



P-11

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Última versión: 03	Fecha de implementación: 21 de diciembre de 2021	
Preparado por: Departamento de Calidad y Atención al Usuario 03 de marzo de 2021	Revisado por: Subcomité de Gestión de Políticas 27 de septiembre de 2021	Aprobado por: Autoridad de Aprobación de Políticas 1 de diciembre de 2021
	ACTA DE SUBCOMITÉ DE GESTIÓN DE POLÍTICAS No. 2021-04	ACTA DE COMITÉ EJECUTIVO No. 2021-05



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 2 de 85

Índice

1. INTRODUCCIÓN	10
1.1. Visión general.....	10
1.2. Nombre del documento e identificación de la DPC.....	12
1.3. Participantes en la PKI.....	12
1.3.1. Prestador de Servicios de Certificación (PSC).....	13
1.3.2. Autoridad de Aprobación de Políticas (AAP).....	13
1.3.3. Autoridades de Certificación (CA).....	13
1.3.4. Autoridades de Registro (RA).....	17
1.3.5. Autoridades de Validación (VA).....	18
1.3.6. Autoridades de Sellado de Tiempo (TSA).....	18
1.3.7. Solicitantes y titulares de certificados.....	19
1.3.8. Terceros que confían en los certificados emitidos por DNFE.....	20
1.4. Uso de los certificados.....	20
1.4.1. Limitaciones y restricciones en el uso de los certificados.....	20
1.5. Administración de las políticas.....	20
1.5.1. Entidad Responsable.....	20
1.5.2. Procedimiento de aprobación y modificación de la Declaración de Prácticas de Certificación.....	21
1.5.3. Datos de Contacto.....	21
1.6. Definiciones y Acrónimos.....	22
1.6.1. Definiciones.....	22
1.6.2. Acrónimos.....	23
2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN	25
2.1. Repositorios.....	25
2.2. Publicación de información de certificación.....	25
2.3. Frecuencia de publicación.....	26
2.4. Controles de acceso a la información de certificación.....	26
3. IDENTIFICACIÓN Y AUTENTICACIÓN	27
3.1. Nombres.....	27
3.1.1. Tipos de nombres.....	27



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 3 de 85

3.1.2.	Necesidad de que los nombres sean significativos.....	27
3.1.3.	Reglas para interpretar varios formatos de nombres	27
3.1.4.	Unicidad de los nombres	27
3.1.5.	Procedimientos de resolución de conflictos sobre nombres	28
3.1.6.	Reconocimiento, autenticación y papel de las marcas registradas	28
3.2.	Validación inicial de la identidad	28
3.2.1.	Medio de prueba de posesión de la clave privada	28
3.2.2.	Autenticación de la identidad de una persona jurídica	28
3.2.3.	Autenticación de la identidad de una persona natural	28
3.2.4.	Información no verificada sobre el solicitante	29
3.2.5.	Comprobación de las facultades de representación	29
3.2.6.	Criterios para operar con CA externas	29
3.3.	Identificación y autenticación para solicitudes de renovación	30
3.4.	Identificación y autenticación para solicitudes de revocación.....	30
4.	REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS	31
4.1.	Solicitud de certificados.....	31
4.1.1.	Quién puede efectuar una solicitud	31
4.1.2.	Registro de las solicitudes de certificados y responsabilidades de los solicitantes	31
4.2.	Tramitación de las solicitudes de certificados	32
4.2.1.	Realización de las funciones de identificación y autenticación	32
4.2.2.	Aprobación o denegación de las solicitudes de certificados	32
4.2.3.	Plazo para la tramitación de las solicitudes de certificados	32
4.3.	Emisión de certificados	32
4.3.1.	Actuaciones de la CA durante la emisión del certificado	32
4.3.2.	Notificación al solicitante de la emisión por la CA del certificado	33
4.4.	Aceptación del certificado	33
4.4.1.	Mecanismo de aceptación del certificado.....	33
4.4.2.	Publicación del certificado por la CA	33
4.4.3.	Notificación de la emisión del certificado por la CA a otras Autoridades	33
4.5.	Par de claves y uso del certificado.....	34
4.5.1.	Uso de la clave privada y del certificado por el titular	34
4.5.2.	Uso de la clave pública y del certificado por los terceros aceptantes	34
4.6.	Renovación de certificados sin cambio de claves	34
4.6.1.	Circunstancias para la renovación de certificados sin cambio de claves	34
4.6.2.	Quién puede solicitar la renovación de los certificados sin cambio de claves.....	35



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código: P-11	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 4 de 85
------------------------	------------------------	--	-----------------

4.6.3.	Tramitación de las peticiones de renovación de certificados sin cambio de claves ...	35
4.6.4.	Notificación de la emisión de un nuevo certificado al titular	35
4.6.5.	Forma de aceptación del certificado sin cambio de claves	35
4.6.6.	Publicación del certificado sin cambio de claves por la CA	35
4.6.7.	Notificación de la emisión del certificado por la CA a otras Autoridades	35
4.7.	Renovación de certificados con cambio de claves	35
4.7.1.	Circunstancias para una renovación con cambio de claves de un certificado	35
4.7.2.	Quién puede pedir la renovación de los certificados	36
4.7.3.	Tramitación de las peticiones de renovación de certificados con cambio de claves ..	36
4.7.4.	Notificación de la emisión de un nuevo certificado al titular	36
4.7.5.	Forma de aceptación del certificado con las claves cambiadas	36
4.7.6.	Publicación del certificado con las nuevas claves por la CA	37
4.7.7.	Notificación de la emisión del certificado por la CA a otras Autoridades	37
4.8.	Modificación de certificados	37
4.8.1.	Circunstancias para la modificación de un certificado	37
4.8.2.	Quién puede solicitar la modificación de los certificados	37
4.8.3.	Tramitación de las peticiones de modificación de certificados	38
4.8.4.	Notificación de la emisión de un certificado modificado al titular	38
4.8.5.	Forma de aceptación del certificado modificado	38
4.8.6.	Publicación del certificado modificado por la CA	38
4.8.7.	Notificación de la modificación del certificado por la CA a otras Autoridades	38
4.9.	Revocación y suspensión de certificados	38
4.9.1.	Circunstancias para la revocación	38
4.9.2.	Quién puede solicitar la revocación	39
4.9.3.	Procedimiento de solicitud de revocación	40
4.9.4.	Periodo de gracia de la solicitud de revocación	41
4.9.5.	Plazo en el que la CA debe resolver la solicitud de revocación	41
4.9.6.	Requisitos de verificación de las revocaciones por los terceros que confían	41
4.9.7.	Frecuencia de emisión de CRL	41
4.9.8.	Tiempo máximo entre la generación y la publicación de las CRL	42
4.9.9.	Disponibilidad de un sistema en línea de verificación del estado de los certificados .	42
4.9.10.	Requisitos de comprobación en línea de revocación	42
4.9.11.	Otras formas de divulgación de información de revocación disponibles	42
4.9.12.	Requisitos especiales de revocación de claves comprometidas	42
4.9.13.	Causas para la suspensión	42
4.9.14.	Quién puede solicitar la suspensión	43
4.9.15.	Procedimiento para la solicitud de suspensión	43
4.9.16.	Límites del periodo de suspensión	43
4.10.	Servicios de información del estado de certificados	43



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código: P-11	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 5 de 85
------------------------	------------------------	--	-----------------

4.10.1.	Características operativas	43
4.10.2.	Disponibilidad del servicio	44
4.10.3.	Características adicionales	44
4.11.	Extinción de la validez de un certificado	44
4.12.	Custodia y recuperación de claves	44
4.12.1.	Prácticas y políticas de custodia y recuperación de claves	44
4.12.2.	Prácticas y políticas de protección y recuperación de la clave de sesión	45
5. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES		
45		
5.1.	Controles físicos	46
5.1.1.	Ubicación física y construcción	46
5.1.2.	Acceso físico	47
5.1.3.	Alimentación eléctrica y aire acondicionado	47
5.1.4.	Exposición al agua	48
5.1.5.	Prevención y protección frente a incendios	48
5.1.6.	Sistema de almacenamiento	48
5.1.7.	Eliminación de residuos	48
5.1.8.	Copias de seguridad fuera de las instalaciones	48
5.2.	Controles de procedimiento	48
5.2.1.	Roles responsables del control y gestión de la RPP-PKI	49
5.2.2.	Número de personas requeridas por tarea	50
5.2.3.	Roles que requieren segregación de funciones	50
5.3.	Controles de personal	50
5.3.1.	Requisitos relativos a la cualificación, conocimiento y experiencia profesionales	50
5.3.2.	Procedimientos de comprobación de antecedentes	51
5.3.3.	Requerimientos de formación	51
5.3.4.	Requerimientos y frecuencia de actualización de la formación	51
5.3.5.	Frecuencia y secuencia de rotación de tareas	52
5.3.6.	Sanciones por actuaciones no autorizadas	52
5.3.7.	Requisitos de contratación de terceros	52
5.3.8.	Documentación proporcionada al personal	52
5.4.	Procedimientos de auditoría de seguridad	53
5.4.1.	Tipos de eventos registrados	53
5.4.2.	Frecuencia de procesado de registros de auditoría	54
5.4.3.	Periodo de conservación de los registros de auditoría	54
5.4.4.	Protección de los registros de auditoría	54



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código: P-11	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 6 de 85
------------------------	------------------------	--	-----------------

5.4.5.	Procedimientos de respaldo de los registros de auditoría	55
5.4.6.	Notificación al sujeto causa del evento	55
5.4.7.	Análisis de vulnerabilidades	55
5.5.	Archivado de registros.....	56
5.5.1.	Tipo de eventos archivados.....	56
5.5.2.	Periodo de conservación de registros	56
5.5.3.	Protección del archivo	56
5.5.4.	Procedimientos de copia de respaldo del archivo	56
5.5.5.	Requerimientos para el sellado de tiempo de los registros	56
5.5.6.	Sistema de archivo de información (interno vs externo)	57
5.5.7.	Procedimientos para obtener y verificar información archivada	57
5.6.	Cambio de claves.....	57
5.7.	Recuperación ante compromiso de clave o catástrofe	57
5.7.1.	Procedimientos de gestión de incidentes y compromisos.....	57
5.7.2.	Alteración de los recursos hardware, software y/o datos	58
5.7.3.	Procedimiento de actuación ante el compromiso de la clave privada de una Autoridad 58	
5.7.4.	Instalación después de un desastre natural u otro tipo de catástrofe	59
5.8.	Cese de una CA o RA	59
5.8.1.	Autoridad de Certificación	59
5.8.2.	Autoridad de Registro	60
6.	CONTROLES DE SEGURIDAD TÉCNICA	61
6.1.	Generación e instalación del par de claves	61
6.1.1.	Generación del par de claves.....	61
6.1.2.	Entrega de la clave privada al titular	61
6.1.3.	Entrega de la clave pública al emisor del certificado	61
6.1.4.	Entrega de la clave pública de la CA a los terceros que confían	61
6.1.5.	Tamaño de las claves.....	62
6.1.6.	Parámetros de generación de la clave pública y verificación de la calidad	62
6.1.7.	Usos admitidos de la clave (campo KeyUsage de X.509 v3).....	62
6.2.	Protección de la clave privada y controles de ingeniería de los módulos	62
6.2.1.	Estándares para los módulos criptográficos	62
6.2.2.	Control multipersona (k de n) de la clave privada	63
6.2.3.	Custodia de la clave privada	63
6.2.4.	Copia de seguridad de la clave privada	63
6.2.5.	Archivado de la clave privada.....	64



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código: P-11	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 7 de 85
------------------------	------------------------	--	-----------------

6.2.6.	Transferencia de la clave privada a o desde el módulo criptográfico	64
6.2.7.	Almacenamiento de la clave privada en un módulo criptográfico	64
6.2.8.	Método de activación de la clave privada	64
6.2.9.	Método de desactivación de la clave privada.....	64
6.2.10.	Método de destrucción de la clave privada	64
6.2.11.	Clasificación de los módulos criptográficos.....	65
6.3.	Otros aspectos de la gestión del par de claves	65
6.3.1.	Archivo de la clave pública	65
6.3.2.	Periodos operativos de los certificados y periodo de uso para el par de claves	65
6.4.	Datos de activación	65
6.4.1.	Generación e instalación de los datos de activación	65
6.4.2.	Protección de los datos de activación	66
6.4.3.	Otros aspectos de los datos de activación	66
6.5.	Controles de seguridad informática	66
6.5.1.	Requerimientos técnicos de seguridad específicos	66
6.5.2.	Evaluación de la seguridad informática.....	66
6.6.	Controles de seguridad del ciclo de vida	66
6.6.1.	Controles de desarrollo de sistemas	67
6.6.2.	Controles de gestión de seguridad.....	67
6.6.3.	Controles de seguridad del ciclo de vida.....	67
6.7.	Controles de seguridad de la red	67
6.8.	Sellado de tiempo.....	67
7.	PERFILES DE LOS CERTIFICADOS, CRL Y OCSP	68
7.1.	Perfil de certificado.....	68
7.1.1.	Número de versión	68
7.1.2.	Extensiones del certificado.....	68
7.1.3.	Identificadores de objeto (OID) de los algoritmos	68
7.1.4.	Formatos de nombres.....	68
7.1.5.	Restricciones de los nombres	68
7.1.6.	Identificador de objeto (OID) de la Política de Certificación.....	69
7.1.7.	Uso de la extensión "PolicyConstraints"	69
7.1.8.	7.1.8 Sintaxis y semántica de los "PolicyQualifier".....	69
7.1.9.	Tratamiento semántico para la extensión crítica "Certificate Policy"	69
7.2.	Perfil de CRL	69
7.2.1.	Número de versión	69



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código: P-11	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 8 de 85
------------------------	------------------------	--	-----------------

