REPÚBLICA DE PANAMÁ
REGISTRO PÚBLICO DE PANAMÁ

RESOLUCIÓN No. DG-198-2024
(De 3 de octubre de 2024)

POR LA CUAL SE DICTA EL REGLAMENTO TÉCNICO No. 6 DE LA DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA QUE ESTABLECE EL MARCO TÉCNICO REGULATORIO Y DE CUMPLIMIENTO PARA EL REGISTRO DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN PRIVADOS Y OTRAS ACTIVIDADES COMPLEMENTARIAS RELACIONADAS CON FIRMA ELECTRÓNICA Y SE DICTAN OTRAS DISPOSICIONES

EL DIRECTOR GENERAL DEL REGISTRO PÚBLICO DE PANAMÁ
En uso de sus facultades legales y reglamentarias,

CONSIDERANDO:

La Ley No. 82 de 9 de noviembre de 2012, otorga al Registro Público de Panamá las atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá;

Que según el artículo No. 4, numeral 1 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 necesario para el desarrollo de las materias de su competencia;

La Dirección Nacional de Firma Electrónica tiene la facultad de reglamentar todas las actividades de los prestadores de servicios de certificación concernientes al registro, comprobación y otorgamiento de firmas electrónicas calificadas a particulares y entidades gubernamentales; es función de la Dirección Nacional de Firma Electrónica dictar y emitir los reglamentos, resoluciones y demás documentos técnicos que considere necesario para el desarrollo de las materias de su competencia;

Que es función de la Dirección Nacional de Firma Electrónica registrar a los prestadores de servicios de certificación;

Que el numeral 6 del artículo No. 3 del Decreto Ejecutivo No. 684 de 18 de octubre de 2013, faculta a la Dirección Nacional de Firma Electrónica a dictar normas técnicas que definan para la administración pública y el sector privado en su interacción con la administración pública, criterios para el uso de la firma electrónica calificada basada en certificados electrónicos calificados mediante reglas comunes, formatos, estándares y algoritmos de creación y validación, así como las directrices de utilización y confianza de los certificados electrónicos calificados y el sellado de tiempo;

Que el artículo No. 20 del Decreto Ejecutivo No. 684 de 18 de octubre de 2013, establece que la Dirección Nacional de Firma Electrónica reglamentará el contenido de la Declaración de Prácticas de Certificación;

Que el presente reglamento técnico tiene como objetivo establecer el marco reglamentario para el registro de los prestadores de servicios de certificación de carácter privado ante la Dirección Nacional de Firma Electrónica;

RESUELVE:

PRIMERO. APROBAR el Reglamento Técnico No. 6 de la Dirección Nacional de Firma Electrónica, que establece el Marco Técnico Regulatorio y de Cumplimiento para el registro de los prestadores de servicios de certificación privados y otras actividades complementarias relacionadas con firma electrónica y se dictan otras disposiciones el cual es del tenor siguiente:

TEXTO ÚNICO
REGLAMENTO TÉCNICO No. 6
DE LA DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Artículo No. 1.- (Objeto). El presente reglamento tiene como objetivo establecer los criterios de cumplimiento de las empresas de carácter privado que apliquen para obtener el registro y la autorización de parte de la Dirección Nacional de Firma Electrónica para convertirse en prestadores de servicios de certificación y regular sus actividades.

Artículo No. 2.- (Alcance). Las disposiciones previstas en la presente norma son de aplicación y obligatorio cumplimiento a todas las personas jurídicas nacionales que sean prestadores de servicios de certificación en el territorio nacional como terceros de confianza, incluyendo a las empresas nacionales o extranjeras que sean facilitadores o prestadores de servicios de infraestructuras de clave pública asociados de manera contractual con los prestadores de servicio de certificación que operen en el territorio nacional.

Artículo No. 3.- Servicios de certificación y otros servicios y actividades complementarias). Tomando en cuenta el artículo No. No. 22 de la ley 51 de 2008 el presente reglamento técnico únicamente autoriza a los prestadores de servicios de certificación a ofrecer o facilitar los siguientes servicios de certificación y actividades complementarias relacionadas a las firmas electrónicas:

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. Conservación de firmas o sellos Electrónicos.
6. Emisión de firmas electrónicas calificadas en la nube.
7. Entrega electrónica calificada.

Artículo No. 4.- (Reconocimiento de organismos de normalización y de estándares internacionales). En virtud de la presente reglamentación se consideran válidos los estándares para sistemas confiables establecidos en las normas del IETF, los RFC, el Comité Europeo de Normalización (CEN), el Instituto Europeo de Normas de Telecomunicación (ETSI), la Organización Internacional de Normalización (ISO), la Unión Internacional de Telecomunicaciones (UIT) y las iniciativas sectoriales como el Foro de Autoridades de Certificación y Programas de Exploración de Internet "CA/B Fórum".

Artículo No. 5.- (Estándares de cumplimiento). Los prestadores de servicios de certificación privados, dependiendo de los servicios de certificación u otros servicios y actividades complementarias que la Dirección Nacional de Firma Electrónica les autorice a brindar, para garantizar que mantienen sistemas confiables deberán cumplir mínimamente con los siguientes estándares de referencia:

CUADRO 1

Servicios de certificación y otros servicios y actividades complementarias	Estándares de referencia
Emisión de certificados de firma electrónica calificada.	ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2.
Emisión de certificados de sello	ETSI EN 319 401, EN 319 411-1, ETSI

electrónico.	EN 319 411-2.
Sellado de Tiempo y estampado cronológico.	ETSI EN 319 401, ETSI EN 319 421.
Verificación de firmas o sellos electrónicos.	ETSI EN 319 401, ETSI TS 119 102-2, ETSI EN 319 102-1.
Conservación de firmas o sellos Electrónicos.	ETSI EN 319 401, ETSI TS 119 511.
Emisión de firmas electrónicas calificadas en la nube.	ETSI EN 319 401, ETSI TS 119 431-1, ETSI TS 119 431-2, ETSI TS 119 432.
Servicios de entrega electrónica calificada.	ETSI EN 319 401, ETSI EN 319 521, ETSI EN 319 522, ETSI EN 319 531, ETSI EN 319 532.

Artículo No. 6.- (Formatos de firma electrónica calificada aceptados).

XadES	ETSI TS 319 132
CadES	ETSI TS 319 122
PadES	ETSI TS 319 142

Artículo No. 7.- Para los efectos de la presente reglamentación se considerán Dispositivos Seguro de Creación de Firma Electrónica, los que acrediten contar con alguna de las certificaciones emitidas contra los estándares internacionales FIPS 140-2 del National Institute of Standards and Technology (NIST) o los organismos designados por los países firmantes del Common Criteria Recognition Agreement (CCRA) en base a la norma ISO 15408.

Artículo No. 8.- (Declaración de prácticas de certificación, políticas de certificación y perfiles de certificados electrónicos calificados)
Los prestadores de servicios de certificación deberán formular y publicar una declaración de prácticas de certificación y políticas de certificación en los términos establecidos en el artículo No. 27 de la Ley 82 de 2012; el artículo No. 20 del Decreto Ejecutivo 684 de 2013; cualquier otra normativa técnica que publique la Dirección Nacional de Firma Electrónica y los siguientes estándares de referencia:

CUADRO 2

Descripción	Estándares de Referencia
Declaración de prácticas de certificación (DPC) y políticas de certificación (PC)	RFC 3647 Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework.
Perfiles de certificación	ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3, ETSI EN 319 412-5, ETSI EN 319 422 (A excepción de la sección 9 del ETSI EN 319 422)

Artículo No. 9.- (Revisión de declaración de prácticas de certificación, políticas de certificación y perfiles de certificados electrónicos calificados). La Dirección Nacional de Firma Electrónica evaluará y aprobará la declaración de prácticas de certificación, las políticas de certificación y los perfiles a emitir por el prestador de servicios de certificación, y podrá rechazarlos si durante el proceso de registro la Dirección Nacional de Firma Electrónica considera que los certificados electrónicos no cumplen con la Ley 51 de 2008 y sus modificaciones; el Decreto Ejecutivo 684 de 2013 y sus modificaciones y los estándares aprobados en el presente reglamento.

Artículo No. 10.- La Dirección Nacional de Firma Electrónica podrá dictar mediante reglamentación técnica guías y normas especiales para la estructura de los certificados electrónicos calificados en sus distintos perfiles los cuales el prestador de servicios de certificación deberá cumplir en todo momento incluso después de su aprobación y registro en la Dirección Nacional de Firma Electrónica. Mientras no se dicten normas especiales,

todos los certificados electrónicos calificados deberán contener la abreviatura "PA" en el campo país del emisor.

Artículo No. 11.- La Dirección Nacional de Firma Electrónica podrá consultar a otras entidades públicas o privadas en la revisión de perfiles y estructura de los certificados electrónicos para verificar la compatibilidad de los certificados electrónicos calificados. En lo referente a la jerarquía de la entidad de certificación (CA) del prestador de servicios de certificación privado, los certificados de usuario final deberán ser emitidos por una entidad de certificación (CA), exclusivamente creada con su ceremonia de llaves, para la República de Panamá.

Artículo No. 12.- (Servicios de emisión de certificados de firma electrónica calificada). Actividad que consiste en emitir certificados electrónicos calificados para firma electrónica calificada.

