DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA POLÍTICA DE CERTIFICACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC)

DOC-PKI-04 Versión 1.0

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Contenido

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

CONTROL DOCUMENTAL

Documento	
Título: DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA POLÍTICA DE CERTIFICACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC)	Nombre Archivo:
Código: **DOC-PKI-04**	Soporte Lógico
Fecha: 28/10/2018	Ubicación Física: DGFDyCE
Versión:1.0	

Registro de Cambios		
Versión	Fecha	Motivo de Cambio

Distribución del documento	
Nombre	Área
Ministerio de Industria y Comercio (MIC)	Dirección General de Firma Digital y Comercio Electrónico(DGFDyCE)
Autoridad Certificadora(CA)	Prestadores de servicios de certificación (PSC)
Documento Público	www.caraiz.gov.py

Control del Documento		
Preparado por:	Revisado por:	Aceptado por:
ING. LUCAS SOTOMAYOR	*ABG LAURA MINARDI*	*M. SC RODYS ROLÓN*

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

1. INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL

Este documento establece los requisitos mínimos que obligatoriamente deberán ser observados por los Prestadores de Servicio de Certificación (PSC) en su carácter de autoridad certificadora (CA), para la formulación y la elaboración de su política de certificación (CP)

Toda Política de Certificación elaborada en al ámbito de la Infraestructura de Clave Pública del Paraguay (PKI Paraguay) debe obligatoriamente adoptar la misma estructura empleada en este documento.

Son 4(cuatro) los tipos de certificados digitales, inicialmente previstos, para los usuarios de la PKI Paraguay, siendo 2 (dos) de firma digital y 2 (dos) de cifrado conforme lo descripto a continuación:

Tipos de certificados de firma digital

I. F1
II. F2

Tipos de certificados de cifrado

I. C1
II. C2

Los tipos de certificado indicados, definen la escala de requisitos de seguridad exigidos a cada cual; los tipos F1 y C1 están asociados a requisitos menos rigurosos y los tipos F2 y C2, exigen requisitos más rigurosos.

Los certificados de firma o de cifrado pueden, conforme a la necesidad, ser emitidos por los PSC, para personas físicas, personas jurídicas, equipos o aplicaciones.

1.2 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

En este ítem debe ser identificada, la Política de Certificación (CP), indicando, como mínimo, el tipo de certificado al que está asociada.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

También se debe identificar el documento de Declaración de Prácticas de Certificación (CPS) del PSC, donde estarán descriptos sus prácticas y procedimientos de certificación.

1.3 PARTICIPANTES DE LA PKI

1.3.1. AUTORIDADES CERTIFICADORAS (CA)

En este ítem se debe identificar las CA, integrantes de la PKI Paraguay que implementa la CP.

1.3.2. AUTORIDADES DE REGISTRO (RA)

En este ítem se identifica la dirección de página web (URL) donde están publicados los datos referentes a las autoridades de registro (RA) habilitados por el PSC para los procesos de recepción, validación y direccionamiento de solicitudes de emisión o de revocación de los certificados digitales, y de identificación de sus solicitantes. Las informaciones a ser publicadas en el sitio son:

a) identificación y vinculación de todas las RA habilitadas, con informaciones sobre las CP que implementan;
b) para cada RA habilitada, consignar las direcciones de sus instalaciones técnicas, cuyo funcionamiento haya sido autorizado por la CA Raíz.
c) Para cada RA habilitada, consignar el tipo de vínculo con eventuales locales provisorios autorizados por la CA Raíz, con fecha de creación y cierre de actividades;
d) identificación y vínculo de las RA deshabilitadas dentro de la cadena PKI Paraguay, con su respectiva fecha de cese de actividades;
e) instalaciones técnicas de la RA habilitada que ha dejado de operar, con su respectiva fecha de cierre de actividades;
f) acuerdos operacionales celebrados entre las RA vinculada con otra RA dentro de la PKI Paraguay, si fuera el caso.

El PSC deberá mantener las informaciones permanentemente actualizadas.