7.2.2.	CRL y extensiones.....	69
7.3.	Perfil de OCSP	70
7.3.1.	Número(s) de versión	70
7.3.2.	Extensiones OCSP	70
8.	AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES	71
8.1.	Frecuencia o circunstancias de los controles para cada Autoridad	71
8.2.	Identificación/cualificación del auditor	71
8.3.	Relación entre el auditor y la Autoridad auditada	71
8.4.	Aspectos cubiertos por los controles	71
8.5.	Acciones a tomar como resultado de la detección de deficiencias.....	72
8.6.	Comunicación de resultados	72
9.	OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD	73
9.1.	Tarifas.....	73
9.1.1.	Tarifas de emisión de certificado o renovación	73
9.1.2.	Tarifas de acceso a los certificados	73
9.1.3.	Tarifas de acceso a la información de estado o revocación	73
9.1.4.	Tarifas de otros servicios tales como información de políticas	73
9.1.5.	Política de reembolso	73
9.2.	Responsabilidades económicas.....	74
9.3.	Confidencialidad de la información	74
9.3.1.	Ámbito de la información confidencial	74
9.3.2.	Información no confidencial.....	75
9.3.3.	Deber de secreto profesional	75
9.4.	Protección de la información personal	76
9.5.	Derechos de propiedad intelectual.....	76
9.6.	Representaciones y garantías.....	76
9.6.1.	Obligaciones de las CAs	76
9.6.2.	Obligaciones de las RAs	78
9.6.3.	Obligaciones de los titulares de los certificados.....	78
9.6.4.	Obligaciones de los terceros que confían o acepten los certificados	79
9.7.	Exención de responsabilidades.....	80
9.8.	Limitaciones de las responsabilidades.....	81



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código: P-11	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 9 de 85
------------------------	------------------------	--	-----------------

9.9. Indemnizaciones	81
9.9.1. Indemnizaciones por daños ocasionados por RPP-PKI.....	82
9.9.2. Indemnizaciones por los daños ocasionados por los Suscriptores.....	82
9.9.3. Indemnizaciones por los daños ocasionados por los Terceros que confían.....	82
9.10. Período de validez.....	82
9.10.1. Plazo	82
9.10.2. Sustitución y derogación de la DPC	83
9.10.3. Efectos de la finalización	83
9.11. Notificaciones individuales y comunicaciones con los participantes	83
9.12. Procedimientos de cambios en las especificaciones	83
9.12.1. Procedimiento para los cambios	83
9.12.2. Circunstancias en las que el OID debe ser cambiado	84
9.13. Reclamaciones.....	84
9.14. Normativa aplicable.....	84
9.15. Cumplimiento de la normativa aplicable	85
9.16. Estipulaciones diversas.....	85
9.16.1. Cláusula de aceptación completa.....	85
9.16.2. Independencia	85
9.16.3. Resolución por la vía judicial	¡Error! Marcador no definido.
9.17. Otras estipulaciones.....	¡Error! Marcador no definido.



REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 10 de 85

1. INTRODUCCIÓN

El presente documento corresponde a la Declaración de Prácticas de Certificación (DPC) que estipula el funcionamiento y operaciones de la Infraestructura de Clave Pública (en adelante PKI) de la Autoridad Certificadora del Registro Público de Panamá, en concordancia con 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.

La expedición de certificados electrónicos a otras entidades o corporaciones que deseen actuar como Autoridades de Certificación subordinadas o secundarias, emitiendo certificados electrónicos bajo la jerarquía del Certificado de la Autoridad Certificadora de Panamá, requerirá la aprobación del Comité Ejecutivo.

1.1. Visión general

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 N° 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 N° 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



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 11 de 85

claves, hasta la posterior emisión, distribución, uso, revocación/suspensión y renovación de estos.

La presente Declaración de Prácticas de Certificación (en adelante DPC), emitida de conformidad con la Ley N° 82 de 2012 y la Ley N° 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.

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 N° 82 de 2012 y la Ley N° 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.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código: P-11	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 12 de 85
------------------------	------------------------	--	------------------

1.2. Nombre del documento e identificación de la DPC

Nombre del documento Declaración de Prácticas de Certificación de la PKI del Registro Público de Panamá

Versión del documento 0.3

Estado del documento Actualizado

Fecha de emisión 26/09/2012

Fecha de Actualización 27/09/2021 - Acta de subcomité Ejecutivo No. AR-2021-04

Fecha de expiración No aplicable

OID (Object Identifier) 2.16.591.1.2.1

Ubicación de la DPC <http://www.pki.gob.pa/normativa/index.html>

1.3. Participantes en la PKI

Las entidades y personas intervinientes en la PKI son las que se enumeran a continuación:

1. Prestador de Servicios de Certificación (PSC)
2. Autoridad de Aprobación de Políticas (AAP)
3. Autoridades de Certificación (CA)
4. Autoridades de Registro (RA)
5. Autoridades de Validación (VA)
6. Autoridades de Sellado de Tiempo (TSA)
7. Solicitantes y Titulares de certificados
8. Terceros que confían en los certificados de la PKI del Registro Público de Panamá



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 13 de 85

1.3.1. Prestador de Servicios de Certificación (PSC)

Según la definición dispuesta por la Ley N° 51 de 2008 modificada por la Ley N° 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 PKI del Registro Público de Panamá. 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 N° 82 de 2012 y la Ley N° 51 de 2008.

1.3.2. Autoridad de Aprobación de Políticas (AAP)

La Autoridad de Aprobación de Políticas (AAP) del Comité Ejecutivo, es el responsable de la aprobación de la presente DPC y de las Políticas de Certificación de la RPP-PKI, así como de la aprobación de las modificaciones de dichos documentos.

Asimismo, la AAP es la responsable, en caso de que se tuviese que evaluar la posibilidad de que una CA externa interactúe con la RPP-PKI, de determinar la adecuación de la DPC de dicha CA a la Política de Certificación afectada.

La AAP es responsable de analizar los informes de las auditorías, totales o parciales, que se hagan de la RPP-PKI, así como de determinar, en caso necesario, las acciones correctoras a ejecutar.

1.3.3. Autoridades de Certificación (CA)

Son las personas, políticas, procedimientos y sistemas informáticos encargados de la emisión de certificados electrónicos y de la asignación a sus titulares. Así mismo, efectúan la renovación y revocación de los mencionados certificados y la generación de claves públicas y privadas, cuando así lo establecen sus prácticas y políticas.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 14 de 85

La arquitectura general, a nivel jerárquico, de la RPP-PKI es la siguiente:



1.3.3.1. Autoridad Certificadora de Panamá

La RPP-PKI emite todos los certificados objeto de la presente DPC bajo la jerarquía del Certificado Raíz. El certificado raíz es un certificado *auto-firmado*, en el que se inicia la cadena de confianza.

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.

El titular del certificado Raíz es el propio Registro Público de Panamá, y se emite y revoca por orden del Comité Ejecutivo.

Los datos más relevantes de la Autoridad Certificadora de Panamá son los siguientes:

Nombre distintivo	CN=AUTORIDAD CERTIFICADORA DE PANAMA, O=FIRMA ELECTRONICA, C=PA
Número de serie	403D B5E6 C915 73D4 518A 8515 6FE9 E7EC
Nombre distintivo del emisor	CN=AUTORIDAD CERTIFICADORA DE PANAMA, O=FIRMA ELECTRONICA, C=PA
Fecha de emisión	2013-05-08 12:02:13



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 15 de 85

Fecha de expiración 2053-05-08 12:02:13

Longitud de clave RSA 4096

Huella digital (SHA-1) 98BB 7426 2814 B7D9 FC41 3C2A 166C 1662 729E
24F8

URL de publicación del certificado <http://www.pki.gob.pa/cacerts/caraiz.crt>

URL de publicación de la ARL <http://www.pki.gob.pa/crls/caraiz.crl>

1.3.3.2. Autoridades de Certificación Subordinadas

Bajo el Certificado Raíz de Panamá, se encuentran los certificados 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 datos más relevantes de la **CA de Gobierno** son los siguientes:

Nombre distintivo CN=CA DE GOBIERNO DE PANAMA, O=FIRMA ELECTRONICA, C=PA

Número de serie 20 68 26 57 9f e0 88 f9 51 8c 0a 67 68 35 d6 b7

Nombre distintivo del emisor CN=AUTORIDAD CERTIFICADORA DE PANAMA, O=FIRMA ELECTRONICA, C=PA

Fecha de emisión 2013-05-09 15:43:19

Fecha de expiración 2033-05-09 15:43:19

Longitud de clave RSA 2048

Huella digital (SHA-1) 8f 4c 93 da 3d 07 9b aa 36 6f 9c 16 db 4a ef 32 53 b0
ae 86

URL de publicación del certificado <http://www.pki.gob.pa/cacerts/cagob.crt>



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 16 de 85

URL de publicación de <http://www.pki.gob.pa/crls/cagob.crl>
la CRL

Tipos de certificados emitidos Autenticación de Funcionario Público
Firma de Funcionario Público
Servidor SSL
Firma de Código
Servicio OCSP
Servicio TSP

En el caso de la **CA Panama Clase 2** los datos más relevantes son los siguientes:

Nombre distintivo CN=CA PANAMA CLASE 2, O=FIRMA ELECTRONICA, C=PA

Número de serie 71 84 c5 5b e9 40 a8 33 51 8c 0a 9e ff 29 15 97

Nombre distintivo del emisor CN=AUTORIDAD CERTIFICADORA DE PANAMA, O=FIRMA ELECTRONICA, C=PA

Fecha de emisión 2013-05-09 15:44:14

Fecha de expiración 2033-05-09 15:44:14

Longitud de clave RSA 2048

Huella digital (SHA-1) cf 79 f1 b8 4f 9f 22 80 d7 f3 da 21 1c c0 09 ef b4 e9 21 77

URL de publicación del <http://www.pki.gob.pa/cacerts/capc2.crt>
certificado

URL de publicación de <http://www.pki.gob.pa/crls/capc2.crl>
la CRL

Tipos de certificados emitidos Autenticación de Persona Natural



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 17 de 85

Firma de Persona Natural
Autenticación de Representante de Persona Jurídica
Firma de Representante de Persona Jurídica
Autenticación de Colaborador de Persona Jurídica
Firma de Colaborador de Persona Jurídica
Autenticación de Profesional
Firma de Profesional
Autenticación de Factura Electrónica
Firma de Factura Electrónica
Servidor SSL
Firma de Código

1.3.4. Autoridades de Registro (RA)

Son las personas, políticas, procedimientos y sistemas informáticos encargados de la verificación de la identidad de los solicitantes de certificados electrónicos y si procede, de los atributos asociados a los mismos.

Las Autoridades de Registro (RA) llevarán a cabo la identificación de los solicitantes de certificados conforme a las normas de esta DPC y el acuerdo suscrito con la CA. Para ello, cada RA contará con un puesto de inscripción y un puesto de emisión:

1.3.4.1. Puesto de Inscripción

Las tareas realizadas en el puesto de inscripción son:

- Registro de datos de un solicitante de certificados electrónicos.
- Verificación de la identidad de un solicitante de certificados electrónicos.
- Personalización gráfica del dispositivo criptográfico en el que se generará el certificado electrónico que será entregado al solicitante.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 18 de 85

1.3.4.2. Puesto de Emisión

Las tareas realizadas en el puesto de emisión son:

- Verificación de que el solicitante de certificados electrónicos ha realizado su registro en el puesto de inscripción
- Solicitud de los certificados a la CA correspondiente en función del perfil del certificado electrónico solicitado, así como su posterior entrega al titular.

1.3.5. Autoridades de Validación (VA)

La Autoridad de Validación (VA) tiene como función la comprobación del estado de los certificados emitidos por la RPP-PKI, mediante el protocolo Online Certificate Status Protocol (OCSP), que determina el estado actual de un certificado electrónico a solicitud de un tercero que confía sin requerir el acceso a listas de certificados revocados por éstas.

Este mecanismo de validación es complementario a la publicación de las listas de certificados revocados (CRL).

1.3.6. Autoridades de Sellado de Tiempo (TSA)

La Autoridad de Sellado de Tiempo (TSA) es la responsable de la prestación de los servicios recogidos a continuación, de forma que proporcione confianza a sus usuarios: solicitantes, titulares y terceros que confían.

Los servicios de sellado de tiempo se estructuran en dos partes:

- **Suministro de los sellos de tiempo:** los componentes técnicos y organizativos que emiten los sellos de tiempo (TST).
- **Gestión del sellado de tiempo:** los componentes técnicos y organizativos que supervisan y controlan la operativa del sellado de tiempo, incluyendo la sincronización temporal con la fuente de referencia UTC.

La TSA tiene la responsabilidad de operar una o varias Unidades de Sellado de Tiempo (TSU) las cuales crearán y firmarán los sellos de tiempo (TST) en nombre de la TSA, cada TSU ha de tener su propia clave privada.

La TSA queda identificada en el certificado electrónico de firma que se utilice en el servicio de sellado de tiempo.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 19 de 85

1.3.7. Solicitantes y titulares de certificados

Se definen como entidades finales aquellas personas físicas sujetos de derechos, con capacidad suficiente para solicitar y obtener un certificado electrónico de la RPP-PKI, a título propio o en su condición de representante de una persona jurídica.

A los efectos anteriores tendrán la consideración de Entidades Finales:

- Solicitante
- Titular

1.3.7.1. Solicitante

Cuando un ciudadano interesado en obtener un certificado, llena el formulario de petición de cita en la página web <https://www.firmaelectronica.gob.pa>, adquiere la condición de Solicitante. La solicitud de un certificado no implica la concesión de este, la cual queda supeditada al éxito del procedimiento de Registro ante el Puesto de Inscripción, previa verificación de los atributos cuya certificación se solicita.

Sólo las personas mayores de edad podrán solicitar y, en su caso, obtener certificados electrónicos emitidos por la RPP-PKI.

1.3.7.2. Titular

Los datos de identificación del titular están contenidos en los campos “Subject” y “Subject Alternative Names” del certificado definido dentro del estándar X509 de la ITU.

Dado que la RPP-PKI únicamente expide certificados electrónicos a personas naturales, en el caso de los Certificados de Representante de Persona Jurídica, tendrá la consideración de titular, aquel que ostente la representación de una persona jurídica, incluyéndose los datos de ésta en el certificado.

La identidad del titular figurará en el DN del certificado electrónico en el campo CN=Common Name, dentro de la extensión subject del certificado. Los datos identificativos del titular podrán ser así mismo incluidos, dependiendo del tipo de certificado, con formato RFC822 en una extensión de nombre alternativo



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 20 de 85

subjectAltName, de conformidad con lo que se estipule en las políticas particulares aplicables a cada certificado.

1.3.8. Terceros que confían en los certificados emitidos por DNFE

En el ámbito de esta DPC, los terceros que confían son las personas o entidades diferentes del titular que deciden aceptar y confiar en los certificados emitidos por la RPP-PKI.

Las Políticas de Certificación de cada uno de los tipos de certificados son quienes determinan los terceros que confían para cada certificado.

