Suprema Corte de Justicia

República Oriental del Uruguay

Autoridad de Certificación
Poder Judicial

POLÍTICAS DE CERTIFICACIÓN Y
DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

OID: **2.16.858.2.10000232.66565.20150601**

Versión: 1.0
2015

Índice de contenido

VERSIONES DEL DOCUMENTO

Versión	Cambio	Fecha
1.0	Versión inicial	1/06/15

1. INTRODUCCIÓN

1.1. Propósito

El propósito del presente documento es describir las Políticas de Certificación (CP) y Declaración de Prácticas de Certificación (CPS) del Poder Judicial, como Prestador no homologado de servicios de Certificación interno de la Institución.
El documento se estructura en conformidad al marco normativo vigente y según el RFC 3647 "Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework".

1.2. Nombre e identificación del documento

En el marco normativo de la UNAOID éste documento se identifica por el identificador de objeto (OID): 2.16.858.2.10000232.66565.20150601

Nombre del documento	CP-CPS_SCJ.pdf
Versión del documento	1.0
Referencia al documento OID (Object Identifier)	**2.16.858.2.10000232.66565.20150601**
Fecha de emisión	01-06-2015
Fecha de aprobación	
Localización de la URL	http://comunicaciones.gub.uy/pki/cp-cps_scj.pdf

1.3. Participantes de la PKI

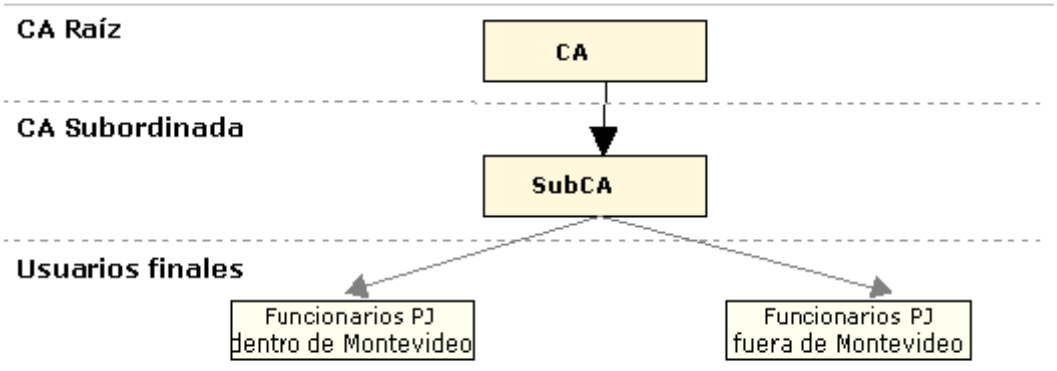
La Infraestructura de Certificación Electrónica del Poder Judicial (PKI - Public Key Infraestructure/Infraestructura de Clave Pública), es la suma de equipos (hardware) y programas informáticos (software), dispositivos criptográficos, políticas y pautas, prácticas y procedimientos dispuestos, que rigen el ciclo de vida de un certificado digital para firma electrónica, incluyendo la publicación de información y consulta del estado de vigencia y de validez de dichos certificados.

1.3.1 Autoridad de Certificación (CA)

La Autoridad de Certificación se encarga de:

- mantener y actualizar el repositorio público de información
- desarrollar, publicar y mantener actualizado su documento de Políticas y Prácticas de Certificación
- emitir y revocar certificados a usuarios internos de la Institución.

Está compuesta por una CA Raíz y una CA subordinada (SubCA), de acuerdo a la siguiente estructura jerárquica:



Estructura jerárquica de la PKI

CA Raíz: "CA-Suprema Corte de Justicia" como Autoridad de Certificación de primer nivel. Es el primer eslabón de la cadena de confianza y le compete emitir y en su caso revocar el certificado de la CA Subordinada.

CA Subordinada: "SubCA-Suprema Corte de Justicia" como Autoridad de Certificación Subordinada. Su función es la emisión y revocación de certificados de usuario final para funcionarios del Poder Judicial dentro y fuera de Montevideo.

1.3.2 Autoridad de Registro (RA)

La Autoridad de Registro es la entidad dentro del Prestador de Servicios de Certificación que registra y procesa las solicitudes de emisión y revocación de certificados digitales para firma electrónica por parte de los peticionantes . En éste sentido es la única comunicación requerida entre el Prestador de Servicios de Certificación y el peticionante.

La RA es la encargada de:

a) Validar la identidad y cualquier otra circunstancia personal de los solicitantes de certificados que sean relevantes para el fin propio de éstos.
b) Informar al solicitante con carácter previo a la emisión del certificado, respecto a las condiciones precisas para la utilización del mismo y sus limitaciones de uso.
c) Recibir la solicitud o petición vía Web o ingresarla en forma excepcional al sistema la solicitud o petición.
d) Aprobar solicitudes o peticiones y enviarlas a la CA (Autoridad de Certificación) para que ésta las procese.
e) Compulsar la exactitud de la información contenida en el certificado emitido por la CA.
f) Emitir el Certificado y dejarlo disponible para su instalación.
g) Publicar en los repositorios de la sección 2.9.

1.3.3 Peticionante (usuario)

El peticionante es la persona física que formula una solicitud o petición de expedición de certificado digital ante la RA y hace uso del mismo para firmar electrónicamente en el ejercicio de su función dentro del Poder Judicial. El peticionante y el usuario deben coincidir.
El peticionante contrae derechos y obligaciones al utilizar certificados, los cuales se describen en la presente Política de Certificación, y más ampliamente en el documento que suscribe al momento de solicitar la emisión de su certificado de uso personal.

1.3.4 Tercero de confianza

Un tercero de confianza es el individuo o entidad que actúa confiando en las firmas electrónicas emitidas con un certificado expedido por el Poder Judicial.
Los terceros de confianza están obligados a comprobar la validez del certificado siguiendo las etapas prescritas en el presente documento.

1.3.5 Otros participantes

No aplica

1.4. Uso del certificado

1.4.1. Usos apropiados del certificado

Tipo de certificado	Usos
Certificado de CA raíz (CA-Suprema Corte de Justicia)	• Operar la infraestructura PKI • Emisión y revocación de certificados para operación interna de la PKI • Emisión del certificado SubCA
Certificado de CA Subordinada (SubCA-Suprema Corte de Justicia)	• Operar la infraestructura PKI • Emisión y revocación de certificados a usuarios finales dentro de la cadena de confianza
Certificado de usuario final para funcionarios del Poder Judicial de Montevideo e Interior	• Firmar electrónicamente documentos digitales actuando en el ejercicio de las funciones inherentes al cargo que detenta en el Poder Judicial.

1.4.2. Usos prohibidos del certificado

Los Certificados emitidos por el Poder Judicial se utilizarán únicamente conforme a las presentes Políticas y Declaración de Prácticas de Certificación.

El usuario final (funcionario del Poder Judicial) no podrá hacer uso del certificado con fines comerciales, ya sea en forma gratuita u onerosa.

1.5. Administración de las Políticas de Certificación

l1.5.1. Organización que administra el documento

Nombre	**Suprema Corte de Justicia**
Dirección de contacto	**uane@poderjudicial.gub.uy**
Dirección	**Colonia 978 piso 5**
Número de teléfono	**598 29082472**
Número de fax	**598 29082472**

1.5.2. Vinculación de las Políticas de Certificación con otros documentos.

Las Políticas de Certificación contenidas en éste documento son el cúmulo de normas y pautas que regulan la generación y revocación de certificados digitales para firma electrónica.
La Declaración de Prácticas de Certificación contiene los procedimientos relacionados con la emisión y revocación de certificados electrónicos, los que deben reflejar el grado de adhesión a las Políticas de Certificación.
La Suprema Corte de Justicia es el órgano competente para aprobar y actualizar las Políticas de Certificación (CP) y determinar la adecuación de las Prácticas de Certificación (CPS) a dichas Políticas.