Artículo No. 13.- (Servicios de emisión sellos electrónicos calificados). Comprende el servicio de emisión y generación de certificados electrónicos de sellos electrónicos calificados para dispositivos electrónicos como computadoras, servidores, entre otros.

El Sello electrónico calificado se crea y mantiene únicamente en un dispositivo seguro de creación de firmas de tipo HSM token o tarjeta criptográfica.

Artículo No. 14.- (Sellado de tiempo y estampado cronológico). Se define el sellado de tiempo y estampado cronológico como un conjunto de datos de forma electrónica utilizados como medio para vincular inequívocamente la existencia de un documento a un instante de tiempo y constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados. Eso incluye el mecanismo que demuestra la integridad de una serie de datos desde un momento determinado y que los mismos no han sido alterados desde el momento que se hizo la firma.

De conformidad con el artículo No. 9 de la Ley 51 de 2008, para garantizar la fe pública en actos notariales con firmas electrónicas y otras leyes que exijan el uso de sellado de tiempo se requiere a todos los prestadores de servicios de certificación que emitan firmas electrónicas calificadas con sellado de tiempo ajustado a la hora UTC-5.

Artículo No. 15.- (Servicios de verificación de firmas y sellos electrónicos calificados). Como actividad complementaria relacionada a las firmas electrónicas, se define el proceso de verificación de una firma electrónica calificada o de un sello electrónico calificado, como la acción realizada por un prestador de servicios de certificación para verificar que:

1. El certificado que respalda la firma o el sello es, en el momento de la firma, un certificado electrónico calificado emitido por un prestador de servicios de certificación registrado ante la Dirección Nacional de Firma Electrónica;
2. Los datos de verificación de la firma o el sello corresponden a los datos proporcionados a la parte usuaria;
3. El conjunto único de datos que representa al firmante en el certificado se facilite correctamente a la parte usuaria;
4. La integridad de los datos firmados no se haya visto comprometida.

El sistema utilizado para verificar la firma electrónica calificada o el sello electrónico calificado ofrecerá a la parte usuaria el resultado correcto del proceso de verificación y le permitirá recibir el resultado del proceso de verificación de una manera automatizada que sea fiable, eficiente e incluya la firma o el sello electrónico calificado del prestador de servicios de certificación que brinde el servicio de verificación. El servicio de verificación calificado solo podrá brindarse por un prestador de servicios de certificación registrado en la Dirección Nacional de Firma Electrónica.

Los servicios calificados de verificación de firmas y sellos electrónicos calificados solo podrán verificar certificados electrónicos extranjeros de prestadores de servicios de certificación no registrados en la Dirección Nacional de Firma Electrónica, mediante

autorización expresa de la Dirección Nacional de Firma Electrónica una vez que la Dirección Nacional de Firma Electrónica emita el reglamento técnico respectivo sobre esta materia.

Artículo No. 16.- (Servicio de conservación de firmas electrónicas y sellos electrónicos calificados) Como actividad complementaria relacionada a las firmas electrónicas, se entenderán como servicios de conservación de firmas electrónicas calificadas y sellos electrónicos calificados, a los servicios ofrecidos por prestadores de servicios de certificación privados que utilicen procedimientos y tecnologías capaces de preservar la integridad de la firma electrónica calificada o el sello electrónico calificado durante el transcurso del tiempo.

Para lo concerniente al uso de firma electrónica calificada en el proceso de almacenamiento tecnológico de documentos regulado por el Ministerio de Comercio e Industrias (MICI), para garantizar la integridad de los documentos almacenados tecnológicamente, se podrá utilizar el servicio de conservación de firmas electrónicas y sellos electrónicos calificados brindado por un prestador de servicios de certificación para brindar el máximo nivel de integridad al repositorio.

En el caso de que el prestador de servicios de conservación de firmas electrónicas y sellos electrónicos calificados, desee brindar el servicio de almacenamiento tecnológico de documentos a terceros, deberá gestionar ante la Dirección General de Comercio Electrónico (DGCE), del Ministerio de Comercio e Industrias (MICI), la solicitud como prestador de servicio de almacenamiento tecnológico de documentos y cumplir con los requisitos establecidos en la Ley 51 de 2008.

Artículo No. 17.- (Servicios de creación de firmas electrónicas calificadas en la nube). La firma electrónica calificada en la nube es un servicio de firma electrónica calificada donde el certificado electrónico calificado es gestionado por un Módulo de Seguridad de Hardware (HSM) del prestador de servicios de certificación. Posteriormente, el firmante accede a dicho certificado cuando requiere aplicar la firma a un documento electrónico, donde primero debió ingresar a una plataforma o aplicación por medio de un sistema de autenticación robusto y seguro.

Con respecto a la firma electrónica en la nube de acuerdo al artículo No. 3 del Decreto Ejecutivo N° 83 de 2023, no se considerará que el almacenamiento de los datos de creación de firma está fuera del control exclusivo del firmante cuando la gestión de este almacenamiento es realizada por el prestador de servicios de certificación siempre que este los gestione con autorización expresa del firmante y el prestador de servicios de certificación los proteja frente a cualquier alteración, destrucción o acceso no autorizado, así como cuando garantice su continua disponibilidad para el firmante. En este caso, el prestador de servicios de certificación deberá proveer al firmante de un factor de autenticación que el firmante tendrá bajo su responsabilidad y control exclusivo.

Artículo No. 18.- (Servicios de entrega electrónica calificada) Como actividad complementaria relacionada a las firmas electrónicas, se define el servicio de entrega electrónica calificada, al servicio brindado por un prestador de servicios de certificación que permite transmitir datos entre partes terceras por medios electrónicos y aporta pruebas relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío la entrega y/o la recepción de los datos. El servicio de entrega electrónica calificada protege los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizada.

Los datos enviados y recibidos mediante un servicio calificado de entrega electrónica calificada disfrutarán de las presunciones que la ley otorga a los servicios calificados en el envío de dichos datos por el remitente identificado, la recepción por el destinatario identificado y la exactitud de la fecha y hora de envío y recepción de los datos que indica el servicio de entrega electrónica calificada.

El Servicio de entrega electrónica calificada se podrá prestar en diferentes modalidades de acuerdo a las previsiones del artículo No. 31 de este reglamento y sujetas al cumplimiento de los diferentes estándares de acuerdo al artículo No. 5 del presente reglamento.

Articulo 19.- (Comprobación de identidad del solicitante de un certificado electrónico calificado). Los prestadores de servicios de certificación privados, al momento de realizar la comprobación de identidad de un solicitante de certificado electrónico calificado, se les requerirá como mínimo que:

1. Al expedir un certificado electrónico calificado se debe verificar de manera fiable por sí o a través de un tercero, la identidad declarada o cualquier atributo de la persona física a la que se le expide el certificado electrónico calificado;
2. En todos los casos se deberá verificar de manera fiable por sí o a través de terceros, la identidad declarada y cualquier atributo de la persona física a la que se le expide el certificado electrónico calificado, comparándolos con el rostro impreso en el documento utilizado para acreditar la identidad que será cédula o pasaporte y el rostro de la persona en el momento de la acreditación.
3. Cuando se realice la acreditación del solicitante de un certificado calificado mediante la modalidad de comparecencia virtual en línea a través de identificación remota entre el solicitante y un prestador de servicios de certificación, se deben utilizar métodos fiables, auditables y seguros de identificación electrónica, cuyo objetivo sea evitar el fraude de identidad, el uso indebido o la alteración de la identidad. El sistema y procedimiento remoto utilizado para acreditar la identidad del solicitante del certificado de firma electrónica calificada deberá cumplir con las previsiones del Apéndice 1 de este reglamento.
4. Con el fin de simplificar y agilizar los procedimientos de identificación y evitar que una misma persona, ya identificada de manera segura deba acreditarse de manera presencial o mediante comparecencia virtual en línea, el prestador de servicios de certificación privado podrá valerse para dar por cumplida su obligación de comprobar la identidad y otras circunstancias personales a partir de bases de datos fiables que consten ante terceros como un mecanismo técnico. Para ello, el prestador de servicios de certificación privado deberá formalizar el acceso a dichas bases de datos mediante contratos o acuerdos de colaboración. A los efectos de este literal, se entenderán como bases de datos fiables, aquellas basadas en identificaciones realizadas por instituciones bancarias debidamente acreditadas en la República de Panamá según la normativa aplicable.
5. Alternativamente, cuando la identidad y otras circunstancias personales de los solicitantes de certificados de firma electrónica calificada ya le constasen al prestador de servicios de certificación o a sus autoridades de registro en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubiese empleado alguno de los métodos indicados en este artículo y el período de tiempo transcurrido desde la identificación fuese no mayor de un (1) año, no será necesaria la acreditación del solicitante de manera presencial o mediante comparecencia virtual en línea.
6. Cuando exista un certificado vigente emitido por el mismo prestador de servicios de certificación, tampoco será necesaria la acreditación del solicitante de manera presencial o mediante comparecencia virtual en línea.
7. Garantizar la protección, la confidencialidad y el debido uso de la información suministrada por el suscriptor de conformidad con el artículo No. 23 numeral 11 de la Ley 51 de 2008 y cumpliendo con toda normativa de protección de datos que emita la autoridad competente.
8. Adicionalmente el prestador de servicios de certificación podrá también verificar el resto de la información que aparece en el documento de identidad; solicitar información adicional del interesado y tomar cualquier medida investigativa que considere pertinente a tal efecto. El prestador de servicios de certificación no le emitirá el certificado electrónico a quienes se opongan a dichas medidas.