A los efectos de esta DPC, tercero que confía es cualquier usuario que deposita su confianza en los certificados emitidos por la RPP-PKI, y que son utilizados para la firma de comunicaciones, documentos electrónicos, o en la autenticación ante sistemas basada en certificados electrónicos.

La RPP-PKI no asume ningún tipo de responsabilidad ante terceros, incluso de buena fe, que no hayan verificado convenientemente la vigencia de los Certificados.

1.4. Uso de los certificados

Las Políticas de Certificación correspondientes a cada tipo de certificado son las que determinan los usos apropiados que debe darse a cada certificado. No es objetivo de esta DPC la determinación de dichos usos.

1.4.1. Limitaciones y restricciones en el uso de los certificados

Los certificados deben emplearse de acuerdo con las funciones y finalidades definidas en su correspondiente PC, sin que puedan utilizarse para otras tareas y otros fines no contemplados en aquella.

1.5. Administración de las políticas

1.5.1. Entidad Responsable

El Registro Público de Panamá, a través del Comité Ejecutivo, establecerá los términos y redacción de la DPC de RPP-PKI. Las actualizaciones y revisiones a la DPC de RPP-PKI se realizarán periódicamente para asegurar que se mantienen



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 21 de 85

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 dos años.

1.5.2. Procedimiento de aprobación y modificación de la Declaración de Prácticas de Certificación

La aprobación inicial y de las subsiguientes modificaciones de la DPC, corresponde en exclusiva al Comité Ejecutivo, en virtud de las facultades delegadas por el Registro Público de Panamá.

Cualquier modificación en la DPC será introducida, y publicada en la página web de la Dirección Nacional de Firma Electrónica (<http://www.pki.gob.pa/normativa/index.htm>). Los titulares disconformes con las modificaciones introducidas podrán solicitar la revocación de su certificado electrónico.

La revocación interesada y voluntaria por el usuario disconforme con las disposiciones incorporadas con carácter sobrevenido a esta DPC, no otorgará al titular ningún derecho a ser compensado por tal motivo.

1.5.3. Datos de Contacto

Para consultas o comentarios relacionados con la presente DPC el interesado deberá dirigirse a la Autoridad de Aprobación de Políticas a través de alguno de los siguientes medios:

Dirección Nacional de Firma Electrónica

Avenida 12 de octubre, Plaza La Hispanidad, Local A-7, Ciudad de Panamá

Email: servicios@firmaelectronica.gob.pa

Tel: +507 504-3900



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 22 de 85

1.6. Definiciones y Acrónimos

1.6.1. Definiciones

En el ámbito de la presente DPC los términos empleados son los siguientes:

Autenticación: proceso de verificar la identidad de solicitante o titular de un certificado de la República de Panamá.

Certificado electrónico: documento electrónico expedido por un prestador de servicios de certificación de firmas electrónicas, que vincula los datos de verificación de una firma electrónica a un firmante y confirma su identidad.

Componente informático: cualquier dispositivo software o hardware susceptible de utilizar certificados electrónicos para su propio uso, con el objeto de identificarse o intercambiar datos firmados o cifrados con terceros aceptantes.

Identificación: proceso de establecer la identidad de un solicitante o titular de un certificado de la República de Panamá.

Infraestructura de Clave Pública: conjunto de individuos, políticas, procedimientos y sistemas de la información necesarios para proporcionar servicios de autenticación, cifrado, integridad y no repudio mediante el uso de criptografía de clave asimétrica y certificados electrónicos.

Prestador de Servicios de Certificación: 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.

Solicitante: persona natural o jurídica que solicita un certificado electrónico para sí mismo o para un componente informático.

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.

Tercero que confía: persona o entidad diferente del titular, que decide aceptar y confiar en un certificado electrónico emitido por la DNFE.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 23 de 85

1.6.2. Acrónimos

AAP: Autoridad de Aprobación de Políticas.

C: Country (País). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

CA: Certification Authority (Autoridad de Certificación).

CDP: CRL Distribution Point (Punto de Distribución de CRL).

CN: Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

CP: Certificate Policy (Política de Certificación).

CPS: Certification Practice Statement (Declaración de Prácticas de Certificación).

CRL: Certificate Revocation List (Lista de Revocación de Certificados).

CSR: Certificate Signing Request (petición de certificado). Conjunto de datos, que contienen una clave pública y su firma electrónica utilizando la clave privada asociada, enviado a la Autoridad de Certificación para la emisión de un certificado electrónico que contenga dicha clave pública.

CWA: CEN Workshop Agreement.

DN: Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de un directorio X.500.

DNFE: Dirección Nacional de Firma Electrónica, del Registro Público de Panamá.

FIPS: Federal Information Processing Standard.

HSM: Hardware Security Module. Módulo de seguridad criptográfica empleado para el almacenamiento de claves y realización de operaciones criptográficas seguras.

IETF: Internet Engineering Task Force (Organismo de estandarización de Internet).

O: Organisation (Organización). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 24 de 85

OCSP: Online Certificate Status Protocol. Protocolo para la verificación online de la validez de un certificado electrónico.

OID: Object Identifier (Identificador Único de Objeto).

OU: Organisational Unit (Unidad Organizativa). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

PSC: Proveedor de Servicios de Certificación.

PIN: Personal Identification Number (Número de Identificación Personal). Password que protege el acceso a un dispositivo criptográfico.

PKCS: Public Key Cryptography Standards. Estándares de PKI desarrollados por los laboratorios de **RSA** aceptados internacionalmente.

RPP-PKI: Infraestructura de Clave Pública del Registro Público de Panamá.

PKI: Public Key Infrastructure (Infraestructura de Clave Pública).

PUK: PIN Unlock Key. Password que permite desbloquear un dispositivo criptográfico bloqueado por haber introducido en repetidas ocasiones un PIN erróneo de forma consecutiva.

RA: Registration Authority (Autoridad de Registro).

RFC: Request For Comments. Standard desarrollado por el IETF.

VA: Validation Authority (Autoridad de Validación).



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 25 de 85

2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

2.1. Repositorios

El repositorio de RPP-PKI consiste en un servicio Web de acceso libre. Dicho repositorio no contiene ninguna información de naturaleza confidencial.

ARL	http://www.pki.gob.pa/crls/caraiz.crl
CRL CA de Gobierno	http://www.pki.gob.pa/crls/cagob.crl
CRL CA Panama Clase 2	http://www.pki.gob.pa/crls/capc2.crl
Servicio de validación en línea que implementa el protocolo OCSP	http://ocsp.pki.gob.pa
Servicio de Sello de Tiempo (Time Stamping Protocol)	http://tsp.pki.gob.pa
Certificado Autoridad Certificadora de Panama	http://www.pki.gob.pa/cacerts/caraiz.crt
Certificado CA de Gobierno	http://www.pki.gob.pa/cacerts/cagob.crt
Certificado CA Panama Clase 2	http://www.pki.gob.pa/cacerts/capc2.crt
Prácticas y Políticas de Certificación	http://www.pki.gob.pa/normativa/index.html

2.2. Publicación de información de certificación

Es obligación de las CAs pertenecientes a la jerarquía de confianza de la RPP-PKI publicar la información relativa a sus prácticas, sus certificados y el estado actual de dichos certificados.

La presente DPC es pública y se encuentra disponible en el sitio web de la RPP-PKI, al que se hace referencia en el apartado 2.1. Repositorios, en formato PDF.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 26 de 85

Las Políticas de Certificación de la RPP-PKI son públicas y se encuentran disponibles en el sitio web de la RPP-PKI, al que se hace referencia en el apartado 2.1. Repositorios, en formato PDF.

Las listas de revocación de certificados (CRL) de la RPP-PKI son públicas y se encuentran disponibles, en formato CRL v2, en el repositorio y sitio web de la RPP-PKI al que se hace referencia en el apartado 2.1. Repositorios.

Las listas de revocación de certificados estarán firmadas electrónicamente por las CA de la RPP-PKI que las emitan.

La información sobre el estado de los certificados se podrá consultar accediendo directamente a las CRL o mediante el servicio de validación en línea disponible que implementa el protocolo OCSP.

2.3. Frecuencia de publicación

La DPC y las Políticas de Certificación se publicarán en el momento de su creación y se volverán a publicar en el momento en que se apruebe cualquier modificación sobre las mismas. Las modificaciones se harán públicas en el sitio web referido en el apartado 2.1. Repositorios.

La CA añadirá los certificados revocados a la CRL pertinente dentro del periodo de tiempo estipulado en el punto 4.9.7. Frecuencia de emisión de CRLs.

2.4. Controles de acceso a la información de certificación

El acceso para la consulta de las DPC y PC es abierto, pero sólo la RPP-PKI está autorizada a modificar, sustituir o eliminar información de su repositorio y sitio web. Para ello, la RPP-PKI establecerá controles que impidan a personas no autorizadas manipular la información contenida en los repositorios.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 27 de 85

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Nombres

3.1.1. Tipos de nombres

Todos los titulares de certificados requieren un nombre distintivo (Distinguished Name) conforme con el estándar X.500.

El procedimiento de asignación de los nombres distintivos a los suscriptores para cada uno de los tipos de certificados se encuentra definido en el documento de Política de Certificación que corresponda en cada caso. Dicha definición debe estar en consonancia con las directrices generales descritas en este capítulo de la DPC.

3.1.2. Necesidad de que los nombres sean significativos

En todos los casos se recomienda que los nombres distintivos de los titulares de los certificados sean significativos.

En cualquier supuesto el dotar a los nombres distintivos de significado viene dado por la política a tal efecto desarrollada y descrita en el documento de Política de Certificación correspondiente al certificado en cuestión.

3.1.3. Reglas para interpretar varios formatos de nombres

La regla utilizada por la RPP-PKI para interpretar los nombres distintivos de los titulares de certificados que emite es ISO/IEC 9595 (X.500) Distinguished Name (DN).

3.1.4. Unicidad de los nombres

El conjunto de nombre distintivo (Distinguished Name) más el contenido de la extensión Policy Identifier debe ser único y no ambiguo.

Los procedimientos de garantía de la unicidad para cada tipo de certificado están establecidos en la Política de Certificación correspondiente.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 28 de 85

3.1.5. Procedimientos de resolución de conflictos sobre nombres

Cualquier conflicto concerniente a la propiedad de nombres se resolverá según lo estipulado en el punto 9.13. *Reclamaciones* de esta DPC.

3.1.6. Reconocimiento, autenticación y papel de las marcas registradas

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.

3.2. Validación inicial de la identidad

3.2.1. Medio de prueba de posesión de la clave privada

En caso de que el par de claves sea generado por el solicitante del certificado, la posesión de la clave privada, correspondiente a la clave pública para la que solicita que se genere el certificado, quedará probada mediante el envío de la petición de certificado (CSR), en la cual se incluirá la clave pública firmada mediante la clave privada asociada.

Este procedimiento podrá ser modificado por el que establezca en cada caso la Política de Certificación aplicable.

3.2.2. Autenticación de la identidad de una persona jurídica

En caso de que sea aplicable, cada PC establecerá el procedimiento de autenticación de la identidad de una persona jurídica.

3.2.3. Autenticación de la identidad de una persona natural

La Política de Certificación aplicable a cada tipo de certificado definirá el procedimiento de identificación individual.

En cada PC se establecerá la información a proporcionar por el solicitante, determinándose entre otros aspectos los siguientes:

- Tipos de documentos de identidad válidos para la identificación, siguiendo con lo indicado en la Resolución No. DG-087-2019.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 29 de 85

- Procedimiento de identificación por la CA o RA del individuo.
- Necesidad o no de identificación presencial.
- Forma de acreditar la pertenencia a una determinada organización o colectivo profesional.

3.2.4. Información no verificada sobre el solicitante

Cada PC establecerá qué parte de la información suministrada en la solicitud de un certificado no se verifica necesariamente.

3.2.5. Comprobación de las facultades de representación

En los casos de emisión de certificados de componentes informáticos la verificación de las facultades del responsable para la solicitud de estos vendrá establecida en la PC específica.

3.2.6. Criterios para operar con CA externas

Antes de establecer relaciones de interactividad con CA externas, se ha de determinar la adecuación de dichas CA al cumplimiento de ciertos requisitos. Los criterios mínimos, que pueden ser ampliados en cada caso por la AAP, para considerar a una CA adecuada para interactuar con la RPP-PKI son:

- La CA externa ha de proporcionar un nivel de seguridad en la gestión de los certificados, a lo largo de su ciclo de vida, como mínimo, igual al de la RPP-PKI. Esta exigencia se recogerá en la DPC y PC correspondientes y en su cumplimiento por la CA.
- Deberá aportar el informe de auditoría de una Autoridad externa de reconocido prestigio relativa a sus operaciones como medio de verificación del nivel de seguridad existente. La AAP podrá declarar exentas de este requisito a las CA que estime oportuno.
- Establecer un convenio de colaboración en el que se fijen los compromisos adquiridos en materia de seguridad para los certificados incluidos en la interacción.

Aunque una CA cumpla los requisitos anteriores, la AAP podrá denegar la solicitud de interactividad sin necesidad de aportar ninguna justificación.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 30 de 85

La interactividad puede llevarse a cabo mediante certificación cruzada, certificación unilateral u otras formas.

3.3. Identificación y autenticación para solicitudes de renovación

El proceso de identificación y autenticación individual se define por la Política de Certificación aplicable a cada tipo de certificado.

3.4. Identificación y autenticación para solicitudes de revocación

El proceso de identificación y autenticación individual se define por la Política de Certificación aplicable a cada tipo de certificado, debiendo ser como mínimo tan estricto como el aplicado en la solicitud inicial del certificado.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 31 de 85

4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

4.1. Solicitud de certificados

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.

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

En general, es atribución de cada Autoridad de Registro de la RPP-PKI determinar la adecuación del tipo de certificado a las características de las funciones del solicitante, de acuerdo con lo previsto en la Política de Certificación aplicable en cada caso. La Autoridad de Registro podrá autorizar o denegar la solicitud de certificación.

Las solicitudes de los certificados, una vez completadas, serán enviadas a la Autoridad de Certificación por la Autoridad de Registro de la RPP-PKI.

Como regla general, todo solicitante que desee un certificado deberá:

- Cumplimentar el formulario de solicitud del certificado con toda la información que la RPP-PKI requiera para la emisión de este. Cabe destacar que no toda la información solicitada aparecerá en el certificado y que ésta será conservada, de manera confidencial, por la Autoridad de Certificación.
- Entregar la solicitud del certificado, que incluye la clave pública, en el caso de que el par de claves lo haya generado el solicitante, a la RA correspondiente y el certificado se genere directamente a partir de la solicitud. En la correspondiente PC se establecerá el procedimiento de entrega.