1.5.3. Procedimientos de aprobación de la Declaración de Prácticas de Certificación

La aprobación de ésta Política, así como toda modificación introducida en ella, es responsabilidad de la Suprema Corte de Justicia. La Política modificada se publicará como una nueva versión, manteniéndose un registro de la fecha y cambios realizados.

1.6. Definiciones y acrónimos

CA (Certification Authority / Autoridad de Certificación): es quien de conformidad con la legislación sobre firma electrónica expide certificados electrónicos. Es la autoridad en la que confían los usuarios de los sistemas de certificación para crear, asignar y revocar certificados. En el presente documento la autoridad de certificación comprende tanto a la CA Raíz como a la CA Subordinada y en todos los casos se identifica como la Suprema Corte de Justicia.

Cadena de certificación: lista de certificados que contiene al menos un certificado y el certificado raíz de la Suprema Corte de Justicia.

Certificado electrónico: documento digital firmado electrónicamente que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica (Ley 18.600 Art.2).

Certificado raíz: certificado electrónico expedido y firmado por la misma autoridad certificadora que lo emite.

Clave: secuencia de símbolos.

CP (Certification Policy / Política de Certificación): documento que establece las condiciones de uso y los procedimientos seguidos para emitir certificados.

CPS (Certificate Practice Statement / Declaración de Prácticas de Certificación): declaración de la Suprema Corte de Justicia sobre las prácticas de certificación

CRL (Certificate Revocation List / Lista de Revocación de Certificados): lista donde figura exclusivamente la relación de certificados revocados (no los caducados).

Datos de creación de Firma (Clave Privada): son datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

Datos de verificación de Firma (Clave Pública): son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

Dispositivo seguro de creación de firma: componente informático que sirve para aplicar los datos de creación de firma**.**

Documento electrónico: representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo.

HSM (Hardware Security Module / Hardware de Seguridad): módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.

Número de serie de Certificado: valor entero y único que está asociado inequívocamente a un certificado expedido por Suprema Corte de Justicia.

OID (Object Identifier): identificador de objeto único. Permite entre otras cosas, identificar la política de certificación (CP) asociada a un certificado.

PIN (Personal Identification Number): clave personal que permite el uso del dispositivo electrónico que contiene el certificado digital.

PKCS#10 (Certification Request Syntax Standard): estándar desarrollado por RSA Labs, y aceptado internacionalmente que define la sintaxis de una petición de certificado.

PKI (Public Key Infrastructure / Infraestructura de Clave Publica): Es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas.

PKI (Public Key Infrastucture / Infraestructura de Claves Públicas): infraestructura que soporta la emisión y gestión de claves y certificados para los servicios de autenticación, cifrado, integridad, o no repudio.

Prestador de Servicios de Certificación (PSC): es aquella persona física o jurídica que, de conformidad con la legislación vigente, expide certificados digitales para firma electrónica. En el presente documento se corresponde con las Autoridades de Certificación pertenecientes a la jerarquía de la Suprema Corte de Justicia.

PUK (Personal Unblocking Key): número o clave específica sólo conocida por la persona que tiene que acceder al dispositivo criptografico (token) que se utiliza para desbloquear el acceso al mismo.

RA (Registration Authority / Autoridad de Registro): es la autoridad encargada de registrar, aprobar solicitudes de emisión y de revocación de certificados digitales para firma electrónica, hacer entrega de los mismos y publicar en repositorios el estado de revocación de los mismos.

Solicitante: persona física que previa identificación, solicita la emisión o la revocación de un certificado.

Terceros aceptantes o partes confiantes: aquellas personas que depositan su confianza en un certificado de la Suprema Corte de Justicia, comprobando la validez y vigencia del certificado.

Usuario o firmante: persona cuya identidad queda vinculada a los datos firmados electrónicamente, a través de una clave pública certificada por el Prestador de Servicios de Certificación. El concepto de firmante, será referido en los certificados y en las aplicaciones informáticas relacionadas con su emisión, como el campo "sujeto" del certificado (Subject).

X.509: estándar desarrollado por la UIT (Unión Internacional de Telecomunicaciones – ITU por su siglas en inglés), que define el formato electrónico básico para certificados electrónicos.

Documentos de referencia

Los siguientes documentos han sido aplicados para la confección del presente:

- RFC 2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".
- RFC 3039 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile.
- RFC 3161: "Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)".
- RFC 3280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- RFC 3628: "Policy Requirements for Time-Stamping Authorities (TSAs)". INTE-ISO-21188:2007 "Infraestructura de llave pública para servicios financieros — Estructura de prácticas y políticas.
- RFC 3647: "Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework".

2. ASPECTOS GENERALES DE LA POLÍTICA DE CERTIFICACIÓN

2.1. Obligaciones

2.1.1 Obligaciones de la Autoridad de Certificación

- Desarrollar, mantener, actualizar y publicar su propio documento de "Políticas de Certificación y Declaración de Prácticas de Certificación".
- Mantener a disposición permanente del público el documento de "Políticas de Certificación y Declaración de Prácticas de Certificación".
- Emitir su propio certificado y el de la SubCA, según lo establecido en la ceremonia de llaves.
- Publicar su propio certificado y el de la SubCA y proteger las claves privadas de los mismos.
- Revocar su propio certificado y el de la SubCA ante la sospecha real de compromiso de las claves privadas asociadas.
- No retener ni almacenar en ningún caso datos de creación de firma, ni claves privadas de los certificados de usuarios internos del Poder Judicial.
- Atender los requerimientos de revocación solicitados de acuerdo con la legislación vigente y con los procedimientos definidos en el presente documento de "Políticas de Certificación y Declaración de Prácticas de Certificación".
- La emisión y revocación de los certificados expedidos a los usuarios internos del Poder Judicial.
- La emisión y publicación de su Lista de Certificados Revocados (CRL).
- Informar a los usuarios la revocación de sus certificados, junto con la causal para dicha operación.
- Garantizar el acceso permanente y gratuito de los usuarios y terceros aceptantes al sitio de publicación que contiene su propio certificado y el de la SubCA, y la lista de certificados revocados.
- Mantener y garantizar la seguridad de la información tratada y la contenida en los documentos digitales que sean firmados electrónicamente por los funcionarios judiciales habilitados en el ejercicio de su función (disponibilidad, integridad y no repudio).

2.1.2 Obligaciones de la Autoridad de Registro

- Recibir y procesar las solicitudes de emisión y de revocación de certificados presentadas por los usuarios internos del Poder Judicial, de acuerdo a los requerimientos establecidas en el presente documento de "Políticas de Certificación y Declaración de Prácticas de Certificación".
- Validar la identidad de la persona física que solicita la emisión o revocación de un certificado, así como verificar toda la información a incluir en el mismo, de acuerdo a los procedimientos establecidos en el presente documento de "Políticas de Certificación y Declaración de Prácticas de Certificación".
- Notificar a los usuarios internos del Poder Judicial, ante la ocurrencia de algún acontecimiento que así lo requiera según lo estipulado en el presente documento de "Políticas de Certificación y Declaración de Prácticas de Certificación".

2.1.3 Obligaciones de los usuarios de certificados

- Proporcionar declaración exacta y completa de los datos de su identidad u otras circunstancias objeto de certificación.
- Mantener el control exclusivo de sus datos de creación de firma electrónica, no compartirlos e impedir su divulgación.
- Utilizar el certificado únicamente para los propósitos autorizados en cumplimiento de su deber funcional en el Poder Judicial.
- Gestionar la expedición de un nuevo certificado electrónico antes del vencimiento del certificado que tiene vigente.
- Comunicar en forma fehaciente e inmediata al Poder Judicial -Unidad Administradora de Notificaciones Electrónicas- los casos de traslado, ascenso o cese en la función. De igual forma procederá en caso de haber modificaciones en los datos aportados para la emisión del certificado electrónico.
- Realizar en forma inmediata la denuncia policial correspondiente y comunicar de igual forma al Poder Judicial -Unidad Administradora de Notificaciones Electrónicas- el hurto, pérdida o destrucción del dispositivo electrónico, o cualquier otra circunstancia que pueda haber comprometido la clave privada y/o el uso del dispositivo que la contiene; detallando las circunstancias en que se produjo el hecho y solicitando la revocación del certificado.
- Comunicar en forma inmediata y fehaciente al Poder Judicial -Unidad Administradora de Notificaciones Electrónicas- la ocurrencia de alguna falla técnica o cualquier otro problema en el funcionamiento, uso indebido o imposibilidad de uso del certificado electrónico y/o en el dispositivo.

