F-30
Ver. 01
Sep. 2023

REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

CONTROL DE CAMBIOS DE DOCUMENTOS Nº 2023-21

A. Descripción del documento a actualizar:				
P-11 Código	**DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI** Nombre	**0.3** Versión anterior	**0.4** Nueva versión	**22 de septiembre de 2023** Fecha de actualización

Las actualizaciones realizadas a los documentos de la Dirección Nacional de Firma Electrónica son esenciales para mantener su sistema de gestión relevante, eficaz y en cumplimiento con los requisitos legales y reglamentarios; a continuación, se detalla el control de los cambios revisados y aprobados según los procedimientos establecidos:

B. Cambios realizados (modificación):		
Ubicación (Apartado o página)	**Texto anterior**	**Cambio realizado**
1.2 versión **Fecha de actualización**	**0.3** 27/09/2021 - Acta de subcomité Ejecutivo No. AR-2021-04	**0.4** 22/09/2023 Control de Cambios de documento No. 2023-21
EN TODO EL DOCUMENTO (PUBLICACION DE LA DPC)	**http://pki.gob.pa/normativa/index.html**	https://www.firmaelectronica.gob.pa/politicas-certificacion.html
1.5.3 Datos de contacto	**Dirección Nacional de Firma Electrónica** Avenida 12 de octubre, Plaza La Hispanidad, Local A-7, Ciudad de Panamá	**Dirección Nacional de Firma Electrónica** Avenida Samuel Lewis, Local F6, Campo Alegre, Bella Vista, Panamá (Frente a la Fiscalía General de Cuentas).

4.1.1**Quién puede efectuar una solicitud**	En cada Política de Certificación se concreta quién puede solicitar un certificado y la información que se debe suministrar en la solicitud. Asimismo, la PC establece los pasos que deben seguirse para llevar a cabo este proceso	Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.
4.2.1 Realización de las funciones de identificación y autenticación	El proceso de identificación individual se define por la Política de Certificación aplicable a cada tipo de certificado.	Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.
4.2.2 Aprobación o denegación de las solicitudes de certificados	La emisión del certificado tendrá lugar una vez que la RPP-PKI haya llevado a cabo las verificaciones necesarias para validar la solicitud de certificación. El procedimiento por el que se determina la naturaleza y la forma de realizar dichas comprobaciones se establece en la Política de Certificación correspondiente.	Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.
4.3.2 **Notificación al solicitante de la emisión por la CA del certificado**	Cada PC establecerá el mecanismo de notificación mediante el que se informará al solicitante de la emisión de su certificado.	Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.
4.7.1 Circunstancias para una renovación con cambio de claves de un certificado	El proceso de renovación de certificados dependerá de la Política de Certificación que aplique a cada tipo de certificado.	Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.

4.7.2 Quién puede solicitar la renovación de los certificados	En cada Política de Certificación se establecerá quien puede solicitar la renovación del certificado.	Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas. En el caso de los certificados de la CA y las CA´s subordinadas, la notificación sobre la renovación de estos certificados se realiza con 18 meses de anticipación a la fecha de caducidad; el Departamento de Operaciones Técnicas, notifica al Comité Ejecutivo, sobre la expiración de los certificados de la CA y las CA subordinadas. El Comité Ejecutivo determina los requerimientos previos a la renovación, la notificación que se deba realizar a los usuarios suscriptores de los certificados electrónicos y terceros interesados, se realizará con doce (12) meses de anticipación a la fecha de caducidad del certificado de la CA y las CA´s subordinadas.
4.7.4 Notificación de la emisión de un nuevo certificado al titular	En cada PC se establecerá la forma en que el solicitante será informado de que ha sido emitido el correspondiente certificado a su nombre.	Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.
4.7.5 Forma de aceptación del certificado con las claves cambiadas	En cada PC se establecerá la forma de aceptación.	Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.

