F-30
Ver. 00
Mar. 2015

DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

CONTROL DE CAMBIOS DE DOCUMENTOS

Nº 2015-02

Descripción del Documento a Actualizar

Política de Certificación de Certificados de Funcionario Público	RPP-PKI-DPC05	25 de marzo de 2015	1
Documento Actualizado	Código del Documento	Fecha de Actualización	Nueva versión

A continuación se detalla el control de los cambios revisados y aprobados por la **Autoridad de Gestión de Políticas** y el **Comité Ejecutivo de la PKI**:

Ubicación específica del Cambio	Justificación del Cambio	Indicar el texto que desea actualizar	Cambio Propuesto
1. Introducción	Revisión integral del documento	Este documento recoge la Política de Certificación (PC) de los Certificados de Funcionario Público emitidos por la Infraestructura de Clave Pública (en adelante PKI) del Registro Público de Panamá. En esta PC se detalla y completa lo estipulado en la Declaración de Prácticas de Certificación (DPC) de la PKI del Registro Público de Panamá (en adelante, RPP-PKI), conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta Política de Certificación, así como el ámbito de aplicación y las características técnicas de este tipo de certificados. La presente PC se ha estructurado teniendo en cuenta las recomendaciones de la (Request for comments) RFC 3647 "Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework", de IETF. Con el propósito de facilitar la lectura y análisis del documento se incluyen todas las secciones establecidas en dicha RFC apareciendo la frase "No estipulado" en las secciones para las que no se haya previsto nadaLa presente PC se ha estructurado teniendo en cuenta las recomendaciones de la (Request for comments) RCF 3647 "Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework", de IETF. Con el propósito de facilitar la lectura y análisis del documento se incluyen todas las secciones establecidas en dicha RFC apareciendo la frase "No estipulado" en las secciones para las que no se haya previsto nada. Todos los certificados que emite la PKI del Registro Público de Panamá son conformes con la versión 3 del estándar X.509, permitiendo la inclusión de extensiones para certificación de atributosTodos los certificados que emite la PKI del Registro Público de Panamá son conformes con la versión 3 del estándar X.509, permitiendo la inclusión de extensiones para certificación de atributos.	Este documento recoge la Política de Certificación (PC) de los Certificados de Funcionario Público emitidos por la Infraestructura de Clave Pública (en adelante PKI) del Registro Público de Panamá. En esta PC se detalla y completa lo estipulado en la Declaración de Prácticas de Certificación (DPC) de la PKI del Registro Público de Panamá (en adelante, RPP-PKI), conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta Política de Certificación, así como el ámbito de aplicación y las características técnicas de este tipo de certificados. La presente PC se ha estructurado teniendo en cuenta las recomendaciones de la (Request for comments) RFC 3647 "Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework", de IETF. Con el propósito de facilitar la lectura y análisis del documento se incluyen todas las secciones establecidas en dicha RFC apareciendo la frase "No estipulado" en las secciones para las que no se haya previsto nada. Todos los certificados que emite la PKI del Registro Público de Panamá son conformes con la versión 3 del estándar X.509, permitiendo la inclusión de extensiones para certificación de atributos.