La existencia del formulario de solicitud y en general el procedimiento de solicitud de certificados a la RPP-PKI queda definido en la Política de Certificación correspondiente a cada uno de los certificados.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 32 de 85

4.2. Tramitación de las solicitudes de certificados

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.

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.

La RPP-PKI puede negarse a emitir un certificado de cualquier solicitante basándose exclusivamente en su propio criterio, sin que ello implique contraer responsabilidad alguna por las consecuencias que pudieran derivarse de tal negativa.

4.2.3. Plazo para la tramitación de las solicitudes de certificados

Las CA de la RPP-PKI no se hacen responsables de las demoras que puedan surgir en el período comprendido entre la solicitud del certificado y la entrega de este. En todo caso, se establecerán plazos mínimos para la tramitación de las solicitudes de los certificados en las PC correspondientes.

4.3. Emisión de certificados

4.3.1. Actuaciones de la CA durante la emisión del certificado

La emisión del certificado implica la autorización definitiva de la solicitud por parte de la CA. Cuando alguna de las CA de la RPP-PKI emita un certificado de acuerdo con una solicitud de certificación, efectuará las notificaciones que se establecen en el apartado 4.3.2. del presente capítulo.

Todos los certificados iniciarán su vigencia en el momento de su emisión. El periodo de vigencia estará sujeto a una posible extinción anticipada, temporal o definitiva, cuando se den las causas que motiven la suspensión o revocación del certificado.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 33 de 85

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.

4.3.2. 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.

4.4. Aceptación del certificado

4.4.1. Mecanismo de aceptación del certificado

La aceptación del certificado es la acción mediante la cual su titular inicia sus obligaciones respecto a la RPP-PKI.

Los certificados que exijan la presentación de una identificación, requerirán la aceptación explícita del titular del certificado y el reconocimiento de que está de acuerdo con los términos y condiciones contenidos en el formulario de aceptación de las condiciones de los servicios de certificación de la autoridad de certificación de la RPP-PKI, que rige los derechos y obligaciones entre la RPP-PKI y el titular, y de que éste conoce la existencia de la presente Declaración de Prácticas de Certificación, que recoge técnica y operativamente los servicios de certificación electrónica prestados por la RPP-PKI.

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

4.4.2. Publicación del certificado por la CA

Este punto no es aplicable ya que la RPP-PKI, una vez emitido el certificado, no los publica en repositorios.

4.4.3. Notificación de la emisión del certificado por la CA a otras Autoridades

Cuando alguna de las CA de la RPP-PKI emita un certificado de acuerdo con una solicitud de certificación tramitada a través de una RA, enviará una copia de este a la RA que remitió la solicitud.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 34 de 85

4.5. Par de claves y uso del certificado

4.5.1. Uso de la clave privada y del certificado por el titular

Las responsabilidades y limitaciones de uso del par de claves y del certificado se establecerán en la correspondiente PC. En cualquier caso, el titular sólo podrá utilizar la clave privada y el certificado para los usos autorizados en la PC y de acuerdo con lo establecido en los campos 'Key Usage' y 'Extended Key Usage' del certificado. Del mismo modo, el titular solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso, establecidas en la DPC y PC, y sólo para lo que éstas establezcan.

Tras la expiración o revocación del certificado, el titular dejará de usar la clave privada.

4.5.2. Uso de la clave pública y del certificado por los terceros aceptantes

Los Terceros que Confían sólo pueden depositar su confianza en los certificados para aquello que establezca la correspondiente PC y de acuerdo con lo establecido en el campo 'Key Usage' y 'Extended Key Usage' del certificado.

Los Terceros que Confían han de realizar las operaciones de clave pública de manera adecuada para confiar en el certificado, así como asumir la responsabilidad de verificar el estado del certificado utilizando los mecanismos establecidos en esta DPC y en la correspondiente PC.

Asimismo, se adhieren a las condiciones de uso establecidas en dichos documentos.

4.6. Renovación de certificados sin cambio de claves

4.6.1. Circunstancias para la renovación de certificados sin 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.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 35 de 85

4.6.2. Quién puede solicitar la renovación de los certificados sin cambio de claves

No estipulado.

4.6.3. Tramitación de las peticiones de renovación de certificados sin cambio de claves

No estipulado.

4.6.4. Notificación de la emisión de un nuevo certificado al titular

No estipulado.

4.6.5. Forma de aceptación del certificado sin cambio de claves

No estipulado.

4.6.6. Publicación del certificado sin cambio de claves por la CA

No estipulado.

4.6.7. Notificación de la emisión del certificado por la CA a otras Autoridades

No estipulado.

4.7. Renovación de certificados con cambio de claves

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.

Algunos de los motivos, entre otros, por los que se puede renovar un certificado son:

- Expiración del periodo de validez.
- Cambio de datos contenidos en el certificado.
- Claves comprometidas o pérdida de fiabilidad de estas.
- Cambio de formato.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código: P-11	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 36 de 85
------------------------	------------------------	--	------------------

Todas las renovaciones de certificados de la RPP-PKI se realizarán con cambio de claves.

4.7.2. Quién puede pedir la renovación de los certificados

En cada Política de Certificación se establecerá quien puede solicitar la renovación del certificado.

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

La CA comprobará en el proceso de renovación que la información utilizada para verificar la identidad y atributos del titular es todavía válida. Si alguna información del titular ha cambiado, ésta deberá ser verificada y registrada con el acuerdo del titular.

La identificación y autenticación para la renovación de un certificado está definida en la Política de Certificación que corresponda en cada caso, prevaleciendo siempre sobre lo estipulado en este apartado.

En cualquier caso, la renovación de un certificado está supeditada a:

- Que se solicite en debido tiempo y forma, siguiendo las instrucciones y normas que la RPP-PKI específica a tal efecto.
- Que la CA no haya tenido conocimiento cierto de la concurrencia de ninguna causa de revocación / suspensión del certificado.
- Que la solicitud de renovación de los servicios de prestación se refiera al mismo tipo de certificado emitido inicialmente.

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.

4.7.5. Forma de aceptación del certificado con las claves cambiadas

En cada PC se establecerá la forma de aceptación.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 37 de 85

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.

4.7.7. Notificación de la emisión del certificado por la CA a otras Autoridades

Cuando la CA de la RPP-PKI emita un certificado de acuerdo con una solicitud de certificación tramitada a través de una RA, enviará una copia de este a la RA que remitió la solicitud.

4.8. Modificación de certificados

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.

4.8.2. Quién puede solicitar la modificación de los certificados

Este punto no es aplicable ya que los casos de modificaciones de los certificados 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.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 38 de 85

4.8.3. Tramitación de las peticiones de modificación de certificados

No estipulado.

4.8.4. Notificación de la emisión de un certificado modificado al titular

No estipulado.

4.8.5. Forma de aceptación del certificado modificado

No estipulado.

4.8.6. Publicación del certificado modificado por la CA

No estipulado.

4.8.7. Notificación de la modificación del certificado por la CA a otras Autoridades

No estipulado.

4.9. Revocación y suspensión de certificados

4.9.1. Circunstancias para la revocación

La revocación de un certificado es el acto por el cual se invalida un certificado antes de su caducidad. El efecto de la revocación de un certificado es el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación. La revocación de un certificado impide el uso legítimo del mismo por parte del titular.

El proceso de solicitud de revocación se define en la Política de Certificación aplicable a cada tipo de certificado.

La revocación de un certificado implica su publicación en la Lista de Certificados Revocados (CRL) de acceso público. Al expirar el periodo de validez de un Certificado revocado, éste dejará de estar incluido en la CRL.

Sin perjuicio de lo dispuesto en la normativa aplicable un certificado podrá ser revocado por:



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 39 de 85

- El robo, pérdida, revelación, modificación, u otro compromiso o sospecha de compromiso de la clave privada del titular.
- El mal uso deliberado de claves y certificados, o la falta de observancia o contravención de los requerimientos operacionales contenidos en el Formulario de aceptación de las condiciones de los servicios de certificación de la autoridad de certificación de la RPP-PKI, la PC asociada o de la presente DPC.
- El titular de un certificado deja de pertenecer al grupo, circunstancia que le facultaba para la posesión del certificado.
- El cese de la actividad de la RPP-PKI.
- Emisión defectuosa de un certificado debido a que:
 - No se ha cumplido un requisito material para la emisión del certificado.
 - La creencia razonable de que un dato fundamental relativo al certificado es o puede ser falso.
 - Existencia de un error de entrada de datos u otro error de proceso.
- El par de claves generado por un titular se revela como “débil”.
- La información contenida en un certificado o utilizada para realizar su solicitud deja de ser correcta.
- Por orden formulada por el titular o por tercero autorizado.
- El certificado de una RA o CA superior en la jerarquía de confianza del certificado es revocado.
- Por la concurrencia de cualquier otra causa especificada en la presente DPC o en las correspondientes Políticas de Certificación establecidas para cada tipo de Certificado.

La revocación tiene como principal efecto sobre el certificado la terminación inmediata y anticipada del periodo de validez de este, deviniendo el certificado como no válido. La revocación no afectará a las obligaciones subyacentes creadas o comunicadas por esta DPC ni tendrá efectos retroactivos.

4.9.2. Quién puede solicitar la revocación

La RPP-PKI o cualquiera de las Autoridades que la componen pueden solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 40 de 85

compromiso de la clave privada del titular o cualquier otro hecho determinante que recomendara emprender dicha acción.

Asimismo, los titulares de certificados o sus responsables, en el caso de los certificados de componente, también podrán solicitar la revocación de sus certificados, debiendo hacerlo de acuerdo con las condiciones especificadas en el apartado 4.9.3.

La política de identificación para las solicitudes de revocación podrá ser la misma que para el registro inicial. La política de autenticación aceptará solicitudes de revocación firmadas electrónicamente por el titular del certificado, siempre que lo haga con un certificado en vigor diferente del que solicita sea revocado.

Las distintas Políticas de Certificación podrán definir otros procedimientos de identificación que sean más rigurosos.

4.9.3. 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.

De forma general y sin perjuicio de lo definido en las PC se establece que:

- Se comunicará al titular del certificado la revocación de este mediante correo electrónico.
Tras la revocación del certificado el titular deberá cesar en el uso de la clave privada que se corresponda con aquel.
- En el caso de certificados de persona natural, la revocación de un certificado de autenticación conlleva la revocación del resto de certificados asociados a un titular.
- La solicitud de revocación de un certificado recibida con posterioridad a su fecha de caducidad no será atendida.

La información a suministrar para solicitar la revocación de un certificado se establecerá a expensas de lo especificado en la correspondiente Política de Certificación.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 41 de 85

4.9.4. Periodo de gracia de la solicitud de revocación

La revocación se llevará a cabo de forma inmediata a la tramitación de cada solicitud verificada como válida. Por tanto, no existe ningún periodo de gracia asociado a este proceso durante el que se pueda anular la solicitud de revocación.

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.

4.9.6. Requisitos de verificación de las revocaciones por los terceros que confían

La verificación de las revocaciones ya sea mediante consulta directa de la CRL o protocolo OCSP, es obligatoria para cada uso de los certificados por los Terceros que Confían.

Los Terceros que Confían deberán comprobar la validez de la CRL previamente a cada uno de sus usos y descargar la nueva CRL del repositorio de la RPP-PKI al finalizar el periodo de validez de la que posean. Las listas de revocación de certificados guardadas en memoria 'caché', aun no estando caducadas, no garantizan que dispongan de información de revocación actualizada.

Opcionalmente, salvo que la PC de aplicación establezca lo contrario, se podrá recurrir a la Autoridad de Validación para verificar las revocaciones.

Cuando la PC de aplicación admita otras formas de divulgación de información de revocación, los requisitos para la comprobación de dicha información se especificarán en la propia PC.

4.9.7. Frecuencia de emisión de CRL

La RPP-PKI publicará una nueva CRL en su repositorio en el momento en que se produzca cualquier revocación. En cualquier caso, la RPP-PKI publicará una nueva CRL en su repositorio a intervalos no superiores a 24 horas para las CA Subordinadas y a un año para la CA Raíz, aunque no se hayan producido modificaciones en la CRL, es decir, aunque no se haya revocado ningún certificado desde la última publicación.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 42 de 85

4.9.8. Tiempo máximo entre la generación y la publicación de las CRL

Cada PC establecerá el tiempo máximo admisible entre la generación de la CRL y su publicación en el repositorio.

4.9.9. Disponibilidad de un sistema en línea de verificación del estado de los certificados

La RPP-PKI proporciona un servidor web donde publica las CRL para la verificación del estado de los certificados que emite. Asimismo, existe una Autoridad de Validación que, mediante el protocolo OCSP, permite verificar el estado de los certificados.

Las direcciones de acceso vía web a las CRL y a la Autoridad de Validación quedan reflejadas en el apartado 2.1. Repositorio.

4.9.10. Requisitos de comprobación en línea de revocación

En el caso de recurrir a la Autoridad de Validación, el Tercero que Confía debe disponer de un software que sea capaz de operar con el protocolo OCSP para obtener la información sobre el certificado.

4.9.11. Otras formas de divulgación de información de revocación disponibles

Algunas PC pueden admitir a otras formas de aviso de revocación, como los Puntos de Distribución de CRLs (CDP).

4.9.12. Requisitos especiales de revocación de claves comprometidas

No hay ninguna variación en las cláusulas anteriores cuando la revocación sea debida al compromiso de la clave privada.

4.9.13. Causas para la suspensión

La suspensión de la vigencia de los certificados se aplicará (en el caso de que dicha operación esté contemplada por la PC correspondiente), entre otros, en los siguientes casos:

- Cambio temporal de alguna de las circunstancias del titular del certificado que aconsejen la suspensión de los certificados mientras dure el mismo. Al retornarse a la situación inicial se levantará la suspensión del certificado. Las



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 43 de 85

características y requisitos para la suspensión se establecerán en la correspondiente Política de Certificación.

- Comunicación por el titular del certificado de un posible compromiso de sus claves. En el caso de que la sospecha, por su grado de certeza, no aconseje la revocación inmediata, se suspenderán los certificados del titular mientras se averigua el posible compromiso de las claves.

Al término del análisis se determinará si se revocan los certificados o si se levanta la suspensión.

- Resolución judicial o administrativa que lo ordene.

