



P-22

POLÍTICA DE CERTIFICACIÓN CERTIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA

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 ACTA DE SUBCOMITÉ DE GESTIÓN DE POLÍTICAS No. AR-2021-04	Aprobado por: Autoridad de Aprobación de Políticas 1 de diciembre de 2021 ACTA DE COMITÉ EJECUTIVO No. AR-2021-05



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 2 de 50

Índice

1. INTRODUCCIÓN	10
1.1. Visión general.....	10
1.2. Nombre del documento e identificación de la PC	10
1.3. Participantes en la PKI	11
1.3.1. Prestador de Servicios de Certificación (PSC).....	11
1.3.2. Autoridad de Aprobación de Políticas (AAP).....	12
1.3.3. Autoridades de Certificación (CA)	12
1.3.4. Autoridades de Registro (RA).....	14
1.3.5. Autoridades de Validación (VA).....	14
1.3.6. Autoridades de Sellado de Tiempo (TSA)	15
1.3.7. Solicitantes y titulares de certificados.....	15
1.3.8. Terceros que confían en los certificados emitidos por RPP-PKI.....	15
1.4. Uso de los certificados	15
1.4.1. Usos adecuados de los certificados	15
1.4.2. Limitaciones y restricciones en el uso de los certificados	15
1.5. Administración de las políticas	16
1.5.1. Entidad Responsable.....	16
1.5.2. Procedimiento de aprobación y modificación de la Política de Certificación de Certificados de Representante de Persona Jurídica	16
1.5.3. Datos de Contacto	16
1.6. Definiciones y Acrónimos	16
1.6.1. Definiciones	16
1.6.2. Acrónimos	17
2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN	19
2.1. Repositorios.....	19
2.2. Publicación de información de certificación	19
2.3. Frecuencia de publicación.....	19
2.4. Controles de acceso a la información de certificación	19
3. IDENTIFICACIÓN Y AUTENTICACIÓN	20
3.1. Nombres.....	20
3.1.1. Tipos de nombres	20
3.1.2. Necesidad de que los nombres sean significativos.....	20
3.1.3. Reglas para interpretar varios formatos de nombres	20



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 3 de 50

3.1.4.	Unicidad de los nombres	21
3.1.5.	Procedimientos de resolución de conflictos sobre nombres	21
3.1.6.	Reconocimiento, autenticación y papel de las marcas registradas.....	21
3.2.	Validación inicial de la identidad	21
3.2.1.	Medio de prueba de posesión de la clave privada	21
3.2.2.	Autenticación de la identidad de una persona jurídica	21
3.2.3.	Autenticación de la identidad de una persona natural	21
3.2.4.	Información no verificada sobre el solicitante.....	22
3.2.5.	Comprobación de las facultades de representación	22
3.2.6.	Criterios para operar con CA externas	22
3.3.	Identificación y autenticación para solicitudes de renovación.....	22
3.4.	Identificación y autenticación para solicitudes de revocación.....	22
4.	REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS	23
4.1.	Solicitud de certificados.....	23
4.1.1.	Quién puede efectuar una solicitud	23
4.1.2.	Registro de las solicitudes de certificados y responsabilidades de los solicitantes	23
4.2.	Tramitación de las solicitudes de certificados	24
4.2.1.	Realización de las funciones de identificación y autenticación	24
4.2.2.	Aprobación o denegación de las solicitudes de certificados	24
4.2.3.	Plazo para la tramitación de las solicitudes de certificados	24
4.3.	Emisión de certificados.....	24
4.3.1.	Actuaciones de la CA durante la emisión del certificado	24
4.3.2.	Notificación al solicitante de la emisión por la CA del certificado.....	24
4.4.	Aceptación del certificado	25
4.4.1.	Mecanismo de aceptación del certificado.....	25
4.4.2.	Publicación del certificado por la CA	25
4.4.3.	Notificación de la emisión del certificado por la CA a otras Autoridades	25
4.5.	Par de claves y uso del certificado	25
4.5.1.	Uso de la clave privada y del certificado por el titular	25
4.5.2.	Uso de la clave pública y del certificado por los terceros aceptantes	25
4.6.	Renovación de certificados sin cambio de claves.....	26
4.6.1.	Circunstancias para la renovación de certificados sin cambio de claves.....	26
4.6.2.	Quién puede solicitar la renovación de los certificados sin cambio de claves	26
4.6.3.	Tramitación de las peticiones de renovación de certificados sin cambio de claves	26
4.6.4.	Notificación de la emisión de un nuevo certificado al titular	26
4.6.5.	Forma de aceptación del certificado sin cambio de claves	26
4.6.6.	Publicación del certificado sin cambio de claves por la CA	26



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 4 de 50

4.6.7.	Notificación de la emisión del certificado por la CA a otras Autoridades	26
4.7.	Renovación de certificados con cambio de claves	26
4.7.1.	Circunstancias para una renovación con cambio claves de un certificado	26
4.7.2.	Quién puede pedir la renovación de los certificados	26
4.7.3.	Tramitación de las peticiones de renovación de certificados con cambio de claves	27
4.7.4.	Notificación de la emisión de un nuevo certificado al titular	27
4.7.5.	Forma de aceptación del certificado con las claves cambiadas	27
4.7.6.	Publicación del certificado con las nuevas claves por la CA.....	27
4.7.7.	Notificación de la emisión del certificado por la CA a otras Autoridades	27
4.8.	Modificación de certificados	27
4.8.1.	Circunstancias para la modificación de un certificado	27
4.8.2.	Quién puede solicitar la modificación de los certificados	28
4.8.3.	Tramitación de las peticiones de modificación de certificados	28
4.8.4.	Notificación de la emisión de un certificado modificado al titular	28
4.8.5.	Forma de aceptación del certificado modificado	28
4.8.6.	Publicación del certificado modificado por la CA.....	28
4.8.7.	Notificación de la modificación del certificado por la CA a otras Autoridades	28
4.9.	Revocación y suspensión de certificados	28
4.9.1.	Circunstancias para la revocación.....	28
4.9.2.	Quién puede solicitar la revocación.....	29
4.9.3.	Procedimiento de solicitud de revocación	29
4.9.4.	Periodo de gracia de la solicitud de revocación	29
4.9.5.	Plazo en el que la CA debe resolver la solicitud de revocación	29
4.9.6.	Requisitos de verificación de las revocaciones por los terceros que confían	30
4.9.7.	Frecuencia de emisión de CRL	30
4.9.8.	Tiempo máximo entre la generación y la publicación de las CRL.....	30
4.9.9.	Disponibilidad de un sistema en línea de verificación del estado de los certificados	30
4.9.10.	Requisitos de comprobación en línea de revocación	30
4.9.11.	Otras formas de divulgación de información de revocación disponibles.....	30
4.9.12.	Requisitos especiales de revocación de claves comprometidas	30
4.9.13.	Causas para la suspensión	30
4.9.14.	Quién puede solicitar la suspensión	30
4.9.15.	Procedimiento para la solicitud de suspensión	30
4.9.16.	Límites del periodo de suspensión	31
4.10.	Servicios de información del estado de certificados	31
4.10.1.	Características operativas	31
4.10.2.	Disponibilidad del servicio	31
4.10.3.	Características adicionales	31
4.11.	Extinción de la validez de un certificado	31
4.12.	Custodia y recuperación de claves	31