- Conocer y aceptar las estipulaciones establecidas en éste documento de CP y CPS que le sean de aplicación y sus futuras modificaciones, así como la legislación vigente.

2.1.4 Obligaciones de los terceros aceptantes

- Tomar conocimiento y aceptar los términos definidos en el presente documento.
- Verificar la validez de los certificados, en el momento de realizar cualquier operación basada en los mismos, comprobando dentro del propio certificado que el mismo sea válido y que no está caducado.
- Debe además consultar si el certificado ha sido revocado, para lo cual el tercero aceptante debe acceder a la Lista de Certificados Revocados, que se encuentra en el correspondiente sitio Web:
  http://comunicaciones.poderjudicial.gub.uy/pki/listado_revocados_scj.html
- Las verificaciones requeridas en los puntos anteriores deben ser realizadas cada vez que el tercero confíe en un certificado emitido por el Poder Judicial a través de su CA y SubCA.

l2.1.5 Obligaciones de otros participantes

No aplica.

2.2. Responsabilidades

El Poder Judicial como Prestador de Servicios de Certificación no homologado, responderá de acuerdo a las disposiciones establecidas en los arts. 24 y 25 de la Constitución de la República.

2.3. Tarifas

No aplica para ninguna de las prestaciones que brinda el Poder Judicial como PSC no homologado.

2.4. Confidencialidad de la información tratada

En el manejo de la información le es aplicable al Poder Judicial como PSC no homologado, lo dispuesto por las leyes números 18.331 de fecha 8 de agosto de 2008 y 18.381 de fecha 17 de octubre de 2008.

2.4.1. Información fuera del alcance de confidencialidad

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

- La contenida en la presente CP/CPS
- La información contenida en los certificados emitidos.
- La información contenida en las CRL's incluyendo la causa que dio motivo a la revocación.

2.4.2. Responsabilidad sobre la protección de datos privados

Los funcionarios del Poder Judicial que participen en cualquier tarea propia o derivada de la PKI están obligados al deber de secreto profesional y por lo tanto sujetos a la normativa reguladora que les es aplicable.

2.4.3. Notificación y consentimiento para uso de datos privados

El proceso de solicitud de un certificado digital para firma electrónica implica el consentimiento del uso de la información de carácter personal para dicho fin.

2.4.4. Divulgación de datos privados de acuerdo a un proceso administrativo o judicial

Podrán ser comunicados a terceros, sin consentimiento del afectado, siempre que medie orden judicial o norma legal que así lo determine.

2.5 Derechos de propiedad intelectual

Los derechos de propiedad intelectual del sistema de certificación que por el presente se regula son de titularidad exclusiva de la Suprema Corte de Justicia. También lo son las presentes CP/CPS en cualquier de sus versiones, estando prohibida la reproducción sin la autorización expresa de la Suprema Corte de Justicia.

2.6. Normativa aplicable

2.6.1. Ley gobernante

El presente documento de Políticas de Certificación (CP) y Declaración de Prácticas de Certificación (CPS) del Poder Judicial, como Prestador no homologado de Servicios de Certificación orientado a usuarios internos de la Institución, se basa en la normativa vigente en la materia en la República Oriental del Uruguay, las que regulan la obligatoriedad e interpretación del mismo.

2.6.2. Disposiciones para resolución de disputas

En cualquier disputa que involucre a los servicios o prestaciones que brinda el Poder Judicial como PSC no homologado, la parte ofendida notificará primero a la Suprema Corte de Justicia

quién asignará el personal adecuado para resolver el litigio.

2.7. Período de validez

2.7.1. Plazo

La vigencia del presente documento de Políticas de Certificación (CP) y Declaración de Prácticas de Certificación (CPS) del Poder Judicial comenzará en el momento de su publicación en el repositorio y hasta tanto no sea derogada o modificada.

2.7.2. Derogación

La vigencia del documento de Políticas de Certificación (CP) y Declaración de Prácticas de Certificación se debe mantener hasta que todos los certificados emitidos bajo el mismo hayan finalizado (caducados o revocados), o hayan sido reemplazados por otros certificados emitidos por la nueva política.

2.7.3. Efectos de la finalización

Excepto los derechos de propiedad intelectual, una vez sustituida la presente CP/CPS, caducarán todas las obligaciones, derechos y responsabilidades establecidas en la misma.

2.8. Enmiendas

La autoridad con atribuciones para realizar y aprobar cambios sobre éste documento de Políticas de Certificación (CP) y Declaración de Prácticas de Certificación es la Suprema Corte de Justicia. Las modificaciones o enmiendas deben documentarse y mantenerse actualizadas a través de versiones, y deben publicarse en el sitio web.

En el caso de que la Suprema Corte de Justicia entienda que los cambios afectan la aceptabilidad de los certificados, comunicará a los usuarios de los certificados correspondientes el cambio realizado, indicándoles además que deben consultar la nueva CP/CPS en el repositorio establecido.

2.9. Responsabilidad sobre repositorios y publicación de información

Toda la información relacionada a la CA se encuentra en el sitio web http://comunicaciones.poderjudicial.gub.uy/pki siendo éste el enlace directo a la información relacionada con la PKI. La información contenida en el repositorio no es de carácter confidencial.

2.9.1. Publicación de información de certificación

Para los certificados de la CA Raíz y CA Subordinada:
http://comunicaciones.poderjudicial.gub.uy/pki/listado_certificados_scj.html

Para la lista de revocados (CRL):
http://comunicaciones.poderjudicial.gub.uy/pki/listado_revocados_scj.html

Para el presente documento:
http://comunicaciones.poderjudicial.gub.uy/pki/cp-cps_scj.pdf

El repositorio no contiene ninguna información de naturaleza confidencial.

2.9.2. Tiempo o frecuencia de publicación

El presente documento se publicará cada vez que sea modificado.
Se actualizará la Lista de Certificados Revocados (CRL) cuando se produzca la revocación de un certificado.

2.9.3. Controles de acceso a los repositorios

El acceso a lectura de la información del repositorio de la Suprema Corte de Justicia y de su sitio Web, es público, abierto y libre. Sólo el personal designado por la misma podrá modificar, sustituir o eliminar información del repositorio y del sitio web. Se establecen controles que impiden la manipulación de la información contenida en los repositorios sin autorización.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Registro de Nombres

El Poder Judicial expedirá certificados digitales para firma electrónica a los usuarios internos que en el ejercicio de su función se encuentren habilitados para dicho cometido. Dichos certificados serán emitidos bajo las presentes disposiciones de CP y CPS.

El funcionario solicitará la emisión de los certificados ante la Autoridad de Registro del Poder Judicial.

En caso de "solicitudes en forma personal" la mencionada Autoridad de Registro validará el documento presentado, así como la identidad de la persona que solicita el registro, de acuerdo al siguiente requerimiento: cédula de identidad o pasaporte uruguayos, vigentes y en buen estado.

Una vez validado el documento y la identidad del solicitante, el nombre que se colocará en el certificado, será el nombre y apellido de la persona. De la misma forma se determinarán los datos de tipo y número de documento.

En caso de "solicitudes vía web" cotejada con la información disponible, se validará la misma, junto con la información solicitada que debe de ser enviada a la Autoridad de Registro.

3.1.1. Tipos de nombres

El campo DN (Distinguished Name) del certificado contiene toda la información de identificación de la persona para la que se emite el certificado.