4.9.14. Quién puede solicitar la suspensión

La solicitud puede presentarla el titular del certificado o la persona que se establezca en la PC correspondiente.

4.9.15. Procedimiento para la solicitud de suspensión

Cada PC establecerá el procedimiento para la solicitud de suspensión.

4.9.16. Límites del periodo de suspensión

Sin perjuicio de lo definido en las Políticas de Certificación, no se establece un plazo máximo de suspensión de la vigencia de los certificados.

Si durante el tiempo de suspensión del certificado éste caduca o se solicita su revocación, se producirán las mismas consecuencias que para los Certificados no suspendidos en esos mismos casos de caducidad o revocación.

4.10. Servicios de información del estado de certificados

4.10.1. Características operativas

La RPP-PKI dispone como mínimo de dos servicios que proporcionan información sobre el estado de los certificados emitidos por su CA:

- Publicación de las listas de revocación de certificados (CRL). El acceso a las CRL se realiza vía HTTP.
- Servicio de validación en línea (Autoridad de Validación, VA) que implementa el Online Certificate Status Protocol siguiendo la RFC 2560. Mediante el uso



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 44 de 85

de este protocolo es posible obtener el estado actual de un certificado electrónico sin requerir las CRL.

4.10.2. Disponibilidad del servicio

El servicio, en sus dos variantes, está disponible de forma ininterrumpida todos los días del año, tanto para los Terceros que Confían como para los Titulares de los certificados u otras partes que los requieran.

4.10.3. Características adicionales

La RPP-PKI en ningún caso proporcionará un cliente OCSP para hacer uso del Servicio de validación en línea. Es responsabilidad de quien desee utilizar dicho servicio disponer de un Cliente OCSP que cumpla la RFC 2560.

4.11. Extinción de la validez de un certificado

La extinción de la validez de un certificado se produce en los siguientes casos:

- Revocación del certificado por cualquiera de las causas recogidas en el apartado 4.9.1.
- Expiración de la vigencia del certificado.

Si no se solicita la renovación del certificado la extinción de su validez supondrá la extinción de la relación entre el titular y la CA.

4.12. Custodia y recuperación de claves

4.12.1. Prácticas y políticas de custodia y recuperación de claves

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.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 45 de 85

4.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión

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.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 46 de 85

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, tanto interna como independiente para el seguimiento y verificación del cumplimiento de las políticas, directivas y procedimientos en materia de seguridad.

5.1. Controles físicos

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.

Los International Data Center (IDC) donde se aloja la infraestructura disponen de al menos, los siguientes elementos de seguridad física:

- Construcción anti-sísmica.
- Muros perimetrales de concreto armado.
- Generación de energía redundante (3MW).
- Sistema ininterrumpible de energía (UpS).
- Sistema de UPS redundante (625kVAs).
- Doble acometida eléctrica.
- Sistema de enfriamiento de precisión redundante.
- Sistema de detección, extinción y supresión automática de fuego.
- Sistema de detección temprana VESDA y extinción de incendios.
- Sistema de pre-acción con doble interlock.
- Sistema de monitoreo de infraestructura, edificio inteligente (BMS).
- Sistema de tierras físicas y pararrayos.
- Operaciones y seguridad ZAIT x865.
- Suministro de energía eléctrica regulada y con protección.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 47 de 85

- Plantas de emergencia.
- Sistema de aire acondicionado HVAC.
- Seguridad física 24/7 (subsistema de seguridad mediante guardias de seguridad).
- Sistema CCTV con grabación con movimiento.

5.1.2. Acceso físico

La infraestructura de la PKI está físicamente separada de cualquier otro sistema y su acceso dispone de varios niveles de control. Todas las operaciones sensibles se realizan dentro de un recinto físicamente seguro que posee al menos, dos de los siguientes tres requisitos de acceso:

- Tarjeta de proximidad.
- Lectura biométrica.
- Contraseña de acceso.

Las áreas de carga y descarga están aisladas y permanentemente vigiladas por medios humanos y técnicos.

5.1.3. Alimentación eléctrica y aire acondicionado

- Suministro eléctrico:
 - PDU redundadas.
 - Dispone de grupos electrógenos, redundados para aquellas circunstancias en las que se presente un déficit en la generación eléctrica o sean frecuentes y/o prolongados los cortes en el suministro eléctrico.
 - UPS: permite mantener la alimentación ininterrumpida mediante baterías cuando falla el suministro o se produce una anomalía. Alta disponibilidad y redundancia de los equipos.
 - Doble acometida eléctrica para los equipos.
- Aire acondicionado:
 - Sistema de enfriamiento de precisión redundante.
 - Sistema de aire acondicionado HVAC.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 48 de 85

5.1.4. Exposición al agua

- Sistemas de control de humedad y temperatura, monitorizado a tiempo real.
- Sistemas de drenaje y piso elevado.

5.1.5. Prevención y protección frente a incendios

Las salas donde se ubican los activos de la infraestructura de la PKI del Registro Público de Panamá disponen de los medios adecuados – varios niveles de sistemas automáticos de detección y extinción de incendios- para la protección de su contenido contra incendios.

El cableado se encuentra en suelo o techo falso y se dispone de los medios adecuados - detectores en suelo y techo- para la protección de este contra incendios.

5.1.6. Sistema de almacenamiento

La información se dispone en medios de forma segura, según la clasificación de la información en ellas contenidas. Los sistemas de almacenamiento se encuentran en diferentes locaciones, para eliminar el riesgo asociado a una única ubicación.

5.1.7. Eliminación de residuos

Se ha adoptado una política de gestión de residuos que garantiza el almacenamiento seguro de cualquier material que pudiera contener información, así como una política de gestión de los soportes removibles.

5.1.8. Copias de seguridad fuera de las instalaciones

Se dispondrá al menos de una copia en un lugar seguro, fuera de los Centros de Proceso de Datos de la PKI.

5.2. Controles de procedimiento

Por razones de seguridad, la información relativa a los controles de procedimiento se considera material confidencial y sólo se incluye una parte de esta.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 49 de 85

La RPP-PKI procura que toda la gestión, tanto la relativa a los procedimientos operacionales como a la de administración, se lleve a cabo de forma segura, conforme a lo establecido en este documento, realizando auditorías periódicas.

Asimismo, se ha diseñado una segregación de funciones, para evitar que una sola persona pueda conseguir el control total de la infraestructura.

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

Se distinguen los siguientes responsables para el control y gestión del sistema:

5.2.1.1. Roles de gestión de los módulos de seguridad hardware (HSM)

- **Administrador de Seguridad:** Tienen la facultad de realizar las operaciones de administración del HSM, como son la re-inicialización del HSM, la gestión de las políticas del HSM, la creación o eliminación de una partición (en la creación se genera una llave de Operador de Partición) o el reemplazo de la llave del Operador de Partición asignado a una partición.
- **Administrador del Dominio:** Su responsabilidad será la realización de backups, recuperación de HSM e incorporación de nuevos HSM al Dominio de Claves.
- **Operador de la Partición:** Serán responsables de la gestión de la partición creada en el HSM a todos los niveles; gestión de las políticas de la partición, gestión de objetos en la partición y control de acceso a la partición por parte de las aplicaciones. Serán quienes permitan el acceso al HSM para aquellas aplicaciones cuyas claves estén custodiadas en el HSM, controlando así el acceso al mismo.
- **Operador de Acceso Remoto:** Serán los responsables de permitir el acceso a la administración remota del HSM (desde la oficina de DNFE), de modo que sea posible el acceso a los servicios y herramientas de administración sin tener que hacerlo directamente en los IDC.

5.2.1.2. Roles de gestión de la RPP-PKI

- **Oficiales de Seguridad:** Los usuarios pertenecientes a este grupo tienen la responsabilidad global de administrar la implementación de las políticas y prácticas de seguridad.
- **Administradores de Sistema:** Conjunto de usuarios autorizados a realizar ciertas tareas relacionadas con la instalación, configuración y mantenimiento



REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código: P-11	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 50 de 85
------------------------	------------------------	--	------------------

de las entidades de la PKI, pero con acceso limitado a la información relacionada con los parámetros de seguridad.

- **Audidores de Sistema:** Autorizados a consultar archivos, trazas y logs de auditoría de las entidades de la PKI.
- **Oficiales de Registro:** Son los responsables de gestionar la generación/revocación de los certificados. En particular, se definen roles con accesos limitados a los tipos de certificados que puede gestionar:
 - **Operadores de Registro de Dispositivos:** Responsables de gestionar los certificados de dispositivos emitidos por la RPP-PKI.
 - **Operadores de Registro de Personas:** Responsables de gestionar los certificados personales emitidos por la RPP-PKI.

5.2.2. Número de personas requeridas por tarea

Se requiere un mínimo de dos personas para realizar operaciones sobre la RPP-PKI, a excepción de las tareas de gestión de ciclo de vida de certificados de entidades finales, permitidas a un único Operador.

5.2.3. Roles que requieren segregación de funciones

Entre los roles se establecen las siguientes incompatibilidades, de forma que un usuario no pueda tener dos roles marcados como “incompatibles”:

- Incompatibilidad entre el rol auditor (Auditor de Sistema) y cualquier otro rol.
- Incompatibilidad entre los roles administrativos (Oficial de Seguridad y Administrador de Sistemas; Administrador de Sistemas y Oficial de Registro).
- Incompatibilidad entre los roles de gestión de la PKI y los Operadores de la Partición del HSM.

5.3. Controles de personal

5.3.1. Requisitos relativos a la cualificación, conocimiento y experiencia profesionales

El personal que ejecuta tareas de confianza en la RPP-PKI, debe poseer cualificación y experiencia en entornos de servicios de certificación e infraestructura de clave pública. Adicional, el personal debe cumplir con los requerimientos de seguridad dispuestos en la Política de Seguridad de la Información y poseer:



REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 51 de 85

- Nociones y experiencia en firma y certificados electrónicos.
- Formación específica para la función que desempeña.
- Título académico o experiencia equivalente.

5.3.2. Procedimientos de comprobación de antecedentes

La DNFE debe contar con procedimientos para verificar la cualificación y experiencia del personal que ejecuta tareas de confianza, a través de la Oficina Institucional de Recursos Humanos del Registro Público de Panamá. El procedimiento debe incluir:

- Confirmación de empleos anteriores.
- Título académico y cursos obtenidos.
- Verificación de conocimientos específicos.

5.3.3. Requerimientos de formación

El personal de la DNFE debe estar sujeto a una formación específica, incluida en el Plan Anual de Capacitación del Registro Público de Panamá. La información debe incluir:

- Conceptos básicos de PKI.
- Seguridad lógica y física de la operación.
- Servicios prestados por la Autoridad de Certificación.
- Aspectos legales relativos a la prestación de servicios de certificación.
- Declaración de Prácticas de Certificación.
- Procedimientos de operación, administración y mantenimiento para cada rol específico.
- Gestión de incidencias.
- Procedimientos para la recuperación de la operación en caso de desastres, para cada rol específico.

5.3.4. Requerimientos y frecuencia de actualización de la formación

Se proveerá formación al personal de la DNFE ante cambios tecnológicos o en los sistemas de seguridad, introducción de nuevas herramientas, modificación de



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 52 de 85

procedimientos operativos, cambios en la DPC u otros documentos relacionados al funcionamiento, administración y/o gestión de la RPP-PKI.

5.3.5. Frecuencia y secuencia de rotación de tareas

La DNFE efectuará rotaciones de trabajo entre los distintos roles, con el objetivo de incrementar la seguridad y garantizar la continuidad, en caso de ausencia de alguno de los trabajadores de la DNFE.

Antes de asumir las nuevas funciones, el personal debe recibir una capacitación y/o actualización de acuerdo con el rol específico, que le permita cumplir con las tareas satisfactoriamente.

5.3.6. Sanciones por actuaciones no autorizadas

Las prácticas que deben cumplir el personal de la DNFE y el procedimiento sancionador que incumplan las mismas, son recogidas en el Reglamento Interno del RPP y la Resolución de RPP No. 27-2013.

5.3.7. Requisitos de contratación de terceros

La DNFE puede contratar personal externo, consultores o terceros, solamente si existe una relación claramente definida con el contratista y bajo las siguientes condiciones:

- Existe un contrato con cláusulas propias de los roles de gestión y estipula sanciones para las actuaciones no autorizadas.
- No posee personal disponible para los roles de gestión contratados.
- Los contratistas cumplen con los mismos requisitos expuestos en el punto 5.3.1.
- Finalizados los servicios, se dará de baja al usuario y se le revocarán los accesos.

5.3.8. Documentación proporcionada al personal

La DNFE proporciona al personal toda la documentación y buenas prácticas de seguridad de la información necesarias para el correcto desempeño de sus tareas.

Entre la documentación se encuentran:



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 53 de 85

- Declaración de Prácticas de Certificación.
- Procedimientos de instalación, operación, mantenimiento y gestión de la RPP-PKI de acuerdo con el rol específico.
- Política de Seguridad de la Información.
- Modelo de Gobierno.
- Continuidad del negocio.
- Gestión de incidencias.
- Otros que se consideren necesario.

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipos de eventos registrados

La RPP-PKI posee mecanismos para registrar, entre otros, los siguientes tipos de eventos:

- El acceso (logon) a las herramientas de gestión de los componentes de la PKI.
- La solicitud de emisión, renovación y/o revocación de certificados, por parte de las Autoridades de Certificación, registrando tanto el tipo de acción a realizar y sus parámetros, como la identificación de la aplicación, administrador u operador de registro que solicita la acción.
- Las acciones realizadas por los elementos de la PKI. Entre ellas:
 - La generación o revocación de certificados.
 - La actualización de CRL y su publicación en los repositorios.
- Arranque y parada de los servicios online de los componentes de la PKI.
- Los avisos (warnings) y errores producidos en el procesado de una petición de certificación. Asimismo, se registrarán los avisos (warnings) y errores producidos por mecanismos internos de la CA (tales como publicación de certificados y CRL).
- Los intentos de acceso no autorizado a los componentes de la PKI, indicando la identificación de la persona que está realizando el intento.

En cada evento se registrará:



REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 54 de 85

- El tipo de evento registrado.
- La fecha y hora en que se ha producido.
- La identificación del usuario o componente de la PKI que solicitó la acción que provocó el evento.
- El rol con el que actuó el usuario o componente de la PKI que solicitó la acción que provocó el evento.
- El resultado de la acción que provocó el evento.
- La descripción de la acción realizada.
- Los parámetros (contenido) de la solicitud de la acción que provocó el evento.

