Proveedor de Certificados PROCERT, C.A.
Política de Certificados (PC)

Fecha	Agosto, 2025
Edición	1
Versión	1
Elaborado por	Gerencia General agosto 2025
Aprobado	Alta Dirección agosto 2025
Descripción	Política de Certificado (PC)
Vigente	Si

Página

1. Introducción.

El PSC PROCERT procede a la emisión y publicación de presente documento de la política de certificado electrónico, la cual incluye todos los tipos de certificados de valor extendido emitidos a favor de terceros y parte final y el cual tiene como fin, documentar, informar a la alta dirección, personal, proveedores, clientes y parte interesada del PSC PROCERT, cerca del uso autorizado y soporte técnico de los certificados electrónicos emitidos por el PSC PROCERT. Los clientes, proveedores o parte interesada que utilicen los certificados electrónicos emitidos por el PSC PROCERT deberán dar cumplimiento la presente política de certificado, a los fines de conocer las responsabilidades y obligaciones del PSC PROCERT, respecto al ciclo de vida de los certificados, el proceso de gestión de certificados electrónicos. La presente política se encuentre ajustada a los mandatos impuestos por el Decreto Ley de Mensajes de Datos y Firmas Electrónicas (LSMDFE), su Reglamento y marco normativo que regula la materia dentro de la República Bolivariana de Venezuela y a las normas internacionales del CA Browser Fórum y los RFC 2026, RFC 2119, RFC 2560, RFC 3647, RFC 3779, RFC 5055, RFC 5736, RFC 6480, RFC 6481, RFC 6482, RFC 6484, RFC 6486, RFC 6487, RFC 6489 y RFC 6492. Las palabras clave "DEBE", "NO DEBE", "REQUERIDO", "DEBE", "NO DEBE", "DEBE", "NO DEBE", "RECOMENDADO", "PUEDE" y "OPCIONAL" en este documento de la Política de Certificado deben interpretarse como se describe en RFC 2119.

1.1. Descripción General.

El PSC PROCERT posee una Public Key Infraestructure (PKI) que es una infraestructura de clave pública que ha sido creada y soporta la emisión de certificados electrónicos y de los medios de validación del estatus d ellos certificados y reclamos por el funcionamiento de estos por parte de los actuales propietarios de certificados electrónicos en sus distintas configuraciones y bajo la Raíz de Certificación del Estado Venezolano. La capacidad de verificar la situación de los certificados y de su estado es esencial para garantizar la distribución inequívoca de estos recursos de certificación electrónica conforme al RFC 6480. La estructura de la PKI del PSC PROCERT es congruente con el marco de asignación de recursos numéricos de Internet. Y con los suministrados por la IANA a través de los Registros Regionales de Internet (RIR) conforme a lo establecido en el RFC 5736. Los RIR, a su vez, administran la asignación de recursos numéricos a usuarios finales de los certificados electrónicos emitidos por el PSC PROCERT.

La PKI del PSC PROCERT abarca varios tipos de certificados conforme a lo establecido por el RFC 6487. Estos certificados son los siguientes:

- Certificado electrónico de firma para empleados de empresa.
- Certificado electrónico de firma para representantes de empresas públicas.
- Certificado electrónico de firma para representante legal de empresa privada.
- Certificado electrónico de firma para profesionales titulados.
- Certificado electrónico de firma para persona natural.
- Certificado electrónico de firma para funcionario público.
- Certificado electrónico para firma de transacción.
- Certificado electrónico de factura electrónica.
- Certificado Electrónico de banca electrónica.
- Certificado Electrónica para Procesos de Justicia Electrónica.

- Certificado Electrónico para el mercado de capitales.
- Certificado Electrónico para personal diplomático.
- Certificado Electrónico para OCSP.

1.2. Nombre e identificación del documento.
El presente documento es contentivo de la Política de Certificado (PC) del PSC PROCERT y que enuncia, regula y establece los certificados que son emitidos por la PKI del PSC PROCERT. A los fines de su comprobación y validación se le ha asignado a la presente PC el siguiente OID:

- id-cp-ipAddr-asNumber IDENTIFICADOR DE OBJETO: = {iso (1)
- organización-identificada (3) dod (6) internet (1)
- seguridad (5) mecanismos (5) pkix (7) cp (14) 2}

1.3. Participantes de la PKI del PSC PROCERT.
A los fines de la PKI del PSC PROCERT el término suscriptor será sustituido por signatario a los fines de cumplir con la Ley Sobre Mensajes de Datos y Firmas Electrónicas y la normativa de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE); y se refiere a una persona u organización que es objeto de un certificado emitido por la Autoridad de Certificación o Certificaction Authority (CA) del PSC PROCERT CA. El término se usa de esta manera a lo largo de este documento y sin calificación. Igualmente, considere que, a los fines de simplificar este documento, siempre nos referiremos a los participantes signatarios de la PKI del PSC PROCERT como organizaciones o entidades, aunque algunos de ellos sean individuos.

1.3.1. Autoridades de Certificación.
Se refiere a la CA dentro de la PKI del PSC PROCERT encargada de emitir certificados para usuarios finales y que son denominados signatarios. Existe una CA Raíz para la PKI del PSC PROCERT, que firma cada CA, por cada tipo de grupo de certificado emitido, siendo distribuidas de la siguiente manera:

- S/MIME: Es la Autoridad Certificadora (CA) encargada de emitir certificados de seguridad de correo electrónico (S/MIME) a modo multipropósito el cual su uso incluye la firma de documentos (DS).

1.3.2. Autoridad de Registro.
Es la organización interna dentro del PSC PROCERT encargada de validar y comprobar la identificación y los datos suministrados por las personas jurídicas o naturales que compren certificados electrónicos y con el fin de poder dar fe pública que el cliente que detenta y usa un certificado electrónico de la PKI del PSC PROCERT, es quien efectivamente dice ser o representar en el caso de persona jurídica, garantizando de esa manera la identidad del signatario y en consecuencia, legalidad de las responsabilidades y obligaciones derivadas del uso de la firma electrónica bajo los supuestos del decreto ley sobre mensajes de datos y firmas electrónicas y su reglamento. Todos los interesados en obtener un certificado electrónico bajo el decreto ley sobre mensajes de datos y firmas electrónicas, su reglamento y la normativa de la SUSCERTE, deberán remitir copia de la documentación soporte de sus datos y acudir a la cita

fijada por la AR del PSC PROCERT a los efectos de realizar la verificación, validación presencial y documental de los registros, soportes y demás comprobantes que acreditan su identidad y/o representación de los representantes de personas jurídicas que opten por un certificado electrónico.

Si el interesado no atiende la entrevista pautada por la AR del PSC PROCERT quedará anulada su solicitud o petición de registro y se aplicará la retención por penalidad, debiendo en consecuencia el interesado proceder nuevamente a su registro de solicitud de certificado electrónico ante la página web del PSC PROCERT. La documentación soporte utilizada para validar las solicitudes de certificados electrónico, será almacenada por el PSC PROCERT, durante el período de diez (10) años contados a partir de la vigencia del certificado o de cualquiera de sus renovaciones.

1.3.3. Suscriptores o Signatarios

El terminó suscriptor será sustituido por el de signatario a los fines de dar cumplimiento con el Decreto Ley de Mensajes de Datos y Firmas Electrónicas (LSMDFE), su Reglamento y marco normativo que regula la materia dentro de la República Bolivariana de Venezuela. Los signatarios serán todas las personas que reciban certificados electrónicos de la PKI del PSC PROCERT.

1.3.4. Partes que confían

Es todo signatario o persona física o jurídica que sin ser signatario confían en los certificados electrónicos generados por la PKI del PSC PROCERT bajo la Raíz de Certificación del Estado Venezolano.

1.3.5. Otros Participantes

Son aquellas entidades relacionadas a la PKI del PSC PROCERT que asumen una función de CA bajo la mencionada PKI y son responsables de responsable mantener el estándar PKI del PSC PROCERT y publicar los repositorios con los certificados, CRL y objetos firmados de PKI que emite. El PSC PROCERT no posee a la fecha otra entidad participante dentro de su PKI.