Las RA delegadas son autoridades de registro vinculadas a un PSC mediante un contrato de prestación de servicios; el funcionamiento de las mismas deberá estar en conocimiento y autorizadas por la CA raíz.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

1.3.3. PRESTADORES DE SERVICIOS DE SOPORTE (PSS)

Es este ítem se identifica la dirección de página web (URL), donde deberán estar publicados los datos referentes a los Prestadores de Servicio de Soporte (PSS) vinculados al PSC, sea directamente o sea por intermedio de sus RA.

PSS son entidades externas a las que recurre la CA o la RA para desempeñar actividades descritas en esta CP o en una CPS y se clasifican en tres categorías, conforme al tipo de servicio prestado.

a) Disponibilización de infraestructura física y lógica;
b) Disponibilización de recursos humanos especializados;
c) Disponibilización de infraestructura física y lógica y de recursos humanos especializados.

El PSC deberá mantener las informaciones arriba citadas siempre actualizadas

1.3.4. SUSCRIPTORES

En este ítem se especifican las personas físicas o jurídicas que podrán ser titulares de los certificados emitidos según esta CP.

1.3.5. PARTE QUE CONFÍA

Se entenderá por parte que confía, toda persona física o jurídica, diferente al titular del certificado que decide aceptar y confiar en un certificado digital emitido dentro de la jerarquía PKI Paraguay.

Una parte que confía puede o no ser un suscriptor.

1.3.6 OTROS PARTICIPANTES

Sin estipulaciones.

1.4 USO DEL CERTIFICADO

1.4.1 USOS APROPIADOS DEL CERTIFICADO

En este ítem las CP deben deferir los usos para las cuales los certificados definidos en la CP son los adecuados.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

En la definición de las aplicaciones para el tipo de certificado definido por la CP, el PSC debe tener en cuenta el nivel de seguridad previsto para ese tipo de certificado. Este nivel de seguridad estará caracterizado por los requisitos mínimos definidos para aspectos como: tamaño de la llave criptográfica, medios de almacenamiento de clave, proceso de generación de par de claves, procedimiento de identificación del titular del certificado, frecuencia de emisión de la lista de certificados revocados (CRL) y la extensión de periodo de vencimiento del certificado.

Certificados de los tipos F1, F2 serán utilizados en aplicaciones como confirmación de identidad y firma de documentos electrónicos con verificación de integridad de sus informaciones.

Certificados de los tipos C1, C2 serán utilizados en aplicaciones como cifrado de documentos, base de datos, mensajes y otras informaciones electrónicas con la finalidad de asegurar su confidencialidad.

1.4.2. USOS PROHIBIDOS DEL CERTIFICADO

En este Ítem la CP debe relacionar e identificar las CP implementadas por el PSC, que definen los usos para las cuales esté prohibida o restringida el uso del certificado.

1.5 ADMINISTRACIÓN DE LA POLÍTICA

1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

En este Ítem deben ser incluidos, el nombre, la dirección y otras informaciones del PSC responsable de la elaboración de la CP.

1.5.2. PERSONA DE CONTACTO

En este Ítem deben ser incluidos, el nombre, los números de teléfonos, el correo electrónico de la persona de contacto asignado por el PSC.

1.5.3. PERSONA QUE DETERMINA LA ADECUACIÓN DE LA CPS A LA POLÍTICA

En este Ítem debe ser incluido el nombre de la persona que determina la adecuación de la CPS a la CP.

1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA CP

En este Ítem se especifica el procedimiento de aprobación del CP.

Abog. Rodys Bolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

1.6 DEFINICIONES Y ACRÓNIMOS

1.6.1 DEFINICIONES

Acuerdo de Suscriptores: es un acuerdo entre la CA Raíz y el PSC, y entre el PSC y el usuario final, que establece los derechos, obligaciones y responsabilidades de las partes con respecto a la emisión y gestión de los certificados. Éste acuerdo, requiere la aceptación explícita de las partes intervinientes.

Armario ignífugo: armario equipado con sistemas de protección contra el fuego para aislar los productos almacenados en su interior.

Autenticación: proceso técnico que permite determinar la identidad de la persona que firma electrónicamente, en función del mensaje firmado por ésta, y al cual se le vincula. Este proceso no otorga certificación notarial ni fe pública.