Toda esta información puede ser consultada:

- A través de las Consolas de Gestión de los componentes de la PKI, para lo cual deberá autenticarse como Auditor del Sistema.
- A través de la Consola de Administración del Colector centralizado de Eventos, accediendo con un usuario con permisos suficientes.

5.4.2. Frecuencia de procesamiento de registros de auditoría

Los registros se analizarán periódicamente, en las auditorías periódicas de la PKI, y de manera manual cuando sea necesario.

5.4.3. Periodo de conservación de los registros de auditoría

La información generada en los registros de eventos se conserva:

- En la base de datos de la PKI, durante todo el periodo de vida de la PKI.
- En el sistema Colector de Eventos, de modo que sea accesible online durante 30 días y durante todo el periodo de vida de la PKI por medio de backups.

5.4.4. Protección de los registros de auditoría

La información de los registros de eventos se encuentra protegida por mecanismos de firma y cifrado en la BBDD. Las características de este sistema son las siguientes:

- Permite verificar la integridad de la base de datos, es decir, detecta una posible manipulación fraudulenta de los datos.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 55 de 85

- Asegura el no repudio por parte de los autores de las operaciones realizadas sobre los datos. Esto se consigue mediante las firmas electrónicas.
- Guarda un registro histórico de actualización de datos, es decir, almacena versiones sucesivas de cada registro resultante de diferentes operaciones realizadas sobre él. Esto permite guardar un registro de las operaciones realizadas y evita que se pierdan firmas electrónicas realizadas anteriormente por otros usuarios cuando se actualizan los datos.

5.4.5. Procedimientos de respaldo de los registros de auditoría

RPP-PKI garantiza que en todo momento existirá una copia de seguridad de los registros de auditoría de la PKI.

5.4.6. Notificación al sujeto causa del evento

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.

5.4.7. Análisis de vulnerabilidades

La tecnología KeyOne de Safelayer dispone de mecanismos de comprobación de la integridad de los ficheros binarios y de funcionamiento de los sistemas de gestión de certificados. Se basa en la necesidad de que estos ficheros vayan firmados mediante un certificado de firma de código que emite expresamente Safelayer para el Ministerio de Defensa. Cualquier fichero que no sea firmado con este certificado será descartado. El Órgano de Obtención e Implantación será el encargado de custodiar este certificado.

Por otra parte, en el registro de eventos quedarán registrados los intentos de acceso no autorizado a los componentes de PKIFAS, indicando la identificación de la persona que está realizando el intento.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 56 de 85

5.5. Archivado de registros

5.5.1. Tipo de eventos archivados

La PKI del Registro Público de Panamá conserva toda la información relevante sobre las operaciones realizadas con los certificados durante los periodos de tiempo establecidos, incluyendo en este ámbito:

- Datos relativos a los procedimientos de preinscripción, inscripción y emisión de los certificados.
- Datos relativos a los cambios de estado de certificados (suspensión, revocación, etc...)
- Datos relativos a las consultas efectuadas en las Autoridad de Validación y los sellos de tiempo emitidos por la Autoridad de Sello de Tiempo.

5.5.2. Periodo de conservación de registros

Toda la información y documentación relativa a los certificados se conservarán durante un mínimo de 7 años.

5.5.3. Protección del archivo

Los eventos de aplicativos están protegidos de forma que nadie, salvo las propias aplicaciones de visualización, con su debido control de accesos, pueda acceder a ellos. Así mismo, la documentación en papel que se genere con motivo de los procedimientos de la PKI será almacenada de forma segura en las instalaciones de la Dirección Nacional de Firma Electrónica.

5.5.4. Procedimientos de copia de respaldo del archivo

Las copias de respaldo de los archivos se realizan según los procedimientos estándar de respaldo de la Dirección Nacional de Firma Electrónica.

5.5.5. Requerimientos para el sellado de tiempo de los registros

RPP-PKI garantiza el registro del tiempo en que se crean los archivos. El instante de tiempo de los sistemas proviene de una fuente segura que constata la fecha y hora. La fuente de tiempos utilizada, basada en el protocolo NTP, proviene del Centro Nacional de Metrología de Panamá (CENAMEP).



REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 57 de 85

5.5.6. Sistema de archivo de información (interno vs externo)

Todo el archivado de información se realiza de forma interna a la PKI del Registro Público de Panamá.

5.5.7. Procedimientos para obtener y verificar información archivada

Los eventos registrados están protegidos mediante técnicas criptográficas, de forma que nadie salvo las propias aplicaciones de visualización y gestión de eventos pueda acceder a ellos. Sólo el personal autorizado tiene acceso a los archivos físicos de soportes y archivos informáticos, para llevar a cabo verificaciones de integridad u otras.

Esta verificación debe ser llevada a cabo por el Auditor, que debe tener acceso a las herramientas de verificación y control de integridad del registro de eventos de la PKI.

5.6. Cambio de claves

Los procedimientos para proporcionar, en caso de cambio de claves, una nueva clave pública de CA a los titulares y terceros aceptantes de los certificados de esta son los mismos que para proporcionar la clave pública en vigor. En consecuencia, la nueva clave se publicará en el repositorio de RPP-PKI.

5.7. Recuperación ante compromiso de clave o catástrofe

5.7.1. Procedimientos de gestión de incidentes y compromisos

El Prestador de Servicios de Certificación tiene establecido un Plan de Contingencia que define las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación prestados por su PKI.

El Plan de Contingencias contempla, entre otros aspectos, los siguientes:

- La redundancia de los componentes más críticos.
- La puesta en marcha de un centro de respaldo alternativo.
- El chequeo completo y periódico de los servicios de copia de respaldo.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 58 de 85

En el caso de que se produjera un compromiso de los datos de verificación de firma de alguna Autoridad de Certificación, RPP-PKI informará a todos los titulares de certificados de su PKI y terceros que confían conocidos de que todos los certificados y listas de revocación de certificados firmados con estos datos ya no son válidos. Tan pronto como sea posible se procederá al restablecimiento del servicio.

5.7.2. Alteración de los recursos hardware, software y/o datos

Si los recursos hardware, software, y/o datos se alteran o se sospecha que han sido alterados se detendrá el funcionamiento de la PKI hasta que se restablezca la seguridad del entorno con la incorporación de nuevos componentes cuya adecuación pueda acreditarse. De forma simultánea se realizará una auditoría para identificar la causa de la alteración y asegurar que no vuelva a producirse.

En el caso de verse afectados certificados emitidos, se notificará del hecho a los usuarios de estos y se procederá a una nueva certificación.

5.7.3. Procedimiento de actuación ante el compromiso de la clave privada de una Autoridad

En el caso de compromiso de la clave privada de una Autoridad se procederá a su revocación inmediata. Seguidamente, se generará y publicará la correspondiente CRL, cesando el funcionamiento de actividad de la Autoridad y se procederá a la generación, certificación y puesta en marcha de una nueva Autoridad con la misma denominación que la eliminada y con un nuevo par de claves.

En el caso de que la Autoridad afectada sea una CA, el certificado revocado de la misma permanecerá accesible en el repositorio de RPP-PKI con objeto de continuar verificando los certificados emitidos durante su periodo de funcionamiento.

Se notificará a todas las Autoridades afectadas que los certificados y la información sobre su revocación, suministrada con la clave comprometida de la CA, deja de ser válida desde el momento de la notificación, debiendo utilizar para verificar la validez de la información la nueva clave pública de la CA. Dichas Autoridades deberán solicitar un nuevo certificado a la CA una vez que ésta última disponga de un nuevo par de claves.



REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 59 de 85

Los certificados firmados por Autoridades dependientes de la CA afectada en el período comprendido entre el compromiso de la clave y la revocación del certificado correspondiente, serán a su vez revocados, informados sus titulares de tal hecho y se procederá a la emisión de nuevos certificados.

5.7.4. Instalación después de un desastre natural u otro tipo de catástrofe

El sistema de Autoridades de Certificación de RPP-PKI puede ser reconstruido en caso de desastre. Para llevar a cabo esta reconstrucción es necesario contar con:

- Un sistema con hardware, software y dispositivo Hardware Criptográfico de Seguridad similar al existente con anterioridad al desastre.
- Las claves de administrador de todas las Autoridades de Certificación de RPP-PKI.
- Una copia de respaldo de los discos del sistema anterior al desastre.

Con estos elementos es posible reconstruir el sistema tal y como estaba en el momento de la copia de respaldo realizada y, por lo tanto, recuperar la CA, incluidas sus claves privadas.

El almacenado, tanto de las tarjetas de acceso de los administradores de las CA como de las copias de los discos de sistema de cada CA, se lleva a cabo en un lugar diferente, lo suficientemente alejado y protegido como para dificultar al máximo la concurrencia de catástrofes simultáneas en los sistemas en producción y en los elementos de recuperación.

5.8. Cese de una CA o RA

5.8.1. Autoridad de Certificación

En el caso de cese de actividad de alguna de las CA del Registro Público de Panamá, la Dirección Nacional de Firma Electrónica comunicará a cada firmante, con un mínimo de noventa días de anticipación a la fecha de la cesación efectiva de actividades su intención de finalización de prestación de servicio. En dicha notificación se especificará la fecha de la cesación efectiva de actividades, así como los motivos por los cuales se procede a tal cese.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 60 de 85

Asimismo, los certificados que continúen vigentes podrán ser transferidos a otro prestador de servicios de certificación, previo consentimiento del firmante y por cuenta del prestador de servicios de certificación o en caso contrario, serán revocados.

Si al momento del cese de actividades por parte de RPP-PKI el certificado electrónico calificado de un firmante tiene una vigencia pendiente de uso superior a seis meses, el Registro Público de Panamá le reembolsará el importe de la tarifa proporcional a la vigencia no utilizada a menos que dicho certificado haya sido transferido a otro Prestador de Servicios de Certificación.

5.8.2. Autoridad de Registro

Una vez que la Autoridad de Registro cese en el ejercicio de las funciones, transferirá los registros que mantenga a RPP-PKI, mientras exista la obligación de mantener archivada la información, y de no ser así, ésta será destruida.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 61 de 85

6. CONTROLES DE SEGURIDAD TÉCNICA

En el ámbito de la presente DPC se especificarán los detalles concernientes a las claves de las autoridades de certificación. Los detalles relativos a las claves de los titulares de los certificados se podrán consultar en la Política de Certificación que corresponda en función del tipo de certificado.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

Los pares de claves para los componentes internos de RPP-PKI, concretamente CA Raíz y las CA Subordinadas, se generan en módulos de hardware criptográficos con certificación FIPS 140-2 Nivel 3 que tienen instalados en sus respectivos sistemas. Los sistemas de hardware y software que se emplean son conformes a las normas CWA 14167-1 y CWA 14167-2.

Los pares de claves para el resto de los titulares se generan en función de lo estipulado en la Política de Certificación aplicable a cada certificado.

Los dispositivos hardware o software que se utilizan en la generación de claves para cada tipo de certificado emitido por RPP-PKI vienen definidos por la Política de Certificación que le sea de aplicación.

6.1.2. Entrega de la clave privada al titular

El método de entrega de la clave privada a sus titulares depende de cada certificado y será establecido en la Política de Certificación correspondiente a cada certificado.

6.1.3. Entrega de la clave pública al emisor del certificado

El método de entrega de la clave pública al emisor en los casos en que la genere el Titular dependerá de cada certificado y será establecido en la Política de Certificación correspondiente.

6.1.4. Entrega de la clave pública de la CA a los terceros que confían

La clave pública de las CA de RPP-PKI está a disposición de los terceros aceptantes en el Repositorio de RPP-PKI (ver apartado 2.1) sin perjuicio de que una PC pueda establecer mecanismos adicionales de entrega de dichas claves.



REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 62 de 85

6.1.5. Tamaño de las claves

El tamaño de las claves de la Autoridad Certificadora de Panamá es de 4096 y el de las CA de Gobierno y CA Panama Clase 2 es de 2048 bits.

El tamaño de las claves para cada tipo de certificado emitido por RPP-PKI viene definido por la Política de Certificación que le sea de aplicación.

6.1.6. Parámetros de generación de la clave pública y verificación de la calidad

La clave pública de la CA de RPP-PKI está codificada de acuerdo con RFC 3280 y PKCS#1. El algoritmo de generación de claves es RSA.

Los parámetros de generación de claves para cada tipo de certificado emitido por RPP-PKI vienen definidos en la Política de Certificación que le sea de aplicación.

Los procedimientos y medios de comprobación de la calidad de los parámetros de generación de claves para cada tipo de certificado emitido por RPP-PKI vienen definidos por la Política de Certificación que le sea de aplicación.

6.1.7. Usos admitidos de la clave (campo KeyUsage de X.509 v3)

Los usos admitidos de la clave para cada tipo de certificado emitido por RPP-PKI vienen definidos por la Política de Certificación que le sea de aplicación.

Todos los certificados emitidos por RPP-PKI contienen la extensión Key Usage definida por el estándar X.509 v3, la cual se califica como crítica. Asimismo, pueden establecerse limitaciones adicionales mediante la extensión Extended Key Usage.

Ha de tenerse en cuenta que la eficacia de las limitaciones basadas en extensiones de los certificados depende, en ocasiones, de la operatividad de aplicaciones informáticas que no han sido fabricadas ni controladas por RPP-PKI.

6.2. Protección de la clave privada y controles de ingeniería de los módulos

6.2.1. Estándares para los módulos criptográficos

Los módulos utilizados para la creación de claves utilizadas por las CA de RPP-PKI cumplan con la certificación FIPS 140-2 de nivel 3.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 63 de 85

La puesta en marcha de cada una de las Autoridades de Certificación, teniendo en cuenta que se utiliza un módulo Criptográfico de seguridad (HSM), conlleva las siguientes tareas:

- Inicialización del estado del módulo HSM.
- Creación de las claves de los
 - Oficiales de Seguridad
 - Oficiales de Dominio
 - Operadores de la Partición
 - Operadores de Acceso Remoto
- Generación de las claves de la CA.

RPP-PKI utiliza módulos criptográficos hardware y software disponibles comercialmente desarrollados por terceros. RPP-PKI únicamente utiliza módulos criptográficos con certificación FIPS 140-2 Nivel 3.

6.2.2. Control multipersona (k de n) de la clave privada

La clave privada de las CAs de RPP-PKI se encuentra bajo control multipersona. Ésta se activa mediante la inicialización del software de CA por medio de la combinación mínima de operadores de la CA correspondiente. Éste es el único método de activación de dicha clave privada.

