REPÚBLICA DE PANAMÁ
REGISTRO PÚBLICO DE PANAMÁ

RESOLUCIÓN No. DG-033-2023
(De 26 de enero de 2023)

"POR LA CUAL SE DICTA EL REGLAMENTO TÉCNICO No. 3 DE LA DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA QUE CREA UN NUEVO PERFIL DE FIRMA ELECTRÓNICA CALIFICADA, APRUEBA LA FIRMA ELECTRÓNICA CALIFICADA EN LA NUBE Y DICTA OTRAS DISPOSICIONES."

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

CONSIDERANDO:

Que según el artículo 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 artículo 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;

Que según el artículo 10 de la Ley No. 51 de 22 de julio de 2008 tal como fue modificado por el artículo 16 de la Ley No. 82 de 9 de noviembre de 2012 la Dirección Nacional de Firma Electrónica reconocerá como válido y reglamentará nuevas tecnologías que permitan ofrecer la Firma electrónica calificada, que para el presente reglamento, sería la incorporación novedosa de la firma electrónica en la nube la cual permitirá otorgarle 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 Artículo 20-B. de la Ley No. 51 de 22 de julio de 2008 tal como fue adicionado por el artículo 22 de la Ley No. 82 de 9 de noviembre de 2012 la Dirección Nacional de Firma Electrónica tendrá la facultad para 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;

Que según el artículo 20-C, numeral 1, de la Ley No. 51 de 22 de julio de 2008 tal como fue adicionado por el artículo 22 de la Ley No. 82 de 9 de noviembre de 2012 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 según el artículo 26 de la Ley No. 51 de 22 de julio de 2008 tal como fue modificado por el artículo 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 medio de otras personas naturales o jurídicas, públicas o privadas. Adicionalmente en el numeral 3, de ese mismo artículo, 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 novedosa de validación de identidad mediante comparecencia virtual en línea.

Que según el artículo 3, numeral 1 del Decreto Ejecutivo No. 684 de 18 de octubre de 2013 la Dirección Nacional de Firma Electrónica tendrá entre sus funciones dictar normas técnicas sobre la emisión de firma electrónica calificada y certificados electrónicos calificados y que permitan la implementación de la Ley No. 82 de 2012 y la Ley No. 51 de 2008 en los temas de competencia del Registro Público de Panamá, las cuales previa aprobación del Director General o de la Junta Directiva del Registro Público según la materia, se publicarán en la Gaceta Oficial y en el portal electrónico de la Dirección Nacional de Firma Electrónica.

Que adicionalmente, el 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; como también se establecen lineamientos referentes a los estándares técnicos para la declaración de prácticas de certificación, los perfiles de usuarios de los certificados electrónicos para la firma electrónica ofrecidos por el Registro Público de Panamá y la vigencia de los certificados electrónicos calificados;

Que en el primer párrafo del artículo segundo del Reglamento Técnico No. 1 de la Dirección Nacional de Firma Electrónica, aprobado mediante Resolución de Registro Público No. DG-125-2013 del 6 de noviembre de 2013 modificado por el artículo segundo del Reglamento Técnico No. 2 de la Dirección Nacional de Firma Electrónica aprobado mediante Resolución de Registro Público No. DG-087-2019 del 19 de agosto de 2019 establece que los certificados de firma electrónica calificada ofrecidos por el Registro Público de Panamá se dividirán en perfiles según el tipo de usuario y el Registro Público de Panamá ahora cuenta con un nuevo perfil para ser ofrecido al público que es: "Sello electrónico" para uso en dispositivos, aplicaciones y servidores con el propósito de garantizar la integridad y la autenticidad de los documentos a firmar con la posibilidad de automatizar el proceso de firma basado en el artículo 15 de la Ley No. 51 de 2008;