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 5 de 50

- 4.12.1. Prácticas y políticas de custodia y recuperación de claves 31
- 4.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión..... 31

5. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES 31

5.1. Controles físicos	32
5.1.1. Ubicación física y construcción.....	32
5.1.2. Acceso físico.....	32
5.1.3. Alimentación eléctrica y aire acondicionado.....	32
5.1.4. Exposición al agua.....	32
5.1.5. Prevención y protección frente a incendios	32
5.1.6. Sistema de almacenamiento	32
5.1.7. Eliminación de residuos	32
5.1.8. Copias de seguridad fuera de las instalaciones	32
5.2. Controles de procedimiento	32
5.2.1. Roles responsables del control y gestión de la PKI	32
5.2.2. Número de personas requeridas por tarea.....	32
5.2.3. Roles que requieren segregación de funciones	32
5.3. Controles de personal	33
5.3.1. Requisitos relativos a la cualificación, conocimiento y experiencia profesionales	33
5.3.2. Procedimientos de comprobación de antecedentes.....	33
5.3.3. Requerimientos de formación.....	33
5.3.4. Requerimientos y frecuencia de actualización de la formación	33
5.3.5. Frecuencia y secuencia de rotación de tareas	33
5.3.6. Sanciones por actuaciones no autorizadas.....	33
5.3.7. Requisitos de contratación de terceros	33
5.3.8. Documentación proporcionada al personal	33
5.4. Procedimientos de auditoría de seguridad.....	33
5.4.1. Tipos de eventos registrados.....	33
5.4.2. Frecuencia de procesado de registros de auditoría	33
5.4.3. Periodo de conservación de los registros de auditoría	33
5.4.4. Protección de los registros de auditoría	33
5.4.5. Procedimientos de respaldo de los registros de auditoría	33
5.4.6. Sistema de recogida de información de auditoría (interno vs externo)	34
5.4.7. Notificación al sujeto causa del evento	34
5.4.8. Análisis de vulnerabilidades	34
5.5. Archivado de registros.....	34
5.5.1. Tipo de eventos archivados.....	34
5.5.2. Periodo de conservación de registros	34
5.5.3. Protección del archivo	34
5.5.4. Procedimientos de copia de respaldo del archivo	34



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 6 de 50

5.5.5.	Requerimientos para el sellado de tiempo de los registros.....	34
5.5.6.	Sistema de archivo de información de auditoría (interno vs externo)	34
5.5.7.	Procedimientos para obtener y verificar información archivada.....	34
5.6.	Cambio de claves	34
5.7.	Recuperación ante compromiso de clave o catástrofe	34
5.7.1.	Procedimientos de gestión de incidentes y compromisos.....	34
5.7.2.	Alteración de los recursos hardware, software y/o datos	35
5.7.3.	Procedimiento de actuación ante el compromiso de la clave privada de una Autoridad	35
5.7.4.	Instalación después de un desastre natural u otro tipo de catástrofe	35
5.8.	Cese de una CA o RA	35
5.8.1.	Autoridad de Certificación.....	35
5.8.2.	Autoridad de Registro	35

6. CONTROLES DE SEGURIDAD TÉCNICA

36

6.1.	Generación e instalación del par de claves	36
6.1.1.	Generación del par de claves	36
6.1.2.	Entrega de la clave privada al titular	36
6.1.3.	Entrega de la clave pública al emisor del certificado	36
6.1.4.	Entrega de la clave pública de la CA a los terceros que confían	36
6.1.5.	Tamaño de las claves	36
6.1.6.	Parámetros de generación de la clave pública y verificación de la calidad	36
6.1.7.	Usos admitidos de la clave (campo KeyUsage de X.509 v3).....	36
6.2.	Protección de la clave privada y controles de ingeniería de los módulos.....	36
6.2.1.	Estándares para los módulos criptográficos.....	36
6.2.2.	Control multipersona (k de n) de la clave privada	37
6.2.3.	Custodia de la clave privada.....	37
6.2.4.	Copia de seguridad de la clave privada	37
6.2.5.	Archivo de la clave privada.....	37
6.2.6.	Transferencia de la clave privada a o desde el módulo criptográfico	37
6.2.7.	Almacenamiento de la clave privada en un módulo criptográfico	37
6.2.8.	Método de activación de la clave privada.....	37
6.2.9.	Método de desactivación de la clave privada.....	37
6.2.10.	Método de destrucción de la clave privada	37
6.2.11.	Clasificación de los módulos criptográficos	37
6.3.	Otros aspectos de la gestión del par de claves	38
6.3.1.	Archivo de la clave pública	38
6.3.2.	Periodos operativos de los certificados y periodo de uso para el par de claves.....	38
6.4.	Datos de activación	38
6.4.1.	Generación e instalación de los datos de activación	38



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 7 de 50

6.4.2.	Protección de los datos de activación	38
6.4.3.	Otros aspectos de los datos de activación	38
6.5.	Controles de seguridad informática.....	38
6.5.1.	Requerimientos técnicos de seguridad específicos	38
6.5.2.	Evaluación de la seguridad informática	38
6.6.	Controles de seguridad del ciclo de vida.....	38
6.6.1.	Controles de desarrollo de sistemas	38
6.6.2.	Controles de gestión de seguridad	38
6.6.3.	Controles de seguridad del ciclo de vida	38
6.7.	Controles de seguridad de la red	38
6.8.	Sellado de tiempo	39
7.	PERFILES DE LOS CERTIFICADOS, CRL Y OCSP	40
7.1.	Perfil de certificado	40
7.1.1.	Número de versión	40
7.1.2.	Extensiones del certificado	40
7.1.3.	Identificadores de objeto (OID) de los algoritmos	44
7.1.4.	Formatos de nombres.....	44
7.1.5.	Restricciones de los nombres.....	44
7.1.6.	Identificador de objeto (OID) de la Política de Certificación	44
7.1.7.	Uso de la extensión "PolicyConstraints"	44
7.1.8.	Sintaxis y semántica de los "PolicyQualifier"	45
7.1.9.	Tratamiento semántico para la extensión crítica "Certificate Policy"	45
7.2.	Perfil de CRL	45
7.2.1.	Número de versión	45
7.2.2.	CRL y extensiones.....	45
7.3.	Perfil de OCSP	45
7.3.1.	Número(s) de versión	45
7.3.2.	Extensiones OCSP	45
8.	AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES	46
8.1.	Frecuencia o circunstancias de los controles para cada Autoridad	46
8.2.	Identificación/cualificación del auditor	46
8.3.	Relación entre el auditor y la Autoridad auditada	46
8.4.	Aspectos cubiertos por los controles.....	46
8.5.	Acciones a tomar como resultado de la detección de deficiencias.....	46
8.6.	Comunicación de resultados	46