4.7.6 Publicación del certificado con las nuevas claves por la CA	En cada PC se establecerá, si procede, el procedimiento de la publicación del certificado.	Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.
4.9.2 Quién puede solicitar la revocación	….. Las distintas Políticas de Certificación podrán definir otros procedimientos de identificación que sean más rigurosos.	…. Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.
4.9.4 Procedimiento de solicitud de revocación	El procedimiento para la solicitud de la revocación de cada tipo de certificado se definirá en la Política de Certificación correspondiente.	Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.
4.9.5 Plazo en el que la CA debe resolver la solicitud de revocación	Cada PC establecerá el tiempo máximo para la resolución de una solicitud de revocación, si bien se establece como norma general que se haga en menos de 24 horas.	Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.
5. Controles de seguridad física, instalaciones, gestión y operacionales	A fin de asegurar la confiabilidad y seguridad de sus operaciones como prestador de servicios de certificación, la DNFE ha dispuesto e implantado controles de seguridad física y lógica en todas sus instalaciones, al igual que procedimientos de auditoría, que pueden ser internos o externas tanto interna como independiente para el seguimiento y verificación del cumplimiento de las políticas, directivas y procedimientos en materia de seguridad.	A fin de asegurar la confiabilidad y seguridad de sus operaciones como prestador de servicios de certificación, la DNFE ha dispuesto e implantado controles de seguridad física donde se llevan a cabo las actividades críticas o sensibles, con barreras de seguridad y controles apropiados, con mecanismos de control de seguridad para reducir el riesgo de accesos no autorizados o de daños a los recursos informáticos.

5.1.1 **Ubicación física y construcción**	La infraestructura de la RPP-PKI se encuentra ubicada en varios edificios que disponen de medidas de seguridad de control de acceso, de forma que sólo se permita la entrada en los mismos a personas debidamente autorizadas.	El edificio donde se encuentra ubicada la infraestructura de la RPP-PKI, dispone de medidas de seguridad con control de acceso físico, de manera que el desarrollo de sus actividades se realice con las suficientes garantías de confidencialidad y seguridad.
9.13 Reclamaciones	Todas reclamaciones entre usuarios y la PKI del REGISTRO PUBLICO DE PANAMA deberán ser comunicadas por la parte en disputa a la Autoridad de Aprobación de Políticas (DNFE), con el fin de intentar resolverlo entre las mismas partes.	Todas reclamaciones entre usuarios y la PKI del REGISTRO PUBLICO DE PANAMA deberán ser comunicadas a la DNFE con el fin de intentar resolverlo entre las mismas partes. El usuario podrá remitir sus inquietudes o quejas sobre el servicio Al correo electrónico: servicios@firmalectronica.gob.pa las cuales serán resueltas de en un término máximo de 30 días.

C. Adición:

1.3.3.2 tipos de certificados emitidos:

Servidor SSL

Firma de Código

Autenticación de Firma Electrónica Calificada en la Nube

Firma de Firma Electrónica Calificada en la Nube

4.1.2 Registro de las solicitudes de certificados y responsabilidades de los solicitantes

Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.

4.9.3 Plazo para la tramitación de las solicitudes de certificados

Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.

4.3.1 Actuaciones de la CA durante la emisión del certificado

Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.

…..

Todos los certificados iniciarán su vigencia en el momento de su emisión y será de dos años, contados a partir de la fecha y hora de su emisión y concluye cuando haya pasado el tiempo de vigencia que se encuentra en el propio certificado electrónico.

4.4.1 Mecanismo de aceptación del certificado

Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.

4.7.3 Tramitación de las peticiones de renovación de certificados con cambio de claves

Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.

4.8.1 Circunstancias para la modificación de un certificado

Cada Política de Certificación determinará este aspecto para los certificados electrónicos expedido bajo dichas políticas.

5.2.1 Roles responsables del control y gestión de la RPP-PKI

Las personas que desempeñan los roles de confianza están convenientemente formadas y tienen los conocimientos necesarios para la ejecución de los trabajos vinculados con cada rol; adicionalmente, cuando sea necesario, la RPP-PKI proporciona la formación y/o sensibilización necesaria para el personal implicado en la gestión de sus sistemas de confianza.