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 en virtud de lo anterior, la Dirección Nacional de Firma Electrónica de la República de Panamá, recomienda se apruebe una Resolución Técnica que sirva para dictaminar los parámetros y estándares mínimos que deben utilizar los Prestadores de servicios de certificación, para la emisión de Certificados electrónicos calificados;

RESUELVE

PRIMERO. Se aprueba el Reglamento Técnico No. 3 de la Dirección Nacional de Firma Electrónica, el cual es del tenor siguiente:

REGLAMENTO TECNICO No. 3
DE LA DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA
DISPOSICIONES GENERALES

Artículo 1. El presente reglamento técnico será de aplicación y obligatorio cumplimiento para los prestadores de servicios de certificación de carácter público incluyendo el Registro Público de Panamá. La reglamentación técnica de los

prestadores de servicios de certificación de carácter privado se hará en instrumento por separado.

Artículo 2. 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 TS 319 132) CAdES (ETSI TS 319 122) y PAdES (ETSI TS 319 142).

3- Especificaciones para el protocolo de sellado de tiempo: RFC 3161 "Internet X.509 Public Key Infraestructure. 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 validez del sellado de tiempo: Hasta cinco (5) minutos después desde que se aplica 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 3039 "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, digito 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 3 sobre comprobación de identidad)
Lenguaje de escritura del NIP	ASN.1 syntax

9- Algoritmos asimétricos, simétricos y requerimientos de seguridad: PKCS#1 v2.1 (RSA), ANSI X9.31, ANSI X9.62, ETSI TS 199 312, ETSI 319 411-1, ETSI EN 319 411-2, ETSI EN 319 401, ETSI EN 319 421, FIPS PUB 46-3, FIPS PUB 140-2, FIPS 140-3, FIPS PUB 180-1, FIPS PUB 180-2, FIPS 180-4.

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); 2- PKCS#12 (Certificado electrónico para perfiles de factura electrónica); y 3- El módulo de seguridad de hardware (HSM) para firma electrónica en la nube y sello electrónico.

Artículo 3. (Comprobación de identidad). La comprobación de las clases de NIP que se refiere el numeral 8 del artículo 2 del presente reglamento técnico seguirá las siguientes reglas:

El prestador de servicios de certificación le pedirá al solicitante de un certificado electrónico calificado la información que requiera vía formulario de pre-registro (físico o electrónico) o vía correo electrónico y adicionalmente le pedirá al solicitante la aceptación de condiciones de uso del certificado electrónico. El solicitante de un certificado electrónico calificado comparecerá físicamente o de manera virtual (únicamente para firma electrónica en la nube) ante el prestador de servicios de certificación y se le capturarán los datos biométricos.

Luego, el prestador de servicios de certificación deberá verificar los datos de identidad al solicitante según el perfil del certificado electrónico solicitado mediante los siguientes pasos:

1. Pasos de verificación de identidad de datos para perfil de **firma electrónica calificada de persona natural**:

a) **Nacionales:**

a.1) Verificación de identidad modalidad presencial:

a.1.1.) Llenado de pre-registro que será validado por el prestador de servicios de certificación y;

a.1.2.) Comparecencia física del solicitante ante el prestador de servicios de certificación y;

a.1.3.) Captura de datos biométricos (foto y huella dactilar) y;

a.1.4) Cotejo de Cédula de identidad personal contra el Sistema de Verificación de Identidad (SVI) del Tribunal Electoral.

a.2) Verificación de identidad remota para obtención de firma electrónica calificada modalidad en la nube:

a.2.1) Llenado de pre-registro que será validado por el prestador de servicios de certificación y;

a.2.2.) Captura de datos biométricos (foto) y;

a.2.3) Cotejo de cédula de identidad personal contra el Sistema de Verificación de Identidad (SVI) del Tribunal Electoral mediante entrevista por videoconferencia programada por el prestador de servicios de certificación y;

a.2.4.) Respuesta satisfactoria a preguntas de seguridad que se le hagan al solicitante y;

a.2.5.) En caso de información o respuestas dudosas durante el pre-registro o la entrevista por videoconferencia el operador de registro deberá pedir al solicitante comparezca físicamente ante el prestador de servicios de certificación para revisar y completar la validación de identidad del solicitante.