El contenido del campo CN (Common Name) debe ser: nombre/s, apellido/s, tipo de documento que acredite la identidad del usuario y número del mismo. Sólo se considerará como válido el nombre/s y apellido/s, no permitiendo el uso de seudónimos.

Los certificados de usuario final contienen los siguientes campos en el nombre distintivo (DN) del certificado:

Campo	Formato
CN	Nombre/s y apellido/s – Tipo Documento Número de documento. *Ejemplo: "Juan Lago – C.I. 1.065.892-2"*
OU	Departamento de la empresa u organización a la que pertenece (si procede) u otros *Ejemplo: "Poder Judicial"*
O	Organización a la que pertenece / empresa / profesión (según y si procede) / otros *Ejemplo: "Poder Judicial"*
C	País emisor del número de documento

3.1.2. Significado de los nombres

Las reglas definidas en el apartado anterior más el número de serie del certificado, son suficientemente significativos para vincular la clave pública con el usuario (firma).

3.1.3. Anonimato o seudo-anonimato del usuario

Para cumplir con el requisito de no repudio los certificados de firma electrónica emitidos por la Suprema Corte de Justicia no admiten anonimato. El seudónimo no se considera un nombre significativo y no se utilizará como parte del certificado.

3.1.4. Interpretación de formatos de nombres

No aplica debido a que existe un único formato.

3.1.5. Unicidad de los nombres

Los nombres distintivos (DN) deben ser únicos para cada usuario y no inducirán a ambigüedad, garantizando la unicidad por usuario. El número del documento de identidad y el país emisor del mismo (cédula de identidad o pasaporte) garantizan la unicidad del DN por usuario.

3.1.6. Reconocimiento, autenticación y rol de las marcas registradas

La documentación a presentar en el momento de la solicitud de un certificado asegura la utilización legítima y el permiso explícito para la utilización de toda denominación registrada.

3.2. Validación de la identidad inicial

La Autoridad de Registro debe validar la identidad del solicitante previo a la emisión del certificado.

3.2.1. Posesión de la clave privada

Las claves privadas asociadas a certificados de usuarios de la Institución, bajo las normas del presente documento, deberán ser siempre generadas y utilizadas en dispositivos seguros de creación de firmas. El Poder Judicial, a través de la Autoridad de Registro entregará en forma gratuita al peticionante el dispositivo criptográfico (Token).

Tratándose de la primera vez, luego de validada la identidad del peticionante, al inicio del procedimiento de la solicitud, éste deberá cambiar el PIN del dispositivo criptográfico (contraseña personal o clave de acceso al dispositivo Token).

La solicitud de certificado, se realiza por el propio solicitante vía web o eventualmente en forma presencial, única persona que conoce el PIN de acceso al dispositivo. En ése momento se genera en el dispositivo criptográfico, la clave privada del certificado.

Durante la entrega del certificado (instalación de la clave pública en el dispositivo criptográfico Token) el software verifica que la clave pública corresponda con la clave privada contenida en

el dispositivo. Si no corresponde no permite su instalación.

3.2.2. Autenticación de la identidad de una persona jurídica

No aplica para usuarios internos del Poder Judicial. No se emiten certificados para personas jurídicas.

3.2.3. Validación de la identidad de una persona física

El solicitante deberá presentar la documentación que sea exigida por la legislación vigente y por el Poder Judicial al momento de la solicitud para este tipo de trámites.

3.2.4. Información no verificada del solicitante del certificado

No aplica, la información incluida en el certificado es verificada durante el proceso de petición.

3.2.5. Validación de autoridad

No aplica, no se expiden certificados para personas jurídicas.

3.2.6. Criterios para interoperabilidad

No aplica, no se opera con CA's externas.

3.3. Identificación y autenticación de solicitud para renovación de clave

No aplica la solicitud para renovación de claves. En los casos de expiración de un certificado se deberá solicitar la emisión de uno nuevo y en los casos de revocación de un certificado no se podrá re-habilitar el mismo.

3.4. Identificación y autenticación de solicitud de renovación de certificado

No aplica. En todos los casos deber realizarse una solicitud de nuevo certificado.

3.4.1. Identificación y autenticación de solicitud de renovación rutinaria

Debe solicitarse un nuevo certificado. Aplica todo lo especificado para la emisión de nuevos certificados.

3.4.2. Identificación y autenticación de solicitud de renovación de clave después de una revocación – clave no comprometida

Debe solicitarse un nuevo certificado. Aplica todo lo especificado para la emisión de nuevos certificados.

3.5. Identificación y autenticación de solicitud de revocación de la clave

Podrán solicitar la revocación de un certificado las personas indicadas en el numeral 4.10.2.

El procedimiento general de revocación se describe en este documento en el punto 4.10.3.

La validación del documento y de la identidad del solicitante de la revocación debe realizarse en forma personal o remota ante la Autoridad de Registro del PSC - Poder Judicial, salvo las solicitudes realizadas por la propia Suprema Corte de Justicia, en forma implícita o explícita mediante resoluciones.

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

4.1. Solicitud de certificado

4.1.1. Quién puede efectuar una solicitud

Pueden solicitarlo aquellos funcionarios del Poder Judicial que de acuerdo a la legislación y reglamentación vigentes deban hacer uso de certificados digitales para firma electrónica para cumplir sus funciones.

4.2. Procesamiento de la solicitud de certificado

4.2.1. Ejecución de las funciones de identificación y autenticación

La solicitud de certificado se realiza vía web o eventualmente en forma presencial ante los funcionarios de la Autoridad de Registro, de acuerdo al siguiente procedimiento:

Los funcionarios de la RA, validarán la solicitud formulada por el peticionante, mediante la verificación de la información ingresada a través de consultas realizadas en otros sistemas, así como también, con la información solicitada que debe de ser enviada a la Autoridad de Registro.

Tratándose de la primera vez, la Autoridad de Registro, al momento de realizar la petición entregará el dispositivo criptográfico (Token) al solicitante, quien lo conectará al equipo e ingresará un PIN (contraseña de uso personal) para la generación de la clave privada, quedándose consigo el dispositivo hasta que le sea entregado el certificado solicitado.

En caso de solicitud vía web, el solicitante ingresara la misma y la Autoridad de Registro procederá a su validación y emitirá el certificado, dejándolo así disponible para que el solicitante lo instale.

Una vez generada la solicitud en el sistema, el peticionante debe imprimir y firmar el "Contrato de Adjudicación de Certificado Digital y Dispositivo para Uso de Firma Electrónica" el que será enviado a la Autoridad de Registro.

4.3. Aprobación o rechazo de las solicitudes de certificado

La Autoridad de Registro es responsable de aprobar o rechazar las solicitudes.

Se rechaza cualquier solicitud de certificado que no cumpla con las presentes CP y CPS.

Si la RA detecta una anomalía en la información recibida o una falta a los procedimientos definidos, se rechazará la petición, lo que será informado al solicitante y si correspondiese el solicitante realizara una nueva solicitud.

4.3.1. Plazo para procesar las solicitudes de certificado

La Suprema Corte de Justicia dispondrá los recursos necesarios para que las solicitudes de certificados se procesen en los plazos razonables para el servicio.

4.4. Emisión de certificado

La CA es responsable de emitir los certificados digitales para las solicitudes aprobadas por la RA.

Si la CA detecta una anomalía en la información presentada o una falta a los procedimientos definidos, no se emitirá el certificado, lo que será informado a los interesados.

Todos los certificados se emiten en Montevideo.

4.4.1 Acciones de la CA durante la emisión de certificados

La CA debe verificar, que las solicitudes aprobadas vengan firmadas electrónicamente por un operador RA. Una vez creado el certificado, la CA debe remitirlo a la RA.

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

La CA notifica la emisión del certificado a la RA, quien se encarga de notificar al solicitante y dejarlo disponible el certificado para su instalación.