1. Introducción	Revisión integral del documento	La RPP-PKI se constituye como prestador de servicios de certificación de firma electrónica en virtud de la Ley Nº 82 de 2012, que otorga al Registro Público de Panamá atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá, modificando la Ley Nº 51 de 2008 y adopta otras disposiciones. Nace con la finalidad de ofrecer los mecanismos y sistemas necesarios para garantizar la seguridad de las comunicaciones electrónicas en las que intervengan la Administración Pública, los profesionales y representantes de personas jurídicas que se relacionan con la Administración y los ciudadanos en generaldel Registro Público de Panamá (en adelante, RPP-PKI) se constituye como prestador de servicios de certificación de firma electrónica en virtud de la Ley Nº 82 de 2012, que otorga al Registro Público de Panamá atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá, modificando la Ley Nº 51 de 2008 y adopta otras disposiciones. Nace con la finalidad de ofrecer los mecanismos y sistemas necesarios para garantizar la seguridad de las comunicaciones electrónicas en las que intervengan la Administración Pública, los profesionales y representantes de personas jurídicas que se relacionan con la Administración y los ciudadanos en general. El presente documento es la norma básica del servicio de certificación, en la que se establece su naturaleza, estructura y organización, así como los criterios y procedimientos que el Servicio se compromete a seguir en el ejercicio de su actividad, incluyendo desde la solicitud de los certificados y generación de las claves, hasta la posterior emisión, distribución, uso, revocación/suspensión y renovación de los mismosLa Declaración de Prácticas de Certificación (en adelante DPC), es la norma básica del Servicio de Certificación, en la que se establecen su naturaleza, estructura y organización, así como los criterios y procedimientos que el Servicio se compromete a seguir en el ejercicio de su actividad, incluyendo desde la solicitud de los certificados y generación de las claves, hasta la posterior emisión, distribución, uso, revocación/suspensión y renovación de los mismos.	La RPP-PKI se constituye como prestador de servicios de certificación de firma electrónica en virtud de la Ley Nº 82 de 2012, que otorga al Registro Público de Panamá atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá, modificando la Ley Nº 51 de 2008 y adopta otras disposiciones. Nace con la finalidad de ofrecer los mecanismos y sistemas necesarios para garantizar la seguridad de las comunicaciones electrónicas en las que intervengan la Administración Pública, los profesionales y representantes de personas jurídicas que se relacionan con la Administración y los ciudadanos en general

1. Introducción	Revisión integral del documento	La Declaración de Prácticas de Certificación (en adelante DPC), emitida de conformidad con la Ley Nº 82 de 2012 y la Ley Nº 51 de 2008, define y fundamenta el marco normativo general, conforme al cual se desarrollará la actividad de Prestador del Servicio de Certificación del Registro Público de Panamá, en relación con los procesos de solicitud, emisión y gestión del ciclo de vida de los certificados electrónicos, incluyendo los procedimientos de verificación de la vigencia, revocación y renovación de certificadosLa DPC, emitida de conformidad con la Ley Nº 82 de 2012 y la Ley Nº 51 de 2008 define y fundamenta el marco normativo general, conforme al cual se desarrollará la actividad de Prestador del Servicio de Certificación del Registro Público de Panamá, en relación con los procesos de solicitud, emisión y gestión del ciclo de vida de los certificados electrónicos, incluyendo los procedimientos de verificación de la vigencia, revocación y renovación de certificados. Las Políticas de Certificación (en adelante PC) aplicables a cada clase de certificado complementan lo dispuesto con carácter general en la presente DPC. En caso de conflicto o contradicción entre lo dispuesto en la Declaración de Prácticas de Certificación y las citadas Políticas de Certificación, prevalecerá lo estipulado en estas últimasLas Políticas de Certificación (en adelante PC) aplicables a cada clase de certificado complementan lo dispuesto con carácter general en la citada DPC. En caso de conflicto o contradicción entre lo dispuesto en la Declaración de Prácticas de Certificación y las citadas Políticas, prevalecerá lo estipulado en estas últimas. Las PC también definen el ámbito de potenciales titulares de los certificados, así como los usos previstos de los mismos y el conjunto de derechos y obligaciones que asumen el emisor, el titular de los certificados y los terceros que confían en los certificados emitidos por la RPP-PKI. Las PC también definen el ámbito de potenciales titulares de los certificados, así como los usos previstos de los mismos y el conjunto de derechos y obligaciones que asume el emisor, el titular de los certificados y los terceros que confían en los certificados emitidos por la RPP-PKI. La actividad de la RPP-PKI se desarrollará con plena sujeción a las prescripciones de la Ley Nº 82 de 2012 y la Ley Nº 51 de 2008La actividad de la RPP-PKI se desarrollará con plena sujeción a las prescripciones de la Ley Nº 82 de 2012 y la Ley Nº 51 de 2008.	La Declaración de Prácticas de Certificación (en adelante DPC), emitida de conformidad con la Ley Nº 82 de 2012 y la Ley Nº 51 de 2008, define y fundamenta el marco normativo general, conforme al cual se desarrollará la actividad de Prestador del Servicio de Certificación del Registro Público de Panamá, en relación con los procesos de solicitud, emisión y gestión del ciclo de vida de los certificados electrónicos, incluyendo los procedimientos de verificación de la vigencia, revocación y renovación de certificados. Las Políticas de Certificación (en adelante PC) aplicables a cada clase de certificado complementan lo dispuesto con carácter general en la presente DPC. En caso de conflicto o contradicción entre lo dispuesto en la Declaración de Prácticas de Certificación y las citadas Políticas de Certificación, prevalecerá lo estipulado en estas últimas. Las PC también definen el ámbito de potenciales titulares de los certificados, así como los usos previstos de los mismos y el conjunto de derechos y obligaciones que asume el emisor, el titular de los certificados y los terceros que confían en los certificados emitidos por la RPP-PKI. La actividad de la RPP-PKI se desarrollará con plena sujeción a las prescripciones de la Ley Nº 82 de 2012 y la Ley Nº 51 de 2008.
1. Introducción	Revisión integral del documento	Esta PC asume que el lector conoce los conceptos de PKI, certificado y firma electrónica; en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documentoEste documento asume que el lector conoce los conceptos de PKI, certificado y firma electrónica; en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento	Esta PC asume que el lector conoce los conceptos de PKI, certificado y firma electrónica; en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documentoEste

