

**REPÚBLICA DE PANAMÁ
REGISTRO PÚBLICO DE PANAMÁ**

**RESOLUCIÓN No. DG-087-2026
(De 13 de agosto de 2026)**

Por medio de la cual se aprueba el: **“REGLAMENTO TÉCNICO No. 9 DE LA DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA QUE REGULA EL MÉTODO DE VERIFICACIÓN DE IDENTIDAD PARA LOS PERFILES DE FIRMA ELECTRÓNICA CALIFICADA EN LA NUBE, FIRMA ELECTRÓNICA CALIFICADA DE FACTURA ELECTRÓNICA Y SE DICTAN OTRAS DISPOSICIONES.”**

LA DIRECTORA GENERAL DEL REGISTRO PÚBLICO DE PANAMÁ

En uso de sus facultades legales y reglamentarias,

CONSIDERANDO:

Que, según el artículo No. 1 de la Ley No. 82 de 9 de noviembre de 2012, se 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 numeral 1 del artículo No. 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, según el Artículo No. 10 de la Ley No. 51 de 22 de julio de 2008, modificado por el artículo No. 16 de la Ley No. 82 de 9 de noviembre de 2012, la Dirección Nacional de Firma Electrónica tiene la facultad de reglamentar tecnologías que permitan ofrecer la Firma electrónica calificada, la incorporación de la firma electrónica en la nube la cual permitirá otorgar a los solicitantes, un certificado de firma electrónica calificada sin necesidad de entregar dispositivos físicos que gestionar por parte del usuario, lo que habilita su solicitud de manera remota.

Que, según el numeral 1 del artículo 20-C de la Ley No. 51 de 22 de julio de 2008, adicionado por el artículo No. 22 de la Ley No. 82 de 9 de noviembre de 2012, además de las funciones establecidas por ley para la Dirección Nacional de Firma Electrónica, se establecen como funciones en materia de certificación 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, según el Artículo No. 26 de la Ley No. 51 de 22 de julio de 2008, modificado por el artículo No. 28 de la Ley No. 82 de 9 de noviembre de 2012, los prestadores de servicios de certificación podrán realizar las actuaciones de comprobación de identidad por sí mismos o por medio de otras personas naturales o jurídicas, públicas o privadas. En ese mismo sentido, se establece que la comprobación de identidad podrá hacerse mediante 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 y en virtud de ello para el presente reglamento técnico se incorpora la modalidad remota de solicitud de la firma electrónica calificada para factura electrónica;

Que para facilitar la lectura y cumplimiento de la reglamentación técnica de la Dirección Nacional de Firma Electrónica de la República de Panamá se derogan las reglamentaciones técnicas anteriores y se unifican en la presente reglamentación técnica;

Que la Dirección Nacional de Firma Electrónica de la República de Panamá, recomienda se apruebe una Resolución Técnica que sirva para dictaminar, adecuar los parámetros y estándares mínimos que deben utilizar los prestadores de servicios de certificación, para la emisión de Certificados electrónicos calificados.

Que en virtud de lo anterior, la Directora General del Registro Público de Panamá,

RESUELVE:

PRIMERO. APROBAR el REGLAMENTO TÉCNICO No. 9 DE LA DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA QUE REGULA EL MÉTODO DE VERIFICACIÓN DE IDENTIDAD PARA LOS PERFILES DE FIRMA ELECTRÓNICA CALIFICADA EN LA NUBE, FIRMA ELECTRÓNICA CALIFICADA DE FACTURA ELECTRÓNICA Y SE DICTAN OTRAS DISPOSICIONES, el cual es del tenor siguiente:

**TEXTO ÚNICO
REGLAMENTO TÉCNICO No. 9**

DE LA DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Artículo 1. (Objeto). El presente Reglamento Técnico tiene por objeto establecer el método de verificación de identidad aplicable para los perfiles de Firma Electrónica Calificada en la nube y la Firma Electrónica Calificada de Factura Electrónica, así como regular la utilización y el funcionamiento del Certificado Electrónico de Uso Limitado y los procedimientos, requisitos técnicos y operativos necesarios para su correcta implementación, administración, y control, de conformidad con el marco jurídico vigente en materia de firma electrónica.

Artículo 2. (Alcance). Las disposiciones previstas en el presente reglamento son de aplicación y obligatorio cumplimiento para todos los prestadores de servicios de certificación de firma electrónica calificada que operen en la República de Panamá, tanto de carácter público como privado, incluyendo el Registro Público de Panamá, en su calidad de prestador y autoridad certificadora raíz.