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 8 de 50

9. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

47

9.1. Tarifas	47
9.1.1. Tarifas de emisión o renovación de certificado	47
9.1.2. Tarifas de acceso a los certificados	47
9.1.3. Tarifas de acceso a la información de estado o revocación	47
9.1.4. Tarifas de otros servicios tales como información de políticas	47
9.1.5. Política de reembolso	47
9.2. Responsabilidades económicas	47
9.3. Confidencialidad de la información	47
9.3.1. Ámbito de la información confidencial	47
9.3.2. Información no confidencial	47
9.3.3. Deber de secreto profesional	48
9.4. Protección de la información personal	48
9.5. Derechos de propiedad intelectual	48
9.6. Representaciones y garantías	48
9.6.1. Obligaciones de las CA	48
9.6.2. Obligaciones de las RA	48
9.6.3. Obligaciones de los titulares de los certificados	48
9.6.4. Obligaciones de los terceros que confían o aceptan los certificados de RPP-PKI	48
9.6.5. Obligaciones de otros participantes	48
9.7. Exención de responsabilidades	48
9.8. Limitaciones de las responsabilidades	48
9.9. Indemnizaciones	48
9.10. Período de validez	49
9.10.1. Plazo	49
9.10.2. Sustitución y derogación de la PC	49
9.10.3. Efectos de la finalización	49
9.11. Notificaciones individuales y comunicaciones con los participantes	49
9.12. Procedimientos de cambios en las especificaciones	49
9.12.1. Procedimiento para los cambios	49
9.12.2. Circunstancias en las que el OID debe ser cambiado	49
9.13. Reclamaciones	49
9.14. Normativa aplicable	49
9.15. Cumplimiento de la normativa aplicable	49
9.16. Estipulaciones diversas	50
9.16.1. Cláusula de aceptación completa	50



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 9 de 50

9.16.2. Independencia	50
9.16.3. Resolución por la vía judicial	50
9.17. Otras estipulaciones	50



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 10 de 50

1. INTRODUCCIÓN

El presente documento corresponde a la Política de Certificación (PC) de los Certificados de Representantes de Persona Jurídica emitidos por la Infraestructura de Clave Pública (en adelante PKI) del Registro Público de Panamá.

En esta PC se detalla y completa lo estipulado en la Declaración de Prácticas de Certificación (DPC) de la PKI del Registro Público de Panamá (en adelante, RPP-PKI), conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta Política de Certificación, así como el ámbito de aplicación y las características técnicas de este tipo de certificados.

La presente PC se ha estructurado teniendo en cuenta las recomendaciones de la (Request for comments) RCF 3647 “*Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*”, de IETF. Con el propósito de facilitar la lectura y análisis del documento se incluyen todas las secciones establecidas en dicha RFC apareciendo la frase “No estipulado” en las secciones para las que no se haya previsto nada.

Todos los certificados que emite la PKI del Registro Público de Panamá son conformes con la versión 3 del estándar X.509, permitiendo la inclusión de extensiones para certificación de atributos.

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

La presente Declaración de Prácticas de Certificación (en adelante DPC), emitida de conformidad con la Ley 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.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código: P-22	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 11 de 50
------------------------	------------------------	---	------------------

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.

1.2. Nombre del documento e identificación de la PC

Nombre del documento	Política de Certificación de Certificados de Representante de Persona Jurídica
Versión del documento	0.3
Estado del documento	Actualizado
Fecha de emisión	03/10/2012
Fecha de actualización	27/09/2021 – Acta de Comité Ejecutivo No. AR-2021-05
Fecha de expiración	No aplicable
OID (Object Identifier)	2.16.591.1.2.2.2
Ubicación de la PC	http://firmaelectronica/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

1.3.1. Prestador de Servicios de Certificación (PSC)

Según la definición dispuesta por la Ley 51 de Firma Electrónica de Panamá, 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://firmaelectronica.gob.pa/normativa/index.htm>.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 12 de 50

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) es la organización responsable de la aprobación de la presente DPC y de las Políticas de Certificación de 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 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 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.

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



1.3.3.1. Autoridad Certificadora de Panamá

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 de clave secundaria, 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 de la PKI.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 13 de 50

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
Fecha de expiración	2053-05-08 12:02:13
Longitud de clave RSA	4096
Huella digital (SHA-256)	98BB 7426 2814 B7D9 FC41 3C2A 166C 1662 729E 24F8
URL de publicación del certificado	http://firmaelectronica.gob.pa/cacerts/caraiz.crt
URL de publicación de la ARL	http://firmaelectronica.gob.pa/crls/caraiz.crl

1.3.3.2. Autoridad de Certificación Panamá Clase 2

Bajo el Certificado Raíz de Panamá, se encuentran los certificados de de **CA de Gobierno** y de **CA Panamá Clase 2**, bajo cuyas respectivas jerarquías se emiten a su vez todos los certificados que la DNFE emite a entidades finales.

Los Certificados de Representante de Persona Jurídica son emitidos por la CA Panamá Clase 2. Sus 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-256)	cf 79 f1 b8 4f 9f 22 80 d7 f3 da 21 1c c0 09 ef b4 e9 21 77
URL de publicación del certificado	http://firmaelectronica.gob.pa/cacerts/capc2.crt
URL de publicación de la CRL	http://firmaelectronica.gob.pa/crls/capc2.crl



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 14 de 50

Tipos de certificados emitidos	Autenticación de Persona Natural 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 PC 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 entregarán los certificados

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 certificado 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 PKI del Registro Público de Panamá, 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.

 	REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	Política de Certificación de Representante de Persona Jurídica			
	Código: P-22	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 15 de 50

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, suscriptores 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.

1.3.7. Solicitantes y titulares de certificados

Los solicitantes y titulares de certificados se encuentran definidos en la DPC de RPP-PKI. Dentro del ámbito de la presente PC, los solicitantes y titulares de certificados de representante de persona jurídica son las personas naturales que pueden actuar en representación de una persona jurídica.

1.3.8. Terceros que confían en los certificados emitidos por RPP-PKI

Los Terceros que confían son las personas o entidades diferentes del titular que deciden aceptar y confiar en los certificados emitidos por la CA Panamá Clase 2 con el fin de identificar un titular como representante de una persona jurídica.

1.4. Uso de los certificados

1.4.1. Usos adecuados de los certificados

Los certificados regulados por la presente PC sólo deben utilizarse con el propósito de autenticación o firma de su titular, que será siempre una persona natural, así como su condición de representante de una persona jurídica. Para determinar si es posible utilizar un certificado de representante de persona jurídica para autenticación o firma es necesario comprobar el valor de la extensión 'Key Usage' del certificado en cuestión.

1.4.2. Limitaciones y restricciones en el uso de los certificados

Los certificados de representante de persona jurídica no deben emplearse para ninguna actividad no especificada en el punto anterior.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 16 de 50

1.5. Administración de las políticas

1.5.1. Entidad Responsable

Como establezca la DPC de RPP-PKI.

1.5.2. Procedimiento de aprobación y modificación de la Política de Certificación de Certificados de Representante de Persona Jurídica

Como establezca la DPC de RPP-PKI.

1.5.3. Datos de Contacto

Como establezca la DPC de RPP-PKI.

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 suscriptor de un certificado del Registro Público 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 suscriptor de un certificado del Registro Público 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 que solicita un certificado para sí mismo o para un componente informático.

Suscriptor: individuo o componente informático para el que se expide un certificado y es aceptado por éste o por su responsable en el caso de los certificados de componente.

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

Titular: véase suscriptor.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 17 de 50

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.

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.

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

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

RSA aceptados internacionalmente.

PKI: Public Key Infrastructure



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 18 de 50

PUK: PIN Unlock Code. 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

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 19 de 50

2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

2.1. Repositorios

Como establezca la DPC de RPP-PKI.

2.2. Publicación de información de certificación

Como establezca la DPC de RPP-PKI.

2.3. Frecuencia de publicación

Como establezca la DPC de RPP-PKI.