1.3.1 Prestador de Serivicios de Certificación	Revisión integral del documento	Según la definición dispuesta por la Ley Nº 51 de 2008 modificada por la Ley Nº 82 de 2012, un prestador de servicios de certificación es la persona jurídica que emite firmas electrónicas y los certificados electrónicos para identificar el propietario y el estatus de dichas firmas y provee otros servicios relacionados con el uso de las firmas electrónicas. La Dirección Nacional de Firma Electrónica (en adelante DNFE) es un organismo dependiente del Registro Público de Panamá, que actuará como prestador de servicios de certificación de la RPP-PKI.	Según la definición dispuesta por la Ley Nº 51 de 2008 modificada por la Ley Nº 82 de 2012, un prestador de servicios de certificación es la persona jurídica que emite firmas electrónicas y los certificados electrónicos para identificar el propietario y el estatus de dichas firmas y provee otros servicios relacionados con el uso de las firmas electrónicas. La Dirección Nacional de Firma Electrónica (en adelante DNFE) es un organismo dependiente del Registro Público de Panamá, que actuará como prestador de servicios de certificación de la RPP-PKI. La información legal y datos identificativos del Prestador de Servicios de Certificación estarán siempre disponibles en http://www.pki.gob.pa/normativa/index.htm. La DNFE desarrolla su actividad de conformidad con la legislación vigente en la materia, señalada en la Ley Nº 82 de 2012 y la Ley Nº 51 de 2008.
1.3.3.1 Autoridad Certificadora de Panamá	Revisión integral del documento	Subordinados al Certificado Raíz, se encuentran los certificados de jerarquía o de clave secundaria, que serán uno para los certificados de gobierno y otro para los certificados de clase 2.	Subordinados al Certificado Raíz, se encuentran los certificados de jerarquía o subordinados, que serán uno para los certificados de gobierno y otro para los certificados de clase 2.
1.3.3.2 Autoridad de Certificación de Gobierno	Revisión integral del documento	Bajo el Certificado Raíz de Panamá, se encuentran los certificados de de CA de Gobierno y de CA Panamá Clase 2, bajo cuyas respectivas jerarquías se emiten a su vez todos los certificados que la DNFE emite a entidades finales. Los Certificados de Funcionario Público son emitidos por la CA de Gobierno . Sus datos más relevantes son los siguientes:	Bajo el Certificado Raíz de Panamá, se encuentran los certificados de de CA de Gobierno y de CA Panamá Clase 2, bajo cuyas respectivas jerarquías se emiten a su vez todos los certificados que la DNFE emite a entidades finales. Los Certificados de Funcionario Público son emitidos por la CA de Gobierno, cuyos datos más relevantes son los siguientes:
1.3.4 Autoridad de Registro (RA)	Revisión integral del documento	Las Autoridades de Registro (RA) llevarán a cabo la identificación de los solicitantes de certificados conforme a las normas de esta PC y el acuerdo suscrito con la CA.	Las Autoridades de Registro (RA) llevarán a cabo la identificación de los solicitantes de certificados conforme a las normas de la DPC, la presente PC y el acuerdo suscrito con la CA
