempo: • RFC 3628 - "Policy requirements for time-stamping authorities". • RFC 3161 (Time Stamp Protocol) y su actualización RFC 5816.

		• RFC 3628: "Policy Requirements for Time-Stamping Authorities (TSAs)".	
6	Otras especificaciones técnicas relativas al uso de la Firma Electrónica / Digital	**Costa Rica** Los siguientes documentos referenciados son aplicados (entre otros ya mencionados anteriormente) para la confección de las políticas de certificación, según lo normado en la Política de Certificados para la Jerarquía Nacional de Certificadores Registrados: • RFC 2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP". • INTE-ISO/IEC 19011 "Directrices para la auditoría de sistemas de gestión de la calidad y/o ambiental". • INTE-ISO/IEC 17021 Evaluación de la conformidad — Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión.	**PANAMÁ** • RFC 4055] "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" para RSA. • RFC 6960 – X.509 Infraestructura de Clave Pública Internet. PKI Protocolo en línea del Estado del Certificado – OCSP. • RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". • RFC 3739 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".

Realizada esta comparativa y teniendo en consideración que la denominada "firma digital certificada" de la República de Costa Rica y la "firma electrónica calificada" de la República de Panamá se encuentran construidas bajo estándares X.509[1], donde a su vez, los certificados digitales son resguardado bajo normas de seguridad criptográfica FIPS PUB 140-2[2](3) y gestionado mediante controles de seguridad de la información ISO/NCh 27002[3]o similar, se toma la determinación por parte de la Dirección de Gobernanza Digital y Certificadores de Firma Digital, que es necesario verificar que estos elementos son aplicados a la información (certificados de pruebas - Prácticas y Políticas de certificación) presentada por la República de Costa Rica. Para ello, estos contenidos serán validados a través de los controles técnicos de la guía de acreditación de firma electrónica avanzada y esta da como resultado:

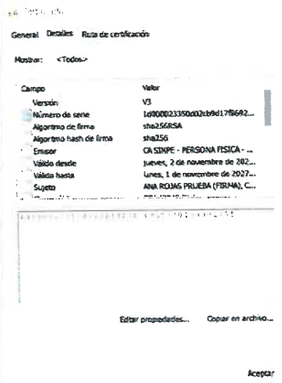
República de Costa Rica

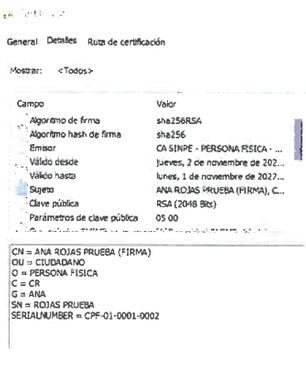
[1] X.509: Standards for Public Key Infrastructure.

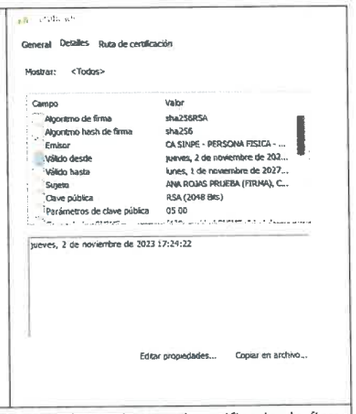
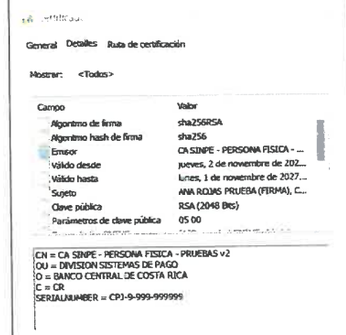
[2] FIPS PUB 140-2: Security Requirements for Cryptographic Modules.

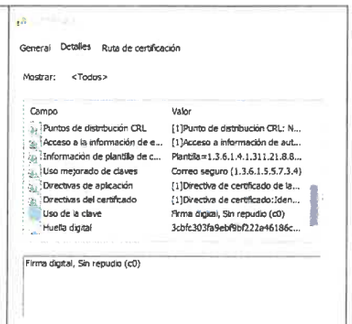
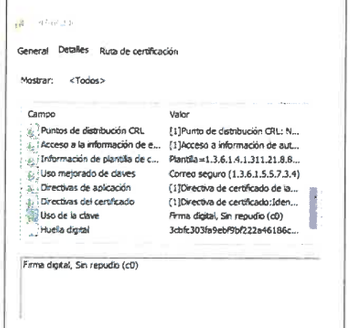
[3] ISO/NCh27002: Código de práctica para la gestión de seguridad de la información.

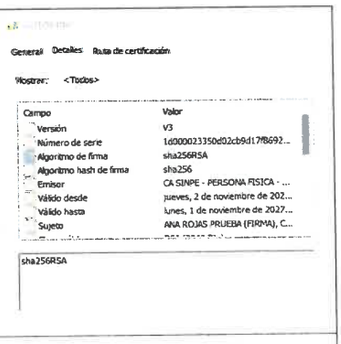
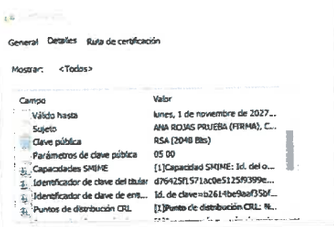
- **TB01: Estructura de Certificados de la República de Costa Rica.**