Son necesarios 2 operadores de RPP-PKI, de un total de 5, para activar y usar la clave privada de la dichas CAs.

6.2.3. Custodia de la clave privada

Las claves privadas de las Autoridades de Certificación que componen RPP-PKI se encuentran alojadas en dispositivos de hardware criptográfico con certificación FIPS-2 de nivel 3 asociadas a las distintas CAs.

6.2.4. Copia de seguridad de la clave privada

Las claves privadas de las CAs de RPP-PKI están archivadas bajo la protección de dispositivos seguros con características similares a las de los HSM y a los que sólo los oficiales de seguridad, oficiales de dominio y operadores de la partición participando conjuntamente tienen acceso.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 64 de 85

6.2.5. Archivado de la clave privada

Las claves privadas nunca serán archivadas para garantizar el no repudio.

6.2.6. Transferencia de la clave privada a o desde el módulo criptográfico

La transferencia de la clave privada sólo se puede hacer entre módulos criptográficos (HSM) y requiere de la intervención de, al menos, 2 de los 9 oficiales de seguridad, 2 de los 5 oficiales de dominio y 2 de los 5 operadores de la partición.

6.2.7. Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas se generan en el módulo criptográfico en el momento de la creación de cada una de las Autoridades de RPP-PKI que hacen uso de dichos módulos y se guardan cifradas.

6.2.8. Método de activación de la clave privada

Tal y como se estipula en el apartado 6.2.1.2 Control multipersona de la clave privada, la clave privada tanto de las CAs de RPP-PKI, se activa mediante la inicialización del software de CA por medio de la combinación mínima de operadores de la CA correspondiente.

Éste es el único método de activación de dicha clave privada.

Concretamente, son necesarios 2 operadores de la partición de RPP-PKI para activar la clave privada de cualquiera de las CAs.

6.2.9. Método de desactivación de la clave privada

El Administrador de Sistemas designado por RPP-PKI puede proceder a la desactivación de la clave de las Autoridades de Certificación de RPP-PKI mediante la parada de la aplicación informática de la CA correspondiente.

6.2.10. Método de destrucción de la clave privada

En el caso de los certificados de personas como se establezca en la PC correspondiente.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 65 de 85

6.2.11. Clasificación de los módulos criptográficos

Los módulos criptográficos utilizados cumplen el estándar FIPS 140-2 nivel 3.

6.3. Otros aspectos de la gestión del par de claves

6.3.1. Archivo de la clave pública

RPP-PKI mantiene un archivo de todos los certificados, los cuales incluyen las claves públicas, emitidos por un periodo de, al menos, siete (7) años. El control de dicho registro está a cargo de los Administradores de cada una de las CAs de RPP-PKI.

El archivo dispone de medios de protección frente a las manipulaciones que pretendan efectuarse sobre la información contenida.

6.3.2. Periodos operativos de los certificados y periodo de uso para el par de claves

El certificado y el par de claves de la Autoridad Certificadora de Panamá tienen una validez de cuarenta (40) años y los de las CA de Gobierno de Panamá y CA Panamá Clase 2 de veinte (20) años.

El periodo de validez del resto de certificados vendrá establecido por la Política de Certificación que corresponda.

6.4. Datos de activación

6.4.1. Generación e instalación de los datos de activación

Para la instauración de una Autoridad de Certificación se deben crear tarjetas criptográficas, que servirán para actividades de recuperación y funcionamiento. La CA opera con cuatro tipos de roles, cada uno con sus correspondientes tarjetas criptográficas:

- Tarjetas de Oficiales de Seguridad
- Tarjetas de Oficiales de Dominio
- Tarjetas de Operadores de la Partición.
- Tarjetas de Operadores de Acceso Remoto.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 66 de 85

Si una o más tarjetas se pierden o dañan, o el administrador olvida su PIN o dejan de ser utilizables por alguna razón, deberá volverse a generar todo el conjunto de tarjetas tan pronto como sea posible utilizando la totalidad de tarjetas de seguridad.

6.4.2. Protección de los datos de activación

Sólo el personal autorizado, en este caso los operadores de la partición correspondientes a cada CA, posee las tarjetas criptográficas con capacidad de activación de las CA y conoce los PIN y contraseñas para acceder a los datos de activación.

6.4.3. Otros aspectos de los datos de activación

No estipulado.

6.5. Controles de seguridad informática

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos, como en el caso de auditorías externas o internas e inspecciones.

6.5.1. Requerimientos técnicos de seguridad específicos

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos.

6.5.2. Evaluación de la seguridad informática

RPP-PKI evalúa de forma permanente su nivel de seguridad de cara a identificar posibles debilidades y establecer las correspondientes acciones correctoras mediante auditorías externas e internas, así con la realización continua de controles de seguridad.

6.6. Controles de seguridad del ciclo de vida

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 67 de 85

6.6.1. Controles de desarrollo de sistemas

Los requisitos de seguridad son exigibles, desde su inicio, tanto en la adquisición de sistemas informáticos como en el desarrollo de estos ya que puedan tener algún impacto sobre la seguridad de RPP-PKI.

6.6.2. Controles de gestión de seguridad

RPP-PKI mantiene un inventario de todos los activos informáticos y realizará una clasificación de estos de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración de los sistemas se audita de forma periódica y se realiza un seguimiento de las necesidades de capacidad.

6.6.3. Controles de seguridad del ciclo de vida

Existen controles de seguridad a lo largo de todo el ciclo de vida de los sistemas con algún impacto en la seguridad de RPP-PKI.

6.7. Controles de seguridad de la red

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos.

6.8. Sellado de tiempo

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”



REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 68 de 85

7. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

7.1. Perfil de certificado

7.1.1. Número de versión

RPP-PKI soporta y utiliza certificados X.509 versión 3 (X.509 v3)

7.1.2. Extensiones del certificado

Las extensiones utilizadas de forma genérica en los certificados son:

- KeyUsage. Calificada como crítica.
- BasicConstraints. Calificada como crítica.
- CertificatePolicies. Calificada como no crítica.
- SubjectAlternativeName. Calificada como no crítica.
- CRLDistributionPoint. Calificada como no crítica.

Las Políticas de Certificación de RPP-PKI pueden establecer variaciones en conjunto de las extensiones utilizadas por cada tipo de certificado.

RPP-PKI tiene definida una política de asignación de OID dentro de su rango privado de numeración por la cual el OID de todas las Extensiones propietarias de Certificados de DNFE comienzan con el prefijo 2.16.591.1.

7.1.3. Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos: SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)

7.1.4. Formatos de nombres

Los certificados emitidos por RPP-PKI contienen el distinguished name X.500 del emisor y del titular del certificado en los campos issuer name y subject name respectivamente.

7.1.5. Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500, que son únicos y no ambiguos.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 69 de 85

7.1.6. Identificador de objeto (OID) de la Política de Certificación

A definir en cada Política de Certificación.

RPP-PKI tiene definida una política de asignación de OID dentro de su rango privado de numeración por la cual el OID de todas las Políticas de Certificación de RPP-PKI comienzan con el prefijo 2.16.591.1.2

7.1.7. Uso de la extensión “PolicyConstraints”

La extensión Policy Constrains del certificado raíz de la AC no es utilizado.

7.1.8. 7.1.8 Sintaxis y semántica de los “PolicyQualifier”

La extensión Certificate Policies contiene los siguientes Policy Qualifiers:

- URL CPS: contiene la URL, la DPC y la PC que rigen el certificado.
- Notice Reference: Nota de texto que se despliega en la pantalla, a instancia de una aplicación o persona, cuando un tercero verifica el certificado.

En el campo Notice Reference se incluirá un texto con información básica sobre el certificado y las políticas a que está sujeto.

7.1.9. Tratamiento semántico para la extensión crítica “Certificate Policy”

La extensión será calificada como nonCritical cuando se emplee con el objeto de mantener la máxima capacidad de poder operar con otras CA del certificado. Esto se hace siguiendo las recomendaciones para aplicaciones estándar de correo electrónico seguro S/MIME [RFC 2632] y autenticación web SSL/TLS [RFC 2246]. El hecho de que la extensión no sea crítica no impide que las aplicaciones utilicen la información contenida en la citada extensión.

7.2. Perfil de CRL

7.2.1. Número de versión

RPP-PKI utiliza CRLs versión 2 (v2).

7.2.2. CRL y extensiones

RPP-PKI soporta y utiliza CRLs conformes al estándar X.509.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 70 de 85

7.3. Perfil de OCSP

7.3.1. Número(s) de versión

El perfil es el definido en la RFC 2560.

7.3.2. Extensiones OCSP

La Autoridad de Validación soporta peticiones firmadas y la extensión NONCE.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 71 de 85

8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

8.1. Frecuencia o circunstancias de los controles para cada Autoridad

Se llevará a cabo una auditoría externa sobre RPP-PKI de forma regular una vez al año. Con ello se garantiza la adecuación de su funcionamiento y operativa con las estipulaciones incluidas en esta DPC y las PC.

8.2. Identificación/cualificación del auditor

Las auditorías serán realizadas por empresas auditoras externas. Todo equipo o persona designada para realizar una auditoría de seguridad sobre RPP-PKI deberá cumplir los siguientes requisitos:

- Adecuada capacitación y experiencia en PKI, seguridad, tecnologías criptográficas y procesos de auditoría.
- Independencia a nivel organizativo de la autoridad de RPP-PKI.

8.3. Relación entre el auditor y la Autoridad auditada

Al margen de la función de auditoría, el auditor externo y la parte auditada (RPP-PKI) no deberán tener relación alguna que pueda derivar en un conflicto de intereses.

8.4. Aspectos cubiertos por los controles

La auditoría determinará la adecuación de los servicios de RPP-PKI con esta DPC y las PC aplicables. También determinará los riesgos del incumplimiento de la adecuación con la operativa definida por esos documentos.

El ámbito de actividad de una auditoría incluirá, al menos a:

- Política de seguridad y privacidad
- Seguridad física
- Evaluación tecnológica
- Administración de los servicios de la CA



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 72 de 85

- Selección de personal
- DPC y PC competentes
- Contratos

8.5. Acciones a tomar como resultado de la detección de deficiencias

La identificación de deficiencias detectadas como resultado de la auditoría dará lugar a la adopción de medidas correctivas. La Autoridad de Aprobación de Políticas (AAP), en colaboración con el auditor, será la responsable de la determinación de estas.

En el caso de observarse deficiencias graves la Autoridad de Aprobación de Políticas podrá adoptar, entre otras, las siguientes decisiones: suspensión temporal de las operaciones hasta que las deficiencias se corrijan, revocación del certificado de la Autoridad, cambios en el personal implicado, invocación de la política de responsabilidades y auditorías globales más frecuentes.

8.6. Comunicación de resultados

El equipo auditor comunicará los resultados de la auditoría a la Autoridad de Aprobación de Políticas de RPP-PKI (AAP), al Gestor de Seguridad de RPP-PKI, así como a los administradores de RPP-PKI y de la Autoridad en la que se detecten incidencias.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 73 de 85

9. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

9.1. Tarifas

9.1.1. Tarifas de emisión de certificado o renovación

Las tarifas de emisión y renovación de cada certificado se especifican en la Política de Certificación que le sea de aplicación.

9.1.2. Tarifas de acceso a los certificados

Las tarifas de acceso a los certificados se especifican en la Política de Certificación que les sea de aplicación.

9.1.3. Tarifas de acceso a la información de estado o revocación

Las tarifas de acceso a la información de estado o revocación de cada certificado se especifican en la Política de Certificación que le sea de aplicación.

9.1.4. Tarifas de otros servicios tales como información de políticas

No se aplicará ninguna tarifa por el servicio de información sobre esta DPC, ni las políticas de certificación administradas por RPP-PKI, ni por ningún otro servicio adicional del que se tenga conocimiento en el momento de la elaboración del presente documento.

Esta disposición podrá ser modificada por la Política de Certificación aplicable en cada caso.

9.1.5. Política de reembolso

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



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 74 de 85

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

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 N° 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 N° 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

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 en 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



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 75 de 85

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.

9.3.1. Ámbito de la información confidencial

Toda información que no sea considerada por el Registro Público de Panamá como pública revestirá el carácter de confidencial. Se declara expresamente como información confidencial:

- Las claves privadas de las Autoridades que componen RPP-PKI.
- La información relativa a las operaciones que lleve a cabo RPP-PKI.
- La información referida a los parámetros de seguridad, control y procedimientos de auditoría.

9.3.2. Información no confidencial

Se considera información pública y por lo tanto accesible por terceros:

- La contenida en la presente Declaración de Prácticas de Certificación.
- La incluida en las Políticas de certificación que le sean de aplicación.
- Los certificados emitidos por RPP-PKI.
- La lista de los certificados suspendidos o revocados.

9.3.3. Deber de secreto profesional

Los empleados de Dirección Nacional de Firma Electrónica, el Registro Público de Panamá y otros organismos externos a ellos que participen en cualesquiera tareas propias o derivadas de RPP-PKI están obligados al deber de secreto profesional y por lo tanto sujetos a la normativa reguladora que les es aplicable recogida fundamentalmente en el Reglamento Interno del Registro Público.

Asimismo, el personal contratado que participe en cualquier actividad u operación de RPP-PKI estará sujeto al deber de secreto en el marco de las obligaciones contractuales contraídas con RPP-PKI y las resoluciones que emita el Registro



REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 76 de 85

Público de Panamá que declaren confidencial y de acceso restringido información relacionada con la RPP-PKI.

9.4. Protección de la información personal

La RPP-PKI está obligada a garantizar la protección, la confidencialidad y el debido uso de la información suministrada por los usuarios de los servicios de certificación de conformidad con el numeral 11 del Artículo 23 de la Ley 51 de 2008.

9.5. Derechos de propiedad intelectual

El Registro Público de Panamá es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta DPC. Se prohíbe, por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva del Registro Público de Panamá sin la autorización expresa por su parte.

Queda prohibido, salvo acuerdo expreso con el Registro Público de Panamá, el uso total o parcial de cualquiera de los OID asignados a RPP-PKI salvo para los usos específicos establecidos por el mismo.

9.6. Representaciones y garantías

9.6.1. Obligaciones de las CAs

Las CA que operan bajo la jerarquía de RPP-PKI deben asegurarse de que todas las obligaciones establecidas en este apartado se recogen, según sea aplicable, en las políticas de certificación. Cada CA es responsable del cumplimiento de sus obligaciones, según se establecen en esta DPC, incluso aunque parte de su actividad sea realizada mediante contratación externa. Asimismo, cada CA proporcionará sus servicios de forma consistente con esta DPC.