5.2.3 Roles que requieren segregación de funciones

Como medida de seguridad se han designado funcionarios a los diferentes roles, garantizando la debida segregación de funciones, independencia e imparcialidad en sus actuaciones.

5.3.6 Sanciones por actuaciones no autorizadas

Las sanciones por acciones no autorizadas, extralimitación de funciones, uso de los sistemas no autorizados, no guardar rigurosa reserva de la información, coacción en beneficio propio o a terceros, se encuentran establecidas en el Reglamento

Interno del RPP, así como la aplicación de las medidas disciplinarias al servidor público que incurra en algunas de las faltas, que en algunos casos, puede dar lugar a la destitución.

5.5.3 Protección del archivo

Los registros de la Autoridad de Certificación (CA) se encuentran protegidos contra pérdida, destrucción no autorizada y falsificación, los procedimientos que ha establecido la DNFE para proteger los registros de la CA son los siguientes:

- **Controles de accesos:** se limita el acceso a los registros y sistemas de la CA a personal autorizado, a través de sistemas de autenticación, como autenticación de dos factores en los aplicativos de la RA donde se generan y almacenan registros de los suscriptores y políticas de accesos lógicos.
- **Cifrado:** Los registros y bases de datos de la CA se encuentran cifrados para proteger la confidencialidad de la información almacenada, de manera que si alguien obtiene acceso físico o lógico a los sistemas, no pueda leer la información sin clave de cifrado correspondiente.
- **Copias de respaldo:** la DNFE mantiene implementado procedimientos de copias de respaldo de los registros de la CA, que se encuentran almacenadas en una ubicación segura con medidas de seguridad y controles de accesos únicamente para las personas autorizadas, de manera que se garantice, la restauración de los registros o datos, en caso de pérdida o daño.
- **Protección física:** Los servidores y sistemas que albergan los registros de la CA se encuentran ubicados en instalaciones seguras con medidas de seguridad física, como controles de accesos, sistemas de alarma y vigilancia.
- **Monitorización:** La DNFE ha implementado sistemas de monitorización y detección de intrusos para detectar actividad anómala o intentos de accesos no autorizados a los registros de la CA.

9.3 Confidencialidad de la información

La RPP-PKI, se compromete a proteger todos los datos a los que tenga acceso como consecuencia de su actividad como entidad de certificación, no obstante, la RPP-PKI se reserva el derecho a revelar a sus funcionarios, los datos confidenciales necesarios para realizar sus funciones. En este caso, los funcionarios son informados y sensibilizados sobres sus obligaciones con la confidencialidad de la información de la RPP-PKI, que adicionalmente, contempla la suscripción de un acuerdo de confidencialidad.

…

Estas obligaciones no se aplican si la información confidencial es requerida de oficio por los Tribunales u órganos administrativos competentes o impuestas por una ley, evento en el cual se revelará la información confidencial dada por el suscriptor, de acuerdo con las normas vigentes.

9.4 Protección de la información personal

La protección de datos personales cumple con la normativa especial de confidencialidad establecida en la Ley de firma electrónica que es la Ley 51 de 2008 modificada por la Ley 82 de 2012 y la Ley 81 de 26 de marzo de 2019 reglamentada por el Decreto Ejecutivo 285 de 28 de mayo de 2021, sobre la de protección de datos de la República de Panamá.

La ley 81 de 2019, en su artículo 4, define el dato personal como cualquier información concerniente a personas naturales, que las identifica o las hace identificables. En este sentido, la Dirección Nacional de Firma Electrónica es la responsable de la custodia de la información del suscriptor requerida mediante el presente documento.