Objetivo			
Comprobar los aspectos mínimos que disponen la Ley y su Reglamento con relación a la conformidad con el estándar, contenidos mínimos, incorporación del RUT, límites y atributos del certificado de firma electrónica avanzada.			
ID	**NOMBRE**	**OBSERVACIÓN**	**EVIDENCIA**
1	Conformidad con el estándar ISO/IEC 9594-8.		
	Se verificará que la estructura básica del certificado esté en conformidad a la norma y que la gramática utilizada tanto en la estructura básica como en las extensiones obligatorias para incluir, puedan ser leídos por cualquier aplicación que cumpla dicho el estándar.	La estructura básica de los certificados de firma digital en Costa Rica cumple con el estándar ISO/IEC 9594-8. Dado que se cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 3 (Identificación y autenticación). Los certificados son emitidos en cumplimiento con el estándar ITU X.509 versión 3.	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación.  POLÍTICA DE CERTIFICADOS PARA LA JERARQUÍA NACIONAL DE CERTIFICADORES REGISTRADOS Dirección de Gobernanza Digital Certificadores de Firma Digital Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones
2	Contenido básico del certificado de firma electrónica avanzada emitido por el PSC.		
	Se verificará que el certificado contiene la siguiente información:		
	a) Un código de identificación único del certificado;	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 3 (Identificación y autenticación). Los certificados son emitidos en cumplimiento con el estándar X.509 versión 3. https://www.mifirmadigital.go.cr/?page_id=25#	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación.  General Detalles Ruta de certificación Mostrar: <Todos> Campo / Valor Versión: V3 Número de serie: 1d9000233500002cb9d17f5692... Algoritmo de firma: sha256RSA Algoritmo hash de firma: sha256 Emisor: CA SINPE - PERSONA FISICA - ... Válido desde: jueves, 2 de noviembre de 202... Válida hasta: lunes, 1 de noviembre de 2027... Sujeto: ANA ROJAS PRUEBA (FIRMA), C... Editar propiedades... Copiar en archivo... Aceptar
	b) Identificación del prestador de	Cumple el requerimiento con el documento "Política de Certificados para	Se adjunta la información en la carpeta "Documentos Verificados" y se deja

	servicio de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada;	la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 3 (Identificación y autenticación). Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 3 (Identificación y autenticación). El certificado contiene el "Identificador de Clave de Entidad Emisora" que permite identificar al emisor del certificado.	registro mediante la imagen que se asocia a continuación. 
	c) Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre completo y número de documento de identidad nacional	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 3 (Identificación y autenticación). En el campo denominado "Sujeto", se identifican: CN=Nombre y Apellido. SERIALNUMBER= Documento de Identidad. C= Código ISSO país.	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante las imágenes que se asocian a continuación. 
	d) Su plazo de vigencia.	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 7 (Perfiles de Certificados, CRL y OCSP).	

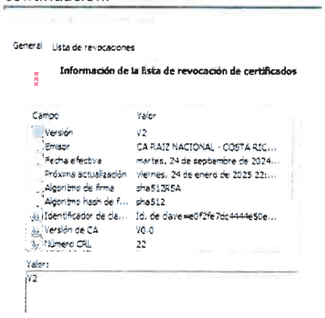
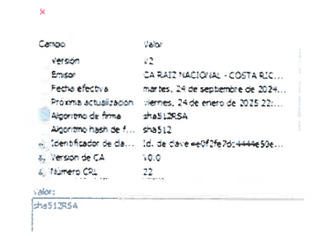
			
3	Lectura y reconocimiento del contenido mínimo cuando existen atributos adicionales en el certificado de firma electrónica avanzada emitido por el PSC.		
	Se verificará que el Certificador Registrado estructure sus certificados de firma electrónica avanzada de forma que los atributos adicionales que introduzca con el fin de incorporar límites al uso del certificado	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 7 (Perfiles de Certificados, CRL y OCSP).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante las imágenes que se asocian a continuación. 
4	Reconocimiento de límites de uso del certificado de firma electrónica avanzada por terceros.		
	Se verificará que el PSC estructure sus certificados de firma electrónica avanzada de forma que los límites de uso, si los hay, sean reconocibles por terceros.	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 1.4.1 (Usos apropiados del certificado).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación.

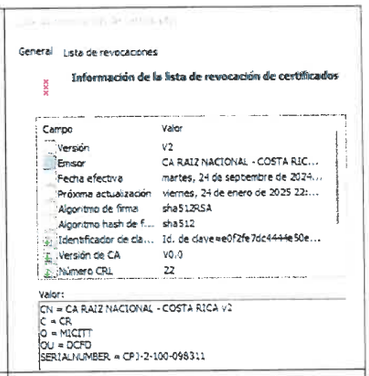
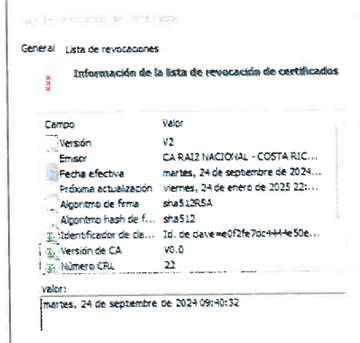
			
5	Uso de clave pública acreditada.		
	Se verificará que los datos de creación de firma del Certificador Registrado para emitir certificados de firma electrónica avanzada no sean utilizados para certificados emitidos bajo otras políticas.	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 1.4.1 (Usos apropiados del certificado).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante las imágenes que se asocian a continuación. 
6	Algoritmos de firma.		
	Se verificará que el Certificador Registrado utilice algoritmos de firma estándares de la industria que provean el adecuado nivel de seguridad tanto para su propia firma como para la firma del titular.	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 7 (Perfiles de Certificados, CRL y OCSP).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación.

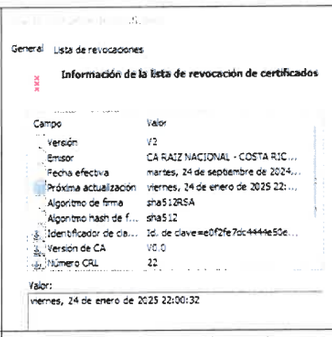
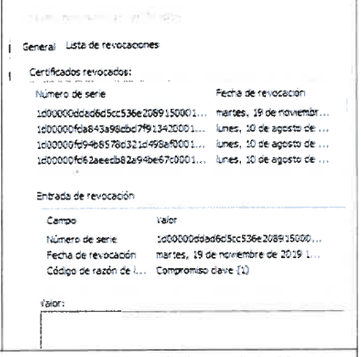
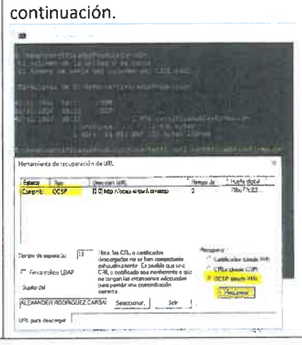
			
7	Largos de llaves.		
	Se verificará que el Certificadores Registrados utilice largos de llave pública y privada tales que provean el nivel de seguridad prevaleciente en la industria tanto para su propia firma como para la firma del titular.	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 7 (Perfiles de Certificados, CRL y OCSP).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación. 
8	Funciones Hash.		
	Se verifica que el Certificador Registrado utilice funciones Hash estándares de la industria, para el proceso de firma, que provean el adecuado nivel de seguridad tanto para su propia firma como para la firma del titular.	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 7 (Perfiles de Certificados, CRL y OCSP).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación. 