Artículo 3. (Estándares de cumplimiento). Los certificados electrónicos y servicios ofrecidos por los prestadores de servicios de certificación de firmas electrónicas calificadas que utilicen tecnología basada en una infraestructura de clave pública deben cumplir los estándares mínimos descritos a continuación:

1. Declaración de prácticas de certificación:

Objeto	Estándar
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".

2. Especificación de formato de firma electrónica admitido: XAdES (ETSI EN 319 132) CADES (ETSI EN 319 122) y PADES (ETSI EN 319 142).

3. Especificaciones para el protocolo de sellado de tiempo: RFC 3161 "Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)".
4. Especificaciones para la autoridad de sellado de tiempo: RFC 3628 "Policy Requirements for Time-Stamping Authorities (TSAs)".
5. Tiempo máximo para la aplicación del sellado de tiempo: Hasta cinco (5) minutos después de aplicada la firma electrónica al documento electrónico.

6. Especificaciones para certificado electrónico calificado para PKI:

Objeto	Estándar
Estructura del certificado	ITU x.509 v3
Certificados calificados	RFC 3739 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile"

7. Especificaciones de la lista de revocación de certificados (CRL):

Objeto	Estándar
Especificación de la CRL	RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"

8. Integración del número de identificación personal (NIP) al certificado.

Objeto	Estándar
Clases de NIP	Cédula de identidad personal, número de pasaporte, número de idoneidad del solicitante, registro único del contribuyente, dígito verificador y clase de contribuyente. El NIP según corresponda debe ser insertado en el certificado y en las credenciales del usuario.
Comprobación del NIP	(Ver artículo 4 sobre comprobación de identidad)
Lenguaje de escritura del NIP	ASN.1 syntax

9. Los prestadores de servicios de certificación deberán utilizar algoritmos criptográficos, parámetros, longitudes de clave y funciones hash vigentes, seguras y apropiadas para servicios de certificación y firma electrónica calificada, conforme a estándares reconocidos internacionalmente tales como ETSI TS 119 312 en su versión vigente, PKCS #1 v2.2 (RFC 8017) para implementaciones basadas en RSA, FIPS 180-4 para funciones hash seguras, FIPS 140-3 para módulos criptográficos, así como las normas ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 y ETSI EN 319 421 en lo que resulte aplicable; en consecuencia, no deberán utilizarse para nuevas emisiones algoritmos o referencias técnicas retiradas, obsoletas o desaconsejadas por sus organismos emisores, sin perjuicio de que los certificados electrónicos y demás objetos criptográficos emitidos válidamente con anterioridad a la entrada en vigencia del presente reglamento mantendrán su validez durante su ciclo de vida, siempre que no hayan expirado, sido revocados o invalidados conforme a derecho.

10. Especificaciones para el protocolo OCSP: RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".



11. Dispositivo seguro de creación de firma: 1- PKCS#11 (Certificado electrónico en SMARTCARD O USB TOKEN para cualquier perfil de Firma Electrónica); y 2- El módulo de seguridad de hardware (HSM) para firma electrónica en la nube con cualquier perfil y sello electrónico. El formato PKCS#12 se utilizará de manera temporal con los certificados electrónicos para los perfiles de Factura Electrónica hasta que la Dirección Nacional de Firma Electrónica actualice su plataforma (para optimizar la integración del actual perfil de factura electrónica en la nube), los sistemas de facturación ofrecidos por los Proveedores Autorizados Calificados aprobados por la Dirección General de Ingresos hayan sido actualizados para utilizar la firma electrónica en la nube (por medio de HSM centralizados) y la Dirección General de Ingresos confirme o actualice sus sistemas para no requerir este formato.

Artículo 4. (Comprobación de identidad).

1. Se requiere el uso de un mecanismo de comprobación de identidad remota aprobado por el Tribunal Electoral de Panamá para validar la identidad de las personas registradas en dicho organismo, que apliquen para los perfiles de Persona Natural, Representante de Persona Jurídica, Colaborador de Persona Jurídica, Profesional, Factura Electrónica y Sello Electrónico para Empresas. En el caso de las personas no registradas en el Tribunal Electoral de Panamá, la validación de identidad se realizará de forma presencial mediante la presentación de su pasaporte vigente, así como de la certificación de estatus migratorio vigente o de la certificación de movimiento migratorio vigente, según corresponda, emitida por el Servicio Nacional de Migración. El prestador de servicios de certificación deberá incorporar estos mecanismos en sus políticas de certificación y documentar su implementación conforme a lo establecido en la normativa aplicable.
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 concurren 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 mediante comparecencia virtual en línea, 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.