4.5. Aceptación del certificado

4.5.1. Forma en la que se acepta el certificado

Luego de emitido, el certificado queda disponible para su instalación en el dispositivo criptográfico del solicitante, el que luego de verificar la exactitud de la información contenida, debe aceptarlo.

4.5.2. Publicación del certificado por la CA

La CA no debe publicar información de los certificados emitidos en los repositorios de acceso público.

4.5.3. Notificación de la emisión del certificado por la CA a otras entidades

La CA sólo notificará de la emisión del certificado a la RA.
La RA es responsable de notificar al solicitante. No se definen entidades externas que necesiten o requieran ser notificadas acerca de los certificados emitidos por las CA.

4.6. Uso del par de claves y del certificado

4.6.1. Uso de la clave privada y del certificado por el usuario

El uso de la clave privada correspondiente a la clave pública contenida en el certificado solamente se permite una vez que el usuario haya aceptado el certificado emitido. Dicho uso debe realizarse en concordancia con la normativa vigente aplicable, lo estipulado en este documento, y los contratos de usuarios respectivos. Los solicitantes deben proteger sus llaves privadas del uso no autorizado y deben discontinuar su uso después de la expiración o revocación del certificado.

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

Los terceros aceptantes sólo deben depositar su confianza en los certificados luego de realizar las siguientes comprobaciones:

- Que el certificado es válido y fue emitido por el PSC - Poder Judicial.
- Que el certificado se está utilizando para uno de los usos permitidos en éste documento.
- Que la fecha en que se valida el certificado debe ser posterior o igual a la fecha de entrada en vigencia del certificado y anterior a la de expiración.
- Que el certificado no se encuentre en la lista de certificados revocados (CRL) emitida por el PSC al momento de la validación.

4.7. Renovación del certificado

La renovación del certificado no está permitida. Cuando un certificado expire debe solicitarse un nuevo certificado, de acuerdo con la sección 4.1 de ésta Política de Certificación.

4.7.1. Circunstancias para la renovación del certificado

No aplica.

4.7.2. Quién puede solicitar una renovación

No aplica.

4.7.3. Procesamiento de solicitud de renovación de certificado

No aplica.

4.7.4. Notificación al solicitante sobre la emisión de un nuevo certificado

No aplica.

4.7.5. Forma en la que se acepta la renovación de un certificado

No aplica.

4.7.6. Publicación por la CA del certificado renovado

No aplica.

4.7.7. Notificación por la CA de la emisión de un certificado a otras entidades

No aplica.

4.8. Re-emisión de claves de certificado

La re-emisión del certificado no está permitida. Cuando un certificado requiera ser re-emitido debe revocarse y solicitarse un nuevo certificado, de acuerdo con la sección 4.1. de esta Política de Certificación.

4.8.1. Circunstancia para re-emisión de claves de certificado

No aplica.

4.8.2. Quién puede solicitar la re-emisión de una nueva clave pública

No aplica.

4.8.3. Procesamiento de solicitud para re-emisión de claves de certificado

No aplica.

4.8.4. Notificación al solicitante de la re-emisión de un nuevo certificado

No aplica.

4.8.5. Forma de aceptación de un certificado re-emitido

No aplica.

4.8.6. Publicación por la CA de los certificados re-emitidos

No aplica.

4.8.7. Notificación por la CA de la re-emisión de un certificado a otras entidades

No aplica.

4.9. Modificación de certificados

La modificación del certificado no está permitida; en ningún caso se modificará la información contenida en el certificado. Cuando se requiera modificar cualquier dato del certificado, el mismo debe revocarse y solicitar un nuevo certificado, de acuerdo con la sección 4.1. de ésta Política de Certificación.

4.9.1. Circunstancias para la modificación del certificado.

No aplica.

4.9.2. Quién puede solicitar una modificación del certificado.

No aplica.

4.9.3. Procesamiento de solicitudes de modificación del certificado.

No aplica.

4.9.4. Notificación al solicitante de la emisión de una modificación del certificado.

No aplica.

4.9.5. Forma de aceptación del certificado modificado

No aplica.

4.9.6. Publicación por la CA de los certificados modificados

No aplica.

4.9.7. Notificación por la CA de la emisión de un certificado a otras entidades

No aplica.

4.10. Revocación de un certificado

4.10.1. Circunstancias para la revocación

Los certificados pueden ser revocados por:

•Solicitud del titular del certificado.

•Sustracción, extravío o destrucción del dispositivo soporte del certificado, debidamente acreditado (denuncia policial).

• Defunción, ausencia o incapacidad del titular, debidamente acreditado.

• Compromiso de la clave privada del certificado.

• Compromiso de las claves privadas de la CA de la Suprema Corte de Justicia.

• Resolución judicial que así lo ordene.

• Datos erróneos o inexactos en el certificado emitido.

• Incumplimiento por parte de la CA, de los funcionarios responsables de la expedición o del solicitante de las obligaciones establecidas en éste documento.

• Cese de la función, suspensión o sanción disciplinaria que así lo indique, destitución y cualquier otra circunstancia que la Suprema Corte de Justicia determine.

4.10.2. Quién puede solicitar una revocación

Estará legitimado para solicitar la revocación de un certificado:

- El titular del mismo.
- Cualquier persona presentando testimonio de la partida de defunción del titular del certificado, o declaratoria judicial de ausencia del titular del certificado, y/o el curador presentando testimonio de declaración de incapacidad del titular del certificado.
- La propia Suprema Corte de Justicia como prestador de servicios de certificación y/o titular de la potestad disciplinaria de los usuarios cuando así lo sea.

- La RA en casos de fallecimiento o pase a retiro del titular debidamente acreditados.

4.10.3. Procedimiento para la solicitud de revocación

La solicitud de revocación de un certificado debe realizarse ante la Autoridad de Registro en la oficina de la Unidad de Administradora de Notificaciones Electrónicas -UANE- .

La solicitud de revocación requiere la identificación del solicitante, verificación de la misma y debe validarse íntegramente por la RA de acuerdo a lo previsto en los apartados 4.10.1 y 4.10.2. Dicha solicitud puede cursarse en forma presencial o remota.

Cuando se solicite una revocación remota, sea por vía telefónica u otro medio fehaciente, la Autoridad de Registro debe requerir al titular sus datos personales y verificar las respuestas contra los datos almacenados. Si los datos coinciden, la solicitud es validada y se procede a la revocación. De lo contrario se frustra la identificación y se cancela el procedimiento de revocación.

Cuando corresponda, el PSC deberá confirmar al titular del certificado la revocación una vez efectivizada la misma.

4.10.4. Período de gracia para la solicitud de revocación

No existe período de gracia asociado a éste proceso.

En los casos de sustracción, extravío o destrucción del dispositivo soporte del certificado y de compromiso de las claves privadas del titular, éste último debe solicitar la revocación lo antes posible y bajo su responsabilidad.

4.10.5. Plazo dentro del cual la CA debe procesar la solicitud de revocación

La Suprema Corte de Justicia dispondrá los recursos necesarios para que las solicitudes de revocación se procesen en los plazos razonables para el servicio y de acuerdo con el procedimiento establecido en el apartado 4.10.3.

4.10.6. Requerimientos de verificación de revocación por terceros aceptantes

Los terceros aceptantes deben evaluar el estado del certificado y el estado de todos los certificados que integran la cadena a la que pertenece el mismo, antes de confiar en él.

En caso de que cualquiera de los certificados integrantes de la cadena de confianza haya sido revocado, la parte que confía es la única responsable de investigar si es razonable la confianza en una firma digital efectuada por un titular. Cualquier confianza de este tipo es asumida únicamente bajo el riesgo de la parte que confía.

Para estos propósitos las partes que confían pueden verificar el estado del certificado mediante el servicio web en él especificado, en la CRL disponible.

4.10.7. Frecuencia de emisión de CRL

La CA Raíz debe actualizar su lista de revocación cada vez que se resuelva una revocación, incluyendo el histórico de las publicaciones.

La SubCA debe actualizar y publicar su lista de revocación cada vez que se resuelva una revocación, incluyendo el histórico de las publicaciones.