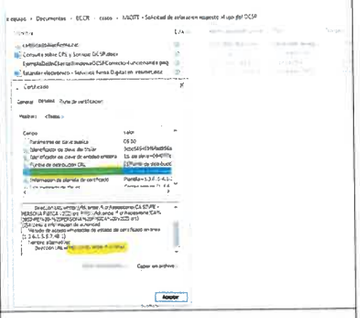
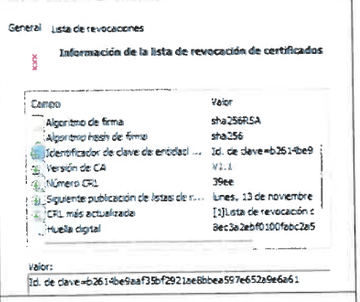
- **TB02: Estructura CRL y Servicio OCSP de la República de Costa Rica.**

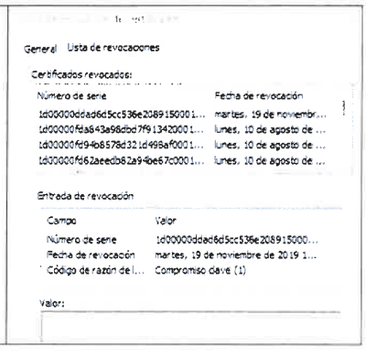
Objetivo

Verificar que las listas de certificados revocados de firma electrónica avanzada tengan el formato y contenido especificado en el estándar, y permita al usuario identificar plenamente al Certificador Registrado emisor de la CRL. Verificar el estado de los certificados de firma electrónica avanzada tengan el formato y contenido especificado en el estándar, y permita al usuario identificar plenamente el estado del certificado emitido por el Certificador emisor.			
ID	**NOMBRE**	**OBSERVACIÓN**	**EVIDENCIA**
1	Contenido Mínimo.		
	Se verificará que la CRL contenga al menos la siguiente información:		
	a) Versión debe tener el valor 2	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 7.2.1 (Número(s) de versión).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación. 
	b) Algoritmo de firma. Este campo debe contener la identificación del algoritmo de firma utilizado.	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 7.2. (Perfil de la CRL).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación. 
	c) Nombre del emisor. Este campo debe contener el nombre de la entidad que emitió y firmó la lista de certificados revocados.	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 7.2. (Perfil de la CRL).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación.

			
	d) Fecha actual. Este campo debe contener la fecha y hora en que fue emitida la lista de certificados revocados (CRL)	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 7.2. (Perfil de la CRL).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación. 
	e) Próxima actualización. Se debería incluir en este campo la fecha en que, a más tardar, se emitirá la próxima lista de certificados revocados.	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 7.2. (Perfil de la CRL).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación:

			
	f) Certificados revocados. En este campo se deben incluir los números de serie de los certificados revocados por el emisor, indicando además la fecha y hora de revocación correspondiente.	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 7.2. (Perfil de la CRL).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación. 
	Se verificará que el Servicio OCSP del PSC esté implementado de acuerdo con el estándar RFC 2560 en sus mecanismos de:		
	a) Petición de Validación y Respuesta.	Se cumple con el estándar RFC 2560. De acuerdo con lo establecido en el documento denominado "ESTÁNDAR ELECTRÓNICO SERVICIOS FIRMA DIGITAL EN INTERNET SERIE DE NORMAS Y PROCEDIMIENTOS". Utilitario estándar del Sistema Operativo Windows (certutil) para probar que somos compatibles con el protocolo OCSP a nivel internacional (Similar a OpenSSL): certutil-url certificadoAValidarConOCSP.cer Detalle del estándar (RFC) del servicio OCSP con el cual somos compatibles:	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación. 

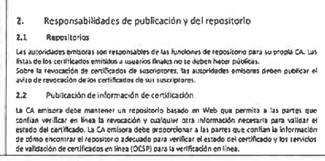
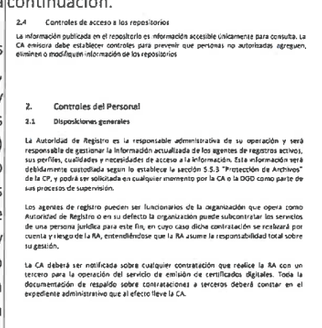
		https://www.ietf.org/rfc/rfc2560.txt	Dirección actual de nuestro servicio de OCSP: (esta "quemado" en cada certificado la ruta de dicho servicio): http://ocsp.sinpe.fi.cr/ocsp 
2	Comprobación de firma.		
	Se verificará que la lista de certificados revocados esté debidamente firmada por el Certificador emisor.	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 7.2. (Perfil de la CRL).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación. 
3	Mecanismo de suspensión de certificados.		
	Se verificará que la lista de certificados revocados puede incluir la información necesaria para indicar el estado de suspensión de un certificado.	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 7.2. (Perfil de la CRL).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación.

- **TB03: Registro de Acceso Público de la República de Costa Rica.**

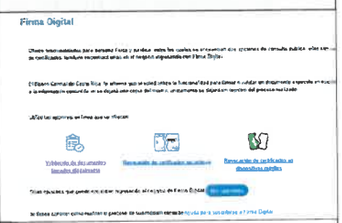
Objetivo			
Asegurar el acceso a información relevante descriptiva del sistema por parte de los titulares y terceros.			
ID	**NOMBRE**	**OBSERVACIÓN**	**EVIDENCIA**
1	Existencia y contenido mínimo del sitio de información pública.		
	El Certificador Registrado debe mantener un sitio de acceso electrónico, en el cual mantenga la información relevante para los titulares y las partes que confían. Debe contener al menos los siguientes documentos:		
	a) Registro de certificados emitidos, indicando código de identificación único del certificado y su estado (vigente, suspendido o revocado)	Actualmente en Costa Rica, se tiene una Autoridad Certificadora, que corresponde al Banco Central de Costa Rica (BCCR). Sin embargo la normativa vigente (Ley N.8454, capítulo tercero) permite la inclusión de más certificadores registrados. Banco Central de Costa Rica: https://www.bccr.fi.cr/firma-digital/informaci%C3%B3n-general/certificados-y-listas-de-revocaci%C3%B3n MICITT: https://www.mifirmadigital.go.cr/	Se deja registro mediante las imágenes que se asocian a continuación: 
	b) Copia de la Lista de certificados revocados (CRL) actualizada cada 24 horas.	Por medio del siguiente enlace, se puede visualizar la lista CRL actualizada: https://www.bccr.fi.cr/firma-digital/informaci%C3%B3n-general/certificados-y-listas-de-revocaci%C3%B3n	Se deja registro mediante las imágenes que se asocian a continuación: 
	c) Si es pertinente, indicar si el certificado ha sido traspasado de	No aplica.	No aplica.