1.4. Uso del certificado

1.4.1. Usos apropiados del certificado

Los certificados electrónicos emitidos bajo la PKI del PSC PROCERT poseen unos usos específicos asignados por estándar y norma interna del PSC PROCERT. Todos los certificados electrónicos de firma asignados a signatarios tienen los siguientes usos:

Usos certificados S/MIME	Uso mejorado certificados S/MIME
Firma electrónica, cifrado de llave, no repudio y cifrado de datos.	Firma de documentos, correo seguro

Uso certificado OCSP	Uso mejorado certificado OCSP
Firma electrónica.	OCSP Signing

Adicionalmente, se utilizan para las siguientes actividades:

1.4.1.1. Certificado electrónico de firma para empleados de empresa: El uso asignado para este tipo de certificado es el siguiente:

- Transacciones en línea.
- Identificar en línea a empleados o trabajadores de empresas públicas o privadas.
- Comunicaciones electrónicas sin representación de empresas públicas o privadas.
- No confiere representación legal de empresas públicas o privadas.

1.4.1.2. Certificado electrónico de firma para representantes de empresas públicas: El uso asignado para este tipo de certificado es el siguiente:

- Certificar a una persona como representante legal de una entidad jurídica pública.
- Transacciones en línea públicas o privadas, en representación de empresas o entidades de derecho público.
- Comunicaciones privadas o públicas en representación de empresas o entidades de derecho público.
- Comercio electrónico en representación de empresas o entidades de derecho público.
- Declaraciones o trámites en línea ante gobierno en representación de empresas o entidades de derecho público.

1.4.1.3. Certificado electrónico de firma para representante legal de empresa privada: El uso asignado para este tipo de certificados es el siguiente:

- Certificar a una persona como representante legal de una entidad jurídica privada.
- Transacciones en línea públicas o privadas, en representación de una sociedad mercantil, civil u otra forma societaria.
- Comunicaciones privadas o públicas en representación de una sociedad mercantil, civil u otra forma societaria.
- Comercio electrónico en representación de una sociedad mercantil, civil u otra forma societaria.
- Declaraciones o trámites en línea ante gobierno en representación de una sociedad mercantil, civil u otra forma societaria.

1.4.1.4. Certificado electrónico de firma para profesionales titulados: El uso asignado para este certificado es el siguiente:

- Transacciones en línea asociadas al ejercicio de profesión u oficio con colegiatura y reconocimiento legal dentro de la República Bolivariana de Venezuela.
- Comunicaciones privadas o públicas asociadas al ejercicio de profesión u oficio con colegiatura y reconocimiento legal dentro de la República Bolivariana de Venezuela.
- Comercio electrónico asociado al ejercicio de profesión u oficio con colegiatura y reconocimiento legal dentro de la República Bolivariana de Venezuela.
- Declaraciones o trámites en línea ante gobierno asociadas al ejercicio de profesión u oficio con colegiatura y reconocimiento legal dentro de la República Bolivariana de Venezuela.

1.4.1.5. Certificado electrónico de firma para persona natural: El uso asignado para este tipo de certificado es el siguiente:

- Transacciones privadas, distintas a prestación de servicios profesionales.
- Comunicaciones privadas o públicas a título personal.
- Compras electrónicas para personas naturales.
- Declaraciones o trámites en línea ante gobierno para personas naturales.

1.4.1.6. Certificado de firma electrónica para funcionario público: El uso asignado para este tipo de certificado es el siguiente:

- Certificar a una persona como funcionario público de carrera, de libre nombramiento o remoción o de elección popular y a que ente de gobierno se encuentra adscrito o pertenece.
- Transacciones en línea públicas o privadas, en representación a entidades de gobierno centralizado o descentralizado.
- Comunicaciones privadas o públicas en representación de Entidades de gobierno centralizado o descentralizado.
- Comercio electrónico en representación de entidades de gobierno centralizado o descentralizado.
- Declaraciones o trámites en línea ante gobierno en representación de entidades de gobierno centralizado o descentralizado.
- Firma Electrónica de correos y documentos electrónicos

1.4.1.7. Certificado electrónico para firma de transacción: El uso asignado para este tipo de certificado es el siguiente:

- Protección de transacción en línea o fuera de conexión.
- Prueba legal del registro de transacción.
- Integridad de la Información.
- No repudio.

- Firma electrónica de archivos y documentos electrónicos.

1.4.1.8. Certificado electrónico para firma de Factura Electrónica: El uso asignado al certificado de Certificado Electrónico de Factura Electrónica es el siguiente:

- Protección de transacción en línea.
- Prueba legal del comprobante electrónico.
- Integridad de la Información.
- No repudio
- Firma Electrónica de documentos electrónicos.

1.4.1.9. Certificado Electrónico de Banca Electrónica: El uso asignado al Certificado Electrónico de Banca Electrónica es el siguiente:

- Firma Electrónica.
- Protección de transacción en línea.
- Prueba legal del comprobante electrónico.
- Integridad de la Información.
- No repudio.

1.4.1.10. Certificado de Firma Electrónica para Procesos de Justicia Electrónica: El uso asignado al certificado de firma electrónica para despacho virtual es el siguiente:

- Firma electrónica de la documentación/comunicaciones electrónicas relacionadas a aquellas acciones que se lleven a cabo en juicio y que sean factibles de ser firmadas electrónicamente y con el fin de garantizar su integridad, autenticidad y no repudio, y sean autorizadas y avaladas de esa forma por el ente que regula la materia.
- Prueba de identidad, No Repudio y Autoría.
- Prueba de integridad de la información.

1.4.1.11. Certificado electrónico para mercado de capitales: El uso asignado al certificado electrónico para mercado de capitales es el siguiente:

- Firma Electrónica.
- Protección de transacción en línea.
- Prueba legal del comprobante electrónico.
- Integridad de la Información.
- No repudio.

1.4.1.12. Certificado de firma electrónica para personal diplomático: El uso asignado al certificado de firma electrónica para personal diplomático es el siguiente:

- Certificar que una persona está acreditada como representante o personal diplomático debidamente acreditado y reconocido por la República Bolivariana de Venezuela.
- Transacciones en línea públicas o privadas, en representación de una república, reino, protectorado o país con los cuales la República Bolivariana de Venezuela mantenga relaciones diplomáticas.
- Comunicaciones privadas o públicas en representación de una república, reino, protectorado o país con los cuales la República Bolivariana de Venezuela mantenga relaciones diplomáticas.
- Comercio electrónico en representación de una república, reino, protectorado o país con los cuales la República Bolivariana de Venezuela mantenga relaciones diplomáticas.
- Declaraciones o trámites en línea ante el Gobierno de la República Bolivariana de Venezuela.
- Firma Electrónica de Correos Electrónicos y Documentos Electrónicos.

1.4.1.13. Certificado Electrónico de OCSP: El uso asignado al Certificado Electrónico OCSP es el siguiente:

- Firma Electrónica.

1.4.2. Usos prohibidos del certificado

Los signatarios de certificados electrónicos generados por la PKI del PSC PROCERT, se obligan a utilizarlos conforme a los usos permitidos y señalados en la sección anterior y los establecidos por el Decreto Ley de Mensajes de Datos y Firmas Electrónicas (LSMDFE), su reglamento y otras normas de carácter sublegal vigentes o cualquier texto normativo que los sustituya y regule la actividad de certificación electrónica dentro de la República Bolivariana de Venezuela, y para el uso para el cual fue adquirido, quedando expresamente indicado que cualquier violación a las normas, usos y/o leyes de la República Bolivariana de Venezuela queda bajo la responsabilidad del signatario, así como los daños y perjuicios que ocasionare y en un todo le será aplicable las previsiones que al efecto estén contenidas en la ley de ilícitos informáticos y supletoriamente el código penal y procesal penal venezolano. El certificado electrónico cuyo signatario viole el uso autorizado, será revocado. Adicionalmente el cliente signatario asume la responsabilidad de indemnizar al PSC PROCERT por daños y perjuicios ocasionados a terceros derivados de reclamos, acciones, efectos de acción, pérdidas o daños (incluyendo multas legales) que se generaren por el uso indebido del servicio contratado.

1.5. Administración de Política

1.5.1. Organización que administra el documento.

Este CP es administrado por:
Gerencia General
Multicentro Empresarial del Este, Núcleo B, Torre Libertador, Piso 13, Oficina B-132, Municipio Chacao, Caracas. 1010.
República Bolivariana de Venezuela.