4.10.8. Tiempo máximo de latencia de las CRL's

No existe período de latencia; las CRL's se publican en el repositorio en forma automática una vez generadas.

4.10.9. Disponibilidad para la comprobación del estado de revocación/estado en línea

La CA raíz y la CA subordinada tienen disponible un repositorio con información del estado de revocación de los certificados emitidos por éstas, el cual puede ser accedido vía Web como se indica en el punto 4.12 de esta Política de Certificación.

4.10.10. Otras formas disponibles de divulgación de revocaciones

No aplica.

4.10.11. Requerimientos especiales por compromiso de claves comprometidas

En caso de compromiso de las claves de la CA y SubCA, la Suprema Corte de Justicia deberá notificar según lo que establezca la normativa vigente al momento.

4.11. Suspensión de un certificado

4.11.1. Circunstancias para la suspensión

No se suspenden certificados. Se debe revocar los certificados y luego solicitar un certificado nuevo.

4.11.2. Quién puede solicitar la suspensión

No aplica.

4.11.3. Procedimiento para la solicitud de una suspensión

No aplica.

4.11.4. Límites del periodo de suspensión

No aplica.

4.12. Servicio de información del estado de certificados

4.12.1. Características operativas

El estado de los certificados estará disponible a través de las CRL's, las cuales serán publicadas y estarán accesibles a través del sitio web http://comunicaciones.poderjudicial.gub.uy/listado_revocados_scj.html

4.12.2. Disponibilidad del servicio

El servicio de información del estado de los certificados estará disponible durante las 24 horas los 365 días del año. En caso de error del sistema u otra circunstancia fuera de control del Poder Judicial, éste dedicará sus mejores esfuerzos para que el servicio se encuentre disponible nuevamente lo antes posible.

4.12.3. Características adicionales

No aplica.

4.13. Finalización de validez del certificado

El certificado perderá validez de las siguientes formas:

- Revocándose antes de su vencimiento.
- Cuando expira el plazo por el que fue concedido.

4.14. Custodia y recuperación de claves

4.14.1. Prácticas y políticas de custodia y recuperación de claves

La CA no realiza custodia ni recuperación de claves. Para todos los casos de clave comprometida se deberá revocar el certificado y emitir uno nuevo.

5. CONTROLES DE INSTALACIÓN, GESTIÓN Y OPERACIÓN

5.1. Controles físicos

5.1.1. Ubicación física y construcción

Las operaciones de la CA se desarrollan dentro de instalaciones del Poder Judicial. Se cuenta con un ambiente de producción y otro de contingencia.

5.1.2. Acceso físico

Todas las operaciones sensibles se realizan dentro de instalaciones del Poder Judicial. Se implementan controles para acceder a las máquinas, dispositivos y aplicaciones críticas;

5.1.3. Alimentación eléctrica y aire acondicionado

Las instalaciones de la CA disponen de sistemas de alimentación eléctrica ininterrumpida (UPS) con una potencia suficiente para mantener los equipos el tiempo necesario para que se apaguen automáticamente. Cuenta con sensor de nivel de humedad.

Las instalaciones de la CA cuentan con sistemas de aire acondicionado.

5.1.4. Prevención y protección de incendios

Las instalaciones de la CA cuentan con detector de humo.

5.1.5. Almacenamiento de medios

Se han establecido los procedimientos para el almacenamiento y respaldo de información. Se cuenta con redundancia de equipos y de discos.

5.1.6. Eliminación del material de almacenamiento de la información

La CA implementa controles para la eliminación de residuos (papel, medios, equipos y cualquier otro desecho) con el fin de prevenir el uso no autorizado, el acceso o divulgación de información privada y confidencial contenida en los desechos.

5.2. Controles de procedimiento

5.2.1. Roles de confianza

Los roles de confianza incluyen a todos las personas que tengan acceso y/o control sobre las funciones relacionadas con las solicitudes de certificados y la generación o revocación de los mismos.

Aunque no son los únicos, se distinguen los siguientes roles para la operación y gestión del sistema:

•Director/Administrador: Responsable de administrar la implementación de las políticas y prácticas de certificación y de las políticas y prácticas de seguridad. Responsable de la infraestructura tecnológica, aprueba la incorporación de equipamiento y dispositivos.

Tiene la responsabilidad de aprobar los procedimientos administrativos y técnicos y el control de acceso a los sistemas.

•Administrador PKI: Se encarga de la configuración general del software de PKI que incluye, entre otros, las tareas relacionadas con la instalación y mantenimiento de las aplicaciones de los sistemas PKI, las configuraciones de acceso a las bases de datos, la configuración de los dispositivos criptográficos a utilizar para la autenticación, los directorios de trabajo del sistema y configuración de permisos de los roles dentro del sistema de PKI. Responsable de las tareas de respaldo y recuperación.

•Receptor de solicitudes de certificados**:** Encargado de la recepción de solicitudes y de validación de la identidad de los solicitantes de certificados y de revocaciones. Entrega los dispositivos criptográficos (Tokens).

•Operador RA**:** Encargado de aprobar las solicitudes de emisión y de revocación de certificados. Encargado de la publicación de las CRL's. Supervisa la tarea de los receptores de solicitudes de certificados.

•Operador CA: Encargado de la emisión y revocación de certificados y de la generación de CRL's.

•Auditor del sistema**:** Se encarga de realizar las auditorías de acuerdo al alcance que defina el Director/Administrador o la Suprema Corte de Justicia. Informan los resultados de las mismas al Director/Administrador y/o a la Suprema Corte de Justicia.

5.2.2. Número de personas requeridas por tarea

La Suprema Corte de Justicia establece la cantidad de personas que ocuparán cada uno de los roles teniendo en cuenta las tareas asignadas a los mismos y la competencia requerida.

5.2.3. Identificación y autenticación para cada rol

Al ingresar al sistema de RA y de CA se identifican mediante certificados electrónicos emitidos por la propia infraestructura de la CA y se autentican por medio de dispositivos criptográficos USB personales.

5.3. Controles de personal

5.3.1. Requisitos relativos a la contratación, conocimiento y experiencia

Los recursos humanos que atienden el servicio de certificación que brinda el Poder Judicial cuentan con la calificación apropiada, experiencia, formación y entrenamiento.

5.3.2. Procedimientos de comprobación de antecedentes

Conforme a la normativa del Poder Judicial.

5.3.3. Requerimientos de formación

Todo el personal involucrado está capacitado apropiadamente. Cuando es necesario, la CA brinda formación y entrenamiento.

5.3.4. Requerimientos y frecuencia para capacitación continua

La CA capacita al personal cuando se presentan cambios significativos en las operaciones de la CA, por ejemplo, cuando se producen actualizaciones de hardware o software, cambios en los sistemas de seguridad, etc.

5.3.5. Frecuencia y secuencia de rotación de tareas

No se realiza rotación rutinaria de tareas.

5.3.6. Sanciones por acciones no autorizadas

La CA debe ejecutar las acciones administrativas y disciplinarias apropiadas contra el personal que violente las normas establecidas en esta CP/CPS. Las sanciones se procesan de acuerdo a la normativa vigente para los funcionarios públicos en general y en particular para los funcionarios judiciales.

5.3.7. Requisitos de contratación de terceros

La CA puede contratar personal externo o consultores para cualquiera de las tareas. Siempre debe existir una relación claramente definida con el contratista y bajo las siguientes condiciones:

a) existe un contrato con cláusulas propias de los roles de confianza y estipula sanciones para las acciones no autorizadas.

b) no se posee personal disponible para llenar los roles de confianza contratados.

c) los contratistas o consultores cumplen con los requisitos previstos para su contratación.

5.3.8. Documentación suministrada al personal

La CA suministra al personal manuales e instructivos y otros documentos vinculados a la ejecución de su rol.

5.4. Procedimientos de bitácora de auditoría

La CA mantiene bitácoras manuales y automáticas, indicando para cada evento la entidad que lo causa, la fecha y hora del mismo.