	otro prestador de servicios de certificación acreditado o ha sido homologado.		
	d) Acceso seguro a los titulares para realizar la revocación o suspensión de certificados vigentes.	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 3.4 (Perfiles de Certificados, CRL y OCSP).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante las imágenes que se asocian a continuación.  FIRMA DIGITAL_ **POLÍTICA DE CERTIFICADOS PARA LA JERARQUÍA NACIONAL DE CERTIFICADORES REGISTRADOS** Dirección de Gobernanza Digital Certificadores de Firma Digital Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones
	e) Política del certificado de firma electrónica avanzada.	Mediante la Ley N.8454 y su reglamento, se regulan las políticas asociadas a la firma digital certificada en Costa Rica, entre ellas la "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados".	Se adjunta registro de la normativa vigente referente, por medio de URL: https://www.mifirmadigital.go.cr/?page_id=25#
	f) Declaración de sus Prácticas de Certificación.	El Director de la Dirección de Gobernanza Digital es 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. Lo anterior, de acuerdo a lo establecido en la Ley N.8454 y su reglamento.	Se adjunta registro de la normativa vigente referente, por medio de URL: https://www.mifirmadigital.go.cr/?page_id=25#
	g) Resoluciones de la Entidad Acreditadora que le afecten.	No aplica.	No aplica.
	h) Servicio de consulta en línea de estado de un certificado (OCSP).	En cumplimiento con el estándar RFC 2560.	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante las imágenes que se asocian a continuación.

			
2	Disponibilidad de la información pública.		
	Se debe asegurar una disponibilidad del sitio no menor al 99%. Para esto se verificará la existencia de mecanismos redundantes o alternativos de conexión y sitios de emergencia que se levanten manual o automáticamente en caso de desastres.	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 2 (Responsabilidades y publicación del repositorio).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante las imágenes que se asocian a continuación. 
3	Seguridad.		
	Se debe proteger la integridad y disponibilidad de la información mediante el uso de tecnología y medidas de seguridad tanto físicas como lógicas que reduzcan los riesgos y consecuencias de ataques maliciosos en contra de los sitios tanto internos como externos.	Cumple el requerimiento con el documento "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados v2", en su numeral 2.4 (Controles de acceso a los repositorios). Además se cuenta con la Directriz para las Autoridades de Registro que establece, entre otras cosas, la operación y procedimientos mínimos adoptados por las Autoridades de Registro (en adelante RA) que gestionan el proceso de emisión y/o revocación de los certificados digitales dentro de la Jerarquía Nacional de Certificadores Registrados de Costa Rica, y es un complemento del documento "Política de Certificados para la jerarquía nacional de certificadores registrados" (en adelante CP).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación. 

- **TB04: Modelo de Confianza de la República de Costa Rica.**

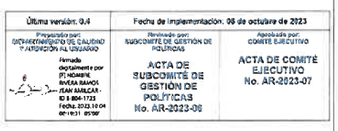
Objetivo

Verificar que el PSC provea a los titulares de certificados de firma electrónica avanzada emitidos por él, de un mecanismo de confianza que le permita comprobar la validez de cualquier certificado de firma electrónica avanzada que reciba.			
ID	**NOMBRE**	**OBSERVACIÓN**	**EVIDENCIA**
1	**Modelo de confianza.**		
	Se evaluará si el modelo de confianza adoptado permite cumplir con el objetivo planteado.	Por medio del sitio https://www.mifirmadigital.go.cr/ se puede verificar los Certificadores Registrados. De igual forma, en la página del Certificador Registrado se dispone de la información referente a la firma digital certificada.	Se deja registro mediante la imagen que se asocia a continuación. Página MICITT:  Página del Certificador Registrado: 
2	**Efectividad.**		
	Se verifica el mecanismo utilizado para implementar el modelo de confianza en forma práctica.	Se cumple mediante herramienta de verificación de documentos https://www.centraldirecto.fi.cr/spa/Bccr.Firma.InformacionPublica.CD.spa/#/	
3	**TSL.**		
	Se evaluará la implantación de TSL de acuerdo con la norma.	No se cuenta con TSL implementada. La validación de los certificados se realiza por medio de CRL y OCSP.	No aplica.

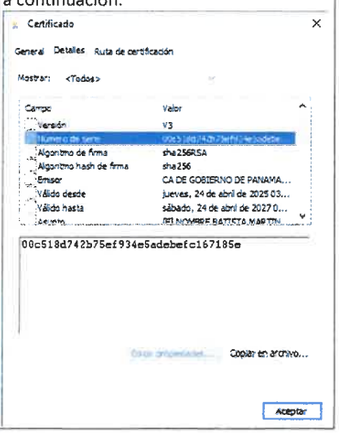
República de Panamá

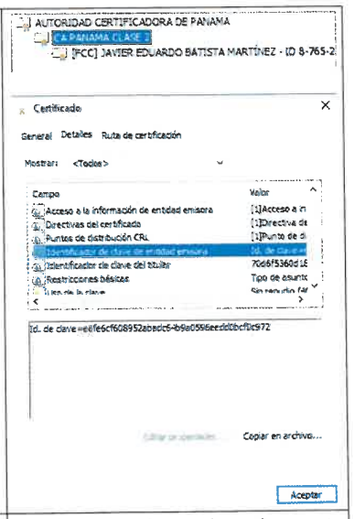
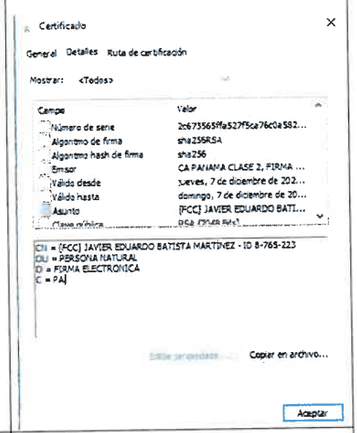
- **TB01: Estructura de Certificados de la República de Panamá.**