1.5.2. Persona de contacto.
La persona encargada de la administración del documento y a quien se debe contactar es el Gerente General

Correo electrónico: gerencia.general@procert.net.ve
Teléfono: +58 (0212) 2674880

1.5.3. Procedimientos de aprobación de CP.
Los procesos asociados a la revisión, aprobación, modificación o ajuste de la documentación del PSC PROCERT serán regulados por la política de documentación y gestión documental (AC-PO-0002). La presente PC será modificada y el reemplazo DEB ser aprobado en caso de modificación en el RFC 6484 o sustitución de este y en la normative de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) de la República Bolivariana de Venezuela.

1.6. Definiciones y Acrónimos
CPS – Certificate Practice Statement o Declaración de Prácticas de Certificación. Una CPS es un documento que especifica las prácticas que una Autoridad de Certificación (CA) del PSC PROCERT emplea en la emisión de certificados bajo su PKI.

IANA - Autoridad de Números Asignados en Internet. IANA es responsable de coordinación global del sistema de direccionamiento IP y números AS Se utiliza para enrutar el tráfico de Internet. IANA distribuye INR a Registros Regionales de Internet (RIR).

INR - Recursos numéricos de Internet. Los INR son valores numéricos para tres conjuntos de parámetros de protocolo, a saber:

- Direcciones IP versión 4,
- Direcciones IP versión 6, y
- Identificadores utilizados en el enrutamiento entre dominios de Internet, actualmente Border Gateway Protocol-4 AS números.

ISP - Proveedor de servicios de Internet. Esta es una organización que administra y proporcionar servicios de Internet a otras organizaciones.

LIR - Registro Local de Internet. En algunas regiones, este término se utiliza para referirse a lo que se llama un ISP en otras regiones.

NIR - Registro Nacional de Internet. Esta es una organización que gestiona la distribución de INR para una parte del área geopolítica cubierta por un Registro Regional. Formulario NIR un segundo nivel opcional en el esquema de árbol utilizado para administrar INR.

RIR - Registro Regional de Internet. Esta es una organización que gestiona la distribución de INR para un área geopolítica.

Objeto firmado por PKI: un objeto firmado por RPKI es un archivo de datos firmado digitalmente. objeto (que no sea un certificado o CRL) que se declara a ser tal por

un Standards Track RFC, y que puede ser validado usando certificados emitidos bajo esta PKI. el contenido y el formato de estas construcciones de datos depende del contexto en el que se lleva a cabo la validación de las reclamaciones de las tenencias actuales de INR. Ejemplos de estos objetos son manifiestos de repositorio [RFC6486] y Autorizaciones de origen de ruta (ROA) [RFC6482].

Certification Authority (CA) o Autoridad de Certificación: Significa una autoridad en la cual confían los signatarios para crear, emitir y manejar el ciclo de vida de los certificados, la cual a los efectos del Decreto Ley de Mensajes de Datos y Firmas Electrónicas debe contar con la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

Register Authority (RA) o Autoridad de registro: Significa la entidad cuyo propósito es suministrar apoyo local a la PKI del PSC PROCERT. La AR desempeña un conjunto de funciones orientadas a la validación, comprobación y conformación de la documentación suministrada, así como la identidad física de un signatario que opte a la compra de una firma o certificado electrónicos generado por la PKI del PSC PROCERT.

Cadena de certificado: Significa una cadena de múltiples certificados necesarios para validar un certificado. Las cadenas de certificado se construyen mediante la vinculación y verificación de la firma electrónica en un certificado con una clave pública que se encuentra en un certificado emitido por la CA de la PKI (AC) de PROCERT, la cual se encuentra subordinada y firmada por el certificado raíz generado por la SUSCERTE.
Certificado: Significa una estructura de datos que utiliza el estándar CCITT ITU X.509, que contiene la clave pública de una entidad junto a información asociada y presentada como "un-forgettable" (inolvidable), mediante una firma electrónica de la Autoridad de Certificación que la generó.

Certificado de clave pública: Significa el certificado electrónico que une a la Clave Pública de una entidad con el identificador distintivo de la entidad y que indica un período de validez específico.

Cifrado: Significa el proceso mediante el cual los datos simples de un texto son transformados para ocultar su significado. El cifrado es un proceso reversible que se efectúa mediante el uso de un algoritmo criptográfico y una clave.

Firma electrónica: Significa el dato añadido o una transformación criptográfica de una unidad de dato que permite al receptor de la unidad de dato probar la fuente y la integridad del dato y protegerse contra falsificaciones, por ejemplo, del destinatario.

Certification Revoke List (CRL) o Lista de certificados revocados: Significa la lista de certificados que han sido revocados o suspendidos por el PSC PROCERT.

On Line Certificate Status Protocol (OCSP) o Protocolo de estatus de certificado en-línea: Es un protocolo utilizado para validar el estatus de un certificado en tiempo real. La respuesta de las solicitudes incluye tres (3) estatus: valido, revocado o desconocido.
PSC: Significa Proveedor de Servicios de Certificación
Revocación: Significa el cambio de estatus de un certificado válido o suspendido a “revocado” a partir de una fecha específica en adelante.

Revocación de certificado: Significa el proceso que consiste en cambiar el estatus de un certificado de válido o suspendido o revocado. Cuando un certificado tiene estatus revocado, esto significa que una entidad ya no se debe confiar en él para ningún fin.

Servicios de certificación: Significa los servicios que se pueden suministrar con relación al manejo del ciclo de vida de los certificados a cualquier nivel de la jerarquía de la ICP, incluyendo servicios auxiliares tales como servicios OCPS, servicios de tiempo compartido, servicios de verificación de identidad, hospedaje de Lista de Certificados Revocados (LCR), etc.

Signatario: Significa la entidad que ha solicitado la emisión de un certificado dentro de la PKI del PSC PROCERT. El proceso de verificación varía de acuerdo con la naturaleza y, donde aplique, el rol operacional dentro de la PKI correspondiente al certificado que la entidad está solicitando.

2. Responsabilidades de publicación y depósito.
   2.1. Repositorios.
   Los certificados, las CRL y los objetos firmados por RPKI (destinados al consumo público) DEBEN estar disponibles para su descarga por parte de todas las partes que confían, para permitirles validar estos datos. Esto motiva el uso de un sistema de repositorio distribuido robusto. Cada CA DEBE mantener un repositorio en línea de acceso público y publicar todos los objetos firmados por RPKI (destinados al consumo público) a través de este repositorio de una manera que se ajuste a Un perfil para la estructura del repositorio de certificados de recursos.

   2.2. Publicación de Información de Certificación.
   Cada CA de la PKI del PSC PROCERT DEBE publicar los certificados (destinados al consumo público) que emite a través del sistema de repositorio. Cada CA de la PKI del PSC PROCERT DEBE publicar las CRL (destinadas al consumo público) que emite a través del sistema de repositorio. Cada CA de la PKI del PSC PROCERT DEBE publicar sus objetos firmados PKI (destinados al consumo público) a través del sistema de repositorio.

   Cada CA de la PKI del PSC PROCERT que emita certificados a entidades fuera de su dominio administrativo DEBE crear y publicar una CPS que cumpla con los requisitos establecidos en esta CP; el PSC PROCERT no mantiene a la fecha entidades fuera de su dominio asociada a su PKI. La publicación significa que las entidades a las que la CA emite certificados DEBEN poder adquirir una copia de la CPS, y DEBEN poder determinar cuándo cambia la CPS.

   2.3. Hora o frecuencia de publicación.
   La DPC de cada CA de la PKI del PSC PROCERT DEBE especificar la siguiente información:

   - El período de tiempo dentro del cual se publicará un certificado después de que la CA emita el certificado.
   - El período de tiempo dentro del cual una CA publicará una CRL con una entrada para un certificado revocado después de revocar ese certificado.
   - Los certificados vencidos y revocados DEBERÍAN ser eliminados del sistema de depósito de RPKI, al vencimiento o revocación, respectivamente.

- Además, tenga en cuenta que cada CA DEBE publicar su CRL antes del valor de Next Update en la CRL programada emitida previamente por la CA.

2.4. Controles de acceso en repositorios.
Cada CA u operador de repositorio DEBE implementar controles de acceso para evitar que personas no autorizadas agreguen, modifiquen o eliminen entradas del repositorio. Una CA u operador de repositorio NO DEBE utilizar intencionalmente medios técnicos para limitar el acceso de lectura a sus CPS, certificados, CRL u objetos firmados por PKI. Estos datos están destinados a ser accesibles al público.