Autoridad de Aplicación (AA): se designa al Ministerio de Industria y Comercio como órgano regulador competente por Ley, establecido por el artículo 38 de la Ley 4610/2012 que modifica y amplía la Ley N° 4017/2010 "De validez jurídica de la Firma Electrónica, Firma Digital, los Mensajes de Datos y el Expediente Electrónico". Ejerce funciones a través de su unidad administrativa, la Dirección General de Firma Digital y Comercio Electrónico, dependiente del Viceministerio de Comercio.

Autoridad de Certificación (CA): entidad que presta servicios de emisión, gestión, revocación u otros servicios inherentes a la certificación digital. En el marco de la PKI Paraguay, son Autoridades de Certificación, la CA Raíz del Paraguay y el PSC.

Autoridad Certificadora Raíz o Autoridad de Certificación Raíz (CA Raíz): es el órgano técnico dentro de la PKI, cuya función principal es habilitar al PSC y emitir a éste, el certificado digital correspondiente. Posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza.

Abog. Blodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Autoridad de Certificación Intermedia (CAI): entidad cuyo certificado de clave pública ha sido firmado digitalmente por la autoridad de certificación raíz; es responsable de la emisión de certificados a usuarios finales.

Autoridad de Registro (RA): entidad responsable de la identificación y autenticación de titulares de certificados digitales; la misma no emite ni firma certificados. Una RA interviene en el proceso de solicitud del certificado, en el proceso de revocación o en ambos. La RA, no necesita ser un organismo separado, sino que puede ser parte de la CA.

Autoridad de Validación (VA): entidad responsable de suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una autoridad de registro y certificados por la autoridad de certificación. La VA, no necesita ser un organismo separado sino que puede ser parte de la CA.

Cadena de certificación: lista ordenada de certificados que contiene un certificado de usuario final y certificados de CA, que termina en un certificado raíz. El emisor del certificado del usuario final es el titular del certificado de CA y a su vez, el emisor del certificado de CA es el titular del certificado de CA Raíz. El usuario final o la parte que confía, debe verificar la validez de los certificados en la cadena.

Ceremonia de claves: procedimiento mediante el cual es generado un par de claves de CA, su clave privada es generada y almacenada en un módulo criptográfico, y debe ser respaldada con el mismo nivel de seguridad que la clave original. Este procedimiento debe ser documentado.

Certificado Digital (CD): es un documento electrónico, generado y firmado por una CA legalmente habilitada para el efecto, el cual vincula un par de claves con una persona física o jurídica confirmando su identidad.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Cifrado: es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido de manera que solo pueda leerlo la persona que disponga de la clave del cifrado adecuada para decodificarla.

Cifrado asimétrico: tipo de cifrado que utiliza un par de claves criptográficas diferentes (ejemplo: privado y público) y matemáticamente relacionadas.

Claves criptográficas: valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.

Clave pública y privada: la criptografía en la que se basa la PKI Paraguay, es la criptografía asimétrica. En ella se emplea un par de claves: lo que se cifra con una de ellas, sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y está incorporada en el certificado digital, mientras que a la otra se le denomina privada y está bajo la custodia del titular del certificado.

Cofre de seguridad: compartimiento para almacenar materiales o documentos sensibles de la CA, debe ser resistente al fuego y ofrecer protección a aperturas forzadas.

Compromiso: violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.

Data Center (Centro de Datos): infraestructura compuesta por el espacio físico para la instalación de equipos informáticos y de comunicación con adecuados sistemas de energía, aire acondicionado y seguridad. Es parte de una CA, constituye un recinto seguro que alberga, entre otras cosas, los módulos criptográficos de hardware, protege la infraestructura tecnológica y es el lugar donde se ejecutan servicios del ciclo de vida del certificado. La importancia del data center radica en la protección que brinda a la clave privada y asegura la confianza en los certificados digitales emitidos por la CA.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Datos de activación: valores de los datos, distintos al par de claves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos.

Declaración de Prácticas de Certificación (CPS): declaración de las prácticas que emplea una CA al emitir certificados y que define la infraestructura, políticas y procedimientos que utiliza la CA para satisfacer los requisitos especificados en la CP vigente.

Delta CRL: partición del CRL, dentro de una unidad de tiempo, que contiene los cambios realizados al CRL base desde su última actualización.