En comparecencia virtual en línea 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.






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. En el caso de la identificación remota asistida por video, se adoptarán medidas organizativas que permitan evidenciar dicha manipulación a través de la interacción con el documento de identidad y con el solicitante, conforme a las indicaciones del operador de la autoridad de registro, mediante interacciones y actuaciones físicas definidas en un protocolo que incluirá acciones tanto comunes como aleatorias y diferenciadas. En caso de que el proceso de identificación no pueda completarse satisfactoriamente por causas atribuibles a condiciones técnicas, tales como baja calidad de imagen, fallas de conectividad o limitaciones del dispositivo utilizado, el prestador podrá permitir un número limitado de reintentos del proceso de verificación remota, debidamente registrados y controlados. No obstante, cuando el rechazo esté motivado por indicios de fraude, inconsistencia de identidad o cualquier otra situación que comprometa la confiabilidad del proceso, no se permitirán nuevos intentos por la vía remota, debiendo el solicitante completar el proceso mediante comparecencia presencial.
4. **(Requisitos de la grabación y de su conservación).** El sistema empleado para la comparecencia virtual en línea deberá cumplir con lo siguiente:
- 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.

Los prestadores de servicios de certificación deberán garantizar la protección, confidencialidad, integridad y uso adecuado de los datos personales recabados durante los procesos de verificación de identidad, incluyendo datos biométricos, audiovisuales y metadatos generados durante el proceso, en cumplimiento de la normativa vigente en materia de protección de datos personales. En particular, deberán adoptar medidas técnicas y organizativas que aseguren que dicha información sea utilizada exclusivamente para los fines de identificación, autenticación y emisión de certificados electrónicos calificados, evitando su uso indebido, acceso no autorizado, alteración o divulgación. Asimismo, deberán garantizar la conservación segura de la información por el tiempo establecido en la normativa aplicable y, una vez cumplida su finalidad y vencidos los plazos legales de conservación, proceder a su eliminación segura o supresión definitiva conforme a mecanismos que impidan su recuperación.



5. **(Requisitos mínimos de seguridad de los sistemas de identificación remota por video).** 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. Para comprobar la correspondencia del titular del documento con el solicitante, el sistema le permitirá al operador de la Autoridad de Registro 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. El sistema biométrico deberá realizar una comparación entre la imagen captada, con el documento de identidad y su validación con el Tribunal Electoral, proveyendo automáticamente un score o puntuación sobre el grado de similitud entre los mismos. El operador del prestador del servicio 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 registropara decidir sobre la aprobación de la solicitud de emisión del certificado.

II. Para la realización de la prueba de vida:

- a. El sistema le permitirá al operador 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. 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).

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. Validación de los datos en la cédula contra la información proveída por el Tribunal Electoral.
 - d. Que el anverso y el reverso del documento corresponden al mismo documento.
 - e. El sistema le permitirá al operador de la Autoridad de Registro verificar visualmente que las imágenes del documento de identidad y fondos de seguridad corresponden con el tipo y versión del documento esperado.
 - f. El sistema le 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 el literal anterior.
6. **(Uso de mecanismos automatizados en la verificación de identidad).** El prestador de servicios de certificación podrá implementar mecanismos de verificación de identidad remota asistidos o automatizados mediante tecnologías de inteligencia artificial, siempre que estos cumplan con los estándares técnicos, de seguridad y confiabilidad establecidos por la Dirección Nacional de Firma Electrónica y se encuentren debidamente documentados en sus políticas y declaración de prácticas de certificación. Dichos mecanismos deberán operar bajo un enfoque de análisis de riesgo, de manera que la verificación automatizada solo podrá aplicarse a casos de bajo riesgo previamente definidos, garantizando en todo momento la trazabilidad, auditabilidad y justificación de las decisiones adoptadas. En todos los casos, el sistema deberá contemplar umbrales de confianza y mecanismos de detección de anomalías que permitan escalar automáticamente a revisión humana aquellos procesos que presenten inconsistencias, riesgo elevado o resultados no concluyentes, manteniéndose la responsabilidad final de la validación de identidad en el prestador de servicios de certificación.
7. **(Sobre aprobación de la solicitud).** El operador de la autoridad de registro 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.