3. Identificación y autenticación.

3.1. Denominación.

3.1.1. Tipos de nombres.
El nombre distinguido de cada CA de la PKI del PSC PROCERT y entidad final consta de un solo atributo CommonName (CN) con un valor generado por el emisor del certificado. Opcionalmente, el atributo serialNumber PUEDE incluirse junto con el nombre común (para formar un terminal relativo conjunto de nombres distinguidos), para distinguir entre instancias sucesivas de certificados asociados con la misma entidad.

3.1.2. Necesidad de que los nombres sean significativos.
El nombre del sujeto en cada certificado DEBE ser "significativo", es decir, el nombre debe transmitir la identidad del signatario o sujeto, a las partes que confían. La razón aquí es que los certificados emitidos bajo la PKI del PSC PROCERT se utilizan para identificar personas, otorgar la autoría y el no repudio y ofrecer prueba legal.

3.1.3. Anonimato o Seudónimo de los Signatarios.
El anonimato no es una función de esta PKI; por lo tanto, no se proporciona soporte explícito para esta función. Igualmente, no se tramitará ninguna solicitud anónima o que no permita establecer la identidad del signatario por parte de la AR.

3.1.4. Reglas para interpretar varias formas de nombres.
No Aplica. Todos los nombres deben ser significativos.

3.1.5. Singularidad de los nombres.
No hay garantía de que los nombres de los sujetos sean globalmente únicos en esta PKI del PSC PROCERT. Cada CA certifica nombres de sujeto que DEBEN ser únicos entre los certificados que emite. Aunque es deseable que estos nombres de sujeto sean únicos en toda la PKI del PSC PROCERT, no se puede garantizar la exclusividad de los nombres dentro de la PKI del PSC PROCERT. Sin embargo, los nombres de los sujetos en los certificados DEBERÍAN construirse de manera que se minimicen las posibilidades de que a dos entidades en la PKI se les asigne el mismo nombre.

3.2. Validación de identidad inicial.

3.2.1. Método para probar la posesión de la clave privada
Cada CA que opere dentro de la PKI del PSC PROCERT DEBE exigir que cada sujeto demuestre prueba de posesión (PoP) de la clave privada correspondiente a la clave pública en el certificado, antes de emitir el

certificado. Cada CA de la PKI del PSC PROCERT determina los medios por los cuales se logra el PoP y DEBEN declararse en la CPS de cada CA de la PKI del PSC PROCERT.

3.2.2. Autenticación de la identidad de la organización.
Cada CA de la PKI del PSC PROCERT que opere dentro del contexto de esta PKI DEBE emplear procedimientos para garantizar que cada certificado que emita refleje con precisión sus registros con respecto a la organización a la que la CA ha solicitado la emisión de un certificado electrónico. Los procedimientos específicos empleados para este fin DEBEN ser descritos por la CPS para cada CA de la PKI del PSC PROCERT.

Las partes que confían pueden esperar que cada CA de la PKI del PSC PROCERT emplee procedimientos proporcionales a los que ya emplea como registro. Esta autenticación es para uso exclusivo de cada CA de la PKI del PSC PROCERT en el trato con las organizaciones a las cuales ha emitido certificados electrónicos y debe confiarse en ella fuera de esta relación CA-signatario.

3.2.3. Autenticación de Identidad Individual.
Cada CA de la PKI del PSC PROCERT que opere dentro del contexto de esta PKI DEBE emplear procedimientos para identificar a cada persona en el caso de los certificados para personas naturales o a los representantes de cada organización en el caso de que se trate de una persona jurídica. Los medios específicos por los cuales cada CA autentica a las personas como representantes de una organización o de sí mismas DEBEN ser descritos por la CPS para cada CA de la PKI del PSC PROCERT. Las partes que confían pueden esperar que cada CA emplee procedimientos proporcionales a los que ya emplea como registro para autenticar a las personas.

3.2.4. Información de suscriptor no verificada.
Una CA NO DEBE incluir ningún dato de suscriptor no verificado en los certificados emitidos bajo esta política de certificados, excepto para las extensiones de acceso a la información del sujeto (SIA).

3.2.5. Validación de Autoridad.
Cada CA que opere dentro del contexto de la PKI del PSC PROCERT DEBE emplear procedimientos para verificar que una persona que dice representar a una organización para la cual se emite un certificado está autorizada para representar a esa organización en este contexto. Los procedimientos DEBEN ser descritos por la CPS para la CA de la cual se trate. Las partes que confían pueden esperar que cada CA emplee procedimientos proporcionales a los que ya emplea como registro, para autenticar a las personas como representantes de los titulares de INR.

3.2.6. Criterios para la Interoperación.
Esta PKI no está pensada ni diseñada para interoperar con ninguna otra PKI.

3.3. Identificación y autenticación para solicitudes de cambio de clave.
3.3.1. Identificación y autenticación para cambio de clave de rutina.

Cada CA que opere dentro del contexto de la PKI del PSC PROCERT DEBE emplear procedimientos para garantizar que una organización que solicita una nueva clave sea el titular legítimo del certificado que se va a volver a generar y DEBE solicitar PoP de la clave privada correspondiente a la nueva clave pública. Los procedimientos empleados para estos fines DEBEN estar descritos en la DPC de la AC de la PKI del PSC PROCERT. Con respecto a la autenticación del titular, las partes que confían pueden esperar que cada CA emplee procedimientos proporcionales a los que ya emplea como registro, en la gestión de datos de los signatarios.

3.3.2. Identificación y autenticación para la renovación de la clave después de la revocación.

Cada CA que opere en la PKI del PSC PROCERT DEBE emplear procedimientos para garantizar que una organización que solicite una nueva clave después de la revocación sea la misma entidad para la que se emitió el certificado revocado y sea el titular legítimo. La CA de la PKI del PSC PROCERT DEBE requerir PoP de la clave privada correspondiente a la nueva clave pública. Los procedimientos específicos empleados para estos fines DEBEN ser descritos por la CPS para la CA de la PKI del PSC PROCERT. Con respecto a la autenticación del titular, las partes que confían pueden esperar que cada CA emplee procedimientos proporcionales a los que ya emplea como registro, en la gestión de las solicitudes de los signatarios. Tenga en cuenta que PUEDE haber diferentes procedimientos para el caso en que el sujeto legítimo aún posee la clave privada original en comparación con el caso en que ya no tiene acceso a esa clave.

3.4. Identificación y Autenticación para Solicitud de Revocación.

Cada CA que opere dentro de la PKI del PSC PROCERT DEBE emplear procedimientos para garantizar que:

- Una organización que solicita la revocación es el titular legítimo del certificado a revocar.
- Cada certificado que revoca refleja con precisión sus registros con respecto a la organización a la que la CA ha distribuido el certificado.
- Un individuo que afirme representar a una organización para la cual se va a revocar un certificado está autorizado a representar a esa organización en este contexto.

Los procedimientos específicos empleados para estos fines DEBEN ser descritos por la CPS para la CA de la PKI del PSC PROCERT. Las partes que confían pueden esperar que cada CA emplee procedimientos proporcionales a los que ya emplea como registro, en la gestión de los certificados y asignación de estos a los signatarios.

4. Requisitos operativos del ciclo de vida del certificado.

4.1. Solicitud de certificado

4.1.1. Quién puede presentar una solicitud de certificado.

Todo interesado en adquirir un certificado electrónico deberá gestionarlo ante la PKI del PSC PROCERT y cumplir los requisitos técnicos y legales exigidos para cada tipo de certificado. El procedimiento de solicitud DEBE estar descrito en la DPC de cada CA de la PKI del PSC PROCERT.

4.1.2. Proceso de inscripción y responsabilidades.

La CPS DEBE describir el proceso y los procedimientos de inscripción para cada CA de la PKI del PSC PROCERT. Una entidad que desee uno o más certificados debe comunicarse con la PKI del PSC PROCERT y suministrar toda la información técnica y legal que le sea requerida. La PKI del PSC PROCERT no está obligada a gestionar las solicitudes de certificados que no cumplan los requisitos técnicos y legales.

4.2. Procesamiento de solicitudes de certificados.

Las CA DEBERÍAN hacer uso de los estándares existentes para el procesamiento de solicitudes de certificados. La sección 6 del perfil de certificado de recursos [RFC 6487] define los formatos de solicitud de certificado estándar que DEBEN admitirse. Cada CA DEBE definir a través de su CPS, los estándares de solicitud/respuesta de certificados que emplea.