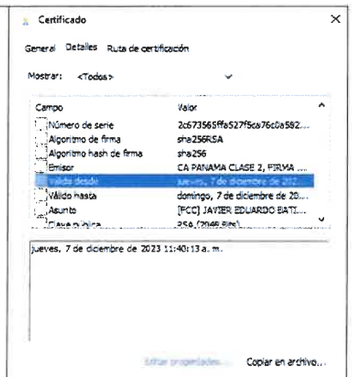
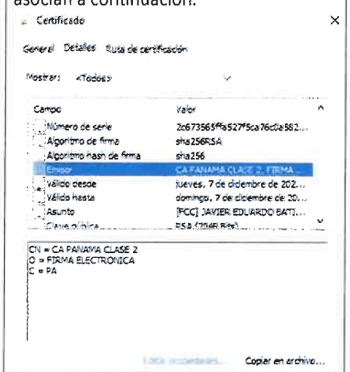
Objetivo			
Comprobar los aspectos mínimos que disponen la Ley y su Reglamento con relación a la conformidad con el estándar, contenidos mínimos, límites y atributos del certificado de firma electrónica avanzada.			
ID	**NOMBRE**	**OBSERVACIÓN**	**EVIDENCIA**

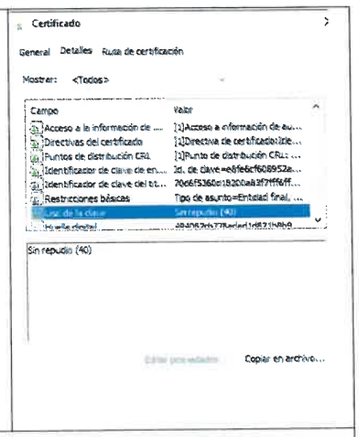
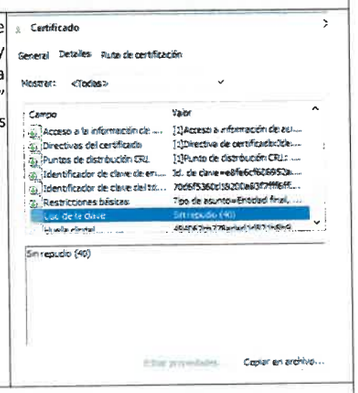
<table>
<tr><td>1</td><td colspan="3">Conformidad con el estándar ITU X.509 versión 3</td></tr>
<tr><td></td><td>Se verificará que la estructura básica del certificado esté en conformidad a la norma y que la gramática utilizada tanto en la estructura básica como en las extensiones obligatorias para incluir, puedan ser leídos por cualquier aplicación que cumpla dicho el estándar.</td><td>Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0", en su numeral 7.1 (Perfil de certificado). Los certificados son emitidos cumpliendo las especificaciones ITU X.509 versión 3.</td><td>Se adjunta la información en la carpeta “Documentos Verificados” y se deja registro mediante la imagen que se asocia a continuación.
P-12
POLITICA DE CERTIFICACIÓN
CERTIFICADO DE PERSONA NATURAL
 

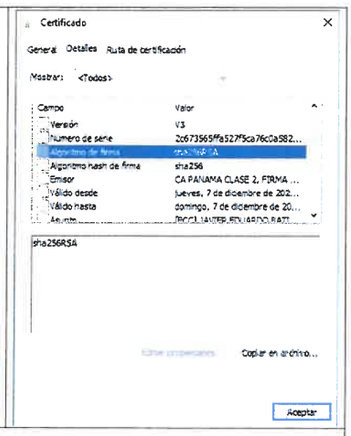
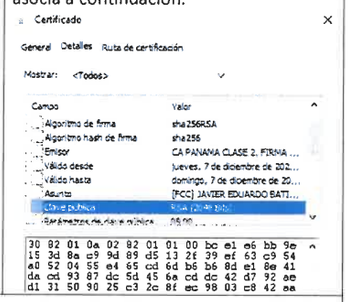
P-27
POLITICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA CALIFICADA EN LA NUBE
 
</td></tr>
<tr><td>2</td><td colspan="3">Contenido básico del certificado de firma electrónica avanzada emitido por el PSC.</td></tr>
<tr><td></td><td colspan="3">Se verificará que el certificado contiene la siguiente información:</td></tr>
<tr><td></td><td>a) Un código de identificación único del certificado;</td><td>Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0", Punto número 7.1 de Perfil de certificado. Los certificados son emitidos cumpliendo las especificaciones ITU X.509 versión 3.
https://www.firmaelectronica.gob.pa/normativa/P-12-Politica-de-Certificacion-de-Certificados-de-Persona-Natural.pdf

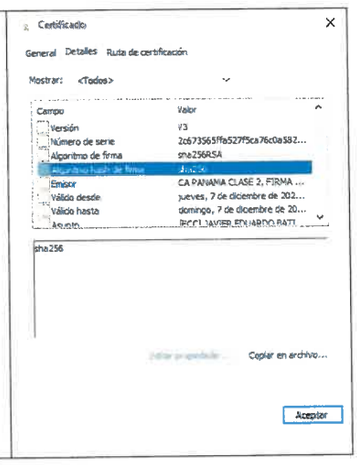
https://www.firmaelectronica.gob.pa/normativa/P-27-PC-Firma-Electronica-en-la-Nube.pdf</td><td>Se adjunta la información en la carpeta “Documentos Verificados” y se deja registro mediante la imagen que se asocia a continuación.
 
</td></tr>
</table>

	b) Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, número de identificación tributaria, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada;	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0" Punto número 7.1 de Perfil de certificado. Certificado Intermedio "CA PANAMA CLASE 2" y el certificado del titular "[FCC] NOMBRE(S) APELLIDO(S) – ID NUMERO-CEDULA". Adicionalmente se puede identificar el "Identificador de Clave de Entidad Emisora" el cual permite Identificar al emisor del certificado.	
	c) Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico, su número de identificación tributaria, cedula de vecindad, código único de identificación o pasaporte según corresponda.	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0", Punto número 7.1 de Perfil de certificado. Campo Asunto, allí se identifican CN= [FCC] NOMBRE(S) APELLIDO(S) – ID NUMERO-CEDULA, OU = PERSONA NATURAL, O = FIRMA ELECTRONICA, C = Código ISO del País.	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante las imágenes que se asocian a continuación. 
	d) Su plazo de vigencia.	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0", en su numeral 7.1 (Perfil de certificado), campo validez desde, hasta.	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante las imágenes que se asocian a continuación.