5.4.1. Tipos de eventos registrados

La CA guarda todos los eventos que tengan lugar durante el ciclo de vida de un certificado y todos los datos ingresados durante el proceso de certificación.

5.4.2. Frecuencia del procesamiento de información

Cada área de trabajo establece la frecuencia adecuada para el procesamiento de la información.

Las bitácoras de auditoría deben ser revisadas en respuesta a una alerta, por irregularidades o incidentes dentro de los sistemas de la CA.

5.4.3. Período de conservación de los registros de auditoría

Los registros de auditoría no se destruyen. Se implementan los mecanismos necesarios para archivarlos adecuadamente.

5.4.4. Protección de la bitácora de auditoría

Aplican todos los controles descritos en los apartados 5.1 Controles físicos y 5.2 Controles de procedimiento. Se implementan controles para prevenir la modificación y la eliminación de los registros de auditoría siguiendo el procedimiento de respaldo que se referencia en el documento de nombre "Política de Seguridad".

5.4.5. Procedimientos de respaldo de la bitácora de auditoría

La bitácora electrónica de auditoría se respalda siguiendo el procedimiento de respaldo que se referencia en el documento de nombre "Política de Seguridad".

5.4.6. Recopilación para auditoría

Los registros para auditoría se mantienen dentro de las instalaciones donde se generan.

5.4.7. Notificación al sujeto que causa el evento

Cuando un evento es almacenado en la bitácora, no se notifica al causante de dicho evento.

5.4.8. Análisis de vulnerabilidades

Se realiza periódicamente el análisis de vulnerabilidades utilizando las herramientas disponibles y tomando como referencia el documento de nombre "Politica de Seguridad". El Administrador/Director decidirá si corresponde o no la comunicación de los resultados de dicho análisis a la Suprema Corte de Justicia.

5.5. Archivo de registros

5.5.1. Tipos de registros archivados

Cada área de trabajo de la CA establece en sus procedimientos los registros y los archivos adecuados para cumplir con las funciones asignadas.

5.5.2. Período de retención de archivos

Todos los archivos deben mantenerse por igual período que la validez de la CA raíz.

5.5.3. Protección de archivos

Cada área de trabajo de la CA establece el tratamiento, el control y la protección adecuada para sus archivos. Durante las auditorías se brinda el acceso al equipo auditor a todos los archivos.

5.5.4 Requerimientos para el sellado de tiempo de los registros

Cada registro contiene la fecha de su realización. En los registros electrónicos además de la fecha consta la hora, minuto y segundo.

5.5.5. Sistema de recopilación de archivos

Los registros se mantienen dentro de las instalaciones donde se generan.

5.5.6. Procedimientos para obtener y verificar la información archivada

Solamente el personal autorizado está habilitado para obtener acceso al archivo.

5.6. Cambio de claves de una CA y CA Subordinada

No se realizan cambios de claves de la CA ni de la SubCA sino que se generarán nuevas claves en cuyo caso los procedimientos para proporcionar las nuevas claves públicas de esa nueva CA a los titulares y terceros aceptantes, son los mismos que para proporcionar las claves públicas en vigor.

5.7. Recuperación en caso de compromiso o catástrofe

5.7.1 Procedimientos de gestión de incidentes y vulnerabilidades

La CA cuenta con procedimientos formales para el reporte de incidentes de los cuales debe dar cuenta a la jerarquía inmediata.
La CA mantendrá un plan de recuperación de desastres; si el equipo de la CA es dañado entonces las operaciones de la CA deben restablecerse lo más pronto posible, dando prioridad a la capacidad de revocar certificados.

5.7.2. Mal funcionamiento de recursos físicos, lógicos y/o datos

Posterior a una corrupción de recursos computacionales, software o datos, la CA afectada debe realizar un reporte a la jerarquía inmediata del incidente a efectos que ésta tome las medidas que estime convenientes.

5.7.3. Procedimientos ante clave privada comprometida

Si la clave de la CA raíz o CA subordinada es comprometida se deberá informar inmediatamente a la Suprema Corte de Justicia a fin de que tome las medidas que estime pertinentes, entre ellas el proceder a la revocación de los certificados correspondientes y publicación de la CRL actualizada.

5.7.4. Continuidad del servicio luego de una falla grave

Se proveerá de un mecanismo de recuperación ante una falla grave y tal como estaba al momento de la última copia de respaldo realizada.

5.8. Cese de una CA o RA

Solamente la Suprema Corte de Justicia podrá poner fin a la actividad de la CA. En las circunstancias que la CA ponga un término a sus actividades, la CA dejará de emitir nuevos certificados pero se mantendrán todos los servicios de verificación de validez de los certificados emitidos hasta la fecha de vencimiento del último certificado de usuario final. No se cesará la actividad de la RA sin cese de actividades de la CA.

6. CONTROLES TÉCNICOS DE SEGURIDAD

6.1 Generación e instalación del par de claves

6.1.1. Generación del par de claves

Certificados de CA raíz y CA Subordinada:
El acto de generación del par de llaves debe realizarse en las instalaciones del PSC, en presencia de los funcionarios designados.

Debe elaborarse un guión detallado de las actividades a realizar para poner en marcha su Autoridad Certificadora.

Este deberá cubrir todo el proceso de instalación, a saber: aplicaciones de CA, configuración de las aplicaciones, generación y respaldo de llaves, generación de la solicitud de firma del certificado, instalación del certificado de la AC y puesta en funcionamiento de las funcionalidades de gestión de certificados y CRL's.

Certificados de usuario final:
La generación del par de claves de los solicitantes cumplen al menos con el estándar FIPS 140-2, nivel 2.

6.1.2. Entrega de la clave privada al titular del certificado

La clave privada del titular se mantiene dentro del dispositivo USB (Token) que la genera. El dispositivo siempre está en poder del titular.

6.1.3. Entrega de la clave pública al emisor del certificado (CA).

En el momento que se genera la solicitud, la clave pública es entregada al emisor del certificado (CA) por el dispositivo USB.

6.1.4. Entrega de la clave pública de la CA a terceros

La distribución de la clave pública se realiza a través del certificado digital y del repositorio público.

6.1.5. Tamaño de las claves

El largo de clave de la CA Raíz y CA Subordinada es RSA 4096 bits.
El par de claves de usuario para firma digital generado es RSA y tiene un largo de 1024 bits.

6.1.6. Parámetros de generación de la clave pública y verificación

Las claves públicas de la CA Raíz y de la CA Subordinada es RSA 4096 bits y se generan en el acto de generación del par de llaves con todas las medidas de seguridad necesarias

La clave pública del usuario es RSA 1024 bits y se genera en un dispositivo criptográfico USB que cumple con el estándar FIPS 140-2 Nivel 2.

6.2. Protección de la clave privada y controles de módulos criptográficos

6.2.1. Protección de la clave privada de la Autoridad Certificadora

Certificados de CA raíz y CA Subordinada:
Se generan y se protegen con las medidas de seguridad necesarias.

Certificados de usuario final:
La generación de las llaves de los solicitantes requiere que los módulos de criptografía cumplan al menos con el estándar FIPS 140-2 nivel 2.

Únicamente el solicitante del certificado puede utilizar la clave privada correspondiente, mediante un PIN o contraseña personal, de conocimiento exclusivo del solicitante. Cuando la clave privada no esté siendo utilizada debe desactivarse.

La protección de dicha clave es responsabilidad exclusiva del solicitante y no puede ser delegada.

6.2.2. Respaldo de la clave privada

Los respaldos de llaves privadas de la CA y SubCA son únicamente para propósitos de recuperación en caso de desastre y se emiten en el acto de generación de claves de las mismas. Están protegidas con las medidas de seguridad necesarias.

La recuperación de las claves de la CA y SubCA debe llevarse a cabo de una forma segura como el proceso de respaldo.

No se respaldan las claves privadas de certificados de los solicitantes por ningún motivo, y éstas permanecen dentro del dispositivo criptográfico donde fueron generadas.