2.4. Controles de acceso a la información de certificación

Como establezca la DPC de RPP-PKI.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 20 de 50

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.

A continuación se define el procedimiento de asignación de los nombres distintivos para los certificados de representante de persona jurídica de RPP-PKI.

3.1.1.1. Certificado de autenticación

Campo	Valor	Descripción
C	PA	País
O	FIRMA ELECTRONICA	Organización
OU	PERSONA JURIDICA	Unidad Organizacional
CN	[A] NOMBRE <apellidos nombre> – ID <cedula/pasaporte>	Nombre Común

3.1.1.2. Certificado de firma

Campo	Valor	Descripción
C	PA	País
O	FIRMA ELECTRONICA	Organización
OU	PERSONA JURIDICA	Unidad Organizacional
CN	[F] NOMBRE <apellidos nombre> – ID <cedula/pasaporte>	Nombre Común

3.1.2. Necesidad de que los nombres sean significativos

En todos los casos los nombres distintivos de los titulares de los certificados deben ser significativos, ajustándose a las normas impuestas en el apartado anterior.

3.1.3. Reglas para interpretar varios formatos de nombres

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

 	REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	Política de Certificación de Representante de Persona Jurídica			
	Código: P-22	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 21 de 50

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. El uso del número de cédula de identidad o pasaporte en el PKI del Registro Público de Panamá (RPP-PKI) garantiza la unicidad del mismo. De manera adicional, el prefijo [A] para el certificado de autenticación y el prefijo [F] para el de firma garantizan que el nombre sea distinto en cada caso.

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 9.11 Reclamaciones y jurisdicción de esta PC.

3.1.6. Reconocimiento, autenticación y papel de las marcas registradas

Como establezca la DPC de la RPP-PKI.

3.2. **Validación inicial de la identidad**

3.2.1. Medio de prueba de posesión de la clave privada

Las claves de los certificados de representante de persona jurídica serán generadas por el titular de las mismas por lo que 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.

3.2.2. Autenticación de la identidad de una persona jurídica

La identidad de una persona jurídica se verifica a través del Certificado de Sociedad emitido por el Registro Público de Panamá, donde se comprueben los datos relativos a la constitución y personalidad jurídica, así como el nombre, la extensión y la vigencia de las facultades de representación legal del solicitante (Artículo 26 de la Ley 82 de 2012).

3.2.3. Autenticación de la identidad de una persona natural

El solicitante de certificados de representante de persona jurídica deberá proporcionar la siguiente información:

- Datos personales:
 - Primer nombre.
 - Segundo nombre.
 - Primer Apellido.
 - Segundo Apellido
 - Cédula de identidad personal
 - Dirección de correo electrónico
 - Fecha de nacimiento
- Datos del perfil:
 - Razón social
 - RUC
 - Ficha
 - Rollo
 - Imagen



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 22 de 50

Para poder autenticar la identidad de la persona natural, el solicitante deberá comparecer en el puesto de inscripción con su cédula de identidad personal. Además, de los datos proporcionados en la solicitud de cita, en el puesto de inscripción se capturarán los datos biométricos del solicitante.

Por otra parte, los datos del perfil se contrastarán con los datos registrados en el Registro Público.

3.2.4. Información no verificada sobre el solicitante

Toda la información recabada durante la expedición anterior ha de ser verificada.

3.2.5. Comprobación de las facultades de representación

Este punto no es aplicable ya que para poder autenticar la identidad de un Representante de Persona Jurídica, la persona natural que hace la representación de la persona jurídica, debe comparecer personalmente al puesto de inscripción con su cédula de identidad personal.

3.2.6. Criterios para operar con CA externas

Como establezca la DPC de RPP-PKI.

3.3. Identificación y autenticación para solicitudes de renovación

La identificación y autenticación de los titulares de los certificados para las solicitudes de renovación por cualquier motivo especificado en el apartado 4.7 del presente documento se realizará mediante la cédula de identidad de dicho titular.

3.4. Identificación y autenticación para solicitudes de revocación

La identificación y autenticación de los titulares de los certificados para las solicitudes de renovación por cualquier causa se realizará mediante la cédula de identidad de dicho titular.

 	REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	Política de Certificación de Representante de Persona Jurídica			
	Código: P-22	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 23 de 50

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

4.1. Solicitud de certificados

4.1.1. Quién puede efectuar una solicitud

La solicitud de certificado de representante de persona jurídica será efectuada por la persona natural que vaya a ser titular del mismo. Para ello, el solicitante deberá realizar una preinscripción en el portal Web de RPP-PKI aportando todos los datos especificados en el apartado 3.2.3 del presente documento.

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

El procedimiento de solicitud de certificados de representante de persona jurídica es el siguiente:

1. La persona natural que será titular del certificado a emitir solicita una cita en uno de los puestos de inscripción a través del portal Web de preinscripción de RPP-PKI. Para obtener una cita, la información que debe aportar el solicitante es la siguiente:
 - a. Datos personales:
 - i. Primer nombre.
 - ii. Segundo nombre.
 - iii. Primer Apellido.
 - iv. Segundo Apellido
 - v. Cédula de identidad personal
 - vi. Dirección de correo electrónico
 - vii. Fecha de nacimiento
 - b. Datos del perfil:
 - i. Razón social
 - ii. RUC
 - iii. Ficha
 - iv. Rollo
 - v. Imagen
2. El día y hora a la que el solicitante tenga su cita deberá presentarse en el puesto de inscripción, identificándose mediante su cédula de identidad personal y certificación del Registro Público donde aparezca clara y expresamente su capacidad de actuar en el momento de la solicitud como representante legal de la persona jurídica. No se admitirá ningún otro tipo de documentación tal como poderes o autorizaciones ajenas a la certificación del Registro Público para demostrar la condición de representante legal. La información proporcionada por el solicitante será contrastada con el Registro Público, de modo que se verifique la capacidad de representación de la persona jurídica. En el puesto de inscripción se realizará el registro de los datos biométricos del solicitante, así como la expedición de su dispositivo criptográfico sin certificados. Para proceder a la expedición del dispositivo criptográfico, es necesario que éste haya firmado el documento de aceptación de condiciones.
3. Una vez que el solicitante haya obtenido su dispositivo criptográfico, en el puesto de emisión se procederá a la generación de sus certificados en el dispositivo criptográfico que acaba de obtener el solicitante.

Es responsabilidad del solicitante de certificados garantizar la completitud y veracidad de toda la información aportada para obtener sus certificados de representante de persona jurídica con

	REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	Política de Certificación de Representante de Persona Jurídica			
	Código: P-22	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 24 de 50

independencia de las comprobaciones realizadas por el prestador de servicios de certificación para verificarla.

4.2. Tramitación de las solicitudes de certificados

4.2.1. Realización de las funciones de identificación y autenticación

La realización de las funciones de identificación y autenticación requerirá la presencia física del solicitante junto con su cédula de identificación personal en el puesto de inscripción. En el puesto de emisión, la identificación y autenticación del usuario se realizará con el dispositivo criptográfico que éste ha obtenido en el puesto de inscripción.

El proceso de identificación y autenticación de un solicitante está descrito en el apartado 3.2.3 del presente documento.

4.2.2. Aprobación o denegación de las solicitudes de certificados

La emisión del certificado tendrá lugar una vez que 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 el apartado anterior.