9. Utilizar sistemas y productos fiables que estén protegidos contra alteración y que garanticen la seguridad y la fiabilidad técnicas de los procesos que sustentan.
10. Utilizar sistemas fiables para almacenar los datos que se les faciliten de forma verificable y que pueda comprobarse la autenticidad de los datos.
11. Tomar medidas adecuadas contra la falsificación y el robo de datos.
12. Registrar, guardar, custodiar y mantener accesible, durante un período 7 años según las disposiciones del artículo No. 23 numeral 15 de la Ley 51 del 2008, toda la información pertinente referente a los datos expedidos y recibidos, en particular al objeto de que sirvan de prueba en los procedimientos legales; incluyendo guardar y custodiar confidencialmente los videos y fotografías utilizados para la comprobación de la identidad.
13. Cumplir con los demás requisitos establecidos en la Ley y su reglamentación y el presente reglamento.

Como lo establece el artículo No. 26 de la Ley 51 de 2008, el responsable de la comprobación de identidad será siempre en todos los casos, el prestador de servicios de certificación.

Artículo No. 20.- (Requisitos para la delegación del proceso de comprobación de identidad por parte de prestador de servicios de certificación hacia terceros como AR-Autoridad de registro o en inglés RA). De conformidad con el artículo No. 28 de la Ley No. 82 de 9 de noviembre de 2012, los prestadores de servicios de certificación privados podrán realizar las actuaciones de comprobación de identidad por medio de otras personas naturales o jurídicas, públicas o privadas.

Si el prestador de servicio de certificación delega las actuaciones y procesos de comprobación de identidad, aquello deberá constar en el informe de auditoria en el momento de realizar la solicitud de registro. Si dicha delegación se diese posterior al registro entonces deberá constar en los informes de auditoria a presentar con la solicitud de renovación de dicho registro.

Cuando los prestadores de servicio de certificación delegan las actuaciones y procesos de comprobación de identidad deberán cumplir con al menos los siguientes requisitos:

1. Existir una relación contractual entre el prestador de servicios de certificación privado y el tercero.
2. El proceso para delegar las actuaciones así como los procesos de comprobación de identidad hacia terceros deben estar establecidos en la declaración de prácticas del prestador de servicios de certificación.
3. El tercero delegado deberá cumplir con todas las responsabilidades exigidas al provedor de servicios de certificación orientadas a los procesos de comprobación de identidad, seguridad de la información, privacidad y protección de datos personales.
4. El tercero delegado deberá cumplir con las disposiciones de comprobación de identidad del presente reglamento.
5. Las auditorías exigidas en el Decreto Ejecutivo 684 de 2013 podrán incluir al tercero delegado si así lo estima el auditor, por ende, el prestador de servicios de certificación debe asegurarse al autorizar una delegación, de que a sus auditores se le permita acceso completo a todos los sistemas y procedimientos delegados para realizar su labor de auditoría cuando el auditor lo estime conveniente.

Como lo establece el artículo No. 26 de la Ley 51 de 2008 aunque se deleguen las actuaciones de comprobación de identidad en todos los casos el responsable de la comprobación de identidad será siempre el prestador de servicios de certificación.

Artículo No. 21.- (Obligaciones que deben cumplir los prestadores de servicios de certificación privados). Todos los prestadores de servicios de certificación deberán cumplir con todas las disposiciones y obligaciones establecidas la Ley N° 51 de 2008 modificada por la Ley N° 82 de 2012 en especial el artículo No. 23 de la Ley N° 51 de

2008; el Decreto Ejecutivo N° 684 de 2013 Decreto Ejecutivo N°83 de 2023; y adicionalmente las siguientes disposiciones:

1. Contar con un plan de cese de actividades actualizado para garantizar la continuidad del servicio.
2. Garantizar un tratamiento lícito de los datos personales de conformidad con la legislación y normativa vigente.
3. Establecer y mantener actualizado el repositorio de certificados.
4. Registrar las revocaciones de certificados calificados en su repositorio y publicarán el estado de la revocación en un plazo de 24 horas como máximo después de la recepción de la solicitud. La revocación será efectiva inmediatamente después de su publicación.
5. Tener una página web con toda la información de todos sus servicios de certificación disponible al público en idioma español y publicar en su página web en todo momento y de manera muy visible la frase: "Prestador de Servicios de Certificación, registrado en la República de Panamá mediante Resolución __ (número y fecha de registro –vigente-) del Registro Público de Panamá".

Artículo No. 22.- Efectos de este reglamento técnico. La Dirección Nacional de Firma Electrónica expedirá, mantendrá y publicará en el registro pertinente, la información sobre los prestadores de servicios de certificación en su portal electrónico. Esta información incluirá referencia a los servicios de certificación que les fueron autorizados.

Adicionalmente, de conformidad con el artículo No. 11 de la Ley 51 de 2008, toda resolución de registro, suspensión o cancelación al prestador de servicios de certificación será publicada en la Gaceta Oficial.

Artículo No. 23.- (Presentación de solicitudes y procedimiento de Registro). Los interesados en obtener el registro o la autorización para constituirse como prestador de servicios de certificación, podrán presentar dicha solicitud a través de medios físicos u otros que la Dirección Nacional de Firma Electrónica determine. Dicha solicitud, quedará sujeta a los requisitos de registro y procedimiento establecidos en el Título III, Capítulos I y II del Decreto Ejecutivos 684 de 2013 y Decreto Ejecutivo 82 del 23 de marzo de 2023, así como el presente reglamento.

La documentación requerida como soporte de la solicitud que provenga del extranjero deberá estar redactada en idioma español o traducido a éste por traductor público autorizado y debidamente apostillada o legalizada por la via consular.

Sin embargo, en cuanto a los apéndices técnicos de la misma, distintos a documentación de carácter legal, la Dirección Nacional de Firma Electrónica estimará la pertinencia o no del cumplimiento de la presente disposición.

Artículo No. 24.- (Informe de auditoría)
Los Prestadores de Servicios de Certificación Privados deberán presentar además del informe de auditoría para su registro, uno cada (2) años a la Dirección Nacional de Firma Electrónica para la renovación de su registro, que demuestre una satisfactoria evaluación de conformidad de cada uno de los servicios que prestan. De conformidad con el artículo No. 16 del Decreto Ejecutivo 684 de 2013, el informe bianual para la renovación del registro contendrá dos informes satisfactorios para cada uno de los dos años respectivos.

El informe de auditoría debe incluir, como mínimo, la siguiente información, sin perjuicio de que la Dirección Nacional de Firma Electrónica pueda requerir información adicional al sujeto auditado:

1. El informe de audítoria debe indicar expresamente si, a juicio de la firma auditora, tanto el prestador de servicios de certificación como los servicios de certificación que presta, cumplen o no los requisitos mínimos de una infraestructura de clave pública, de equipo de personas, de infraestructura física tecnológica, procedimientos y sistemas de seguridad, según la normativa técnica vigente.

2. Deberá en su informe presentar un reporte de su evaluación presencial en sitio, sobre el cumplimiento de su infraestructura física según la normativa técnica vigente. Dicha evaluación en sitio deberá haberse realizado a no más de un año de la presentación del informe de auditoría.
3. Para cada servicio, descripción detallada de la arquitectura física, lógica y funcional.
4. Identificación de la firma auditora, incluyendo datos de inscripción de la sociedad, su domicilio y datos de contacto (número de teléfono y correo electrónico del contacto de la misma).
5. Identificación del responsable o responsables del informe de auditoría o evaluación técnica y sus datos de contacto.
6. Datos identificativos del prestador de servicios certificación, incluyendo su nombre tal y como se recojan en los registros oficiales, dirección física, dirección web así como correo electrónico y persona de contacto.
7. En el supuesto de que el auditor indique una certificación de dispositivo seguro de creación de firma o sello electrónicos, se deberá adjuntar copia o enlace de la certificación expedida por el organismo de certificación correspondiente en la que figure expresamente la calificación de dispositivo seguro de creación de firma o sello, así como la indicación del servicio o servicios en los que se utilice el producto
8. Lista detallada de toda la documentación del prestador, pública e interna, auditada. Debe incluir al menos:
    a) Declaración de prácticas de certificación.
    b) Políticas de cada uno de los servicios de certificación.
    c) Contratos de condiciones y términos de uso de cada servicio a brindar.
    d) Plan de cese conforme la normativa aplicable.
    e) Documentación relacionada con el análisis y evaluación de riesgos.
    f) Plan de notificación de brechas de seguridad.
    g) Lista de documentos internos de apoyo a la declaración de prácticas de certificación, utilizados por el prestador para proporcionar los servicios de certificación evaluados bajo la correspondiente política.
    h) Información de constitución de la sociedad.
9. El informe debe identificar el período de tiempo empleado para realizar la auditoría y los recursos utilizados, así como el esfuerzo dedicado por cada auditor de existir más de uno.
10. El informe indicará un listado detallado de los puntos y objetivos de control empleados en la auditoría, conforme a los requisitos establecidos por la normativa y estándares técnicos que sean de aplicación, especificando en su caso las ausencias de conformidad y su nivel de relevancia.
11. Cuando la conformidad sea evaluada, adicionalmente, de acuerdo con un estándar específico, se proporcionará el mismo como un documento separado del informe de evaluación conforme, con una indicación expresa de las no conformidades y su relevancia.
12. El informe incluirá la descripción, los resultados y la evaluación de un número significativo de ejemplos para todos los tipos relevantes de resultados obtenidos de los servicios evaluados.
13. El informe detallará la lista de terceros a los que el prestador haya delegado total o parcialmente procesos de sus servicios de certificación electrónica.
14. El informe indicará el calendario de auditorías.
15. El informe indicará bajo qué circunstancias una firma auditora ha de realizar, en su caso, evaluaciones adicionales a las planificadas.