b) **Extranjeros**:

b.1) Verificación de identidad modalidad presencial (En todos los casos, incluso firma electrónica en la nube):

b.1.1) Llenado de pre-registro que será validado por el prestador de servicios de certificación y;

a.1.2.) Comparecencia física del solicitante ante el prestador de servicios de certificación y;

b.1.3.) Captura de datos biométricos (foto y huella dactilar) y;

b.1.4) Cotejo de su información contra el Sistema de Verificación de Identidad (SVI) del Tribunal Electoral si tiene Carné de Residente Permanente; o a falta del carné, cotejo de su pasaporte contra bases de datos en línea del Estado de la autoridad competente (Migración) o contra una certificación de estatus migratorio (extranjeros residentes) u certificación de movimiento migratorio (extranjeros no residentes) de esta entidad. La verificación del pasaporte contra certificaciones de Migración sólo se hará de no contar con el modo de verificación en línea.

b.1.5.) Para extranjeros la modalidad de firma electrónica en la nube estará disponible únicamente para extranjeros residentes permanentes. En este caso la captura de datos biométricos sólo incluirá la foto sino está disponible la captura de huella dactilar.

2. Pasos de verificación para perfil de **firma electrónica calificada de profesionales**:

2.1 – Verificación de identidad de la persona natural solicitante igual que el perfil de firma de persona natural y;

2.2. – Cotejo del número de idoneidad o datos de la licencia profesional para ejercer contra bases de datos de autoridades competentes o contra bases de datos establecidas por convenio con el gremio de la profesión o disciplina respectiva 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.

3. Pasos de verificación para perfil de **firma electrónica calificada de representante legal de persona jurídica**:

3.1. – Verificación de identidad de la persona natural solicitante igual que el perfil de firma de persona natural y;

3.2. – Cotejo de datos del representante legal contra certificación de Registro Público donde conste de forma clara y precisa los datos relativos a la constitución y personalidad jurídica, así como el nombre, la extensión y la vigencia de las facultades de representación legal del solicitante. (Numeral 2 del Artículo 26 de la Ley 51 de 2008).

4. Pasos de verificación para perfil de **firma electrónica calificada de colaborador de persona jurídica**:

4.1. – Verificación de identidad de la persona natural solicitante igual que el perfil de firma de persona natural y;

4.2. – Cotejo de datos de constitución y personalidad jurídica de la empresa contra certificación de Registro Público donde conste de forme clara y precisa los datos relativos a la constitución y personalidad jurídica. (Numeral 2 del Artículo 26 de la Ley 51 de 2008) y;

4.3 – Cotejo de datos del administrador autorizado o representante legal de la persona jurídica explícitamente autorizado para firmar a través del pacto social o poder dado por la persona jurídica e inscrito en el Registro Público contra la información que aparezca en el certificado del Registro Público donde establezca su condición de tal ya sea como administrador o como representante legal (nombre, extensión y vigencia) y que además en el certificado del Registro Público se indique donde consultar datos de registro de autorizaciones adicionales y/o limitantes de haberlas, de firmas impuestas al solicitante por cuantía o materia que la persona jurídica le imponga al solicitante ya sea en el poder o en el pacto social. Esta indicación de datos de inscripción de poder o autorización de donde consultar las limitaciones será insertada junto con el NIP en el certificado electrónico de conformidad con el artículo 15 de la Ley 51 de 2008.

5. Pasos de verificación para perfil de **firma electrónica calificada de factura electrónica**:

5.1. - Verificación de identidad de la persona natural solicitante igual que el perfil de firma de persona natural y;

5.2. – Cotejo de RUC, digito verificador, clase de contribuyente y tercero vinculado con el contribuyente (quien debe ser el solicitante de la Firma Electrónica) contra la información que aparezca registrada en el sistema E-TAX de la DGI.