Emisión: comprende la generación del certificado, cuyo proceso es una función de la CA

Emisor del certificado: organización cuyo nombre aparece en el campo emisor de un certificado.

Estándares Técnicos Internacionales: requisitos de orden técnico y de uso internacional que deben observarse en la emisión de firmas electrónicas y en las prácticas de certificación.

Firma Digital: es una firma electrónica certificada por un prestador habilitado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincula únicamente al mismo y a los datos a lo que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Grupo Electrógeno: máquina encargada de generar electricidad a partir de un motor de gasolina o diésel. La instalación de este equipo deberá ser de tal forma que al interrumpirse el suministro de energía eléctrica del proveedor externo, el mismo debe arrancar automáticamente tomando la carga de las instalaciones del data center de la CA, incluyendo los circuitos de iluminación, de los equipos informáticos, equipos de refrigeración, circuitos de monitoreo, prevención de incendios; en fin de todos los circuitos eléctricos críticos para el funcionamiento de las instalaciones tecnológicas.

Habilitación: autorización que otorga el MIC al PSC para emitir certificados digitales a usuarios finales, una vez cumplidos los requisitos y condiciones establecidos en la norma.

Huella digital (Código de verificación o resumen): secuencia de bits de longitud fija obtenida como resultado de procesar un mensaje de datos con un algoritmo, de tal manera que: (1) el mensaje de datos produzca siempre el mismo código de verificación cada vez que se le aplique dicho algoritmo (2) sea improbable, a través de medios técnicos, que el mensaje de datos pueda ser derivado o reconstruido a partir del código de verificación producido por el algoritmo (3) sea improbable, por medios técnicos, que se pueda encontrar dos mensajes de datos que produzcan el mismo código de verificación al usar el mismo algoritmo.

Identificación: procedimiento de reconocimiento de la identidad de un solicitante o titular de certificado dentro de la jerarquía PKI Paraguay.

Identificador de Objeto (OID): los identificadores de objeto son un sistema de identificación para entidades físicas o virtuales basado en una estructura arbórea de componentes de identificación. El árbol de OID se define plenamente en las Recomendaciones UIT-T y las normas internacionales ISO.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Infraestructura de Clave Pública (PKI): es un conjunto de personas, políticas, procedimientos y sistemas informáticos necesarios para proporcionar servicios de autenticación, integridad y no repudio, mediante el uso de criptografía de claves públicas y privadas y de certificados digitales, así como la publicación de información, consultas de vigencia y validez de los mismos

Integridad: característica que indica que un mensaje de datos o un documentos electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.

Jerarquía PKI: jerarquía de confianza que se conforma por un conjunto de autoridades de certificación que mantienen relaciones de confianza por las cuales una CA de nivel superior (CA Raíz) garantiza la confiabilidad de una o varias de nivel inferior (PSC) y a su vez, de los certificados emitidos por éstos a los suscriptores.

Lista de certificados revocados (CRL): lista emitida por una CA, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.

Módulo criptográfico: software o hardware criptográfico que genera y almacena claves criptográficas.

Módulo de Seguridad de Hardware (HSM, Hardware Security Module): dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas.

No Repudio: refiere que la posesión de un documento electrónico y la firma digital asociada al mismo, será prueba efectiva del contenido y del autor del documento.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Par de claves: son las claves privada y pública de un criptosistema asimétrico. La clave privada y la clave pública están relacionadas matemáticamente y poseen ciertas propiedades, entre ellas que es imposible deducir la clave privada de la clave pública conocida.

PKCS#1: estándar de criptografía de clave pública #1, desarrollado por RSA Security Inc., que proporciona las definiciones básicas y recomendaciones para la implementación de algoritmo RSA para criptografía de clave pública.

PKCS#10 (Certification Request Syntax Standard): Estándar desarrollado por RSA que define la sintaxis de una petición de certificado.

Parte que confía: es toda persona física o jurídica diferente del titular, que decide aceptar y confiar en un certificado emitido bajo la jerarquía de la PKI Paraguay.

Perfil del certificado: especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).

Período de operación: periodo de vigencia de un certificado, que comienza en la fecha y la hora en que es emitido por una CA, y termina en la fecha y la hora en que expira o se revoca el mismo.