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 RPP-PKI no se hacen responsables de las demoras que puedan surgir en el período comprendido entre la solicitud del certificado y la entrega del mismo. En cualquier caso, el plazo para la tramitación de las solicitudes de certificados vendrá limitado por la disponibilidad de citas en los puestos de inscripción y emisión a los que desee acudir el solicitante.

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 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.

4.3.2. Notificación al solicitante de la emisión por la CA del certificado

La emisión del certificado electrónico a Representante de Persona Jurídica es presencial por lo tanto la notificación es inmediata. En el momento de la entrega de la cédula de identidad personal y la copia del documento de aceptación de condiciones firmada, se le indica al suscriptor su responsabilidad en el uso de su certificado electrónico. De igual forma se le indicará como obtener la presente PC.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 25 de 50

4.4. Aceptación del certificado

4.4.1. Mecanismo de aceptación del certificado

Los titulares de los certificados de representante de persona jurídica deberán aceptar los términos y condiciones contenidos en el formulario de aceptación de condiciones de los servicios de certificación de RPP-PKI mediante firma manuscrita.

4.4.2. Publicación del certificado por la CA

Este punto no es aplicable ya que los certificados electrónicos de Representante de Persona Jurídica no se publicarán en ningún repositorio.

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

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

4.5. Par de claves y uso del certificado

Los Certificados de Representante de Persona Jurídica son certificados de uso intransferible que acreditan la identidad de su titular, así como su condición de representante de una persona jurídica. Se emiten para el exclusivo uso en el ámbito de sus funciones como representante de personas jurídicas o relacionadas con su actividad como tal.

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

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 para el exclusivo uso en el ámbito de sus funciones como representante de personas jurídicas o relacionadas con su actividad como tal.

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 el exclusivo uso en el ámbito de las funciones del titular como representante de persona jurídica o relacionadas con su actividad como tal 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 la DPC de RPP-PKI y en la presente PC.

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

 	REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	Política de Certificación de Representante de Persona Jurídica			
	Código: P-22	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 26 de 50

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 PC se realizarán con cambio de claves. En consecuencia, no se recogen el resto de los puntos referente a renovación de certificados sin cambio de claves (puntos 4.6.2, 4.6.3, 4.6.4, 4.6.5, 4.6.6, 4.6.7) que establece la RFC 3647, lo que implica, a efectos de esta DPC, su no estipulación.

4.6.2. 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 claves de un 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 las mismas.
- Cambio de formato.

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

4.7.2. Quién puede pedir la renovación de los certificados

La renovación de los certificados únicamente puede ser solicitada por el titular de los mismos.

 	REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	Política de Certificación de Representante de Persona Jurídica			
	Código: P-22	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 27 de 50

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

La RA 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 solicitud de renovación de certificados con cambio de claves se realizará de forma presencial en el puesto de emisión. Para la identificación y autenticación del usuario éste deberá presentar su cédula de identidad y, a no ser que se haya perdido por cualquier causa el dispositivo criptográfico donde se emitieron los certificados a renovar deberá presentarse dicho dispositivo criptográfico.

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 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

La emisión del nuevo certificado electrónico a Representante de Persona Jurídica es presencial por lo tanto la notificación es inmediata mediante la comunicación de la finalización satisfactoria del proceso de renovación del certificado electrónico.

4.7.5. Forma de aceptación del certificado con las claves cambiadas

El solicitante deberá volver a firmar el documento de aceptación de condiciones para poder proceder a la renovación del certificado con cambio de claves.

4.7.6. Publicación del certificado con las nuevas claves por la CA

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

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

Cuando la CA de RPP-PKI emita un certificado de acuerdo con una solicitud de certificación tramitada a través de una RA, enviará una copia del mismo 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 (DN).

 	REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	Política de Certificación de Representante de Persona Jurídica			
	Código: P-22	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 28 de 50

Todas las modificaciones de certificados realizadas en el ámbito de esta PC 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 del certificado electrónico a Representante de Persona Jurídica serán tratados como una renovación de certificados, por lo que le aplican los apartados anteriores al respecto. En consecuencia, no se recogen el resto de los puntos referente a modificación de certificados (puntos 4.8.3, 4.8.4, 4.8.5, 4.8.6, 4.8.7) que establece la RFC 3647, lo que implica, a efectos de esta DPC, su no estipulación.

4.8.3. 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.

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:

- 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 RPP-PKI, la presente PC o de la DPC de RPP-PKI.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 29 de 50

- 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 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 deviene en inexacta.
- 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 del mismo, deviniendo el certificado como no válido. La revocación no afectará a las obligaciones subyacentes creadas o comunicadas por esta PC ni tendrá efectos retroactivos.

4.9.2. Quién puede solicitar la revocación

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

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

4.9.3. Procedimiento de solicitud de revocación

La solicitud de revocación de los certificados de representante de persona jurídica únicamente la podrá efectuar el titular de los mismos de manera presencial en el puesto de inscripción. Para ello, deberá identificarse con su cédula de identidad.

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

Las solicitudes de revocación deben resolverse tan rápido como sea posible en un tiempo no superior a 24 horas en días laborables y nunca superior a 72 horas en fines de semana y/o días festivos.

 	REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	Política de Certificación de Representante de Persona Jurídica			
	Código: P-22	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 30 de 50

4.9.6. [Requisitos de verificación de las revocaciones por los terceros que confían](#)

Como establezca la DPC de RPP-PKI.

4.9.7. [Frecuencia de emisión de CRL](#)

Como establezca la DPC de RPP-PKI.

4.9.8. [Tiempo máximo entre la generación y la publicación de las CRL](#)

El tiempo máximo entre la generación de una CRL y su correspondiente publicación en el repositorio es de 6 horas.

4.9.9. [Disponibilidad de un sistema en línea de verificación del estado de los certificados](#)

Como establezca la DPC de RPP-PKI.

4.9.10. [Requisitos de comprobación en línea de revocación](#)

Como establezca la DPC de RPP-PKI.

4.9.11. [Otras formas de divulgación de información de revocación disponibles](#)

No estipulado

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, 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.
- 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.

4.9.14. [Quién puede solicitar la suspensión](#)

La solicitud puede presentarla el titular del certificado.

4.9.15. [Procedimiento para la solicitud de suspensión](#)

En caso de pérdida o deterioro de su dispositivo criptográfico, un titular de certificados de representante legal de persona jurídica podrá solicitar la suspensión temporal de los mismos mediante una llamada telefónica al número +507 504 3900 o correo electrónico a la dirección servicios@firmaelectronica.gob.pa. En este caso, el usuario deberá dar su número de cédula y sus códigos de suspensión para identificarse. Adicional, la suspensión podrá solicitarse

 	REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	Política de Certificación de Representante de Persona Jurídica			
	Código: P-22	Versión: 0.3	Fecha de implementación: 21 de diciembre de 2021	Página: 31 de 50

mediante el mismo procedimiento establecido para la revocación en el apartado 4.9.3 del presente documento.

4.9.16. Límites del periodo de suspensión

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

Como establezca la DPC de RPP-PKI.

4.10.2. Disponibilidad del servicio

Como establezca la DPC de RPP-PKI.

4.10.3. Características adicionales

Como establezca la DPC de RPP-PKI.

4.11. Extinción de la validez de un certificado

Como establezca la DPC de RPP-PKI.