4.2.1. Realización de funciones de identificación y autenticación.

Las prácticas existentes empleadas por los registros y los ISP para identificar y autenticar organizaciones que reciben INR forman la base para emisión de certificados a estos suscriptores. Es importante tener en cuenta que la PKI de recursos DEBE utilizarse para autenticar la identidad de una organización, y para vincular a los suscriptores a la INR que tienen. La PKI del PSC PROCERT DEBE garantizar la identidad de los signatarios y verificar que sus procedimientos para gestionar solicitudes de certificados cumplan con la debida validación de la información de identidad de los signatarios y verificar los nombres de organizaciones legales, etc.

4.2.2. Aprobación o Rechazo de Solicitudes de Certificado.

Las solicitudes de certificados DEBEN ser aprobadas en base a las prácticas comerciales, técnicas y legales de la PKI del PSC PROCERT. Cada CA DEBE seguir los procedimientos especificados en la Sección 3.2.1 para verificar que el solicitante posee la clave privada correspondiente a la clave pública que se vinculará al certificado que la CA emite al solicitante. Los detalles de cómo se aprueban las solicitudes de certificados DEBEN estar descritos en la CPS de la CA en cuestión.

4.2.3. Tiempo para procesar las solicitudes de certificados.

Toda solicitud de certificado electrónica deberá ser acompañada de los requisitos exigidos por la RA de la PKI del PSC PROCERT, cumplir los procesos de la RA y cumplir con el pago del certificado para el procesamiento de la solicitud. Una vez cumplidos estos pasos el lapso de emisión de certificado no supera las seis (6) horas. El lapso de procesamiento y emisión de certificados se encuentra descrito en la CPS del PSC PROCERT.

4.3. Emisión de certificados.

4.3.1. Acciones de CA durante la emisión de certificados.

Si una CA determina que la solicitud es aceptable, DEBE emitir el certificado correspondiente y publicarlo en el sistema de repositorio distribuido de la PKI del PSC PROCERT mediante la publicación del certificado en la sede de la CA. El signatario deberá descargar su certificado y modificar la clave de acceso a su usuario dentro del sistema de RA d la PKI del PSC PROCERT.

4.3.2. Notificación al Suscriptor por parte de la CA de Emisión de Certificado.
La CA DEBE notificar al signatario cuando se publique el certificado. El medio por el cual se notifica al signatario es mediante correo electrónico enviado a la dirección de correo electrónico previamente validada por la RA de la PKI del PSC PROCERT. El proceso de notificación de gestión del certificado se encuentra definido en la CPS del PSC PROCERT.

4.4. Aceptación del certificado.

4.4.1. Conducta que constituye la aceptación del certificado.
Dentro de las seis (6) horas siguientes a la validación conforme de todos los requisitos técnicos y legales, se procederá a la aprobación del certificado electrónico, lo cual será debidamente notificado al signatario. La descarga del certificado y su uso se constituye en la aceptación del mismos por parte del signatario; esta información se encuentra indicada en la CPS del PSC PROCERT. Aprobado el certificado electrónico por la CA se DEBE colocar el certificado en el repositorio y notificar al signatario. Esto PUEDE hacerse sin la revisión y aceptación del signatario. Los lapsos para la publicación del certificado y notificación al suscriptor se encuentran definidos en la CPS del PSC PROCERT.

4.4.2. Publicación del Certificado por la CA
Los certificados DEBEN publicarse en el sistema de repositorio distribuido de PKI mediante la publicación del certificado en el punto de publicación del repositorio de la CA según la conducta descrita en la Sección 4.4.1. Los procedimientos para la publicación DEBEN ser definidos por cada CA en su CPS.

4.4.3. Notificación de Emisión de Certificados por parte de la CA a Otras Entidades.
La CPS de cada CA DEBE indicar si se notificará a otras entidades cuando se emita un certificado. La PKI del PSC PROCERT no mantiene a la fecha relación con otras entidades y por ende no está obligada a notificar.

4.5. Par de claves y uso de certificados.
A continuación, se proporciona un resumen del modelo de uso para la PKI del PSC PROCERT.

4.5.1. Uso del certificado y la clave privada del suscriptor.
Cada titular de un INR es elegible para solicitar un certificado de CA X.509 [X.509] que contenga las extensiones RFC 3779 apropiadas. Los titulares de certificados de recursos de CA también PUEDEN emitir certificados EE para permitir la verificación de los objetos firmados por RPKI que generan.

4.5.2. Uso de certificado y clave pública de usuario de confianza.
La confianza en un certificado debe ser razonable dadas las circunstancias. Si las circunstancias indican la necesidad de garantías adicionales, la parte que confía debe obtener dichas garantías para que dicha confianza se considere razonable. Antes de cualquier acto de confianza, las partes que confían DEBEN (1) verificar de forma independiente que el certificado se utilizará para un propósito adecuado que no esté prohibido o restringido por esta CP (consulte la Sección 1.4), y (2) evaluar el estado del certificado y

todos los certificados de la cadena (terminando en un ancla de confianza (TA) aceptada por el RP) que emitió los certificados correspondientes al certificado en cuestión.

Si alguno de los certificados en la cadena de certificados ha sido revocado o ha caducado, la parte que confía es la única responsable de determinar si la confianza en una firma digital para ser verificada por el certificado en cuestión es aceptable. Cualquier confianza de este tipo se realiza únicamente a riesgo de la parte que confía. Si una parte que confía determina que el uso del certificado es apropiado, la parte que confía debe utilizar el software y/o los hardware adecuados para realizar la verificación de la firma digital como condición para confiar en el certificado. Además, la parte que confía DEBE validar el certificado de manera coherente con el perfil de certificado RPKI [RFC6487], que especifica el algoritmo de validación ampliado para los certificados PKI.

4.6. Renovación de certificado.

Esta sección describe los procedimientos para la renovación del certificado. La renovación del certificado es la emisión de un nuevo certificado para reemplazar uno anterior antes de su vencimiento. Solo se modifican las fechas de validez y el número de serie (el campo del certificado, no el atributo DN). La clave pública y toda la demás información siguen siendo las mismas.

4.6.1. Circunstancia para la Renovación del Certificado.

Un certificado DEBE ser procesado para su renovación según su fecha de vencimiento o una solicitud de renovación del signatario. Antes del vencimiento del certificado de un signatario existente, es responsabilidad del signatario renovar el certificado para mantener la continuidad del uso del certificado. Si la CA emisora inicia el proceso de renovación en función de la fecha de vencimiento del certificado, esa CA DEBE notificar al titular antes del proceso de renovación.

El intervalo de validez del certificado nuevo (renovado) DEBERÍA superponerse al del certificado anterior para garantizar la continuidad del uso del certificado. Se RECOMIENDA que el certificado renovado se emita y publique al menos 1 semana antes del vencimiento del certificado que reemplaza. La renovación del certificado DEBE incorporar la misma clave pública que el certificado anterior, a menos que se haya informado que la clave privada está comprometida. Si se utiliza un nuevo par de claves, se aplican las estipulaciones de la Sección 4.8.

4.6.2. Quién puede solicitar la renovación.

Solo el signatario del certificado o la CA emisora a solicitud del signatario puede iniciar el proceso de renovación. El signatario del certificado PUEDE solicitar una renovación anticipada, por ejemplo, si espera no estar disponible para respaldar el proceso de renovación durante el período de vencimiento normal. Una CA emisora PUEDE iniciar el proceso de renovación en función de la fecha de vencimiento del certificado.

4.6.3. Procesamiento de solicitudes de renovación de certificados.
Los procedimientos de renovación DEBEN garantizar que la persona u organización que busca renovar un certificado sea de hecho el signatario autorizado del certificado y el titular legítimo del INR asociado con el certificado renovado. El proceso de renovación DEBE verificar que el certificado en cuestión no ha sido revocado.

4.6.4. Notificación de Emisión de Nuevo Certificado al Suscriptor.
No hay estipulaciones adicionales más allá de las de la Sección 4.3.2.

4.6.5. Conducta que constituye la aceptación de un certificado de renovación.
No hay estipulaciones adicionales más allá de las de la Sección 4.4.1.

4.6.6. Publicación del Certificado de Renovación por la CA.
No hay estipulaciones adicionales más allá de las de la Sección 4.4.2.