Los datos personales de los suscriptores son utilizados para el servicio de certificación, para diferentes funciones tales como:

1. Comprobación de identidad de los suscriptores y/o firmantes de los certificados electrónicos calificados.
2. Emisión y gestión de certificados electrónicos calificados.
3. Gestión del ciclo de vida del certificado que incluye: suspensión, renovación, reactivación y revocación.
4. Comunicaciones relativas al servicio.
5. Custodia y mantenimiento del archivo relativo al certificado electrónico calificado.
6. Gestión administrativa derivada del servicio.

El prestador de servicios de certificación, como responsable del tratamiento de datos personales, garantiza la protección, la confidencialidad y el debido uso de la información suministrada por el suscriptor al prestador de servicios de certificación de conformidad con el artículo 23 numeral 11 de la Ley 51 de 2008 modificada por la ley 82 de 2012 limitando su empleo a las necesidades propias del servicio de certificación descritas en el párrafo anterior; el prestador de servicios de certificación, no comunicara, transferirá o cederá sus datos personales a terceros, su consentimiento expreso, salvo que medie una obligación legal o será parte de una investigación judicial, entre otros supuestos.

Para que esta garantía aplique es indispensable que el suscriptor brinde información veraz al prestador de servicio de certificación y que el prestador de servicios de certificación haya podido comprobar la veracidad de dicha información.

Los derechos que los titulares del tratamiento de datos personales pueden ejercer conforma a la Ley 81 de 2019 reglamentada por el Decreto Ejecutivo 285 de 2021, son los siguientes:

9.1 Derecho de acceso: Permite al titular obtener sus datos personales que se encuentren almacenados o sujetos a tratamiento en bases de datos de instituciones públicas o privadas, además de conocer el origen y la para los cuales han sido recabados.

9.2 Derecho de rectificación: Permite al titular solicitar la corrección de sus datos personales que sean incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes. La rectificación podrá implicar la emisión de un nuevo certificado electrónico.
Para ejercer los derechos de accesos, el suscriptor debe dirigirse a la Dirección Nacional de Firma Electrónica.

La RPP-PKI se compromete a salvaguardar la confidencialidad de la información y no ponerla a disposición ni revelarla a individuos no autorizados; adicionalmente, en materia de tratamiento de los datos personales, la RPP-PKI aplica el principio de confidencialidad a través del cual, para aquellos datos personales que no tienen naturaleza de públicos, se garantiza la reserva de la información, realizando el suministro o comunicación solo en los casos autorizados por la Ley.

9.12.1 Procedimiento para los cambios

…

La Autoridad de Aprobación de Políticas en conjunto con el Comité Ejecutivo establecerán la frecuencia de evaluación de la DPC y sus PC, no obstante, en ningún caso este plazo será mayor de dos (2) años.

Cualquiera modificación en la DPC y las PCs será publicada de forma inmediata en el URL de acceso a estas.

D. Eliminación:

4.3.1 Actuaciones de la CA durante la emisión del certificado

Todo lo especificado en este apartado queda supeditado a lo estipulado por las distintas Políticas de Certificación para la emisión de certificados acogidos a las mismas.

4.4.1 Mecanismo de aceptación del certificado

En la PC correspondiente se podrán detallar o ampliar la forma en que se acepta el certificado.

4.8.1 Circunstancias para la modificación de un certificado

Se habla de modificación de un certificado cuando se emite uno nuevo debido a cambios en la información del certificado, no relacionados con su clave pública o expiración del periodo de validez.

Las modificaciones de los certificados pueden venir dadas por diferentes motivos tales como:

- Cambio de nombre.
- Cambio en las funciones dentro de la organización.
- Reorganización como resultado del cambio en el Nombre Distintivo.

Todas las modificaciones de certificados realizadas en el ámbito de esta DPC se tratarán como una renovación de certificados, por lo que son de aplicación los apartados anteriores al respecto.

Observaciones adicionales: Las actualizaciones realizadas al documento se aprobaron en reunión de Comité Ejecutivo – Acta de Reunión AR-2023-07.