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 de Representante de Persona Jurídica (clave privada) se generan dentro de un dispositivo criptográfico y no pueden ser exportadas en ningún caso. La responsabilidad de la custodia del dispositivo criptográfico donde está contenido el certificado electrónico recae enteramente sobre el titular.

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

Este punto no aplica ya que la recuperación de la clave de sesión es responsabilidad del suscriptor del certificado electrónico; el método de recuperación empleado es a través de un número PUK que se le entrega al suscriptor al momento de generarse su dispositivo criptográfico.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 32 de 50

5. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

5.1. Controles físicos

5.1.1. Ubicación física y construcción

Como establezca la DPC de RPP-PKI.

5.1.2. Acceso físico

Como establezca la DPC de RPP-PKI.

5.1.3. Alimentación eléctrica y aire acondicionado

Como establezca la DPC de RPP-PKI.

5.1.4. Exposición al agua

Como establezca la DPC de RPP-PKI.

5.1.5. Prevención y protección frente a incendios

Como establezca la DPC de RPP-PKI.

5.1.6. Sistema de almacenamiento

Como establezca la DPC de RPP-PKI.

5.1.7. Eliminación de residuos

Como establezca la DPC de RPP-PKI.

5.1.8. Copias de seguridad fuera de las instalaciones

Como establezca la DPC de RPP-PKI.

5.2. Controles de procedimiento

5.2.1. Roles responsables del control y gestión de la PKI

Como establezca la DPC de RPP-PKI.

5.2.2. Número de personas requeridas por tarea

Como establezca la DPC de RPP-PKI.

5.2.3. Roles que requieren segregación de funciones

Como establezca la DPC de RPP-PKI.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 33 de 50

5.3. Controles de personal

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

Como establezca la DPC de RPP-PKI.

5.3.2. Procedimientos de comprobación de antecedentes

Como establezca la DPC de RPP-PKI.

5.3.3. Requerimientos de formación

Como establezca la DPC de RPP-PKI.

5.3.4. Requerimientos y frecuencia de actualización de la formación

Como establezca la DPC de RPP-PKI.

5.3.5. Frecuencia y secuencia de rotación de tareas

Como establezca la DPC de RPP-PKI.

5.3.6. Sanciones por actuaciones no autorizadas

Como establezca la DPC de RPP-PKI.

5.3.7. Requisitos de contratación de terceros

Como establezca la DPC de RPP-PKI.

5.3.8. Documentación proporcionada al personal

Como establezca la DPC de RPP-PKI.

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipos de eventos registrados

Como establezca la DPC de RPP-PKI.

5.4.2. Frecuencia de procesado de registros de auditoría

Como establezca la DPC de RPP-PKI.

5.4.3. Periodo de conservación de los registros de auditoría

Como establezca la DPC de RPP-PKI.

5.4.4. Protección de los registros de auditoría

Como establezca la DPC de RPP-PKI.

5.4.5. Procedimientos de respaldo de los registros de auditoría

Como establezca la DPC de RPP-PKI.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 34 de 50

5.4.6. [Sistema de recogida de información de auditoría \(interno vs externo\)](#)

Como establezca la DPC de RPP-PKI.

5.4.7. [Notificación al sujeto causa del evento](#)

Como establezca la DPC de RPP-PKI.

5.4.8. [Análisis de vulnerabilidades](#)

Como establezca la DPC de RPP-PKI.

5.5. **Archivado de registros**

5.5.1. [Tipo de eventos archivados](#)

Como establezca la DPC de RPP-PKI.

5.5.2. [Periodo de conservación de registros](#)

Como establezca la DPC de RPP-PKI.

5.5.3. [Protección del archivo](#)

Como establezca la DPC de RPP-PKI.

5.5.4. [Procedimientos de copia de respaldo del archivo](#)

Como establezca la DPC de RPP-PKI.

5.5.5. [Requerimientos para el sellado de tiempo de los registros](#)

Como establezca la DPC de RPP-PKI.

5.5.6. [Sistema de archivo de información de auditoría \(interno vs externo\)](#)

Como establezca la DPC de RPP-PKI.

5.5.7. [Procedimientos para obtener y verificar información archivada](#)

Como establezca la DPC de RPP-PKI.

5.6. **Cambio de claves**

Como establezca la DPC de RPP-PKI.

5.7. **Recuperación ante compromiso de clave o catástrofe**

5.7.1. [Procedimientos de gestión de incidentes y compromisos](#)

Como establezca la DPC de RPP-PKI.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 35 de 50

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

Como establezca la DPC de RPP-PKI.

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

Como establezca la DPC de RPP-PKI.

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

Como establezca la DPC de RPP-PKI.

5.8. Cese de una CA o RA

5.8.1. Autoridad de Certificación

Como establezca la DPC de RPP-PKI.

5.8.2. Autoridad de Registro

Como establezca la DPC de RPP-PKI.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 36 de 50

6. CONTROLES DE SEGURIDAD TÉCNICA

Los controles de seguridad técnica aplicables a los diferentes componentes de la PKI se encuentran descritos en la DPC de RPP-PKI. En este apartado únicamente se describen los controles de seguridad técnica particulares del tipo de certificados tratado.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

Los pares de claves para los certificados de representante de persona jurídica se generan en dispositivos criptográficos hardware con certificación FIPS 140-2 Nivel 2.

6.1.2. Entrega de la clave privada al titular

La clave privada de los certificados de representante de persona jurídica es generada por el propio titular en su dispositivo criptográfico, por lo que en ningún caso será entregada al mismo.

6.1.3. Entrega de la clave pública al emisor del certificado

La clave pública de los certificados de representante de persona jurídica se genera en el dispositivo criptográfico del titular en el puesto de emisión siendo la RA la responsable de entregar dicha clave pública a la CA.

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 que confían en el Repositorio de RPP-PKI (ver apartado 2.1).

6.1.5. Tamaño de las claves

El tamaño de las claves de los certificados de representante de persona jurídica es de 2048 bits.

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

La clave pública de los certificados de representante de persona jurídica de RPP-PKI está codificada de acuerdo con RFC 3280 y PKCS#1 siendo el algoritmo de generación de claves RSA.

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

Los usos admitidos de la clave para los certificados de representante de persona jurídica vienen dados por el valor de las extensiones Key Usage y Extended Key Usage de los mismos. El contenido de dichas extensiones para cada uno de los tipos de certificados de representante de persona jurídica se puede consultar en el apartado 7.1.2 del presente documento.

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

6.2.1. Estándares para los módulos criptográficos

Las tarjetas criptográficas con certificados para firma electrónica avanzada, aptas como dispositivos seguros de creación de firma, contarán con la certificación FIPS 140-2 Nivel 2.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 37 de 50

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

Las claves privadas de los certificados de representante de persona jurídica no se encuentran bajo control multipersona. El control de dicha clave privada recae enteramente sobre el suscriptor.

6.2.3. Custodia de la clave privada

La custodia de las claves privadas de los certificados de representante de persona jurídica la realizan los propios titulares de las mismas.

6.2.4. Copia de seguridad de la clave privada

En ningún caso se realizarán copias de seguridad de las claves privadas de firma de representantes de persona jurídica para garantizar el no repudio.

6.2.5. Archivo de la clave privada

Las claves privadas de firma de representantes de persona jurídica nunca serán archivadas para garantizar el no repudio.