En caso de que se detecte alguna anomalía en cualquiera de los procesos antes mencionados y la identificación no sea considerada válida para la emisión de la firma electrónica, la solicitud únicamente podrá volverse a procesar mediante comparecencia presencial en las oficinas del prestador de servicios de certificación, quedando excluida la posibilidad de un nuevo intento de manera virtual, salvo en los casos de reintentos permitidos por causas técnicas conforme al numeral 3 del presente artículo.



8. 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 descritos previamente, incluyendo la firma electrónica o manuscrita del contrato de aceptación.
9. 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 emitida por el Servicio Nacional de Migración (extranjeros residentes) o la certificación de movimiento migratorio vigente emitida por el Servicio Nacional de Migración (extranjeros no residentes). Dicho procedimiento de atención de forma presencial se mantendrá vigente mientras no se implemente una herramienta aprobada por la AIG y el Servicio Nacional de Migración que permita una validación remota que certifique inequívocamente la identidad del extranjero.
10. Los perfiles de Representante de Persona Jurídica, Colaborador de Persona Jurídica y Sello Electrónico para Empresas deberán realizar una validación adicional utilizando el 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 de Panamá no esté disponible para empresas privadas, se requerirá el Certificado emitido por el Registro Público de Panamá, de conformidad con el numeral 2 del artículo No. 26 de la Ley No. 51 de 22 de julio de 2008, modificada por el artículo No. 28 de la Ley No. 82 de 9 de noviembre de 2012, para proceder con la emisión de los certificados electrónicos calificados.
11. Los perfiles de Factura Electrónica para Persona Natural y Persona Jurídica deberán realizar una validación adicional 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, los certificados electrónicos calificados de los perfiles mencionados en el presente artículo serán validados por algún método alternativo de validación que haya sido aprobado por la DGI y el prestador de servicios de certificación.
 - a. Para que el prestador de servicios de certificación pueda proceder con la atención remota de los certificados electrónicos para los perfiles de Factura Electrónica en la nube (gestionados por HSM centralizados) se deberá habilitar un medio virtual seguro para la entrega de dichos certificados (y así evitar la atención de manera presencial); donde el certificado podrá ser emitido con la autorización de una solicitud firmada con firma electrónica



calificada, correspondiente a cualquier perfil de persona conforme a la normativa vigente (a excepción de factura electrónica y certificados electrónicos para dispositivos), aceptando el procedimiento técnico detallado por el prestador de servicios de certificación.

- b. Mientras que se utilice el formato PKCS#12 para los perfiles de Factura Electrónica, el certificado podrá ser solicitado por medio de la preinscripción online para que sea emitido de manera remota y entregado por un medio virtual seguro utilizando el correo electrónico del apoderado validado por medio del servicio Web de la DGI o con el documento de "Solicitud Apoderado para Retiro de Firma Electrónica" y en base a las instrucciones detalladas por el prestador de servicios de certificación.
 - c. El presente numeral para validar los perfiles de Factura Electrónica para Persona Natural y Persona Jurídica aplica para los prestadores de servicios de certificación públicos y privados.
12. El perfil de profesional idóneo deberá realizar una validación adicional 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, se podrá utilizar algún método alternativo de validación que haya sido aprobado por medio de un convenio entre el gremio de profesionales con el prestador de servicios de certificación.
13. Pasos de verificación para el perfil de firma electrónica calificada de sello electrónico para dispositivos, aplicaciones o servicios automatizados:
- 13.1 La Persona Jurídica debe enviar al prestador de servicios de certificación una solicitud firmada con su perfil de firma electrónica calificada de representante de persona jurídica o de colaborador de persona jurídica, válida en la República de Panamá, que identifique a la persona natural responsable de custodiar el certificado electrónico dentro de la empresa y, cuando sea distinta, a la persona natural autorizada para descargarlo, y que detalle los siguientes datos:

- RUC de la Empresa.
- Nombre del departamento, dirección o unidad organizacional que la empresa desee que aparezca en el certificado electrónico. (No excederse de 64 caracteres incluidos los espacios en blanco).
- Nombre de la empresa solicitante
- Nombre completo, cédula o pasaporte y correo electrónico de la persona natural solicitante (custodio) del certificado electrónico.
- Nombre completo, cédula o pasaporte y correo electrónico de la persona natural que descargará el certificado electrónico.
- Nombre del dispositivo, aplicación o servicio automatizado que requiere el certificado electrónico. (No excederse de 64 caracteres incluido los espacios en blanco).