Se consideran firmas auditoras aptas para auditar a los prestadores de servicios de certificación, a entidades nacionales o extranjeras, registradas como auditores, ante la Dirección Nacional de Firma Electrónica, una vez se reglamente el proceso de registro según el artículo No. 32 del Decreto Ejecutivo N° 684 de 2013, modificado por el artículo No. 7 del Decreto Ejecutivo N° 83 de 2023.

En lo que compete al audito de los prestadores de servicios de certificación, serán válidos también los informes de auditoría proveniente del extranjero, presentados por firmas no registradas en la Dirección Nacional de Firma Electrónica, cuando la empresa pueda cumplir mínimamente con lo siguiente:

1. El informe de auditoría fue hecho por una empresa auditora que cuente con al menos una persona certificada como auditor de seguridad de la información ISO/IEC 27001 o sistemas de información CISA de ISACA.
2. Que la empresa auditora o al menos uno de sus auditores cuente con más de 5 años de experiencia en entornos de infraestructura de clave pública (PKI).
3. Que la empresa auditora o al menos uno de sus auditores cuente con experiencia en al menos la realización de 5 auditorías a distintos proveedores de infraestructura de clave pública o prestadores de servicios de certificación que de manera verificable por la Dirección Nacional de Firma Electrónica, mantengan vigentes una de las siguientes certificaciones ETSI 319 401; ISO/IEC 27001:2013 o Web Trust.
4. En caso de prestadores de servicios de certificación que requieran o utilicen infraestructura o servicios tecnológicos prestados desde el extranjero, la auditoría deberá contar con dos dictámenes favorables: Uno acerca del cumplimiento por parte del tercero en el exterior y el otro del cumplimiento del prestador de servicios de certificación del territorio nacional.
5. Toda documentación de auditoría que provenga del extranjero deberá estar traducida al idioma español por traductor público autorizado y debidamente apostillada o legalizada por la via consular de conformidad con el artículo No. 35 del Decreto Ejecutivo N° 684 de 2013 modificado por el artículo No. 8 del Decreto Ejecutivo N° 83 de 2023. Se exceptúa de la traducción la nomenclatura y descripciones técnicas que a criterio y juicio de la Dirección Nacional de Firma Electrónica por su naturaleza técnica carezcan de equivalente apropiado al español.

Artículo No. 25.- (Oficinas y dirección física de atención al público). Los prestadores de servicios de certificación privados deberán tener en la República de Panamá oficinas y registrar su dirección física de atención en la República de Panamá ante la Dirección Nacional de Firma Electrónica. Cualquier cambio deberá ser informado a la Dirección Nacional de Firma Electrónica, en un plazo no mayor de TREINTA (30) días, contados a partir de su materialización.

Artículo No. 26.- (Notificaciones). Las notificaciones realizadas por la Dirección Nacional de Firma Electrónica en virtud de los procedimientos establecidos en este reglamento, serán formuladas por cualquier medio físico o electrónico.

Artículo No. 27.- (Autorización para constituirse como prestador de servicio de certificación ante la Dirección Nacional de Firma Electrónica).
La autorización para operar como prestadores de servicios de certificación privados es efectiva solo sobre los servicios para los cuales la Dirección Nacional de Firma Electrónica ha emitido su autorización. La incorporación de nuevos servicios por parte de un prestador de servicios de certificación privado requiere de un proceso de autorización adicional específico unicamente a los servicios adicionados.

Artículo No. 28.- (Facultad de Inspección). La Dirección ejercerá la facultad de inspección sobre los prestadores de servicios de certificación privados y velará por el cumplimiento de las disposiciones legales y reglamentarias por parte de los mismos, en atención a las atribuciones otorgadas por la Ley N°51 de 2008, la Ley N°82 de 2012 y sus reglamentos de aplicación los Decretos Ejecutivos N° 684 de 2013 y N° 83 de 2023. En cumplimiento de lo anterior, tanto la Dirección Nacional de Firma Electrónica como cualquier auditor reconocido por la misma, podrá solicitar acceso a los centros de datos de los prestadores de servicios de certificación para evaluar su infraestructura física.

1. Los certificados electrónicos de los perfiles de Funcionario Público y Sello Electrónico para Gobierno, solo podrán ser emitidos por la Dirección Nacional de

Firma Electrónica del Registro Público de Panamá debido a que según los artículos 1 y 2 de la Ley 82 de 9 de noviembre de 2012 el Registro Público de Panamá, es la autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá y prestador de servicios de certificación electrónica para el Gobierno Nacional.

2. Debido a la importancia legal y seguridad jurídica que se debe requerir para los certificados electrónicos calificados en todos los perfiles distintos al de Persona Natural, será obligatoria la atención presencial de los usuarios (clientes) para los siguientes perfiles: Representante de Persona Jurídica, Colaborador de Persona Jurídica, Factura Electrónica, Profesional y Sello Electrónico para Empresas; independiente del medio que sea utilizado para almacenar las claves privadas de los certificados electrónicos (tarjetas inteligentes, Tokens USB y HSM en la Nube) por parte del prestador de servicios de certificación. De esta forma, la atención por videollamada remota (aplicando todas las validaciones de servicios web, biométricas, etc. mencionadas en el presente reglamento) estaría limitada al perfil de Persona Natural, teniendo en cuenta que también se permite la atención presencial para aquellos usuarios de este perfil que deseen acudir a las instalaciones de los prestadores de servicios de certificación para obtener sus certificados electrónicos. A medida que la Dirección Nacional de Firma Electrónica vaya creando los reglamentos técnicos para realizar la atención remota de los perfiles mencionados, se procederá posteriormente con la publicación de los reglamentos correspondientes para que los prestadores de servicios de certificación acreditados puedan brindar dichos servicios de la misma manera.

3. Todos los certificados electrónicos calificados emitidos por los prestadores de servicios de certificación deberán guardar sus claves privadas en un dispositivo criptográfico seguro, ya sea en tarjetas inteligentes / tokens USB (PKCS#11) o HSM (Firma Electrónica en la Nube), los cuales deberán cumplir con el estándar FIPS 140-3. En caso de que el prestador de servicios de certificación utilice un HSM que cumpla con el estándar FIPS 140-2 nivel 3, deberá demostrar que su dispositivo podrá ser actualizado para que sea compatible con FIPS 140-3 y cumplir con los plazos para realizar dicha actualización, de lo contrario deberá proceder con el reemplazo de esos equipos antes del 21 de septiembre del 2026 (ya que después de esa fecha, todos los certificados FIPS 140-2 serán incluidos en la lista histórica). En caso de que se utilicen HSM rentados, los mismos deberán ser del tipo dedicado, es decir, no podrán ser compartidos con otros clientes del proveedor, por lo que deberá demostrar que son dedicados a resguardar las claves privadas generadas en la ceremonia de claves de la Autoridad de Certificación propia de la PKI del prestador de servicios de certificación. En caso de utilizar firma electrónica en la nube, los HSM deberán ser también dedicados y distintos a los empleados para guardar las claves privadas de la ceremonia de claves y será necesario mostrar evidencias de que las claves privadas de los certificados electrónicos calificados de los clientes del prestador de servicios de certificación son guardadas o gestionadas por dichos HSM. No se le permiten a los prestadores de servicios de certificación bajo ninguna circunstancia, el uso del formato PKCS#12 para ningún tipo de certificado electrónico calificado de los diferentes perfiles reglamentados debido a medidas de seguridad, por lo tanto y por ahora, solamente la Dirección Nacional de Firma Electrónica podrá utilizar dicho formato para la emisión de los certificados de factura electrónica (tal como se indica en el numeral 11 del artículo No. 2 del Reglamento Técnico No. 5 de la Dirección Nacional de Firma Electrónica y debido a requerimientos técnicos actuales de los sistemas de facturación, hasta que la Dirección General de Ingresos actualice sus sistemas para no requerir este formato), los cuales son emitidos actualmente bajo un estricto procedimiento de validación de los datos de los clientes (personas naturales y jurídicas con avisos de operaciones registrados en el sistema E-TAX de la DGI y validados por el servicio web que ofrecen, donde los clientes entregan la documentación necesaria que es verificada por los operadores de registro). Los prestadores de servicios de certificación deben suministrar el API de sus HSM a sus clientes de firma electrónica en la nube para que las claves privadas de los certificados electrónicos almacenados en esos dispositivos puedan ser utilizadas (de

forma segura) por los sistemas informáticos utilizados por los clientes y que normalmente se emplean en las diferentes organizaciones.