Las CAs que operan bajo la jerarquía de RPP-PKI tienen las siguientes obligaciones:

- Realizar sus operaciones en conformidad con esta DPC.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 77 de 85

- Proteger sus claves privadas.
- Emitir certificados en conformidad con las Políticas de Certificación que les sean de aplicación.
- Tras la recepción de una solicitud válida de certificado, emitir certificados conformes con el estándar X.509 v3 y con los requerimientos de la solicitud.
- Emitir certificados que sean conformes con la información conocida en el momento de su emisión, y libres de errores de entrada de datos.
- Publicar los certificados cuando sea necesario para interactuar con otros usuarios o sistemas informáticos que así lo requieran.
- Revocar los certificados en los términos de la sección 4.4 Suspensión y Revocación de Certificados y publicar los certificados revocados en la CRL en el servicio de directorio y servicio Web referidos en el apartado 2.1 Repositorio, con la frecuencia estipulada en el punto 4.9.7 Frecuencia de emisión de CRLs
- Publicar esta DPC y las PC aplicables en el sitio web referido en el apartado 2.1 Repositorio.
- Comunicar los cambios de esta DPC y de las PC de acuerdo con lo establecido en el apartado 9.10.2 Periodo y mecanismo de Notificación
- Conservar los documentos de aceptación de condiciones de los servicios de certificación de la autoridad de certificación del Registro Público de Panamá firmados, en papel o electrónicamente, con los solicitantes de certificados en los que estos se dan por enterados de sus obligaciones y derechos, consienten en el tratamiento de sus datos personales por la CA y confirman que la información proporcionada es correcta.
- Garantizar la disponibilidad de las CRLs de acuerdo con las disposiciones de la sección 4.9.9 de la presente DPC.
- En el caso que la CA proceda a la revocación de un certificado, notificarlo a los usuarios de certificados en conformidad con las Políticas de certificación que les sean de aplicación.
- Colaborar con las auditorías dirigidas por RPP-PKI para validar la renovación de las propias claves.
- Operar de acuerdo con la legislación aplicable.
- Proteger, en caso de haberlas, las claves bajo su custodia.



REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 78 de 85

- No almacenar, ni copiar en ningún caso los datos de creación de firma, clave privada, de los titulares de certificados emitidos con el propósito de utilizarse para firma electrónica.
- Mantener la confidencialidad de la información relativa a los titulares y suscriptores de certificados electrónicos, limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o pedido del titular o suscriptor del certificado original.

Conservar registrada toda la información y documentación relativa a un certificado calificado durante siete años.

9.6.2. Obligaciones de las RAs

Las RAs operativas en RPP-PKI deben cumplir las siguientes obligaciones:

- Identificar correctamente al Titular y/o Solicitante y a la organización que represente, conforme a los procedimientos que se establecen en esta DPC y en las Políticas de Certificación específicas para cada tipo de certificado, utilizando cualquiera de los medios admitidos en derecho.
- Formalizar la expedición de Certificados con el Titular en los términos y condiciones que establezcan las Políticas de Certificación
- Almacenar de forma segura y por un periodo razonable la documentación aportada en el proceso de emisión del certificado y en el proceso de suspensión/revocación del mismo.
- Llevar a cabo cualesquiera otras funciones que le correspondan, a través del personal que sea necesario en cada caso, conforme se establece en esta DPC.

9.6.3. Obligaciones de los titulares de los certificados

Es obligación de los titulares de los certificados emitidos bajo la presente DPC:

- Suministrar información exacta, completa y veraz con relación a los datos que los encargados de su verificación les soliciten para realizar el proceso de registro.
- Informar a los responsables de RPP-PKI de cualquier modificación de esta información.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 79 de 85

- Conocer y aceptar las condiciones de utilización de los certificados, en particular las contenidas en esta DPC y en las PC que sean de aplicación, así como las modificaciones de estas.
- Limitar y adecuar el uso del certificado al ámbito estipulado por la Política de Certificación pertinente y la presente DPC.
- Poner el cuidado y medios necesarios para garantizar la custodia de su tarjeta criptográfica, evitando su pérdida, divulgación, modificación o uso no autorizado.
- El proceso de obtención de los certificados exige la elección personal de un PIN de control de la tarjeta criptográfica y de activación de las claves privadas y un PUK de desbloqueo. Es responsabilidad del titular mantener bajo su exclusivo conocimiento el valor del PIN y el del PUK.
- Solicitar inmediatamente la suspensión o revocación de un certificado en el caso de detección de inexactitudes en la información contenida en el mismo o tener conocimiento o sospecha del compromiso de la clave privada correspondiente a la clave pública contenida en el certificado, entre otras causas por: pérdida, robo, compromiso potencial, conocimiento por terceros del PIN y/o PUK.
- No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica (hardware y software) de los servicios de certificación.
- No transferir ni delegar a un tercero sus responsabilidades sobre un certificado que le haya sido asignado.
- Cualquier otra que se derive de la ley, su reglamentación, de esta DPC o de las Políticas de Certificación.

9.6.4. Obligaciones de los terceros que confían o acepten los certificados

Es obligación de los terceros que aceptan y confían en los certificados emitidos por RPP-PKI:

- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y la Política de Certificación pertinente.
- Verificar la validez de los certificados en el momento de la recepción de los documentos firmados electrónicamente mediante la comprobación de que el certificado es válido y no ha caducado o ha sido suspendido o revocado.
- Asumir su responsabilidad en la verificación de las firmas electrónicas.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código: P-11	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 80 de 85
------------------------	------------------------	--	------------------

- Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados que acepta y en que confía.
- Tener conocimiento de las garantías y responsabilidades derivadas de la aceptación de los certificados en los que confía y aceptar sujetarse a las mismas.
- Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación de este.

9.7. Exención de responsabilidades

RPP-PKI solo responderá en el caso de incumplimiento de las obligaciones contenidas en la Ley 82 de 2012 y la Ley 51 de 2008, en la presente DPC y en las Políticas de Certificación específicas.

RPP-PKI sólo responderá de los daños y perjuicios causados por el uso indebido del certificado, cuando se haya consignado en él o en su Política de Certificación asociada, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.

RPP-PKI, en tanto que Prestador de Servicios de Certificación, no se responsabiliza del contenido de los documentos firmados con sus certificados, ni de cualquier otro uso de sus certificados, como pueden ser procesos de cifrado de mensajes de datos o comunicaciones.

RPP-PKI no representa en forma alguna a los usuarios ni a terceras partes aceptantes de los certificados que emite.

RPP-PKI no asume ninguna responsabilidad en caso de cualquier tipo de pérdida o perjuicio:

- De los servicios que presta, en caso de guerra, catástrofes naturales o cualquier otro supuesto de caso fortuito o de fuerza mayor: alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico y/o telefónico, virus informáticos, deficiencias en los servicios de telecomunicaciones o el compromiso de las claves asimétricas derivado de un riesgo tecnológico imprevisible.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 81 de 85

- Ocasionados durante el periodo comprendido entre la solicitud de un certificado y su entrega al usuario.
- Ocasionados durante el periodo comprendido entre la revocación de un certificado y el momento de publicación de la siguiente CRL.
- Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos, la Política de Certificación pertinente y esta DPC.
- Ocasionados por el mal uso de la información contenida en el certificado.
- Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por RPP-PKI.
- RPP-PKI no asumirá responsabilidad alguna en relación al uso de los Certificados emitidos por sus CAs y el par de claves privada/pública asociado a sus titulares para cualquier actividad no especificada en la DPC o en las Políticas de Certificación correspondientes.
- RPP-PKI, como Prestador de Servicios de Certificación, no será responsable del contenido de los documentos electrónicos, ni mensajes de datos firmados con sus certificados ni de cualquier otro uso de sus certificados, como pueden ser procesos de cifrado o comunicaciones.

9.8. Limitaciones de las responsabilidades

A excepción de lo establecido por las disposiciones de la presente DPC y en la ley 51 de 2008 y su reglamento, RPP-PKI no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros que confían.

9.9. Indemnizaciones

El Registro Público de Panamá responderá ante el tribunal contencioso administrativo correspondiente por los daños y perjuicios que se cause al firmante, terceros o a cualquier persona, en el ejercicio de su actividad como prestador de servicios de certificación en los términos establecidos en la ley 82 de 2012, su reglamentación y la presente DPC. A tal efecto para el cálculo del monto de la indemnización se aplicarán las normas generales del procedimiento administrativo y responsabilidad contractual o extracontractual correspondientes.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 82 de 85

9.9.1. Indemnizaciones por daños ocasionados por RPP-PKI

Las indemnizaciones que tenga que asumir El Registro Público (RPP-PKI) por daños efectuados a terceros se hará en base a los términos establecidos en la ley 82 de 2012 y la ley 51 de 2008, su reglamentación y la presente DPC. La RPP-PKI no asume ninguna otra responsabilidad ante titulares de certificados o terceros que confían o acepten los certificados.

9.9.2. Indemnizaciones por los daños ocasionados por los Suscriptores

Tanto suscriptores como terceros son responsables por apoderarse, destruir, modificar, adulterar, indebidamente los datos de una firma o certificado electrónico durante o después de la fecha de creación del certificado y son sujetos a indemnizaciones por responsabilidad civil y penal según lo determinen los tribunales correspondientes de conformidad con el Artículo 35-A de la Ley 51 de 2008

Las Autoridades de Certificación certificadas por la Autoridad Certificadora Raíz de Panamá que indebidamente utilicen los servicios de la RPP-PKI también estarán sujetas a la Responsabilidad Civil en el caso de tratarse de entidades privadas o la Responsabilidad Administrativa en el caso de entidades públicas y adicionalmente al régimen sancionatorio y de multas que puede imponer la DNFE de conformidad con Capítulo V de la Ley 51 de 2008.

9.9.3. Indemnizaciones por los daños ocasionados por los Terceros que confían

Tanto suscriptores como terceros son responsables por apoderarse, destruir, modificar, adulterar, indebidamente los datos de una firma o certificado electrónico durante o después de la fecha de creación del certificado y son sujetos a indemnizaciones por responsabilidad civil y penal según lo determinen los tribunales correspondientes de conformidad con el Artículo 35-A de la Ley 51 de 2008

9.10. Período de validez

9.10.1. Plazo

Esta DPC entra en vigor desde el momento de su publicación en el repositorio de RPP-PKI.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 83 de 85

Esta DPC estará en vigor mientras no se derogue expresamente por la emisión de una nueva versión o por la renovación de las claves de la Autoridad Certificadora de Panamá, momento en que obligatoriamente se dictará una nueva versión.

9.10.2. Sustitución y derogación de la DPC

Esta DPC será sustituida por una nueva versión con independencia de la trascendencia de los cambios efectuados en la misma, de forma que siempre se aplicará en su totalidad.

Cuando la DPC quede derogada se retirará del repositorio público de RPP-PKI, si bien se conservará durante 7 años.

9.10.3. Efectos de la finalización

Las obligaciones y restricciones que establece esta DPC, en referencia a auditorías, información confidencial, obligaciones y responsabilidades de RPP-PKI, nacidas bajo su vigencia, subsistirán tras su sustitución o derogación por una nueva versión en todo en lo que no se oponga a ésta.

9.11. Notificaciones individuales y comunicaciones con los participantes

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las prácticas descritas en esta DPC se realizará mediante mensaje electrónico o por escrito mediante correo certificado dirigido a cualquiera de las direcciones contenidas en el punto 1.5 Administración de las Políticas. Las comunicaciones electrónicas producirán sus efectos una vez que las reciba el destinatario al que van dirigidas.

9.12. Procedimientos de cambios en las especificaciones

9.12.1. Procedimiento para los cambios

La Autoridad con atribuciones para realizar y aprobar cambios sobre la DPC y las PCs de RPP-PKI es la Autoridad de Aprobación de Políticas (AAP). Los datos de contacto de la AAP se encuentran en el apartado 1.5 Administración de las Políticas de esta DPC.



REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 84 de 85

9.12.2. Circunstancias en las que el OID debe ser cambiado

En los casos en que, a juicio de la AAP, los cambios de las especificaciones no afecten a la aceptabilidad de los certificados se procederá al incremento del número menor de versión del documento y el último número de Identificador de Objeto (OID) que lo representa, manteniendo el número mayor de la versión del documento, así como el resto de su OID asociado. No se considera necesario comunicar este tipo de modificaciones a los usuarios de los certificados correspondientes a la PC o DPC modificada.

En el caso de que la AAP juzgue que los cambios a la especificación pueden afectar a la aceptabilidad de los certificados para propósitos específicos se procederá al incremento del número mayor de versión del documento y la puesta a cero del número menor de la misma.

También se modificarán los dos últimos números del Identificador de Objeto (OID) que lo representa. Este tipo de modificaciones se comunicará a los usuarios de los certificados correspondientes a la PC o DPC modificada.

9.13. Reclamaciones

Todas reclamaciones entre usuarios y la PKI del REGISTRO PÚBLICO 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.

En el caso de que no se llegue a un acuerdo entre las partes, la resolución de cualquier conflicto que pudiera surgir se someterá luego de agotada la vía gubernativa al tribunal CONTENCIOSO-ADMINISTRATIVO correspondiente.

9.14. Normativa aplicable

Las operaciones y funcionamiento de RPP-PKI, así como la presente Declaración de Prácticas de Certificación y las Políticas de Certificación que sean de aplicación para cada tipo de certificado, estarán sujetas a la normativa que les sea aplicable y en especial a la Ley 82 de 2012 y la Ley 51 de 2008.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI

Código:
P-11

Versión:
0.3

Fecha de
implementación:
21 de diciembre de 2021

Página: 85 de 85

9.15. Cumplimiento de la normativa aplicable

Es responsabilidad de la Autoridad de Aprobación de Políticas velar por el cumplimiento de la legislación aplicable recogida en el apartado anterior.

9.16. Estipulaciones diversas

9.16.1. Cláusula de aceptación completa

Todos los Terceros que Confían asumen en su totalidad el contenido de la última versión de esta DPC y de las PC que sean de aplicación.

9.16.2. Independencia

En el caso de que una o más estipulaciones de esta DPC sean o llegasen a ser inválidas, nulas, o inexigibles legalmente, se entenderá por no puesta, salvo que dichas estipulaciones fueran esenciales de manera que al excluirlas de la DPC careciera ésta de toda eficacia jurídica.