- Limitaciones adicionales que la Persona Jurídica desee anotar en el certificado electrónico: (Campo opcional. No excederse de 64 caracteres incluidos los espacios en blanco)- Basado en el Artículo 15 de la Ley 51 de 2008.

13.2 Este perfil de certificado electrónico se emite en un dispositivo seguro de creación de firma tipo HSM de acuerdo a lo previsto en el numeral 11 del artículo 3 de este reglamento, por lo que la persona jurídica deberá generar el par de claves criptográficas en el dispositivo y remitir el archivo de solicitud de firma de certificado (Certificate Signing Request - CSR) asociado al par de claves al prestador de servicios de certificación para su revisión y firma.

13.3 El proceso de generación de las claves criptográficas en el HSM se documentará mediante acta, que deberá recoger evidencias fotográficas o en video sobre el procedimiento de generación de las claves criptográficas y la generación del archivo CSR, suscrita por todos los involucrados en el proceso de generación. Una copia de la misma deberá ser remitida conjuntamente con el archivo CSR al prestador de servicios de certificación para la emisión del certificado.

13.4 Verificación de la identidad de la persona natural responsable de custodiar el certificado electrónico y, cuando sea distinta, de la persona natural autorizada para descargarlo, conforme al procedimiento aplicable al perfil de firma electrónica calificada de persona natural, en modalidad presencial o remota.

13.5 Presentar certificación de Registro Público donde conste los datos relativos a la constitución y personalidad jurídica de la persona jurídica.

13.6 Realizadas las verificaciones correspondientes, el prestador de servicios de certificación procederá a la firma del CSR asociado al par de claves y pondrá el certificado electrónico emitido a disposición de la persona natural autorizada para descargarlo, a través del correo electrónico indicado en la solicitud. Una vez descargado, la persona jurídica solicitante deberá proceder a la importación del certificado de sello electrónico en el respectivo HSM asociado al par de claves criptográficas.

Artículo 5. (Certificado Electrónico de Uso Limitado). El presente artículo tiene por objeto regular la utilización y funcionamiento del Certificado Electrónico de Uso Limitado, como una modalidad operativa de la firma electrónica calificada, estableciendo los parámetros generales para su adecuada implementación y operación.

Se define el Certificado Electrónico de Uso Limitado como aquel cuya utilización está restringida a una o más firmas electrónicas, conforme a los límites y condiciones establecidos en las políticas de certificación del prestador de servicios de certificación aprobadas por la Dirección Nacional de Firma Electrónica. Este tipo de certificado incorpora mecanismos técnicos que permiten controlar, limitar y registrar su uso, garantizando que no pueda ser utilizado más allá de las condiciones autorizadas.

Los perfiles que podrán utilizar el Certificado Electrónico de Uso Limitado son los siguientes:

- Persona Natural.
- Representante de Persona Jurídica.
- Colaborador de Persona Jurídica.
- Profesional (idóneo).



En el caso del Certificado Electrónico de Uso Limitado, especialmente en la modalidad de uso único, el prestador de servicios de certificación deberá garantizar que la identidad del firmante sea validada en el momento de cada transacción de firma electrónica, mediante mecanismos de autenticación robusta que permitan vincular inequívocamente al titular con el acto de firma. Dichos mecanismos deberán contemplar, como mínimo, el uso de factores de autenticación adicionales, la vinculación expresa de la autenticación con la transacción específica a firmar y la generación de evidencias electrónicas que permitan reconstruir el proceso de firma, incluyendo, entre otros, la fecha y hora, identificador de la transacción, datos del dispositivo o sesión y el hash del documento firmado. El prestador de servicios de certificación podrá aplicar esquemas de autenticación basados en niveles de riesgo, incrementando los controles de verificación en aquellos casos que así lo requieran.

La supervisión a posteriori por parte de un operador de la autoridad de registro será obligatoria, salvo en aquellos casos de verificación automatizada debidamente autorizados para certificados electrónicos de uso limitado en modalidad de uso único, en los cuales dicha supervisión podrá realizarse de manera selectiva o basada en criterios de riesgo.