1.3.7 Solicitantes y Titulares de Certificados	Revisión integral del documento	Los solicitantes y titulares de certificados se encuentran definidos en la DPC de la RPP-PKI. Dentro del ámbito de la presente PC, los solicitantes y titulares de certificados de funcionario público son las personas naturales en su condición de funcionario de la administración pública	Los solicitantes y titulares de certificados se encuentran definidos en la DPC de la RPP-PKI. Dentro del ámbito de la presente PC, los solicitantes y titulares de certificados de funcionario público son las personas naturales en su condición de funcionario de la administración pública, que laboran en instituciones que tengan convenios de colaboración suscritos con la RPP-PKI.
1.3.8 Terceros que confían en los certificados emitidos por RPP-PKI	Revisión integral del documento	Los Terceros que confían son las personas o entidades diferentes del titular que deciden aceptar y confiar en los certificados emitidos por la CA del Gobierno de Panamá, con el fin de identificar un titular en su condición de funcionario de la administración pública	Los Terceros que confían son las personas o entidades diferentes del titular que deciden aceptar y confiar en los certificados emitidos por la CA del Gobierno de Panamá, con el fin de identificar un titular en su condición de funcionario de la administración pública. Un tercero que confía puede o no ser también un titular de un certificado.
1.5.1 Entidad Responsable	Revisión integral del documento	El Registro Público de Panamá, a través del Comité Ejecutivo de la PKI, establecerá los términos y redacción de la DPC de RPP-PKI.	El Registro Público de Panamá, a través del Comité Ejecutivo de la PKI, establecerá los términos y redacción de la DPC de RPP-PKI. Las actualizaciones y revisiones a la DPC de RPP-PKI se realizaran periódicamente para asegurar que se mantienen vigentes. La Autoridad de Aprobación de Políticas en conjunto con el Comité Ejecutivo establecerán la frecuencia de evaluación, no obstante, en ningún caso este plazo será mayor de un año.
1.6.1. Definiciones	Revisión integral del documento	En el ámbito de la presente DPC los términos empleados son los siguientes	En el ámbito de la presente PC los términos empleados son los siguientes
1.6.1. Definiciones	Revisión integral del documento	Autenticación: proceso de verificar la identidad de solicitante o titular de un certificado del Registro Público de Panamá.	Autenticación: proceso de verificar la identidad de solicitante o titular de un certificado de la República de Panamá.
1.6.1. Definiciones	Revisión integral del documento	Identificación: proceso de establecer la identidad de un solicitante o titular de un certificado del Registro Público de Panamá	Identificación: proceso de establecer la identidad de un solicitante o titular de un certificado de la República de Panamá.
1.6.1. Definiciones	Revisión integral del documento	Solicitante: persona natural o jurídica que solicita un certificado para sí mismo o para un componente informático.	Solicitante: persona natural o jurídica que solicita un certificado electrónico para sí mismo o para un componente informático.
1.6.1. Definiciones	Revisión integral del documento	Titular: individuo o componente informático para el que se expide un certificado y es aceptado por éste o por su responsable en el caso de los certificados de componente.	Titular: individuo o componente informático para el que se expide un certificado electrónico y es aceptado por éste o por su responsable en el caso de los certificados de componente.
3.1.6 Reconocimiento, autenticación y papel de las marcas registradas	Revisión integral del documento	No Estipulado	Como establezca la DPC de la RPP-PKI.