6.2.3. Archivo de la clave privada

Se asegura que las claves privadas de la CA y de la SubCA permanecen confidenciales y se mantiene su integridad.

6.2.4. Transferencia de la clave privada hacia o desde un módulo criptográfico.

En el evento que una clave privada de la CA sea transportada, la misma será encriptada durante su transporte.

6.3. Método de activación de la clave privada

Se entiende por "activación" al proceso previo a la utilización de la clave privada que permite hacerla disponible para ser usada.

Certificados de CA Raíz y CA Subordinada:
Para la activación de la clave de la CA se requiere del uso de los dispositivos criptográficos de un administrador y de un operador.

Solo el personal autorizado posee los dispositivos criptográficos y conoce las claves de acceso para acceder a los datos de activación.

Certificados de usuario final:

El método de activación se realiza mediante el dispositivo criptográfico correspondiente y el PIN o contraseña personal de conocimiento exclusivo del titular.

El usuario final es el único responsable de la protección de los datos de activación de sus claves privadas. Esta responsabilidad está a su vez plasmada en el contrato en soporte papel que suscriben el peticionante y el Poder Judicial.

6.4. Método de desactivación de la clave privada

Certificados de CA Raíz y CA Subordinada:

Para desactivar las claves de la CA debe removerse manualmente dichas claves

Certificados de usuario final:

Mediante la remoción del dispositivo.

6.5. Método para destruir la clave privada

Certificados de CA Raíz y CA Subordinada:

Para destruir las claves de la CA Raíz y CA Subordinada es obligatorio que la clave sea destruida siguiendo los procedimientos establecidos con previa autorización de la Suprema Corte de Justicia.

Certificados de usuario final:

La clave en el dispositivo criptográfico es destruida siguiendo los procedimientos establecidos y mediante los técnicos designados a tal fin.

6.6. Otros aspectos sobre la gestión del par de claves

6.6.1. Períodos operativos de los certificados y período de uso del par de claves

Los períodos de utilización de las claves son los determinados por la duración del certificado, transcurridos los cuales no podrán continuar utilizándose.

La siguiente tabla muestra la validez para cada tipo de certificado.

Tipo de certificado	**Validez**
Certificado de CA raíz (CA)	20 años
Certificado de CA Subordinada (SubCA)	10 años
Certificado para usuarios del Poder Judicial	5 años

6.7. Controles de seguridad informática

La CA implementa procedimientos que permitan una operación segura. Se instrumentan los siguientes aspectos:

- Definición de roles y responsabilidades;
- Clasificación de la información;
- Seguridad vinculada a los recursos humanos;
- Seguridad lógica de los sistemas y redes;
- Control del acceso lógico;
- Seguridad física del ambiente y de los sistemas;
- Gestión de respaldos;
- Continuidad de la operativa y disponibilidad;
- Registros de auditoría;
- Respuesta a incidentes.

6.7.1. Controles de seguridad del ciclo de vida

Todos los medios a ser incorporados, retirados o trasladados fuera de las fronteras de la organización están sujetos a previa autorización en procedimientos definidos para ello.

6.8. Controles de seguridad de la red

El acceso a la operación de la CA está limitada al personal autorizado. La conexión está sujeta a estrictos controles de seguridad a nivel de red, mediante firewalls, controles de acceso y auditorías (logs).

7. PERFILES DE CERTIFICADOS y DE CRL

7.1. Perfil de certificado de usuario

7.1.1. Número de versión

Todos los certificados emitidos por la Suprema Corte de Justicia utilizan el estándar X.509 versión 3.

Certificado CA Raiz

Campo	Contenido
Versión	v3
Numero de Serie	0
Algoritmo de firma	SHA-256 withRSA
Nombre Distintivo del Emisor	CN=CA-Suprema Corte de Justicia, OU=Poder Judicial, O=Poder Judicial, C=UY
Validez	20 años
Tamaño de la Clave Pública	Tipo de clave: RSA Longitud de clave = 4096 bits
DN	
CN	CA-Suprema Corte de Justicia
OU	Poder Judicial
O	Poder Judicial
C	UY
Identificador de Clave	
Identificador de Autoridad Certificadora	----------
Restricciones Básicas:	
CA	TRUE
Largo de ruta	Sin límite
Uso	DigitalSignature, Certificate Sign, CRL Sign
Nombre alternativo del asunto	uane@poderjudicial.gub.uy
Nombre alternativo del emisor	uane@poderjudicial.gub.uy

Acceso a la información de la autoridad:	http://comunicaciones.poderjudicial.gub.uy/pki/ca_scj.crt
Distribución de CRL:	
Punto de distribución	http://comunicaciones.poderjudicial.gub.uy/pki/cert_crl.crl

Certificado SubCA

Campo	Contenido
Versión	v3
Numero de Serie	A completar luego de la inicialización
Algoritmo de firma	SHA-256 withRSA
Nombre Distintivo del Emisor	CN=CA-Suprema Corte de Justicia, OU=Poder Judicial, O=Poder Judicial, C=UY
Validez	10 años
Tamaño de la Clave Pública	Tipo de clave: RSA Longitud de clave = 4096 bits
DN	
CN	SubCA-Suprema Corte de Justicia
OU	Poder Judicial
O	Poder Judicial
C	UY
Identificador de Clave	
Identificador de Autoridad Certificadora	----------
Restricciones Básicas:	
CA	TRUE
Largo de ruta	Sin límite
Políticas de Certificado:OID	

	2.16.858.2.10000232.66565.20150601
CPS	http://comunicaciones.poderjudicial.gub.uy/pki/cp-cps_scj.pdf
Uso	DigitalSignature, Certificate Sign, CRL Sign
Nombre alternativo del asunto	uane@poderjudicial.gub.uy
Nombre alternativo del emisor	uane@poderjudicial.gub.uy
Acceso a la información de la autoridad:	http://comunicaciones.poderjudicial.gub.uy/pki/ca_scj.crt
Distribución de CRL:	
Punto de distribución	http://comunicaciones.poderjudicial.gub.uy/pki/cert_crl.crl

7.2 Perfil de la CRL

La CRL se emite desplegando los siguientes datos:

Listado de certificados de usuario revocados:

Campo	*Contenido*
Clave	Clave que identifica el certificado del usuario
Nombre	Nombre del usuario del certificado
Emisión	Fecha de emisión del certificado
Expiración	Fecha en que expira el certificado
Revocación	Fecha en que se revoca el certificado
Motivo	Motivo por el cual se revoca el certificado

Listado de certificados de CA revocados:

Campo	*Contenido*
Clave	Clave que identifica el certificado del certificado de la CA
Nombre	Nombre de a quien pertenece el certificado
Emisión	Fecha de emisión del certificado
Expiración	Fecha en que expira el certificado
Revocación	Fecha en que se revoca el certificado
Motivo	Motivo por el cual se revoca el certificado

8. AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES

8.1. Frecuencia o circunstancias de los controles

Cada área de trabajo establece la frecuencia para sus revisiones y evaluaciones.
La Suprema Corte de Justicia podrá resolver la realización de auditorías y la frecuencia de las mismas.

8.2. Identificación/calificaciones del auditor

Todo equipo o persona designada para realizar una auditoría sobre el sistema de la PKI deberá contar con la adecuada capacitación y experiencia.

8.3. Relación entre el auditor y la entidad auditada

Al margen de la función de auditoría, el auditor externo y Poder Judicial no deberán tener relación alguna que pueda derivar en un conflicto de intereses.

8.4. Aspectos cubiertos por los controles

La auditoría determinará la adecuación de los servicios de PKI del Poder Judicial con ésta CP/CPS. También determinará los riesgos del incumplimiento de alguna de las políticas definidas por éste documento.

8.5. Comunicación de resultados

El equipo auditor comunicará los resultados a las autoridades responsables de la CA y a cada uno de los Ministros de la Suprema Corte de Justicia.