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

En ningún caso es posible transferir las claves privadas de firma de representantes de persona jurídica para garantizar el no repudio.

6.2.7. Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas de firma de representantes de persona jurídica se generan en el dispositivo criptográfico en el momento de la generación de los certificados.

6.2.8. Método de activación de la clave privada

La activación de la clave privada la podrá efectuar el titular de la misma mediante el uso de su PIN.

6.2.9. Método de desactivación de la clave privada

La desactivación de la clave privada de Representante de Persona Jurídica se realizará mediante solicitud del titular del certificado electrónico. Esta desactivación se tratará como una revocación del certificado electrónico por lo que se seguirá el procedimiento establecido para tal fin.

6.2.10. Método de destrucción de la clave privada

La destrucción de la clave privada debe ser precedida por una revocación del certificado electrónico asociado a la clave, si esta estuviese todavía vigente. La DNFE dispondrá de un método de destrucción de forma que impida su robo o uso no autorizado.

6.2.11. Clasificación de los módulos criptográficos

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



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 38 de 50

6.3. Otros aspectos de la gestión del par de claves

6.3.1. Archivo de la clave pública

Como establezca la DPC de RPP-PKI.

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

El periodo de validez de los Certificados de Representante de Persona Jurídica es de dos (2) años desde el momento de emisión del mismo.

6.4. Datos de activación

6.4.1. Generación e instalación de los datos de activación

Como establezca la DPC de RPP-PKI.

6.4.2. Protección de los datos de activación

Como establezca la DPC de RPP-PKI.

6.4.3. Otros aspectos de los datos de activación

Como establezca la DPC de RPP-PKI.

6.5. Controles de seguridad informática

6.5.1. Requerimientos técnicos de seguridad específicos

Como establezca la DPC de RPP-PKI.

6.5.2. Evaluación de la seguridad informática

Como establezca la DPC de RPP-PKI.

6.6. Controles de seguridad del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Como establezca la DPC de RPP-PKI.

6.6.2. Controles de gestión de seguridad

Como establezca la DPC de RPP-PKI.

6.6.3. Controles de seguridad del ciclo de vida

Como establezca la DPC de RPP-PKI.

6.7. Controles de seguridad de la red

Como establezca la DPC de RPP-PKI.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 39 de 50

6.8. Sellado de tiempo

Como establezca la DPC de RPP-PKI.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 40 de 50

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.

A continuación se detalla el contenido de las extensiones más significativas de los certificados de representante de persona jurídica emitidos por RPP-PKI:

7.1.2.1. Certificados de Autenticación

La estructura del certificado, referente a la extensión *subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	PA	País
O	FIRMA ELECTRONICA	Organización
OU	PROFESIONAL	Unidad Organizacional
CN	[A] NOMBRE <apellidos nombre> – ID <cedula/pasaporte>	Nombre Común

Descripción del resto de campos más relevantes del perfil de certificado para el certificado de Autenticación de Profesional de Panamá:

Campo	Contenido Propuesto	Crítica
1. Signature Algorithm	sha256WithRSAEncryption	
2. Issuer	C=PA, O=FIRMA ELECTRONICA, CN=CA PANAMA CLASE 2	



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 41 de 50

3. Validez	2 años	
4. Subject	C=PA, O=FIRMA ELECTRONICA, OU=PROFESIONAL CN=[A] NOMBRE <apellidos nombre> – ID <cedula/pasaporte>	
5. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: 2048 bits	
6. Certificate Policies	Se utilizará	NO
Policy Identifier	2.16.591.1.2.2.3.1	
URL CPS	<i>[DPC-URL]</i>	
Notice Referente	Certificado sujeto a la Declaración de Prácticas de Certificación de Firma Electrónica de Panamá (2012)	
7. Subject Alternate Names	Rfc822Name = Dirección de correo electrónico [OID RPP-PKI].1.1.1: Primer Nombre [OID RPP-PKI].1.1.2: Segundo Nombre [OID RPP-PKI].1.1.3: Primer Apellido [OID RPP-PKI].1.1.4: Segundo Apellido [OID RPP-PKI].1.1.5: Cédula de identidad personal [OID RPP-PKI].1.1.6: Fecha de Nacimiento [OID RPP-PKI].1.3.1: Profesión [OID RPP-PKI].1.3.2: N° de idoneidad	NO
8. CRLDistributionPoints	<i>[HTTP URI PC2 CRL]</i>	NO
9. Auth. Information Access	Se utilizará	NO
calssuers	<i>[HTTP URI PC2 CA]</i>	
Ocsp	<i>[HTTP URI OCSP]</i>	
10. KeyUsage	Digital Signature Key Agreement	SI



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 42 de 50

11. extKeyUsage	clientAuth (1.3.6.1.5.5.7.3.2) anyExtendedKeyUsage (2.5.29.37.0)	SI
12. Subject Key Identifier	SHA-1 hash de la clave pública	NO
13. Authority Key Identifier	Se utilizará	NO
KeyIdentifier	SHA-1 hash de la clave pública del emisor	
AuthorityCertIssuer	No utilizado	
AuthorityCertSerialNumber	No utilizado	

7.1.2.2. Certificados de Firma

La estructura del certificado, referente a la extensión *subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	PA	País
O	FIRMA ELECTRONICA	Organización
OU	PROFESIONAL	Unidad Organizacional
CN	[F] NOMBRE <apellidos nombre> – ID <cedula/pasaporte>	Nombre Común

Descripción del resto de campos más relevantes del perfil de certificado para el certificado de Firma de Profesional de Panamá:

Campo	Contenido Propuesto	Crítica
1. Signature Algorithm	sha256WithRSAEncryption	
2. Issuer	C=PA, O=FIRMA ELECTRONICA, CN=CA PANAMA CLASE 2	
3. Validez	2 años	
4. Subject	C=PA, O=FIRMA ELECTRONICA, OU=PROFESIONAL CN=[F] NOMBRE <apellidos nombre> – ID <cedula/pasaporte>	



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 43 de 50

5. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: 2048 bits	
6. Certificate Policies	Se utilizará	NO
Policy Identifier	2.16.591.1.2.2.3.2	
URL CPS	<i>[DPC-URL]</i>	
Notice Referente	Certificado sujeto a la Declaración de Prácticas de Certificación de Firma Electrónica de Panamá (2012)	
7. Subject Alternate Names	Rfc822Name = Dirección de correo electrónico [OID RPP-PKI].1.1.1: Primer Nombre [OID RPP-PKI].1.1.2: Segundo Nombre [OID RPP-PKI].1.1.3: Primer Apellido [OID RPP-PKI].1.1.4: Segundo Apellido [OID RPP-PKI].1.1.5: Cédula de identidad personal [OID RPP-PKI].1.1.6: Fecha de Nacimiento [OID RPP-PKI].1.3.1: Profesión [OID RPP-PKI].1.3.2: N° de idoneidad	NO
8. CRLDistributionPoints	<i>[HTTP URI PC2 CRL]</i>	NO
9. Auth. Information Access	Se utilizará	NO
calssuers	<i>[HTTP URI PC2 CA]</i>	
Ocsp	<i>[HTTP URI OCSP]</i>	
10. KeyUsage	nonRepudiation	SI
11. extKeyUsage	emailProtection (1.3.6.1.5.5.7.3.4) anyExtendedKeyUsage (2.5.29.37.0)	SI
12. Subject Key Identifier	SHA-1 hash de la clave pública	NO
13. Authority Key Identifier	Se utilizará	NO
KeyIdentifier	SHA-1 hash de la clave pública del emisor	



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 44 de 50

AuthorityCertIssuer	No utilizado	
AuthorityCertSerialNumber	No utilizado	
14. qcStatements	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) ¹	NO

7.1.3. Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos: SHA256 with RSA Encryption (1.2.840.113549.1.1.11)

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

Las restricciones de los nombres se encuentran descritas en el apartado 3.1.1 del presente documento.