3.2.2 Autenticación de la identidad de una persona jurídica	Revisión integral del documento	No Estipulado	Este punto no es aplicable a esta PC. El procedimiento de autenticación de la identidad de una persona jurídica está documentado en la PC correspondiente.
3.2.3 Autenticación de la identidad de una persona jurídica	Revisión integral del documento	Autenticación de la identidad de una persona jurídica	Autenticación de la identidad de un Funcionario Público
3.2.4 Información no verificada sobre el solicitante	Revisión integral del documento	No Estipulado	Toda la información recabada durante la expedición anterior ha de ser verificada.
3.2.5 Comprobación de las facultades de representación	Revisión integral del documento	No Estipulado	Este punto no es aplicable ya que para poder autenticar la identidad de un funcionario público este debe comparecer personalmente al puesto de inscripción con su cédula de identidad personal.
4.1.1 Quién puede efectuar una solicitud	Revisión integral del documento	La solicitud de certificado de funcionario público será efectuada por la(s) persona(s) designada por la institución para realizar este trámite con la DNFE, posterior Convenio firmado con la RPP-PKI para las condiciones de uso de los certificados de persona natural que vaya a ser titular del mismo.	La solicitud de certificado de funcionario público será efectuada por la(s) persona(s) designada por la institución para realizar este trámite con la DNFE, posterior Convenio firmado con la RPP-PKI para las condiciones de uso de los certificados de funcionario público.
4.1.2 Registro de las solicitudes de certificados y responsabilidades de los solicitantes	Revisión integral del documento	La persona Natural	El funcionario público
4.3.2 Notificación al solicitante de la emisión por la CA del Certificaco	Revisión integral del documento	No Estipulado	La emisión del certificado electrónico a Funcionarios Públicos es presencial por lo tanto la notificación es inmediata. En el momento de la entrega de la cédula de identidad personal y el documento de aceptación de condiciones se le indica al funcionario público su responsabilidad en el uso de su certificado electrónico. De igual forma se le indicará como obtener la presente PC.
4.4.2 Publicación del Certificado por la CA	Revisión integral del documento	En cada PC se detallarán los repositorios de Publicación del certificado.	Este punto no es aplicable ya que los certificados electrónicos de funcionario público no se publicarán en ningún repositorio.
4.6.1 Circunstancias para la renovación de certificados sin cambio de claves	Revisión integral del documento	Todas las renovaciones de certificados realizadas en el ámbito de esta DPC se realizarán con cambio de claves.	Todas las renovaciones de certificados realizadas en el ámbito de esta PC se realizarán con cambio de claves. En consecuencia, no se recogen el resto de los puntos referente a renovación de certificados sin cambio de claves (puntos 4.6.2, 4.6.3, 4.6.4, 4.6.5, 4.6.6, 4.6.7) que establece la RFC 3647, lo que implica, a efectos de esta DPC, su no estipulación.
4.7.4 Notificación de la emisión de un nuevo certificado al titular	Revisión integral del documento	No Estipulado	La notificación se hace con la entrega del nuevo dispositivo criptográfico que contiene su certificado electrónico o mediante la comunicación de la finalización satisfactoria del proceso de renovación del certificado electrónico. Cada vez que se renueva un certificado electrónico el funcionario público deberá firmar un nuevo documento con fecha actualizada de licencia de uso y aceptación de condiciones.
4.7.6 Publicación del certificado con las nuevas claves por la CA	Revisión integral del documento	No Estipulado	Este punto no es aplicable ya que la RPP-PKI, una vez emitido el certificado, no los publica en repositorios.
4.8.2 Quién puede solicitar la modificación de los certificados	Revisión integral del documento	No Estipulado	Este punto no es aplicable ya que los casos de modificaciones de los certificados serán tratadas como una renovación de certificados, por lo que le aplican los apartados anteriores al respecto. En consecuencia, no se recogen el resto de los puntos referente a modificación de certificados (puntos 4.8.3, 4.8.4, 4.8.5, 4.8.6, 4.8.7) que establece la RFC 3647, lo que implica, a efectos de esta DPC, su no estipulación.
4.9.14 Quién puede solicitar la suspensión	Revisión integral del documento	La solicitud puede presentarla el titular del certificado.	La solicitud puede presentarla el titular del certificado o la organización a la cual pertenece mediante resolución administrativa, nota del representante legal de la entidad o de la Oficina Institucional de Recursos Humanos de la entidad. (Art. 29 del Decreto Ejecutivo 684 de 2013)
4.12.1 Prácticas y políticas de custodia y recuperación de claves	Revisión integral del documento	No Estipulado	Este punto no es aplicable ya que los datos de creación de certificado electrónico de funcionario público (clave privada) se generan dentro de una tarjeta criptográfica y no pueden ser exportadas en ningún caso. La responsabilidad de la custodia de la tarjeta criptográfica donde está contenido el certificado electrónico recae enteramente sobre el titular.