4. La Firma Electrónica en la Nube deberá emplear como mínimo alguno de los siguientes mecanismos de autenticación de dos factores para ofrecer una mayor seguridad jurídica a sus usuarios, al momento en que escriben sus contraseñas de firma electrónica:

    a. Autenticación por correo electrónico / SMS: Cada vez que un usuario vaya a firmar un documento con su certificado electrónico calificado en la nube, deberá recibir por parte del prestador de servicios de certificación, una contraseña de un solo uso (OTP por sus siglas en inglés) en su correo electrónico o por mensaje de texto (SMS) a su teléfono móvil para que sea utilizada en conjunto con su contraseña de firma electrónica (la cual definió durante su proceso de emisión la primera vez o utilizar la más reciente en caso de que la haya cambiado). El código de verificación OTP debe tener entre 5 a 10 dígitos, por lo que puede ser numérico o alfanumérico y es válido por un tiempo limitado (el cual debe ser configurable en la plataforma del prestador de servicios de certificación). No se permitirá en ninguna circunstancia, un código fijo como segundo factor de autenticación en conjunto con su contraseña de firma, por lo tanto, es obligatorio la generación de un código de verificación distinto (OTP) cada vez que se requiera firmar documentos con un certificado electrónico calificado.

    b. Token de hardware: es básicamente un dispositivo físico, por ejemplo: una llave de seguridad, tarjeta inteligente o dongle USB; el cual genera un token único que es válido por un tiempo limitado y que deberá ser escrito en conjunto con la contraseña de firma del usuario.

    c. Token de software: se trata de una aplicación autenticadora que envía un código OTP basado en tiempo o evento, la cual puede estar instalada en la computadora o teléfono móvil del usuario. Tal como sucede con el token de hardware, se genera un código de verificación de manera dinámica que dura un breve período de tiempo (debe ser también configurable en la plataforma del prestador de servicios de certificación) y que deberá escribirlo al momento en que indica su contraseña de firma.

    d. Notificación emergente: el prestador de servicios de certificación puede ofrecer también una aplicación móvil segura que puede ser instalada en el dispositivo de confianza del cliente para que, al momento de firmar, el usuario reciba una alerta de forma directa en dicha aplicación para que esté anuente sobre el intento de autenticación y pueda aprobarlo o denegarlo con un solo toque después de que haya escrito su contraseña de firma.

    e. Autenticación Biométrica: al momento en que el usuario procede en aplicar su firma electrónica a un documento escribiendo su contraseña, se procede con la validación o autenticación biométrica de su rostro (reconocimiento facial) o huella dactilar en una aplicación que podría estar instalada en su teléfono móvil, para que dicho proceso actúe como un segundo factor de autenticación y se realice el proceso de firma.

5. Como método oficial de validación de los certificados electrónicos emitidos por los prestadores de servicios de certificación y que debe ser utilizado por los sistemas informáticos empleados por el Gobierno Nacional en las diferentes Instituciones, se requiere de la creación de una Lista de Confianza de los prestadores de servicios de certificación acreditados (TSL - Trust Services List), la cual tendrá los certificados raíces necesarios para que todos los sistemas puedan verificar si los certificados electrónicos de los firmantes fueron emitidos por un prestador de servicios de certificación acreditado. Hasta que la Dirección Nacional de Firma Electrónica no proceda con la creación del reglamento técnico

que regule a la Lista de Confianza y que no se realice la publicación de una primera versión oficial del TSL, los sistemas informáticos del Gobierno no están obligados en validar las firmas de los prestadores de servicios de certificación acreditados. Tal como se realiza actualmente, los sistema del Gobierno Nacional que deseen adoptar el uso de la firma electrónica calificada en la República de Panamá, deberán utilizar únicamente los certificados de las Autoridades Raíz e Intermedias de la Dirección Nacional de Firma Electrónica, los cuales se pueden descargar desde el sitio web oficial: https://www.firmaelectronica.gob.pa/ o utilizando directamente las direcciones URL de cada certificado electrónico de la Autoridad de Certificación correspondiente (información disponible en los campos de los certificados electrónicos de cada usuario y que normalmente es validado por los sistemas):

- http://www.pki.gob.pa/cacerts/caraiz.crt
- http://www.pki.gob.pa/cacerts/capc2.crt
- http://www.pki.gob.pa/cacerts/cagob.crt

6. Cada prestador de servicios de certificación aprobado debe tener disponible en su página web, un validador online que les permita a sus usuarios poder adjuntar los documentos firmados y que proceda a mostrar en pantalla, si cuentan con firma electrónica calificada válida emitida por ese prestador de servicios de certificación. Dicho validador debe ser capaz de mostrar mensajes de error en caso de que el usuario adjunte un documento firmado por otro prestador de servicios de certificación acreditado en Panamá o en algún otro país para evitar confusiones, ya que esa herramienta debería solamente enfocarse en los documentos firmados con los certificados electrónicos calificados del prestador de servicios de certificación. De igual forma, deben existir manuales de configuración disponibles al público que expliquen cómo configurar sus certificados electrónicos para firmar y validar documentos en diferentes programas, el proceso para desbloquear sus certificados electrónicos, procedimiento para solicitar la revocación o suspensión de sus certificados electrónicos, documentación con los errores habituales, entre otros manuales de ayuda. También deben estar disponibles sus certificados raíces a descargar, los controladores (drivers) para los dispositivos criptográficos que les ofrezcan a sus clientes (tarjetas inteligentes / tokens USB en caso de aplicar), documentación del API de acceso para sus HSM de la Firma en la Nube, aplicaciones para firmar en caso de que aplique, SDK para desarrolladores, entre otros componentes.

7. Para los prestadores de servicios de certificación que no utilicen sus centros de datos primario o secundario en la República de Panamá, no serán necesarias las visitas físicas a dichos centros de datos (donde opere la plataforma PKI), por parte de los auditores ni del personal de la Dirección Nacional de Firma Electrónica, si los mismos cumplen con las certificaciones y los estándares de cumplimiento vigentes al momento de realizar la auditoría, los cuales se listan a continuación:

   - ISO 9001 (Sistema de gestión de la calidad).
   - ISO/IEC 27001 (Estándar para la seguridad de la información).
   - ISO/IEC 27017 (Controles de Seguridad para Servicios Cloud).
   - ISO/IEC 27018 (Protección de la información de identificación personal).
   - ISO/IEC 27701 (Estándar de privacidad internacional que se centra en la recogida y el tratamiento de información personal identificable).
   - SOC 1 (Controles internos de los proveedores de servicios en la nube que puedan ser relevantes para los informes financieros de los clientes).
   - SOC 2 (Informe basado en los Criterios de Servicios de Confianza).
   - SOC 3 (Informe público sobre controles internos en materia de seguridad, disponibilidad, integridad del tratamiento de datos y confidencialidad).
   - CSA STAR (Registro de seguridad, confianza, garantía y riesgo).

- PCI DSS (Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago).

En base a lo mencionado, el acceso obligatorio para el auditor y personal de la Dirección Nacional de Firma Electrónica se limitará al ámbito lógico de la plataforma PKI, es decir, a los sistemas de los equipos utilizados en la infraestructura para comprobar el correcto funcionamiento y nivel de seguridad de las diversas aplicaciones, bases de datos, entre otros componentes; por lo que será responsabilidad del auditor acreditado, mostrar las certificaciones de dichos centros para que su acreditación pueda continuar en firme. Si los centros de datos (primario o secundario) ubicados en el extranjero cuentan con menos certificaciones u otras equivalentes, la inspección física del auditor será obligatoria y deberá ser detallado en los informes de auditoría para ambos centros de datos. De igual forma, el prestador de servicios de certificación tendrá la opción de utilizar los centros de datos disponibles en la República de Panamá, donde se requerirá de la inspección física por parte de los auditores y del personal técnico de la Dirección Nacional de Firma Electrónica. Se debe tener en cuenta que tanto el centro de datos principal como los centros de datos secundarios (donde opere su plataforma) deberán cumplir con certificaciones equivalentes para tener el mismo nivel de confiabilidad y seguridad. La Dirección Nacional de Firma Electrónica se reserva el derecho a su criterio de realizar las inspecciones y validaciones de las certificaciones y de toda documentación presentada por el auditor.

Artículo No. 29. – APÉNDICE I (Otros requisitos técnicos de comprobación de identidad remota). El prestador de servicios de certificación empleará sistemas y procedimientos de identificación remota de acuerdo con los requisitos mínimos seguridad establecidos en este apéndice.

1. **(Requisitos de los documentos de identidad utilizados en el proceso de identificación).** La identificación del solicitante se acreditará mediante la validación de la cédula de identidad o pasaporte.

2. **(Condiciones generales del proceso de identificación)**. Se informará al solicitante, de manera clara y comprensible, los términos y condiciones del proceso de identificación remota, así como de las recomendaciones de seguridad aplicables. Así mismo, el proceso de identificación se interrumpirá o no se considerará válido cuando concurra alguna de las siguientes circunstancias:

    a. existan indicios de falsedad o manipulación del documento de identificación;
    b. existan indicios de falta de correspondencia entre el titular del documento y el solicitante;
    c. las condiciones de la comunicación impidan o dificulten verificar la autenticidad e integridad del documento de identificación y la correspondencia entre el titular del documento y el solicitante;
    d. existan indicios de uso de archivos pregrabados;
    e. existan indicios de que para la transmisión de video no se ha utilizado un único dispositivo.