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

Los OID para esta PC son los siguientes:

[OID RPP-PKI].2.2.2.X.Y Política de Certificación para Certificados de Representante de Persona Jurídica

[OID RPP-PKI].2.2.2.1.X.Y Política de Certificación para Certificados de Autenticación de Representante de Persona Jurídica

[OID RPP-PKI].2.2.2.2.X.Y Política de Certificación para Certificados de Firma de Representante de Persona Jurídica

Dónde:

- [OID RPP-PKI] representa el OID 2.16.591.1
- X.Y representa la versión

7.1.7. Uso de la extensión "PolicyConstraints"

No estipulado.

¹ Indica que el certificado es compatible con la definición de certificado cualificado de IETF (RFC 3039).



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 45 de 50

7.1.8. Sintaxis y semántica de los "PolicyQualifier"

El contenido de la extensión Certificate Policies puede consultarse en el apartado 7.1.2 del presente documento.

7.1.9. Tratamiento semántico para la extensión crítica "Certificate Policy"

Como establezca la DPC de la RPP-PKI.

7.2. Perfil de CRL

7.2.1. Número de versión

Como establezca la DPC de RPP-PKI.

7.2.2. CRL y extensiones

Como establezca la DPC de RPP-PKI.

7.3. Perfil de OCSP

7.3.1. Número(s) de versión

Como establezca la DPC de RPP-PKI.

7.3.2. Extensiones OCSP

Como establezca la DPC de RPP-PKI.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 46 de 50

8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

8.1. Frecuencia o circunstancias de los controles para cada Autoridad

Como establezca la DPC de RPP-PKI.

8.2. Identificación/cualificación del auditor

Como establezca la DPC de RPP-PKI.

8.3. Relación entre el auditor y la Autoridad auditada

Como establezca la DPC de RPP-PKI.

8.4. Aspectos cubiertos por los controles

Como establezca la DPC de RPP-PKI.

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

Como establezca la DPC de RPP-PKI.

8.6. Comunicación de resultados

Como establezca la DPC de RPP-PKI.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 47 de 50

9. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

9.1. Tarifas

Las tarifas correspondientes a la gestión de certificados se encuentran detalladas en la dirección <http://www.pki.gob.pa/normativa/tarifas.htm>.

9.1.1. Tarifas de emisión o renovación de certificado

Las tarifas correspondientes a la emisión o renovación de certificado se encuentran detalladas en la dirección <http://www.pki.gob.pa/normativa/tarifas.htm>.

9.1.2. Tarifas de acceso a los certificados

Las tarifas correspondientes a la emisión o renovación de certificado se encuentran detalladas en la dirección <http://www.pki.gob.pa/normativa/tarifas.htm>.

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

Las tarifas correspondientes a la emisión o renovación de certificado se encuentran detalladas en la dirección <http://www.pki.gob.pa/normativa/tarifas.htm>.

9.1.4. Tarifas de otros servicios tales como información de políticas

Las tarifas correspondientes a la emisión o renovación de certificado se encuentran detalladas en la dirección <http://www.pki.gob.pa/normativa/tarifas.htm>.

9.1.5. Política de reembolso

Si al momento del cese de actividades por parte de la RPP-PKI, el certificado electrónico calificado de un firmante tiene una vigencia pendiente de uso superior a seis meses, la RPP-PKI deberá reembolsarle el importe de la tarifa proporcional a la vigencia no utilizada, a menos de que la RPP-PKI al cese en sus actividades haya transferido los certificados a otro prestador de servicios de certificación. (Último párrafo del art. 32 de la Ley 51 de 2008 modificada por la Ley 82 de 2012).

9.2. Responsabilidades económicas

Como establezca la DPC de RPP-PKI.

9.3. Confidencialidad de la información

Se establece el siguiente régimen de confidencialidad de los datos relativos a RPP-PKI:

9.3.1. Ámbito de la información confidencial

Como establezca la DPC de RPP-PKI.

9.3.2. Información no confidencial

Como establezca la DPC de RPP-PKI.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 48 de 50

9.3.3. Deber de secreto profesional

Como establezca la DPC de RPP-PKI.

9.4. Protección de la información personal

Como establezca la DPC de RPP-PKI.

9.5. Derechos de propiedad intelectual

Como establezca la DPC de RPP-PKI.

9.6. Representaciones y garantías

9.6.1. Obligaciones de las CA

Como establezca la DPC de RPP-PKI.

9.6.2. Obligaciones de las RA

Como establezca la DPC de RPP-PKI.

9.6.3. Obligaciones de los titulares de los certificados

Como establezca la DPC de RPP-PKI.

9.6.4. Obligaciones de los terceros que confían o aceptan los certificados de RPP-PKI

Como establezca la DPC de RPP-PKI.

9.6.5. Obligaciones de otros participantes

Como establezca la DPC de RPP-PKI.

9.7. Exención de responsabilidades

Adicional a lo establecido en la DPC de la RPP-PKI, los certificados regulados por la presente PC sólo deben utilizarse con el propósito de autenticación o firma de su titular, que será siempre una persona natural actuando en su condición de representante legal de una persona jurídica específica, por lo que el Registro Público de Panamá no se hace responsable por el uso indebido por parte del suscriptor del certificado electrónico fuera de este ámbito.

9.8. Limitaciones de las responsabilidades

Como establezca la DPC de RPP-PKI.

9.9. Indemnizaciones

Como establezca la DPC de RPP-PKI.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 49 de 50

9.10. Período de validez

9.10.1. Plazo

Esta PC entra en vigor desde el momento de su publicación en el repositorio de RPP-PKI y se mantendrá vigente 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 PC

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

Cuando la PC 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 PC, 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

Como establezca la DPC de RPP-PKI.

9.12. Procedimientos de cambios en las especificaciones

9.12.1. Procedimiento para los cambios

Como establezca la DPC de RPP-PKI.

9.12.2. Circunstancias en las que el OID debe ser cambiado

Como establezca la DPC de RPP-PKI.

9.13. Reclamaciones

Como establezca la DPC de RPP-PKI.

9.14. Normativa aplicable

Como establezca la DPC de RPP-PKI.

9.15. Cumplimiento de la normativa aplicable

Como establezca la DPC de RPP-PKI.



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

Política de Certificación de Representante de Persona Jurídica

Código:
P-22

Versión:
0.3

Fecha de implementación:
21 de diciembre de 2021

Página: 50 de 50

9.16. Estipulaciones diversas

9.16.1. Cláusula de aceptación completa

Como establezca la DPC de RPP-PKI.

9.16.2. Independencia

En el caso de que una o más estipulaciones de esta PC 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 PC careciera ésta de toda eficacia jurídica.

9.16.3. Resolución por la vía judicial

Como establezca la DPC de RPP-PKI.

9.17. Otras estipulaciones

No se contemplan otras estipulaciones.