4.12.2 Prácticas y políticas de protección y recuperación de la clave de sesión	Revisión integral del documento	No Estipulado	Este punto no aplica ya que la recuperación de la clave de sesión es responsabilidad del suscriptor del certificado electrónico; el método de recuperación empleado es a través de un número PUK que se le entrega al suscriptor al momento de generarse su tarjeta criptográfica.
5.4.6 Notificación al sujeto causa del evento	Revisión integral del documento	No Estipulado	Las incidencias son puestas en conocimiento de la Dirección con independencia de que se activen las oportunas acciones correctivas a través del sistema de incidencias establecido para conducir a su solución de la forma más rápida posible según lo describe el Procedimiento de Gestión de Incidencias establecido.
6.2.9 Método de desactivación de la Clave Privada	Revisión integral del documento	No Estipulado	La desactivación de la clave privada de funcionario público se realizará mediante solicitud del titular del certificado electrónico o por la Oficina Institucional de Recursos Humanos. Esta desactivación se tratará como una revocación del certificado electrónico por lo que se seguirá el procedimiento establecido para tal fin.
6.2.10 Método de destrucción de la clave privada	Revisión integral del documento	No Estipulado	La destrucción de la clave privada debe ser precedida por una revocación del certificado electrónico asociado a la clave, si esta estuviese todavía vigente. La DNFE dispondrá de un método de destrucción de forma que impida su robo o uso no autorizado.
6.8 Sellado de Tiempo	Revisión integral del documento	No Estipulado	El formato de los Sellos de Tiempo emitidos por el Servicio de Sellado de Tiempo será según lo indicado en la RFC 3161 – "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)" y la normativa ETSI 102 023 – "Requisitos para las Políticas de las Autoridades de Sellado de Tiempo"
7.1.9 Uso de la extensión "PolicyConstraints	Revisión integral del documento	No Estipulado	Como establezca la DPC de la RPP-PKI.
9.7 Exención de responsabilidades	Revisión integral del documento	Como establezca la DPC de la RPP-PKI.	Adicional a lo establecido en la DPC de la RPP-PKI, los certificados regulados por la presente Política de Certificación sólo deben utilizarse con el propósito de autenticación o firma de personas naturales con cargos en la administración pública en el ejercicio de sus funciones por lo que el Registro Público de Panamá no se hace responsable por el uso indebido por parte del suscriptor del certificado electrónico fuera de este ámbito.
9.17 Otras estipulaciones	Revisión integral del documento	No Estipulado	No se contemplan otras estipulaciones.