Artículo 6. (Vigencia del Certificado Electrónico de Uso Limitado). El Certificado Electrónico de Uso Limitado podrá emitirse bajo las siguientes modalidades:

- a. Certificado de uso único, cuya vigencia será la estrictamente necesaria para completar una única transacción de firma electrónica, quedando automáticamente inhabilitado o sin posibilidad de uso una vez ejecutada dicha firma;
- b. Certificado de uso limitado con vigencia extendida, con una duración máxima de hasta un (1) año, durante la cual el titular podrá adquirir un número determinado de firmas electrónicas, así como recargar paquetes adicionales de firmas, conforme a las condiciones establecidas por el prestador de servicios de certificación.

En ambos casos, el prestador de servicios de certificación deberá garantizar la implementación de mecanismos que aseguren el control efectivo del uso del certificado electrónico, conforme a la modalidad aplicable, evitando su utilización indebida o fuera de los límites autorizados.

Asimismo, el prestador de servicios de certificación deberá establecer en sus políticas de certificación las condiciones aplicables a cada modalidad, incluyendo la vigencia, los mecanismos de autenticación, control de uso y recarga, así como las medidas de seguridad necesarias para garantizar la integridad del proceso y la adecuada vinculación del titular con cada acto de firma.

En el caso de los certificados con vigencia extendida, la expiración del certificado implicará la pérdida de cualquier firma no utilizada, sin posibilidad de transferencia o reutilización posterior.

Artículo 7. (Limitación de utilización del Certificado Electrónico de Uso Limitado). El Prestador de Servicios de Certificación (PSC), tanto público como privado, deberá establecer, mediante sus políticas de certificación y de ciclo de vida del certificado, los mecanismos de control que regulen la utilización del Certificado Electrónico de Uso Limitado, conforme a las modalidades previstas en el artículo anterior.



Dichos mecanismos deberán garantizar que el certificado:

- a. Sea utilizado exclusivamente para una única firma electrónica, en el caso de certificados de uso único; o
- b. Sea utilizado hasta el número máximo de firmas autorizadas, en el caso de certificados de uso limitado con vigencia extendida.

En el caso del certificado de uso único, una vez completada la transacción correspondiente, el certificado deberá quedar automáticamente inhabilitado y sin posibilidad de uso adicional. En el caso del certificado de uso limitado con vigencia extendida, al agotarse el número de firmas autorizadas, el certificado deberá quedar automáticamente bloqueado o inhabilitado para nuevas operaciones de firma hasta que el titular adquiera o recargue un paquete adicional, siempre que el certificado permanezca vigente.

El prestador de servicios de certificación será responsable de asegurar que estos mecanismos se implementen de forma efectiva, trazable y auditable.

Artículo 8. (Identificación del solicitante del Certificado Electrónico de Uso Limitado).

El proceso de verificación de identidad para la emisión del certificado deberá cumplir los mismos estándares aplicables a la emisión de un certificado electrónico calificado.

Cuando la solicitud de emisión del certificado sea presentada ante un intermediario, dicho intermediario podrá participar en la ejecución del proceso de verificación de identidad del solicitante, así como en la obtención de su consentimiento y el resguardo de la documentación correspondiente, conforme a los procedimientos establecidos por el prestador de servicios de certificación.

Sin perjuicio de lo anterior, el prestador de servicios de certificación será en todo momento responsable frente al solicitante, la Dirección Nacional de Firma Electrónica y terceros, por la correcta comprobación de la identidad, de conformidad con lo establecido en el artículo 26 de la Ley 51 de 2008 y la normativa aplicable. El intermediario responderá frente al prestador de servicios de certificación por la correcta ejecución de las actividades que le hayan sido delegadas.

Las funciones del intermediario comprenderán, como mínimo:

- a. Validación de identidad del solicitante: Verificar la identidad del solicitante mediante los mecanismos de autenticación, validación documental, biometría u otros procedimientos autorizados, asegurando que el proceso cumpla los estándares definidos por el prestador de servicios de certificación.
- b. Custodia y resguardo de evidencia del proceso de validación: Conservar de manera íntegra, confidencial y segura la documentación y evidencia generada durante la verificación de identidad, incluyendo registros audiovisuales, imágenes, metadatos y cualquier otra información necesaria para respaldar la autenticación realizada, durante el período exigido por la normativa aplicable.