    Si el proceso de identificación se realiza de forma síncrona, el prestador dispondrá de un procedimiento para llevar a cabo la entrevista de identificación del solicitante del certificado y una guía de diálogo para los operadores de la autoridad de registro.

    Si el proceso de identificación se realiza de forma asíncrona, un operador de la autoridad de registro supervisará a posteriori el proceso de identificación grabado y comprobará las evidencias e imágenes generadas por el sistema para aceptar o rechazar la validez del proceso de identificación.

    Para el caso de solicitud de certificados electrónicos a utilizarse para una sola transacción, la comparecencia virtual en línea podrá realizarse ante un agente automatizado, en cuyo caso la aprobación de la emisión del certificado de firma

electrónica calificada, se realizará con observancia de las medidas de seguridad previstas en este apéndice.

3. **(Requisitos para la comprobación de la identidad y otras circunstancias personales de los solicitantes)**. El prestador mediante el procedimiento de comparecencia virtual en línea verificará la autenticidad, vigencia, integridad física y lógica del documento de identificación utilizado y la correspondencia del titular del documento con el solicitante. En este sentido, se tomarán las medidas adecuadas para detectar una posible manipulación de la imagen de video, del documento de identidad o del solicitante. Para ello se implantarán las siguientes medidas mínimas:
    a. En el caso de la identificación remota por video síncrona: Se tomarán medidas organizativas que hagan patente dicha manipulación a través de la interacción con el documento de identidad utilizado y con el solicitante, según las indicaciones del operador de la autoridad de registro, a través de interacciones y actuaciones físicas que figurarán en un protocolo que incluirá acciones tanto comunes como aleatorias y diferenciadas.
    b. En el caso de la identificación remota por video no asistida y en los casos permitidos que la comparecencia virtual en línea se realice ante agente automatizado: El sistema requerirá al solicitante la realización de interacciones y actuaciones físicas, que figurarán en un protocolo que incluirá acciones tanto comunes como aleatorias y diferenciadas.

4. **(Requisitos de la grabación y de su conservación).** El sistema empleado para la comparecencia virtual en línea deberá:
    a. El proceso de identificación se grabará íntegramente y sin interrupciones.
    b. Se constatará de manera fehaciente la fecha y hora de la grabación mediante el uso de un sello de tiempo calificado.
    c. Se garantizará la integridad, la autenticidad, la confidencialidad y la conservación a largo plazo de la grabación.
    d. Se conservará una copia de la grabación del proceso íntegro de identificación durante un periodo mínimo de tiempo de 7 años.
    e. Se conservarán, por el mismo periodo de tiempo, fotos o capturas de pantalla del solicitante y del documento de identidad utilizado, en las que serán claramente reconocibles tanto la persona como el anverso y el reverso del documento de identidad.

5. **(Requisitos mínimos de seguridad de los sistemas de identificación remota por vídeo).** El sistema utilizado para la identificación mediante comparecencia virtual en línea de los solicitantes de certificados de firma electrónica calificada garantizará que:

    I. En el proceso de identificación:
        a. Se realiza desde un único dispositivo.
        b. Se ejecuta en tiempo real.
        c. Se detecta la utilización de archivos pregrabados.
        d. En el caso de que la calidad de la imagen y el sonido (para la identificación remota por video asistida) no permita la identificación inequívoca no generará una identificación positiva.
        e. Se comprueba la correspondencia del titular del documento con el solicitante:
            - Si es síncrona, el sistema permitirá al operador de la Autoridad de Registro o al agente automatizado (el agente automátizado sólo será permitido para la emisión de los certificados calificados de un solo uso) analizar las características biométricas del solicitante y la correspondencia de la información incluida en el documento de identidad con la instantánea o imagen del solicitante.

            - Si es asíncrona, el sistema biométrico deberá realizar una comparación entre la imagen captada y el documento de identidad,

proveyendo automáticamente un score o puntuación sobre el grado de similitud entre los mismos. El prestador de servicios de certificación, basado en el grado de fiabilidad aportado por el sistema implementado y el correspondiente análisis de riesgos deberá valorar el nivel de exposición a fallos y ataques que corresponda, estableciendo el procedimiento y criterios que debe seguir el operador de la autoridad registro para decidir sobre la aprobación de la solicitud de emisión del certificado.

II. Para la realización de la prueba de vida:
   a. Si es síncrona, el sistema permitirá al operador o al agente automatizado (en los casos permitidos) comprobar que la persona está viva utilizando un procedimiento para llevar a cabo la entrevista de identificación del solicitante del certificado y una guía de diálogo para los agentes, que incluya preguntas aleatorias y dinámicas.
   b. Si es asíncrona, la solución debe establecer medidas técnicas para detectar que la persona está viva a través de los movimientos de los rasgos faciales y el movimiento del solicitante. El sistema biométrico deberá implementar medidas para la detección de ataques de presentación biométrica PAD (Presentation Attack Detection).

   En ambos casos, el prestador de servicios de certificación, basado en el grado de fiabilidad aportado por el sistema implementado y el correspondiente análisis de riesgos deberá valorar el nivel de exposición a fallos y ataques que corresponda, estableciendo el procedimiento y criterios a seguir para la aprobación de la solicitud de emisión del certificado.

III. Para la validación de los documentos de identidad:
   El sistema debe ser capaz de permitir validar la siguiente información:
   a. Autenticidad
      - Características del documento: tamaño, patrón, diseño, espaciado entre caracteres y tipografía del documento.
      - Cuando sea posible medidas de seguridad, como hologramas o imágenes laser variable.
   b. Vigencia del documento: Fecha de expiración.
   c. Integridad: Validación de los datos con la MRZ (Verificación de los datos de la zona visible y cumplimiento de norma ICAO 9303).
   d. Que el anverso y el reverso del documento corresponden al mismo documento, siempre que el documento lo permita.
   e. Si es síncrona, el sistema permitirá al operador de la Autoridad de Registro o un agente automatizado (este último solo en los casos permitidos) verificar visualmente que las imágenes del documento de identidad y fondos de seguridad corresponden con el tipo y versión del documento esperado.
   f. Si es asíncrona, el sistema permitirá al operador de la Autoridad de Registro supervisar a posteriori el proceso de identificación grabado y comprobar las evidencias e imágenes generadas del documento de acuerdo con lo especificado en la letra anterior.

6. **(Sobre aprobación de la solicitud)** En cualquiera de los casos de identificación síncrona o asíncrona, el operador de la autoridad registro o agente automatizado en los casos permitidos deberá basar su decisión de aprobación o denegación de la solicitud de emisión del certificado en la calidad de todas las evidencias recabadas en el proceso de identificación, incluyendo el vídeo, la existencia de los elementos de seguridad del documento de identidad extraídos del mismo durante la realización del video y la comparación biométrica realizada.

7. Por cada perfil de certificado electrónico calificado especificado en el artículo 30 del presente Reglamento Técnico, se exige el uso de Servicios Web integrados en los

sistemas de inscripción (registro) y emisión utilizados por las PKI de los prestadores de servicios de certificación; para así poder validar correctamente la información de los usuarios de Firma Electrónica Calificada y de esta forma, disminuir el riesgo de emisión de certificados electrónicos con datos ficticios. Los Servicios Web deben estar programados como módulos que forman parte de los sistemas de inscripción, donde al momento en que el operador de registro del prestador de servicios de certificación escribe algún dato como el número de la cédula del ciudadano, el RUC de la persona jurídica o la idoneidad del profesional, entre otros campos (dependiendo del tipo de perfil) se deberán obtener los datos del usuario del certificado electrónico calificado de manera automática para autocompletar los campos restantes del perfil y proceder con la emisión de sus certificados electrónicos calificados.

8. Los prestadores de servicios de certificación aprobados deberán contar con un portal web de Preinscripción Online, donde cada usuario podrá registrarse utilizando su correo electrónico personal, el cual será validado al recibir un mensaje de correo que contiene un enlace con un código único (que tiene un tiempo de expiración configurable), donde deberá ingresar para así confirmar que es el dueño de la cuenta del correo electrónico que utilizó en el registro. Posteriormente podrá solicitar su certificado electrónico completando los formularios según el tipo de perfil (preinscripción online) y adjuntando los documentos requeridos. Los datos registrados por el ciudadano en el portal web de Preinscripción Online del prestador de servicios de certificación serán validados por medio de los servicios web de cada perfil y el de biometría descritos en los artículos del presente reglamento.

9. Para las atenciones de los certificados electrónicos calificados emitidos de forma remota (Firma en la Nube) y también de forma presencial, el prestador de servicios de certificación deberá contar con un sistema de biometría que obtenga los datos de los perfiles de manera automática, con la ayuda de los servicios web correspondientes, al escribir el número de la cédula del ciudadano, el RUC de la persona jurídica o la idoneidad del profesional, entre otros campos (dependiendo del tipo de perfil) y luego realizar una comparación biométrica del rostro del usuario capturado en la videollamada contra la foto de su cédula también mostrada en la videollamada y finalmente comparar el rostro de esa persona contra la imagen de la cédula obtenida desde el sistema SVI del Tribunal Electoral (donde la foto podrá ser adjuntada en el sistema de inscripción por el operador de registro del prestador de servicios de certificación en caso de que dicha imagen no sea devuelta por el servicio web del Tribunal Electoral). Si las validaciones biométricas del rostro son realizadas correctamente, se continuará con la emisión de los certificados electrónicos calificados, obteniendo los datos por medio de los servicios web. La integración de servicios web con el sistema de biometría aplica tanto para los procesos de identificación realizados de forma síncrona y asíncrona mencionados en el artículo 29 del presente Reglamento Técnico.