			
3	Lectura y reconocimiento del contenido mínimo cuando existen atributos adicionales en el certificado de firma electrónica avanzada emitido por el PSC.		
	Se verificará que el Prestador de Servicios de Certificación autorizado, estructure sus certificados de firma electrónica avanzada de forma que los atributos adicionales que introduzca con el fin de incorporar límites al uso del certificado	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0" Punto número 7.1 de Perfil de certificado.	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante las imágenes que se asocian a continuación. 
4	Reconocimiento de límites de uso del certificado de firma electrónica avanzada por terceros.		
	Se verificará que el PSC estructure sus certificados de firma electrónica avanzada de forma que los límites de uso, si los hay, sean reconocibles por terceros.	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0". Punto número 7.1 de Perfil de certificado mediante la definición de Uso de Claves.	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación.

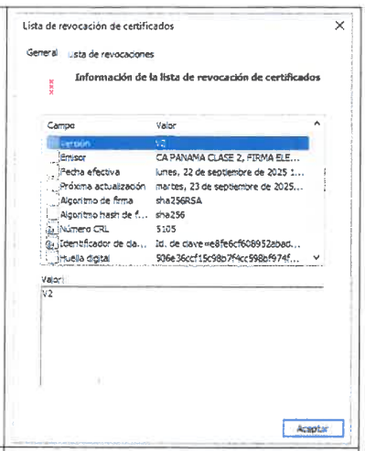
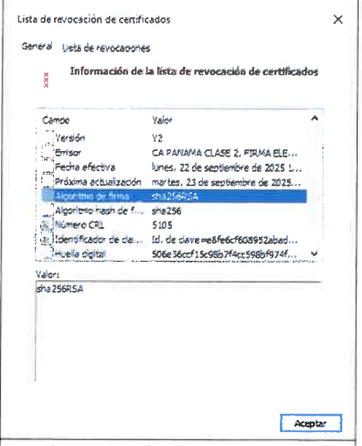
			
5	Uso de clave pública acreditada.		
	Se verificará que los datos de creación de firma del Certificador Registrado para emitir certificados de firma electrónica avanzada no sean utilizados para certificados emitidos bajo otras políticas.	Se establece en "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0" Punto número 1.4 de "Uso de los certificados".	
6	Algoritmos de firma.		
	Se verificará que el Certificador Registrado utilice algoritmos de firma estándares de la industria que provean el adecuado nivel de seguridad tanto para su propia firma como para la firma del titular.	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0". Punto número 7.1 de Perfil de certificado.	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación.

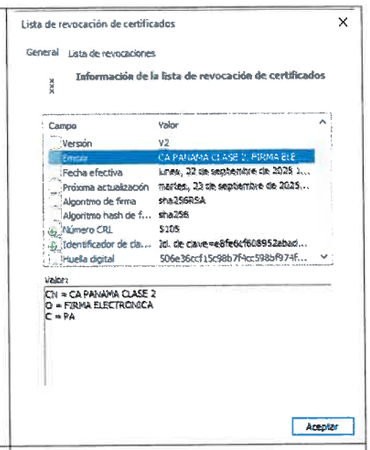
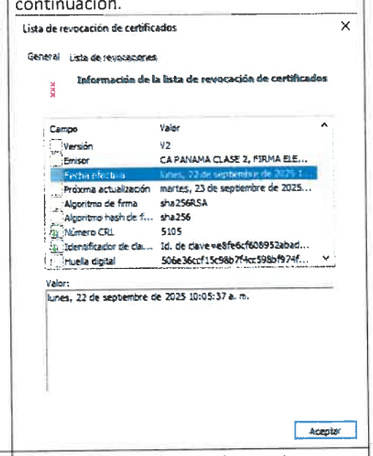
			
7	Largos de llaves.		
	Se verificará que los PSC utilicen largos de llave pública y privada tales que provean el nivel de seguridad prevaleciente en la industria tanto para su propia firma como para la firma del titular.	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0". Punto número 7.1 de Perfil de certificado.	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación. 
8	Funciones Hash.		
	Se verifica que el PSC utilice funciones Hash estándares de la industria, para el proceso de firma, que provean el adecuado nivel de seguridad tanto para su propia firma como para la firma del titular.	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0". Punto número 7.1 de Perfil de certificado.	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación.

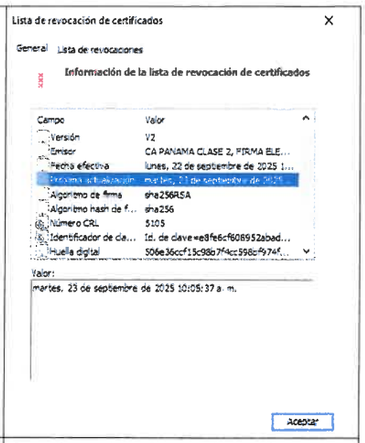
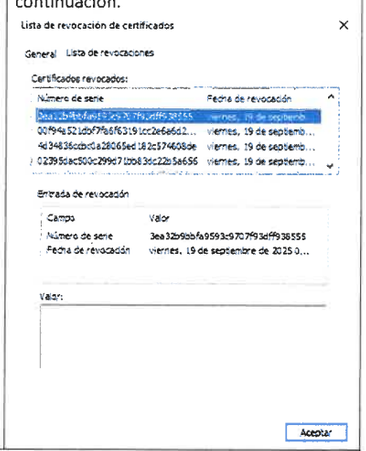
			

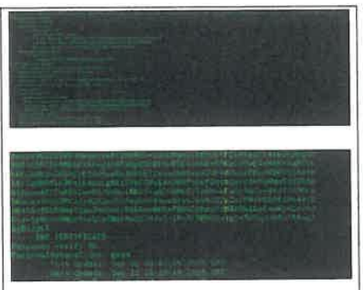
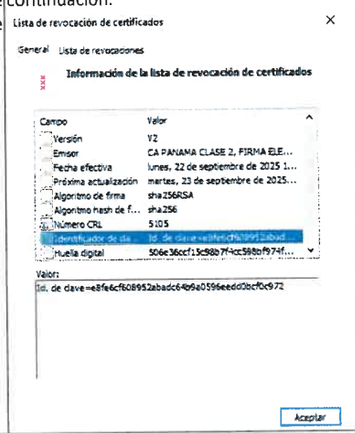
- **TB02: Estructura CRL y Servicio OCSP de la República de Panamá.**

