F-30
Ver. 00
Mar. 2015

DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

CONTROL DE CAMBIOS DE DOCUMENTOS

Nº 2015-01

Descripción del Documento a Actualizar

Declaración de Prácticas de Certificación de la PKI	RPP-PKI-DPC02	25 de marzo de 2015	0.1
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
1.1 Visión General	Revisión integral del documento	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 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.	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.
1.3.4.1 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.
1.5.1 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	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	Este punto no es aplicable dado que la RPP-PKI no asume compromiso alguno sobre el uso de marcas comerciales en la emisión de los certificados electrónicos expedidos bajo la presente política de certificación. La RPP-PKI se reserva el derecho de rechazar una solicitud de certificado electrónico debido a conflictos de nombres de marcas comerciales.
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 la RPP-PKI, una vez emitido el certificado, no los publica en repositorios.

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 DPC 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.
4.8.2 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.
4.12.1 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 (clave privada) se generan dentro de un dispositivo criptográfico y no pueden ser exportadas en ningún caso. La custodia del dispositivo criptográfico 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 dado 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 dispositivo criptográfico
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.
6.2.10 Método de destrucción de la clave privada	Revisión integral del documento	No Estipulado	En el caso de los certificados de personas como se establezca en la PC correspondiente.
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"
7.1.7 Uso de la extensión "PolicyConstraints	Revisión integral del documento	No Estipulado	La extensión Policy Constrains del certificado raíz de la AC no es utilizado.
9.1.5 Política de reembolso	Revisión integral del documento	En el caso de que alguna Política de Certificación especifique alguna tarifa aplicable a la prestación de servicios de certificación o revocación por parte de RPP-PKI para el tipo de certificados que defina, será obligado determinar la política de reembolso correspondiente.	En el caso de que alguna Política de Certificación especifique alguna tarifa aplicable a la prestación de servicios de certificación o revocación por parte de RPP-PKI para el tipo de certificados que defina, será obligado determinar la política de reembolso correspondiente. Si al momento del cese de actividades por parte del prestador de servicios de certificación, el certificado electrónico calificado de un firmante tiene una vigencia pendiente de uso superior a seis meses, el prestador de servicios de certificación deberá reembolsarle el importe de la tarifa proporcional a la vigencia no utilizada, a menos de que el prestador que cese en sus actividades haya transferido los certificados a otro prestador de servicios de certificación.

9.2 Responsabilidades económicas	Revisión integral del documento	RPP-PKI dispone de la solvencia financiera necesaria para hacer frente a las responsabilidades que la legislación vigente le obliga a asumir. Dichas responsabilidades se encuentran cubiertas mediante póliza de responsabilidad civil contractual y extracontractual admitida por la Ley Nº 82, de 9 de noviembre de 2012, que otorga al Registro Público de Panamá atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá, modifica la Ley Nº 51 de 2008 y adopta otras disposiciones, por el importe de un millón de balboas (B/. 1,000,000.00). Las Políticas de Certificación aplicables a cada tipo de certificado establecerán la cuantía máxima hasta la que se extenderá la responsabilidad por daños y perjuicios del RPP-PKI frente a suscriptores y terceros de buena fe.	RPP-PKI dispone de la solvencia financiera necesaria para hacer frente a las responsabilidades que la legislación vigente le obliga a asumir. Dichas responsabilidades se encuentran cubiertas mediante póliza de responsabilidad civil contractual y extracontractual admitida por la Ley Nº 82, de 9 de noviembre de 2012, que otorga al Registro Público de Panamá atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá, modifica la Ley Nº 51 de 2008 y adopta otras disposiciones, por el importe de un millón de balboas (B/. 1,000,000.00). Seguro que cubre todos los perjuicios contractuales y extracontractuales de los firmantes y terceros de buena fe, exenta de culpa derivados de errores y omisiones, o de actos de mala fe de los administradores, representantes legales o empleados del prestador de servicios de certificación en el desarrollo de las actividades para las cuales solicita registro. Para tal fin se cubrirán los anteriores riesgos con una póliza de seguros, cuyo valor total de suma asegurada corresponda hasta la suma de un millón de balboas (B/.1 000 000.00).” Las Políticas de Certificación aplicables a cada tipo de certificado establecerán la cuantía máxima hasta la que se extenderá la responsabilidad por daños y perjuicios del RPP-PKI frente a suscriptores y terceros de buena fe.
9.3 Confidencialidad de la Información	Revisión integral del documento	Se establece el siguiente régimen de confidencialidad de los datos relativos a RPP-PKI:	Se establece el siguiente régimen de confidencialidad de los datos relativos a RPP-PKI: Adicionalmente, toda la información que conozca la DNFE como prestador de servicios de certificación relativa a los datos personales de sus usuarios es mantenida es estricta confidencialidad pues la DNFE está obligada por los arts. 23 y 24 de Ley 51 de 2008 modificada por la Ley 82 de 2012 a mantenerla confidencial. Así mismo todos sus funcionarios, proveedores, y contratistas deben mantener estricta confidencialidad de toda la información que adquieran o manejen puesto que la Ley 51 de 2008 modificada por la Ley 82 de 2012 y la Resolución Técnica 027-2013 declara de carácter confidencial y de acceso restringido por razón de seguridad nacional toda la información que la DNFE considere necesaria relativa a las actividades que realizamos como prestador de servicios de certificación.
9.17 Otras estipulaciones	Revisión integral del documento	No Estipulado	No se contemplan otras estipulaciones.