4.6.7. Notificación de Emisión de Certificados por parte de la CA a Otras Entidades.
No hay estipulaciones adicionales más allá de las de la Sección 4.4.3.

4.7. Renovación de clave de certificado.
En esta sección se describen los procedimientos para la renovación de la clave del certificado. La renovación de la clave del certificado es la emisión de un nuevo certificado para reemplazar uno anterior porque la clave necesita ser reemplazada. A diferencia de la reemisión del certificado, se cambia la clave pública.

4.7.1. Circunstancia para la renovación de la clave del certificado.
La renovación de la clave de un certificado DEBE realizarse solo cuando sea necesario, en función de:

- Conocimiento o sospecha de compromiso o pérdida de la clave privada asociada, o
- La expiración de la vida criptográfica del par de claves asociado

Una operación de cambio de clave de CA tiene consecuencias dramáticas, ya que requiere la reemisión de todos los certificados emitidos por la entidad a la que se le cambió la clave. Por lo tanto, debe realizarse solo cuando sea necesario y de una manera que conserve la capacidad de las partes de confianza para validar certificados cuya ruta de validación incluye la entidad con clave nueva.

La transferencia de clave de CA DEBE seguir los procedimientos definidos en "Transferencia de clave de CA en el PKI" [RFC6489]. Tenga en cuenta que, si se revoca un certificado para reemplazar las extensiones RFC 3779, el certificado de reemplazo DEBE incorporar la misma clave pública en lugar de una clave nueva. Esto se aplica cuando se agregan INR (no se requiere revocación) y cuando se eliminan INR (se requiere revocación (consulte la Sección 4.8.1)). Si la renovación de la clave se basa en una sospecha de compromiso, entonces el certificado anterior DEBE ser revocado.

4.7.2. Quién puede solicitar la certificación de una nueva clave pública.
El titular del certificado puede solicitar una re-clave. Además, la CA que emitió el certificado PUEDE optar por iniciar una nueva clave en función de un informe de compromiso verificado.

4.7.3. Procesamiento de solicitudes de cambio de clave de certificado.
El proceso de cambio de clave sigue los procedimientos generales de generación de certificados como se define en la Sección 4.3.

4.7.4. Notificación de Emisión de Nuevo Certificado al Suscriptor.
No hay estipulaciones adicionales más allá de las de la Sección 4.3.2.

4.7.5. Conducta que constituye la aceptación de un certificado con nueva clave.
No hay estipulaciones adicionales más allá de las de la Sección 4.4.1.

4.7.6. Publicación del Certificado Reemitido por la CA.
No hay estipulaciones adicionales más allá de las de la Sección 4.4.2.

4.7.7. Notificación de Emisión de Certificados por parte de la CA a Otras Entidades.
No hay estipulaciones adicionales más allá de las de la Sección 4.4.3.

4.8. Modificación de certificado.

4.8.1. Circunstancia para la modificación del certificado.
La modificación de un certificado se produce para implementar cambios en los valores de atributos seleccionados en un certificado. En el contexto de la PKI, los únicos cambios que se adaptan a la modificación del certificado son los cambios en las tenencias de INR descritos por las extensiones RFC 3779 y los cambios en la extensión SIA. Cuando se aprueba la modificación de un certificado, se emite un nuevo certificado. Si no se eliminan las existencias de INR del certificado, el nuevo certificado DEBE contener la misma clave pública y la misma fecha de vencimiento que el certificado original, pero con la extensión SIA y/o el conjunto de INR ampliado.

En este caso, no se requiere la revocación del certificado anterior. Cuando los INR previamente distribuidos se eliminan de un certificado, entonces se DEBE revocar el certificado anterior y se DEBE emitir un nuevo certificado que refleje las tenencias de INR modificadas. (La extensión de SIA en el nuevo certificado no cambiará, a menos que el titular de INR afectado proporcione un nuevo valor de SIA).

4.8.2. Quién puede solicitar la modificación del certificado.
El titular del certificado o el emisor pueden iniciar el proceso de modificación del certificado.

4.8.3. Procesamiento de solicitudes de modificación de certificados.
La AC DEBE determinar que la modificación solicitada es adecuada y que se siguen los procedimientos para la emisión de un nuevo certificado (ver Sección 4.3).

4.8.4. Notificación de Emisión de Nuevo Certificado al Suscriptor.
No hay estipulaciones adicionales más allá de las de la Sección 4.3.2.

4.8.5. Conducta que constituye la aceptación del certificado modificado.
No hay estipulaciones adicionales más allá de las de la Sección 4.4.1.

4.8.6. Publicación del Certificado Modificado por la CA.
No hay estipulaciones adicionales más allá de las de la Sección 4.4.2.

4.8.7. Notificación de Emisión de Certificados por parte de la CA a Otras Entidades.
No hay estipulaciones adicionales más allá de las de la Sección 4.4.3.

4.9. Revocación y Suspensión de Certificados.

4.9.1. Circunstancias para la revocación.
Un certificado DEBE ser revocado (y publicado en una CRL) si hay razones para creer que ha habido un compromiso de la clave privada de un suscriptor. Un certificado también PUEDE ser revocado para invalidar un objeto de datos firmado por la clave privada asociada con ese certificado. Otras circunstancias que justifican la revocación de un certificado PUEDEN especificarse en la CPS de una CA. Nota: Si se agregan nuevos INR a la distribución existente de una organización, no es necesario revocar el certificado anterior.

En su lugar, se PUEDE emitir un nuevo certificado con los recursos antiguo y nuevo y la clave anterior. Si se eliminan los INR o si ha habido un compromiso de clave, entonces se DEBE revocar el certificado anterior (y se DEBE realizar una nueva clave en caso de compromiso de clave).

4.9.2. Quién puede solicitar la revocación.
Esto DEBE estar definido en la CPS de la organización que emitió el certificado.

4.9.3. Procedimiento para Solicitud de Revocación.
Un suscriptor PUEDE presentar una solicitud de revocación al emisor del certificado. Esta solicitud DEBE identificar el certificado a revocar y DEBE ser autenticado. Los procedimientos para realizar la solicitud DEBEN estar descritos en la DPC de cada CA. El documento de aprovisionamiento de RPKI [RFC6492] describe un protocolo que PUEDE utilizarse para realizar solicitudes de revocación.

El emisor de un certificado DEBE notificar al suscriptor cuando revoque un certificado. El requisito de notificación se cumple mediante la publicación de CRL. La CPS de una CA DEBE indicar el medio por el cual la CA informará a un suscriptor de la revocación del certificado.

4.9.4. Período de gracia de solicitud de revocación.
Un suscriptor DEBE solicitar la revocación tan pronto como sea posible después de que se haya identificado la necesidad de revocación. No hay un período de gracia especificado para el suscriptor en este proceso.

4.9.5. Plazo dentro del cual la CA debe procesar la solicitud de revocación.
Sin estipulación. Cada CA DEBERÍA especificar su tiempo de procesamiento de revocación esperado en su CPS.

4.9.6. Requisito de verificación de revocación para las partes que confían.
Una parte que confía DEBE adquirir y verificar la CRL programada más reciente del emisor del certificado, cada vez que la parte que confía valida un certificado.

4.9.7. Frecuencia de emisión de CRL.
La frecuencia de emisión de la CRL DEBE ser determinada por cada CA y consignada en su CPS. Cada CRL lleva un valor nextScheduledUpdate, y DEBE publicarse una nueva CRL en ese momento o antes. Una CA DEBE establecer el valor nextUpdate cuando emite una CRL para indicar cuándo se emitirá la próxima CRL programada.

4.9.8. Latencia máxima para CRL.
El CPS para cada CA DEBE especificar la latencia máxima asociada con la publicación de su CRL en el sistema de depósito.

4.10. Servicios de estado de certificados.
Esta PKI no contempla el uso del Protocolo de estado de certificado en línea (OCSP) [RFC2560] o el Protocolo de validación de certificado basado en servidor (SCVP) [RFC5055]. Esto se debe a que se anticipa que los RP primarios (ISP) adquirirán y validarán certificados para todos los titulares de recursos participantes. Estos protocolos no están diseñados para la verificación de estado de certificados masivos a gran escala. Los RP DEBEN comprobar las CRL nuevas al menos una vez al día. Se RECOMIENDA que los RP realicen esta verificación varias veces al día, pero no más de 8 a 12 veces al día (para evitar accesos excesivos al repositorio).