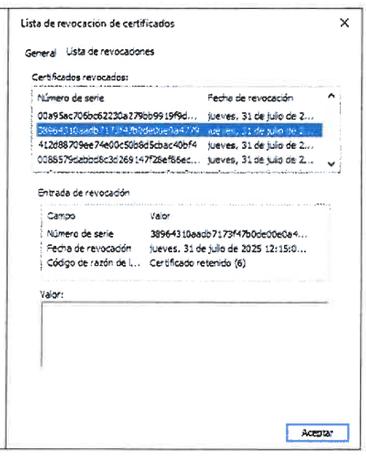
Objetivo			
Verificar que las listas de certificados revocados de firma electrónica avanzada tengan el formato y contenido especificado en el estándar, y permita al usuario identificar plenamente al Prestador de Servicios de Certificación emisor de la CRL. Verificar el estado de los certificados de firma electrónica avanzada tengan el formato y contenido especificado en el estándar, y permita al usuario identificar plenamente el estado del certificado emitido por el PSC emisor.			
ID	**NOMBRE**	**OBSERVACIÓN**	**EVIDENCIA**
1	Contenido Mínimo.		
	Se verificará que la CRL contenga al menos la siguiente información:		
	a) Versión debe tener el valor 2	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0", en su numeral 7.2 (Perfil de CRL) , campo (Versión).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación.

			
	b) Algoritmo de firma. Este campo debe contener la identificación del algoritmo de firma utilizado.	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0", en su numeral 7.2 (Perfil de CRL).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación. 
	c) Nombre del emisor. Este campo debe contener el nombre de la entidad que emitió y firmó la lista de certificados revocados.	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0", en su numeral 7.2 (Perfil de CRL).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación.

			
	d) Fecha efectiva. Este campo debe contener la fecha y hora en que fue emitida la lista de certificados revocados (CRL)	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0", en su numeral 7.2 (Perfil de CRL).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación. 
	e) Próxima actualización. Se debería incluir en este campo la fecha en que, a más tardar, se emitirá la próxima lista de certificados revocados.	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0", en su numeral 7.2 (Perfil de CRL).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación.

			
	f) Certificados revocados. En este campo se deben incluir los números de serie de los certificados revocados por el emisor, indicando además la fecha y hora de revocación correspondiente.	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0", en su numeral 7.2 (Perfil de CRL).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación. 
	Se verificará que el Servicio OCSP del PSC esté implementado de acuerdo con el estándar RFC 6960 en sus mecanismos de:		
	a) Petición de Validación y Respuesta.	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0". Autoridades de Validación (VA) definido en el numeral 1.3.5, "Este mecanismo de validación es complementario a la publicación de las	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación.

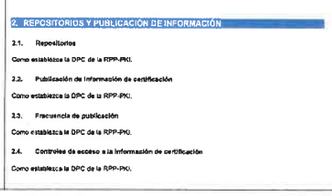
		listas de certificados revocados (CRL)." y 7.3 que establece el Perfil de OCSP.	
2	Comprobación de firma.		
	Se verificará que la lista de certificados revocados esté debidamente firmada por el Certificador emisor.	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0".	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación. 
3	Mecanismo de suspensión de certificados.		
	Se verificará que la lista de certificados revocados puede incluir la información necesaria para indicar el estado de suspensión de un certificado.	Cumple el requerimiento con los documentos "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0", en su numeral 7.2 (Perfil de CRL).	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación.

- **TB03: Registro de Acceso Público de la República de Panamá.**

Objetivo			
Asegurar el acceso a información relevante descriptiva del sistema por parte de los titulares y terceros.			
ID	**NOMBRE**	**OBSERVACIÓN**	**EVIDENCIA**
1	Existencia y contenido mínimo del sitio de información pública.		
	El PSC debe mantener un sitio de acceso electrónico, en el cual mantenga la información relevante para los titulares y las partes que confían. Debe contener al menos los siguientes documentos:		
	a) Registro de certificados emitidos, indicando código de identificación único del certificado y su estado (vigente, suspendido o revocado)	https://www.firmaelectronica.gob.pa/configuracion-firma-electronica.html#cacerts	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante las imágenes que se asocian a continuación.

			
	b) Copia de la Lista de certificados revocados (CRL) actualizada cada 24 horas.	https://www.firmaelectronica.gob.pa/crl.html http://www.pki.gob.pa/crls/capc2.crl	
	c) Si es pertinente, indicar si el certificado ha sido traspasado de otro prestador de servicios de certificación acreditado o ha sido homologado.	No aplica.	No aplica.
	d) Acceso seguro a los titulares para realizar la revocación o suspensión de certificados vigentes.	"Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0" Numeral 3.4. Identificación y autenticación para solicitudes de revocación.	Se adjuntan las políticas denominadas "P-12-Politica-de-Certificacion-de-Certificados-de-Persona-Natural.pdf" y "P-27-PC-Firma-Electronica-en-la-Nube.pdf". 3.4. Identificación y autenticación para solicitudes de revocación La identificación y autenticación de los titulares de los certificados para las solicitudes de revocación por cualquier causa se realizará mediante la cédula de identidad. https://www.firmaelectronica.gob.pa/normativa/P-12-Politica-de-Certificacion-de-Certificados-de-Persona-Natural.pdf
	e) Política del certificado de firma electrónica avanzada.	Se establece según Ley Nº 82 "Que otorga al Registro Público de Panamá atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá, modifica la Ley 51 de 2008 y adopta otras disposiciones. Publicación: 9	Se adjuntan las políticas denominadas "P-12-Politica-de-Certificacion-de-Certificados-de-Persona-Natural.pdf" y "P-27-PC-Firma-Electronica-en-la-Nube.pdf".

