F-30
Ver. 00
Mar. 2015

DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

CONTROL DE CAMBIOS DE DOCUMENTOS

Nº 2015-03

Descripción del Documento a Actualizar

Política de Certificación de Certificados de Persona Natural	RPP-PKI-DPC-04	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	Eliminar la introducción	La PKI del 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 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 presente 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 de la República 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.

1. Introducción	Revisión integral del documento	Eliminar la introducción	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, 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. La actividad de RPP-PKI se desarrollará con plena sujeción a las prescripciones de la Ley Nº 82 de 2012 y la Ley Nº 51 de 2008. Esta DPC 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.
1.3.4.1 Puesto de Inscripción	Revisión integral del documento	* Personalización gráfica del dispositivo criptográfico en el que se entregarán los certificados.	Personalización gráfica del dispositivo criptográfico en el que se generara el certificado electrónico que será entregado al solicitante
1.3.4.2 Puesto de Emisión	Revisión integral del documento	* Solicitud de los certificados a la CA correspondiente en función del certificado solicitado así como su posterior entrega al titular.	* Solicitud de los certificados a la CA correspondiente en función del perfil del certificado electrónico solicitado así como su posterior entrega al titular.
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	Toda la información recabada durante la expedición anterior ha de ser verificada.
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 una persona natural este debe comparecer personalmente al puesto de inscripción con su cédula de identidad personal o pasaporte.
4.3.2 Notificación al solicitante de la emisión por la CA del Certificaco	Revisión integral del documento	El envío de la notificación al solicitante se realizará por medio del correo electrónico provisto por éste durante la inscripción de sus datos, previa a la emisión del certificado.	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. El envío de la notificación al solicitante se realizará por medio del correo electrónico provisto por éste durante la inscripción de sus datos, previa a la emisión del certificado.
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 del certificado electrónico a persona natural serán tratados 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.
4.12.1 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 persona natural (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.
6.2.9 Método de desactivación de la Clave Privada	Revisión integral del documento	No Estipulado	La desactivación de la clave privada de persona natural se realizará mediante solicitud del titular del certificado electrónico. 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.
7.1.9 Uso de la extensión "PolicyConstraints	Revisión integral del documento	No Estipulado	Como establezca la DPC de la RPP-PKI.
9.17 Otras estipulaciones	Revisión integral del documento	No Estipulado	No se contemplan otras estipulaciones.