6. Pasos de verificación para perfil de **firma electrónica calificada de sello electrónico** para dispositivos, aplicaciones o servicios automatizados:

6.1. – La Persona Jurídica debe enviar al prestador de servicios de certificación una solicitud firmada con su perfil de firma electrónica calificada de representante legal de persona jurídica o de firma electrónica calificada de colaborador de persona jurídica, válida en la República de Panamá; que indique la persona natural responsable de custodiar el certificado electrónico dentro de la empresa, que será quien retirará el certificado como solicitante 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 incluido los espacios en blanco)

- Nombre del dispositivo, aplicación o servicio automatizado que requiere el certificado electrónico. (No excederse de 64 caracteres incluido los espacios en blanco)

- Nombre y cédula o pasaporte de la persona natural solicitante que retirará el certificado.

-Email de contacto de la empresa.

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

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 2 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.

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.

6.2. – Verificación de identidad de la persona natural responsable que retira el certificado igual que el perfil de firma de persona natural y;

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

6.4. – Realizadas las verificaciones correspondientes, el prestador de servicios de certificación procederá a la firma del CSR asociado al par de claves y la persona jurídica solicitante podrá retirarlo a través de la persona natural identificada como responsable de su custodia, luego de lo cual deberá proceder a la importación del certificado asociado al par de claves criptográficas en el respectivo HSM.

Artículo 4. (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 5. Con respecto a la firma electrónica 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 6. 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. No obstante, la modalidad nube sólo podrá ser utilizada en trámites específicos previamente autorizados para esa modalidad por la entidad estatal que regule *y/o* gestione el trámite.

Artículo 7. El Registro Público de Panamá emitirá certificados de firma electrónica calificada con comprobación de identidad en modalidad presencial para cualquier perfil mencionado en el presente reglamento pero en modalidad en la nube únicamente para el perfil de firma electrónica calificada de persona natural y el perfil de firma electrónica calificada de funcionario público.

Artículo 8. (Transitorio) Se establece un período de pruebas técnicas de seis (6) meses a partir de la promulgación del presente reglamento en el cual el Registro Público de Panamá no ofrecerá la firma electrónica calificada en la nube de forma general, es decir sólo la ofrecerá limitada y discrecionalmente a efectos de poder verificar la buena marcha técnica de los distintos elementos que componen dicha tecnología.

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

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: Se deroga el Reglamento Técnico No. 1 de la Dirección Nacional de Firma Electrónica contenido en la Resolución del Registro Público de Panamá No. DG-125-2013 del 6 de noviembre de 2013 y el Reglamento Técnico No. 2 de la Dirección Nacional de Firma Electrónica contenido en la Resolución del Registro Público de Panamá No. DG-087-2019 del 19 de agosto de 2019. El presente Reglamento Técnico No. 3 reemplaza a ambos.

CUARTO: Esta resolución entrará a regir a partir de su promulgación y deberá ser publicada en la Gaceta Oficial.

FUNDAMENTO DE DERECHO: Ley No. 3 de 6 de enero de 1999, Ley No. 51 de 22 de julio de 2008, la Ley No. 82 de 9 de noviembre de 2012 y Decreto Ejecutivo 684 de 18 de octubre de 2013.

Dado en la ciudad de Panamá a los veintiséis (26) días del mes de enero de dos mil veintitres (2023).

CUMUNÍQUESE Y CÚMPLASE

BAYARDO A. ORTEGA CARRILLO
Director General
BAOC

REGISTRO PÚBLICO DE PANAMÁ
SECRETARIA GENERAL

ESTE DOCUMENTO ES FIEL COPIA DEL ORIGINAL

30/01/2023
FECHA

SECETARÍA GENERAL