El prestador de servicios de certificación deberá establecer mecanismos de supervisión, control y auditoría sobre los intermediarios, así como definir contractualmente las responsabilidades, niveles de servicio y medidas de seguridad aplicables a su actuación. En el caso de los Certificados Electrónicos de Uso Limitado en modalidad de uso único, el prestador de servicios de certificación podrá implementar procesos de verificación de identidad totalmente automatizados, integrados en un flujo único que comprenda la



validación de identidad, la emisión del certificado y la firma electrónica, siempre que se garantice un nivel de seguridad equivalente al de los procesos asistidos. Para ello, deberán implementarse controles técnicos reforzados, tales como la validación en línea con fuentes oficiales, mecanismos biométricos con prueba de vida y detección de ataques de presentación (PAD), así como la generación y conservación íntegra de evidencias electrónicas del proceso. En estos casos, la revisión humana podrá aplicarse de forma posterior, selectiva o basada en análisis de riesgo, sin interrumpir el flujo transaccional en tiempo real. Para los certificados con vigencia extendida, la verificación de identidad deberá realizarse únicamente al momento de su emisión inicial. Durante el período de vigencia del certificado extendido, el titular no estará obligado a completar un nuevo proceso de validación para la adquisición de nuevas firmas electrónicas calificadas.

Artículo 9. (Proceso de firma electrónica calificada). Para la generación de toda firma electrónica calificada, independientemente de que se utilice un certificado electrónico calificado sin limitación cuantitativa de uso, un certificado de uso único o un certificado de uso limitado con vigencia extendida, el Prestador de Servicios de Certificación (PSC) deberá garantizar de forma obligatoria que la firma cuente con:

- a. Un sellado de tiempo proporcionado por una Autoridad de Sellado de Tiempo (TSA) autorizada.
- b. Mecanismos de validación a largo plazo (LTV) que permitan comprobar la validez de la firma y que el certificado utilizado se encontraba vigente y no había sido revocado al momento de su generación, aun cuando posteriormente dicho certificado expire o sea revocado.

Artículo 10. (Firma electrónica calificada 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.

Artículo 11. Con respecto a la firma electrónica calificada en la nube no se considerará que el almacenamiento de los datos de creación de firma está fuera del control exclusivo del firmante únicamente cuando es realizado por el prestador de servicios de certificación siempre que este los gestione debidamente autorizado por el firmante y 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 algún factor de autenticación adicional tal como un mecanismo biométrico o un código secreto único de seguridad tipo clave o 'pin', que el firmante tendrá bajo su responsabilidad y control exclusivo, el cual el prestador de servicios de certificación no conocerá ni gestionará su custodia.

Artículo 12. Para uso en trámites gubernamentales que requieran firma electrónica calificada se podrán usar certificados electrónicos de firma electrónica calificada emitidos con comprobación de identidad en la modalidad presencial y la modalidad en la nube.

Artículo 13. El Registro Público de Panamá emitirá certificados de firma electrónica calificada con comprobación de identidad en modalidad presencial o remota (síncrona o asíncrona) para cualquier perfil mencionado en el presente reglamento.



SEGUNDO: Los certificados electrónicos de firma electrónica calificada de validez prolongada ofrecidos por el Registro Público, como prestador de servicios de certificación, tendrán un periodo de vigencia de dos (2) años renovables y se dividirán de acuerdo a los siguientes perfiles de usuario (modalidad presencial y nube): Persona natural, representante legal de persona jurídica, colaborador de persona jurídica, profesional idóneo, funcionario público, factura electrónica y sello electrónico para empresas.

Adicionalmente el Registro Público de Panamá ofrecerá certificados electrónicos para uso en protocolos criptográficos de comunicación segura sobre una red electrónica o internet (SSL) y certificados electrónicos para ser usados en códigos fuentes de programación.

TERCERO: El presente Reglamento Técnico No. 9 deroga el Reglamento Técnico No. 5 de la Dirección Nacional de Firma Electrónica contenido en la Resolución No. DG-197-2024 de 3 de octubre de 2024.

CUARTO: 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 trece (13) días del mes de agosto de dos mil veintiséis (2026).

COMUNIQUESE Y CÚMPLASE,



NAIROBIA ESCRUCERIA
Directora General de Registro Público de Panamá


JEAN BATISTA
Director Nacional de Firma Electrónica