5. Controles de las instalaciones, la gestión y las operaciones.

5.1. Controles físicos.
Cada CA DEBE mantener controles de seguridad física para su operación que sean proporcionales a los empleados por la organización en la gestión de la distribución de INR. Los controles físicos empleados para la operación de la CA DEBEN estar especificados en su CPS. A continuación, se muestran los posibles temas que se cubrirán en la CPS. (Estas secciones están tomadas de [RFC3647].)

5.1.1. Ubicación del sitio y construcción
5.1.2. Acceso físico
5.1.3. Electricidad y Aire Acondicionado
5.1.4. Exposiciones al agua
5.1.5. Prevención y Protección contra Incendios
5.1.6. Almacén de datos
5.1.7. Depósito de basura
5.1.8. Copia de seguridad fuera del sitio

5.2. Controles de procedimiento.
Cada CA DEBE mantener controles de seguridad procesal que sean proporcionales a los empleados por la organización en la gestión de la distribución de INR. Los

controles de seguridad procedimental empleados para el funcionamiento de la CA DEBEN estar especificados en su DPC. A continuación, se muestran los posibles temas que se cubrirán en la CPS. (Estas secciones están tomadas de [RFC3647].)

5.2.1. Funciones de confianza
5.2.2. Número de personas requeridas por tarea
5.2.3. Identificación y autenticación para cada rol
5.2.4. Funciones que requieren separación de funciones

5.3. Controles de personal.
Cada CA DEBE mantener controles de seguridad del personal acordes con los empleados por la organización en la gestión de la distribución de INR. Los detalles de cada CA DEBEN especificarse en su CPS.

5.4. Procedimientos de registro de auditoría.
Los detalles de cómo una CA implementa el registro de auditoría descrito en las Secciones 5.4.1 a 5.4.8 DEBEN abordarse en su CPS.

5.4.1. Tipos de eventos registrados.
Los registros de auditoría DEBEN generarse para las operaciones básicas del equipo informático de la autoridad de certificación. Los registros de auditoría DEBEN incluir la fecha, la hora, el usuario o proceso responsable y los datos de contenido resumidos relacionados con el evento. Los eventos auditables incluyen:

- Acceso al equipo informático de CA (p. ej., inicio de sesión, cierre de sesión).
- Mensajes recibidos solicitando acciones de CA (por ejemplo, solicitudes de certificado, solicitudes de revocación de certificado, notificaciones de compromiso).
- Acciones de creación, modificación, revocación o renovación de certificados.
- Publicación de cualquier material en un repositorio.
- Cualquier intento de cambiar o eliminar datos de auditoría.
- Generación de claves.
- Actualizaciones de software y/o configuración de la CA.
- Ajustes de reloj.

5.4.2. Protección del registro de auditoría.
El registro de auditoría DEBE estar protegido según los estándares actuales de la industria.

5.4.3. Procedimientos de copia de seguridad del registro de auditoría.
El registro de auditoría DEBE tener una copia de seguridad según los estándares actuales de la industria.

5.4.4. Evaluaciones de vulnerabilidad.
Los subsistemas RPKI de un registro o ISP DEBERÍAN participar en cualquier evaluación de vulnerabilidad que estas organizaciones ejecuten como parte de su práctica comercial normal.

5.5. Cambio de clave.
Cuando una CA desea cambiar las claves, DEBE generar un nuevo certificado que contenga su nueva clave pública. Consulte [RFC6489] para obtener una descripción de cómo se efectúa el cambio de clave en el RPKI.

5.6. Terminación de CA o RA.
En la RPKI, cada signatario actúa como una CA para los INR especificados que se distribuyeron a esa entidad. Los procedimientos asociados con la terminación de una CA DEBEN estar descritos en la CPS para esa CA. Estos procedimientos DEBEN incluir una disposición para notificar a cada entidad que emitió un certificado a la organización que está operando la CA que está terminando. Dado que la función de RA DEBE ser proporcionada por la misma entidad que opera como CA (consulte la Sección 1.3.2), no existen estipulaciones separadas para los RA.

6. Controles técnicos de seguridad.
Las organizaciones que distribuyen INR a los signatarios de la red tienen autoridad para estas distribuciones. Esta PKI está diseñada para permitir que los ISP y los signatarios de la red demuestren que son los titulares de los INR que se les han distribuido. En consecuencia, los controles de seguridad utilizados por las CA y los signatarios para esta PKI solo necesitan ser tan seguros como los que se aplican a los procedimientos para administrar la distribución de datos INR por parte de las organizaciones existentes. Los detalles de los controles de seguridad de cada CA DEBEN estar descritos en la CPS emitida por la CA.

6.1. Generación e instalación de pares de claves

6.1.1. Generación de pares de claves
En la mayoría de los casos, los pares de claves públicas serán generados por el sujeto, es decir, la organización que recibe la distribución de INR. Sin embargo, algunas CA PUEDEN ofrecer generar pares de claves en nombre de sus sujetos a pedido de los sujetos, por ejemplo, para dar cabida a suscriptores que no tienen la capacidad de realizar la generación de claves de manera segura. (La CA tiene que verificar la calidad de las claves solo si las genera; consulte la Sección 6.1.6). Dado que las claves utilizadas en esta PKI no tienen fines de no repudio, la generación de pares de claves por parte de Cas no socava inherentemente la seguridad de la PKI. Cada CA DEBE describir sus procedimientos de generación de pares de claves en su CPS.

6.1.2. Entrega de clave privada al suscriptor.
Si una CA proporciona servicios de generación de pares de claves para suscriptores, su CPS DEBE describir los medios por los cuales las claves privadas se entregan a los suscriptores de manera segura.

6.1.3. Entrega de clave pública al emisor del certificado.
Cuando se transfiere una clave pública a la CA emisora para su certificación, DEBE entregarse a través de un mecanismo que garantice que la clave pública no ha sido alterada durante el tránsito y que el suscriptor posee la clave privada correspondiente a la clave pública transferida.

6.1.4. Entrega de clave pública de CA a terceros que confían.
Las claves públicas de CA para todas las entidades (que no sean anclas de confianza) están contenidas en certificados emitidos por otras CA. Estos

certificados DEBEN estar publicados en el sistema de repositorios distribuidos de RPKI. Las partes de confianza descargan estos certificados de los repositorios. Los valores de clave pública y los datos asociados para anclas de confianza (supuestas) se distribuyen fuera de banda y son aceptados por las partes que confían en la PKI del PSC PROCERT sobre la base de criterios definidos localmente.

6.1.5. Tamaños de clave.
Los algoritmos y tamaños de clave utilizados en RPKI se especifican en "Un perfil para algoritmos y tamaños de clave para uso en la infraestructura de clave pública de recursos" [RFC6485].

6.1.6. Generación de parámetros de clave pública y control de calidad
Los parámetros de clave pública utilizados en el RPKI se especifican en [RFC6485]. Cada suscriptor es responsable de realizar comprobaciones de la calidad de su par de claves. Una CA no es responsable de realizar dichas comprobaciones para los suscriptores, excepto en el caso de que la CA genere el par de claves en nombre del suscriptor.

6.1.7. Propósitos de uso de clave (según el campo de uso de clave X.509 v3)
Los valores de bit de extensión de uso de clave utilizados en RPKI se especifican en el perfil de certificado de RPKI [RFC6487].

6.2. Protección de clave privada y controles de ingeniería del módulo criptográfico.

6.2.1. Estándares y controles del módulo criptográfico.
Los estándares y controles del módulo criptográfico empleados por cada CA DEBEN estar descritos en la CPS emitida por esa CA.

6.2.2. Clave privada (N de M) Control de varias personas
Las CA PUEDEN emplear controles de múltiples personas para restringir el acceso a sus claves privadas, pero esto no es un requisito para todas las CA en la PKI. La CPS para cada CA DEBE describir qué, en su caso, varias personas controles que emplea.

6.2.3. Custodia de la clave privada.
No se requieren procedimientos de custodia de claves privadas para la RPKI.

6.2.4. Copia de seguridad de clave privada.
Debido a las implicaciones operativas adversas asociadas con la pérdida del uso de una clave privada de CA en la PKI, cada CA DEBE emplear un medio seguro para respaldar sus claves privadas. Los detalles de los procedimientos para realizar copias de seguridad de la clave privada de una CA DEBEN estar descritos en la CPS emitida por la CA.