		de noviembre de 2012. Definiendo la Dirección Nacional de Firma Electrónica.	https://www.firmaelectronica.gob.pa/normativa/P-12-Politica-de-Certificacion-de-Certificados-de-Persona-Natural.pdf https://www.firmaelectronica.gob.pa/normativa/P-27-PC-Firma-Electronica-en-la-Nube.pdf
	f) Declaración de sus Prácticas de Certificación.	Se establece según Ley Nº 82 "Que otorga al Registro Público de Panamá atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá, modifica la Ley 51 de 2008 y adopta otras disposiciones. Publicación: 9 de noviembre de 2012. Definiendo la Dirección Nacional de Firma Electrónica. Asimismo, en "P-11-Declaracion-de-Practicas-de-Certificacion.pdf".	Se deja registro mediante la URL que se asocia a continuación. https://www.firmaelectronica.gob.pa/politicas-certificacion.html https://www.firmaelectronica.gob.pa/normativa/P-11-Declaracion-de-Practicas-de-Certificacion.pdf
	g) Resoluciones de la Entidad Acreditadora que le afecten.	Normativa Aplicable	Se deja registro mediante la URL que se asocia a continuación. https://www.firmaelectronica.gob.pa/legislacion-nacional.html
	h) Servicio de consulta en línea de estado de un certificado (OCSP).		Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación. 
2	Disponibilidad de la información pública.		
	Se debe asegurar una disponibilidad del sitio no menor al 99%. Para esto se verificará la existencia de mecanismos redundantes o alternativos de conexión y sitios de emergencia que se levanten manual o automáticamente en caso de desastres.	Se cumple con lo establecido en "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0" Numeral 2.	Se adjunta la información en la carpeta "Documentos Verificados" y se deja registro mediante la imagen que se asocia a continuación.  2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN 2.1. Repositorios Como establece la DPC de la RPP-PKI. 2.2. Publicación de información de certificación Como establece la DPC de la RPP-PKI. 2.3. Frecuencia de publicación Como establece la DPC de la RPP-PKI. 2.4. Controles de acceso a la información de certificación Como establece la DPC de la RPP-PKI.
3	Seguridad.		

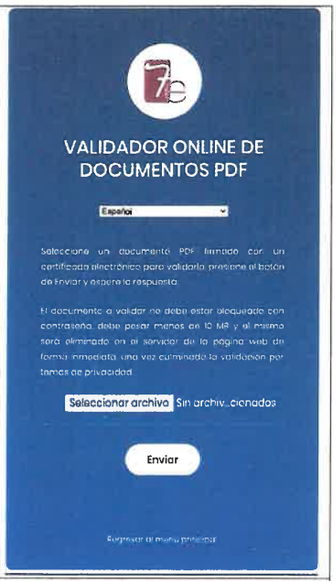
	Se debe proteger la integridad y disponibilidad de la información mediante el uso de tecnología y medidas de seguridad tanto físicas como lógicas que reduzcan los riesgos y consecuencias de ataques maliciosos en contra de los sitios tanto internos como externos.	Cumple el requerimiento establecido en "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0", punto 5.	Se adjunta "Política de Certificación de Certificados de Persona Natural – v0.4" y "Política de Certificación de Firma Electrónica Calificada en la Nube – v0.0". Asimismo, se deja constancia en la imagen debajo. 5. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES 5.1. Controles físicos 5.1.1. Ubicación física y construcción Como establezca la DPC de la RPP-PKI. 5.1.2. Acceso físico Como establezca la DPC de la RPP-PKI 5.1.3. Alimentación eléctrica y aire acondicionado Como establezca la DPC de la RPP-PKI. 5.1.4. Exposición al agua Como establezca la DPC de la RPP-PKI. 5.1.5. Prevención y protección frente a incendios Como establezca la DPC de la RPP-PKI. 5.1.6. Sistema de almacenamiento Como establezca la DPC de la RPP-PKI. 5.1.7. Eliminación de residuos Como establezca la DPC de la RPP-PKI. 5.1.8. Copias de seguridad fuera de las instalaciones Como establezca la DPC de la RPP-PKI.

- **TB04: Modelo de Confianza de la República de Panamá.**

Objetivo			
Verificar que el PSC provea a los titulares de certificados de firma electrónica avanzada emitidos por él, de un mecanismo de confianza que le permita comprobar la validez de cualquier certificado de firma electrónica avanzada que reciba.			
ID	**NOMBRE**	**OBSERVACIÓN**	**EVIDENCIA**
1	**Modelo de confianza.**		
	Se evaluará si el modelo de confianza adoptado permite cumplir con el objetivo planteado.	Cumple el requerimiento con la publicación en Sitio de la Dirección Nacional de Firma Electrónica, se pueden reconocer los diferentes Prestadores De Servicios De Certificación acreditados. https://www.firmaelectronica.gob.pa/configuracion-firma-electronica.html#cacerts https://www.firmaelectronica.gob.pa/psc-acreditados.html	Se deja registro mediante las imágenes que se asocia a continuación.

			 • CON PASO FIRME • DIRECCION NACIONAL DE FIRMA ELECTRONICA Solicitar CONFIGURACIÓN DE LA FIRMA ELECTRÓNICA Manuales de Configuración Certificados de la jerarquía de CA's • Autoridad de Certificación Raíz de Panamá. • Autoridad de Certificación de Gobierno. • Autoridad de Certificación de Panamá Clase 2.

			Gaceta No. 30015-B del 22 de abril de 2024 Nombre del PSC: FIRMATECH, INC. Domicilio: Panamá RUC: 155738626-2-2023 Rep. Legal: Gaspar Humberto Tarté Teléfono: +507 390-9043 Web: Firmatech.io Email: info@firmatech.io Compañía de Seguros: ASSA Numero de Poliza: 07867974 Servicios Autorizados: 1. Emisión de certificados de firma electrónica calificada 2. Emisión de certificados de sello electrónico calificado 3. Sellado de tiempo y estampado cronológico 4. Verificación de firmas o sellos electrónicos 5. Emisión de firma electrónica calificada en la nube Fecha de registro: 03 de abril de 2024
2	**Efectividad.**		
	Se verifica el mecanismo utilizado para implementar el modelo de confianza en forma práctica.	Se cumple mediante herramienta de verificación de documentos https://www.firmaelectronica.gob.pa/validador.html	Se deja registro mediante la imagen que se asocia a continuación.

			
3	**TSL.**		
	Se evaluará la implantación de TSL de acuerdo con la norma.	Cumple el requerimiento con la publicación del sitio web https://www.firmaelectronica.gob.pa/validador.html ya que se podrá soportar TSL para la validación de documentos.	Se deja registro mediante la imagen que se asocia a continuación. 

MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES | GOBIERNO DE COSTA RICA

CONCLUSIÓN

En consideración a los anteriores, se recomienda proceder con los actos administrativos que pongan en vigencia el Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital entre la República de Costa Rica y la República de Panamá.