10. En caso de que un prestador de servicios de certificación realice los procesos de emisión de sus certificados electrónicos de forma presencial, sus sistemas de registro deberán contar con los módulos necesarios para capturar las huellas dactilares de los clientes, ejecutar la validación biométrica del rostro (descrita en el presente reglamento), tomar la fotografía del usuario, impresión del contrato de aceptación, imprimir los códigos (PIN, PUK y suspensión) en un sobre cerrado y finalmente proceder con la emisión del certificado electrónico calificado. En caso de que el certificado se emita en una tarjeta inteligente, la foto del usuario, su nombre completo, cédula y el tipo de perfil, deberán aparecer impresos en la tarjeta. Si se utiliza un Token USB, se procede con la emisión de sus certificados electrónicos, pero se debe realizar también todo el proceso mencionado anteriormente hasta la impresión del sobre. Si se lleva a cabo la atención de forma presencial con la modalidad de firma electrónica en la nube, también se debe realizar el proceso de la captura biométrica de sus datos descrito previamente, incluyendo la impresión del contrato de aceptación para luego proceder con la emisión de los certificados electrónicos, tal como si se hubiera realizado de forma remota en una videollamada en vivo entre el operador de registro y el usuario.

11. Se requiere el uso del Servicio Web para validar el perfil de Persona Natural, el cual deberá ser contratado por el prestador de servicios de certificación directamente con el Tribunal Electoral. El SVI es un servicio que brinda el Tribunal Electoral a través de internet que permite verificar la identidad de las personas y la autenticidad de la cédula de identidad personal con la base de datos del Registro Civil y Cedulación. Se debe contar con el acceso al SVI para que el operador de registro pueda verificar los datos de las personas (incluyendo la foto de la cédula) y también el sistema de inscripción debe incluir el acceso por servicio web (SSVI) para obtener los datos de las personas naturales (primer nombre, segundo nombre, primer apellido, segundo apellido, cédula, fecha de nacimiento, entre otros campos) cuando se captura el número de la cédula del ciudadano que obtendrá su certificado electrónico calificado. También se deben realizar las validaciones descritas en los artículos anteriores del presente reglamento para continuar con la emisión de los certificados electrónicos calificados. Aunque los datos del perfil de Persona Natural son validados con el servicio web del Tribunal Electoral en la fase de emisión de los certificados electrónicos, los mismos debieron ser capturados por los ciudadanos solicitantes por medio del portal web de preinscripción online del prestador de servicios de certificación, donde se debió adjuntar la foto de la cédula para una mejor verificación por parte de los operadores de registro. En el caso de los extranjeros no registrados en el Tribunal Electoral de Panamá, la atención se deberá realizar de forma presencial donde el usuario tendrá que registrarse en el portal web de preinscripción online del prestador de servicios de certificación, adjuntar la foto de su pasaporte vigente, la certificación de estatus migratorio vigente emitido por el Servicio Nacional de Migración (extranjeros residentes) o la certificación de movimiento migratorio vigente emitido por el Servicio Nacional de Migración (extranjeros no residentes).

12. Los perfiles de Representante de Persona Jurídica, Colaborador de Persona Jurídica y Sello Electrónico para Empresas deberán contar con las validaciones del perfil de Persona Natural, descritas anteriormente, para luego realizar otra validación utilizando el número RUC por medio del servicio web ofrecido por el Registro Público de Panamá de las Sociedades Anónimas, el cual devuelve los campos necesarios para completar cada perfil. En caso de que el Servicio Web del Registro Público no esté disponible para empresas privadas, los certificados electrónicos calificados de los perfiles mencionados en el presente artículo serán emitidos solamente por la Dirección Nacional de Firma Electrónica del Registro Público de Panamá, la cual se le otorga las atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá, según consta en el artículo No. 1 de la Ley 82 del 9 de noviembre de 2012.

13. Los perfiles de Factura Electrónica para Persona Natural y Persona Jurídica deberán contar con las validaciones del perfil de Persona Natural, descritas anteriormente, para luego realizar otra validación utilizando el número RUC por medio del servicio web ofrecido por la Dirección General de Ingresos (DGI) del Ministerio de Economía y Finanzas, el cual devuelve los campos necesarios para completar cada perfil. En caso de que el Servicio Web de la DGI no esté disponible para empresas privadas, los certificados electrónicos calificados de los perfiles mencionados en el presente artículo serán emitidos solamente por la Dirección Nacional de Firma Electrónica del Registro Público de Panamá, la cual se le otorga las atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá, según consta en el artículo No. 1 de la Ley 82 del 9 de noviembre de 2012.

14. El perfil de Profesional idóneo deberá contar con las validaciones del perfil de Persona Natural, descritas anteriormente, para luego realizar otra validación utilizando el número de idoneidad del profesional por medio de servicios web ofrecidos por los Gremios en Panamá, bases de datos de autoridades competentes o cotejo contra la información publicada en la Gaceta Oficial en el caso de profesiones o disciplinas que publiquen por este medio las resoluciones oficiales con la respectiva autorización o licencia para ejercer de la persona natural solicitante. En caso de que el Servicio Web de Profesionales no esté disponible para empresas privadas o no exista

un convenio entre el Gremio de Profesionales con el prestador de servicios de certificación, los certificados electrónicos calificados de profesional serán emitidos solamente por la Dirección Nacional de Firma Electrónica del Registro Público de Panamá, la cual se le otorga las atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá, según consta en el artículo No. 1 de la Ley 82 del 9 de noviembre de 2012, siempre y cuando exista un convenio entre la Dirección Nacional de Firma Electrónica con el Gremio de Profesionales mencionado.

Artículo No. 30. – APÉNDICE II Estructura regulada para los atributos OID de los certificados de Firma Electrónica Calificada). Se regula a través de la presente norma técnica, el esquema de estructura de los Identificadores de Objeto (OID) para certificados de firma electrónica calificada con la finalidad de permitir la interoperabilidad entre los sistemas que utilicen certificados electrónicos calificados emitidos por cualquier prestador de servicios de certificación acreditados por el Registro Público de Panamá ya sea público o privado.

La descripción de los números OID (identificador de objeto) utilizados actualmente por la Infraestructura de Clave Pública de la Dirección Nacional de Firma Electrónica y de otras entidades en Panamá se puede revisar en la siguiente tabla, por lo que, la información descrita deberá ser tomada como referencia para el registro de los números OID propios de cada prestador de servicios de certificación:

OID	Descripción
2	Areas de trabajo conjunto entre ISO/IEC (Organización Internacional de Normalización / Comisión Electrotécnica Internacional) y UIT-T (Unión Internacional de Telecomunicaciones - Sector de normalización de las telecomunicaciones) y otros trabajos internacionales
2.16	Registro conjunto (ITU-T e ISO/IEC) dentro de un país.
2.16.591	OID de la República de Panamá.
2.16.591.1	Infraestructura de Clave Pública (PKI) del Registro Público de Panamá.
2.16.591.1.1	Autoridad de Certificación Raíz Panameña.
2.16.591.1.2	Autoridad de Certificación del Gobierno de Panamá.
2.16.591.1.2.1	Políticas de uso de certificados digitales.
2.16.591.1.2.1.1	Certificado de tipo personal.
2.16.591.1.2.1.2	Certificados de Gobierno oficial.
2.16.591.1.2.1.3	Certificado para servidores.
2.16.591.1.2.2	Declaración de Practicas de Certificación.
2.16.591.2	Autoridad de Certificación de Firma del País de Panamá.
2.16.591.3	Autoridad de Certificación de la Autoridad Marítima de Panamá.
2.16.591.4	Autoridad Certificadora del Registro Público de Panamá (para pruebas).

Cada prestador de servicios de certificación procederá a registrar de forma online sus propios números OID, manteniendo los tres (3) primeros dígitos que representan a la República de Panamá (2.16.591), pero el siguiente dígito sería el OID propio del prestador de servicios de certificación, también puede existir otro OID que haga referencia a la Autoridad de Certificación del prestador de servicios de certificación y finalmente, los dos (2) últimos dígitos corresponderán a los campos específicos de los perfiles, los cuales deberán ser iguales a los utilizados en los certificados electrónicos calificados emitidos por la Dirección Nacional de Firma Electrónica (la nomenclatura .X.X. corresponde a los OIDs propios del prestador de servicios de certificación). La Declaración de Practicas de Certificación y políticas del prestador de servicios de certificación también deben estar bajo sus propios números OID registrados.