6.2.5. Archivo de clave privada.
Los detalles del proceso y procedimientos utilizados para archivar la clave privada de la CA DEBEN estar descritos en la CPS emitida por la CA.

6.2.6. Transferencia de clave privada hacia o desde un módulo criptográfico.
Los detalles del proceso y procedimientos utilizados para transferir la clave privada de la CA hacia o desde un módulo criptográfico DEBEN estar descritos en la CPS emitida por la CA.

6.2.7. Almacenamiento de clave privada en módulo criptográfico.
Los detalles del proceso y procedimientos utilizados para almacenar la clave privada de la CA en un módulo criptográfico y protegerla del uso no autorizado DEBEN estar descritos en la CPS emitida por la CA.

6.2.8. Método de activación de una clave privada.
Los detalles del proceso y procedimientos utilizados para activar la clave privada de la CA DEBEN estar descritos en la CPS emitida por la CA.

6.2.9. Método de desactivación de una clave privada.
Los detalles del proceso y procedimientos utilizados para desactivar la clave privada de la CA DEBEN estar descritos en la CPS emitida por la CA.

6.2.10. Método de destrucción de una clave privada.
Los detalles del proceso y procedimientos utilizados para destruir la clave privada de la CA DEBEN estar descritos en la CPS emitida por la CA.

6.2.11. Calificación del módulo criptográfico.
La calificación de seguridad del módulo criptográfico DEBE estar descrita en la CPS emitida por la AC.

6.3. Otros aspectos de la gestión de pares de claves.

6.3.1. Archivo de clave pública.
Debido a que esta PKI no admite el no repudio, no es necesario archivar las claves públicas.

6.3.2. Períodos operativos de certificados y períodos de uso de pares de claves
Los INR en poder de una CA pueden cambiar periódicamente cuando recibe nuevas distribuciones. Para minimizar la interrupción, el par de claves de la CA NO DEBE cambiar cuando se agregan INR a su certificado. Si los certificados de ISP y de suscriptor de la red están vinculados a la duración de los acuerdos de servicio, estos certificados deben tener períodos de validez proporcionales a la duración de estos acuerdos. En cualquier caso, el período de validez de los certificados DEBE ser elegido por la CA emisora y descrito en su CPS.

6.4. Datos de activación.
Cada CA DEBE documentar en su CPS cómo generará, instalará y protegerá sus datos de activación.

6.5. Controles de seguridad informática.
Cada CA DEBERÁ documentar en su CPS los requisitos técnicos de seguridad que emplea para el funcionamiento informático de la CA.

6.6. Controles técnicos del ciclo de vida.

6.6.1. Controles de desarrollo del sistema.

La CPS para cada CA DEBE documentar cualquier control de desarrollo del sistema requerido por esa CA, si corresponde.

6.6.2. Controles de gestión de seguridad.

La CPS de cada CA DEBE documentar los controles de seguridad aplicados al software y equipos utilizados para esta PKI. Estos controles DEBEN ser proporcionales a los utilizados para los sistemas utilizados por las CA para la gestión de los INR.

6.6.3. Controles de seguridad del ciclo de vida.

La CPS de cada CA DEBE documentar cómo se adquirirá, instalará, mantendrá y actualizará el equipo (hardware y software) utilizado para esta PKI. Esto DEBE hacerse de manera acorde con la forma en que se maneja el equipo para la gestión y distribución de INR.

6.7. Controles de seguridad de la red.

La CPS de cada CA DEBE documentar los controles de seguridad de la red empleados para el funcionamiento de la CA. Estos DEBEN ser acordes con la protección que emplea para las computadoras utilizadas para administrar la distribución de INR.

6.8. Marcando la hora.

La RPKI no hace uso de sellos de tiempo.

7. Perfiles de certificados y CRL.
   Consulte el Certificado RPKI y el Perfil CRL [RFC6487].
8. Auditoría de Cumplimiento y Otras Evaluaciones.
   La política de certificados para una PKI típica define los criterios con los que se evalúan las CA potenciales y establece los requisitos que deben cumplir. En esta PKI, las CA ya tienen autoridad para la gestión de INR, y la PKI simplemente admite la verificación de la distribución de estos recursos a los suscriptores de la red. En consecuencia, cualquier auditoría y otras evaluaciones que ya se utilicen para garantizar la seguridad de la gestión de los INR son suficientes para esta PKI. La CPS para cada CA DEBE describir qué auditorías y otras evaluaciones se utilizan.

9. Otros asuntos comerciales y legales.
   Como se indica a lo largo de esta política de certificación, las organizaciones que administran la distribución de INR tienen autoridad en sus roles como administradores de estos datos. DEBEN operar esta PKI para permitir que los titulares de INR generen datos firmados digitalmente que certifiquen estas distribuciones. Por lo tanto, la forma en que las organizaciones en cuestión gestionan sus asuntos legales y comerciales para esta PKI DEBE ser proporcional a la forma en que ya gestionan los asuntos legales y comerciales en sus funciones existentes.

   Dado que no existe un conjunto único de respuestas a esta sección que se aplicaría a todas las organizaciones, los temas enumerados en las Secciones 4.9.1 a 4.9.11 y 4.9.13 a 4.9.17 de RFC 3647 DEBERÍAN cubrirse en la CPS emitida por cada organización. CA, aunque no todas las CA pueden optar por abordar todos estos temas.

9.1. Enmiendas.

9.1.1. Procedimiento de enmienda.

El procedimiento para modificar este CP es a través de una notificación por escrito del IESG en forma de un nuevo (BCP) RFC que actualiza o deja obsoleto este documento.

9.1.2. Mecanismo y plazo de notificación.

Las sucesivas versiones del CP se publicarán con la siguiente mención:

Esta CP entra en vigor el 01/08/2025.

9.1.3. Circunstancias en las que se debe cambiar el OID.

Si el IESG juzga que los cambios en el CP no reducen materialmente la aceptabilidad de los certificados emitidos para fines de RPKI, no habrá cambios en el CP OID. Si el IESG juzga que los cambios en el CP modifican materialmente la aceptabilidad de los certificados para fines de RPKI, entonces DEBE haber un nuevo CP OID y revisión de esta CP.

10. Consideraciones de seguridad.

De acuerdo con X.509, una política de certificados (CP) es "un conjunto de reglas con nombre que indica la aplicabilidad de un certificado a una comunidad particular y/o clase de aplicaciones con requisitos de seguridad comunes". Una parte que confía puede utilizar un CP para ayudar a decidir si un certificado y la vinculación que contiene son lo suficientemente confiables y apropiados para una aplicación en particular.

Este documento describe el CP para la infraestructura de clave pública de recursos (RPKI). Hay documentos separados (CPS) que cubren los factores que determinan el grado en que una parte que confía puede confiar en el enlace incorporado en un certificado. El grado en que se puede confiar en dicha vinculación depende de varios factores, por ejemplo, las prácticas seguidas por la CA al autenticar al sujeto; la política operativa, los procedimientos y los controles técnicos de seguridad de la CA, incluido el alcance de las responsabilidades del suscriptor (por ejemplo, en la protección de la clave privada), y las responsabilidades y los términos y condiciones de responsabilidad declarados de la CA (por ejemplo, garantías, renuncias de garantías y limitaciones de responsabilidad).

Dado que no se puede garantizar la exclusividad del nombre dentro de la RPKI, existe el riesgo de que dos o más CA de la RPKI emitan certificados y CRL con el mismo nombre de emisor. Las implementaciones de validación de rutas que se ajustan al algoritmo de validación de rutas de certificación de recursos (consulte [RFC6487]) verifican que se haya utilizado la misma clave para firmar tanto el destino (el certificado de recursos) como la CRL correspondiente.

Por lo tanto, una colisión de nombres no cambiará el resultado. El uso del algoritmo básico de validación de ruta X.509, que asume la exclusividad del nombre, podría dar como resultado que un certificado revocado se acepte como válido o que un certificado válido se rechace como revocado. Las partes que confían deben asegurarse de que el software que usan para validar los certificados emitidos bajo esta política verifique que se usó la misma clave para firmar tanto el certificado como la CRL correspondiente, como se especifica en [RFC6487].

11. Control de Versiones

Versión	Motivo de Cambio	Publicación	Vigencia
Edición 1	Emisión	1/08/2025	Si