Persona Natural

OID	Descripción	Tipo de Campo
Nombre RFC822	Correo electrónico	Obligatorio
OID.2.16.591.X.X.1.1	Primer nombre	Obligatorio
OID.2.16.591.X.X.1.2	Segundo nombre	Obligatorio si tiene
OID.2.16.591.X.X.1.3	Primer apellido	Obligatorio si tiene
OID.2.16.591.X.X.1.4	Segundo apellido	Obligatorio si tiene
OID.2.16.591.X.X.1.5	Cédula	Obligatorio
OID.2.16.591.X.X.1.6	Fecha de nacimiento	Obligatorio

Representante de Persona Jurídica

OID	Descripción	Tipo de Campo
Nombre RFC822	Correo electrónico	Obligatorio
OID.2.16.591.X.X.1.1	Primer nombre	Obligatorio
OID.2.16.591.X.X.1.2	Segundo nombre	Obligatorio si tiene
OID.2.16.591.X.X.1.3	Primer apellido	Obligatorio si tiene
OID.2.16.591.X.X.1.4	Segundo apellido	Obligatorio si tiene
OID.2.16.591.X.X.1.5	Cédula	Obligatorio
OID.2.16.591.X.X.1.6	Fecha de nacimiento	Obligatorio
OID.2.16.591.X.X.2.1	Nombre de la Persona Jurídica.	Obligatorio
OID.2.16.591.X.X.2.2	Número RUC	Obligatorio
OID.2.16.591.X.X.2.3	Ficha	Obligatorio
OID.2.16.591.X.X.2.4	Rollo	Obligatorio
OID.2.16.591.X.X.2.5	Imagen	Obligatorio

Colaborador de Persona Jurídica

OID	Descripción	Tipo de Campo
Nombre RFC822	Correo electrónico	Obligatorio
OID.2.16.591.X.X.1.1	Primer nombre	Obligatorio
OID.2.16.591.X.X.1.2	Segundo nombre	Obligatorio si tiene
OID.2.16.591.X.X.1.3	Primer apellido	Obligatorio si tiene
OID.2.16.591.X.X.1.4	Segundo apellido	Obligatorio si tiene
OID.2.16.591.X.X.1.5	Cédula	Obligatorio
OID.2.16.591.X.X.1.6	Fecha de nacimiento	Obligatorio
OID.2.16.591.X.X.2.1	Nombre de la Persona Jurídica.	Obligatorio
OID.2.16.591.X.X.2.2	Número RUC	Obligatorio
OID.2.16.591.X.X.5.1	Limitación	Obligatorio

Factura Electrónica

OID	Descripción	Tipo de Campo
Nombre RFC822	Correo electrónico	Obligatorio
OID.2.16.591.X.X.1.1	Primer nombre	Obligatorio
OID.2.16.591.X.X.1.2	Segundo nombre	Obligatorio si tiene
OID.2.16.591.X.X.1.3	Primer apellido	Obligatorio si tiene
OID.2.16.591.X.X.1.4	Segundo apellido	Obligatorio si tiene
OID.2.16.591.X.X.1.5	Cédula	Obligatorio
OID.2.16.591.X.X.1.6	Fecha de nacimiento	Obligatorio
OID.2.16.591.X.X.2.1	Nombre de la Persona Jurídica.	Obligatorio
OID.2.16.591.X.X.2.2	Número RUC	Obligatorio
OID.2.16.591.X.X.6.1	Dígito Verificador	Obligatorio
OID.2.16.591.X.X.6.2	Tipo de Contribuyente	Obligatorio

Profesional idóneo

OID	Descripción	Tipo de Campo
Nombre RFC822	Correo electrónico	Obligatorio
OID.2.16.591.X.X.1.1	Primer nombre	Obligatorio
OID.2.16.591.X.X.1.2	Segundo nombre	Obligatorio si tiene

OID.2.16.591.X.X.1.3	Primer apellido	Obligatorio si tiene
OID.2.16.591.X.X.1.4	Segundo apellido	Obligatorio si tiene
OID.2.16.591.X.X.1.5	Cédula	Obligatorio
OID.2.16.591.X.X.1.6	Fecha de nacimiento	Obligatorio
OID.2.16.591.X.X.3.1	Profesión	Obligatorio
OID.2.16.591.X.X.3.2	Número de Idoneidad	Obligatorio

Sello Electrónico para Empresas

OID	Descripción	Tipo de Campo
Nombre RFC822	Correo electrónico	Obligatorio
OID.2.16.591.X.X.1.1	Primer nombre	Obligatorio
OID.2.16.591.X.X.1.2	Segundo nombre	Obligatorio si tiene
OID.2.16.591.X.X.1.3	Primer apellido	Obligatorio si tiene
OID.2.16.591.X.X.1.4	Segundo apellido	Obligatorio si tiene
OID.2.16.591.X.X.1.6	Fecha de nacimiento	Obligatorio
OID.2.16.591.X.X.2.1	Nombre de la Persona Jurídica.	Obligatorio
OID.2.16.591.X.X.2.2	Número RUC	Obligatorio
OID.2.16.591.X.X.4.1	Nombre de la Entidad	Obligatorio
OID.2.16.591.X.X.5.1	Limitación	Obligatorio

Artículo No. 31. – APÉNDICE III (Modalidades y requisitos para la prestación del servicio de entrega electrónica calificada)

1. El servicio de entrega electrónica calificada deberá cumplir con los siguientes requisitos:
    a. Asegurar con un alto nivel de fiabilidad en la identificación del iniciador;
    b. Garantizar la identificación del destinatario antes de la entrega de los datos;
    c. Proteger el envío y recepción de datos con una firma electrónica calificada, un sello electrónico calificado o un sello de tiempo de un prestador de servicio de certificación, de tal forma que se impida la posibilidad de que se modifiquen los datos sin que se detecte;
    d. Indicar claramente al iniciador y al destinatario, cualquier modificación de los datos a efectos del envío o recepción del mensaje;
    e. Indicar mediante un sello de tiempo electrónico calificado la fecha y hora de envío, recepción y eventual modificación de los datos.

2. En el caso de que el servicio de entrega electrónica calificada esté destinada a garantizar el envío y entrega de un mensaje de datos sin garantizar su apertura o acuse de recibo, adicionalmente a los requisitos previstos en el numeral uno (1) de este artículo No. el servicio deberá cumplir:
    a. Con los requisitos previstos en el estándar ETSI EN 319 401.
    b. Las evidencias que se emitan como constancia del envío y entrega del mensaje de datos, las cuales deberán estar firmadas o selladas utilizando un servicio de firma electrónica calificada o sello electrónico calificado.

3. En el caso de que el servicio de entrega electrónica calificada esté destinada a garantizar el envío, entrega y apertura o lectura de un mensaje de datos con acuse de recibo, adicionalmente a los requisitos previstos en el numeral uno (1) el servicio deberá cumplir:
    a. Con los requisitos previstos en los estándares ETSI EN 319 401 y ETSI EN 319 521.
    b. Las evidencias que se emitan como constancia del envío y entrega del mensaje de datos deberán estar firmadas o selladas utilizando un servicio de firma electrónica calificada o sello electrónico calificado.

4. En el caso de que el servicio de entrega electrónica calificada esté destinada a garantizar el envío, entrega y apertura o lectura de un mensaje de datos con o sin acuse de recibo a través de correos electrónicos registrados (Registered Electronic Mail), adicionalmente a los requisitos previstos en el numeral uno (1) el servicio deberá cumplir:
    a. Con los requisitos previstos en los estándares ETSI EN 319 401, ETSI EN 319 521, ETSI EN 319 522, ETSI EN 319 531 y ETSI EN 319 532.

Artículo No. 32. – Los artículos detallados en este Reglamento Técnico no. 6 son de estricto cumplimiento para los prestadores de servicios de certificación ya registrados, incluyendo a las empresas que aplicarán posteriormente, las cuales deben cumplir el presente reglamento desde el momento de la entrega de toda la documentación (aplicación formal) para su registro ante la Dirección Nacional de Firma Electrónica. De conformidad con el artículo 18 del Decreto Ejecutivo 684 de 18 de octubre de 2013 los prestadores de servicios de certificación ya registrados tendrán un plazo de cuatro (4) meses a partir de la promulgación del presente reglamento para su cumplimiento. En caso de que un prestador de servicios de certificación ya registrado no cumpla con los artículos del presente reglamento se le podrá aplicar el régimen sancionador establecido en la Ley 51 de 22 de julio de 2008, el Decreto Ejecutivo 684 de 18 de octubre de 2013 y adicionalmente aquellos certificados electrónicos emitidos a sus clientes previos al período de 4 meses estos seguirán siendo calificados hasta su vencimiento, por tanto aquellos que se emitan posteriormente no tendrán el carácter de firma electrónica calificada .

SEGUNDO: Esta Resolución deroga la Resolución No. DG-175-2023 de 26 de julio de 2023, publicada en Gaceta Oficial No. 29839-A, del 03 de agosto de 2023.

TERCERO: Esta resolución entrará a regir a partir de su promulgación.

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 del 18 de octubre de 2013 y Decreto Ejecutivo No. 83 del 23 de marzo de 2023.

Dado en la ciudad de Panamá a los TRES (3) días del mes de octubre de dos mil veinticuatro (2024).

COMUNÍQUESE Y CÚMPLASE,

NAIROBIA ESCRUCERIA
Directora General de Registro Público de Panamá

AARON QUIJADA
Director Nacional de Firma Electrónica a.i.

REGISTRO PÚBLICO DE PANAMÁ
TECNOLOGÍA, CALIDAD Y SEGURIDAD REGISTRAL
SECRETARÍA GENERAL

ESTE DOCUMENTO ES FIEL COPIA DEL ORIGINAL

16/10/2024
FECHA

SECETARÍA GENERAL