Período de uso: rrefiere al tiempo establecido para los certificados emitidos dentro la jerarquía de la PKI para determinados usos.

Política: orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

Política de Certificación: (CP) documento en el cual la CA, define el conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad particular y/o una clase de aplicaciones con requisitos comunes de seguridad.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Práctica: modo o método que particularmente observa alguien en sus operaciones.

Prestador de Servicios de Certificación (PSC): entidad habilitada por la AA, encargada de operar una CA en el marco de la PKI Paraguay. El PSC debe contar con un certificado digital emitido por la CA Raíz del Paraguay y solo podrá emitir certificados a usuarios finales.

Registro de Auditoría: registro cronológico de las actividades del sistema, el cual es suficiente para permitir la reconstrucción, revisión e inspección de la secuencia de los ambientes y de las actividades que rodean o que conducen a cada acontecimiento en la ruta de una transacción desde su inicio hasta la salida de los resultados finales.

Repositorio: sitio principal de Internet confiable y accesible, mantenido por la CA con el fin de difundir su información pública.

Rol de confianza: función crítica que desempeña personal de la CA, que si se realiza insatisfactoriamente puede tener un impacto adverso sobre el grado de confianza proporcionado por la CA.

Ruta del certificado: secuencia ordenada de certificados de entidades que, junto a la clave pública de la entidad inicial en la ruta, puede ser procesada para obtener la clave pública de la entidad final en la ruta.

Servicio OCSP: permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la CA sobre el estado de un certificado.

Solicitante de Certificado: persona física o jurídica que solicita la emisión de un certificado a una CA.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Solicitud de Firma de Certificado (CSR): es una petición de certificado digital que se envía a la CA. Mediante la información contendida en el CSR, la CA, puede emitir el certificado digital una vez realizadas las comprobaciones que correspondan.

Suscriptor: persona física o jurídica titular de un certificado digital emitido por una CA.

Usuario final: persona física o jurídica que adquiere un certificado digital de un PSC.

Validez de la firma: aplicabilidad (apto para el uso previsto) y estado (activo, revocado o expirado) de un certificado.

Verificación de la firma: determinación y validación de: a) que la firma digital fue creada durante el periodo operacional de un certificado válido por la clave privada correspondiente a la clave pública que se encuentra en el certificado; b) que el mensaje no ha sido alterado desde que su firma digital fue creada.

X. 500: estándar desarrollado por la ITU que define las recomendaciones del directorio. Da lugar a la serie de recomendaciones siguientes: X.501, X.509, X.511. X.518, X.519, X.520, X.521, X.525.

X. 509: estándar desarrollado por la ITU, que define el formato electrónico básico para certificados electrónicos.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

1.6.2 ACRÓNIMOS

Tabla Nº 1 – Acrónimos

Acrónimo	Descripción
C	País (C por sus siglas en inglés, Country)
CA	Autoridad de Certificación (CA por sus siglas en inglés Certificate Authority)
CAI	Autoridad de Certificación Intermedia (Certificate Authority Intermediate)
CA Raíz	Autoridad Certificadora Raíz del Paraguay
CI	Cédula de identidad
CN	Nombre común (CN por sus siglas en inglés, Common Name)
CP	Políticas de Certificación (CP por sus siglas en inglés, certificate policy)
CPS	Declaración de Prácticas de Certificación (CPS por sus siglas en inglés, certification practice statement)
CRL	Lista de certificados revocados (CRL por sus siglas en inglés, certificate revocation list)
CSR	Solicitud de firma de Certificado (CSR por sus siglas en inglés, certificate Signing Request)
DGFDyCE	Dirección General de Firma Digital y Comercio Electrónico dependiente del Vice Ministerio de Comercio.
DNS	Servicio de nombre de dominio (DNS por sus siglas en inglés Domain Name server)

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

FIPS	Estándares Federales de Procesamiento de la Información (FIPS por sus siglas en inglés, Federal Information Processing Standards).
HSM	Módulo de seguridad criptográfico basado en Hardware (HSM por sus siglas en inglés, Hardware security module)
ISO	Organización Internacional para la Estandarización (ISO por sus siglas en inglés, International Organization for Standardization).
ITU-T	Unión Internacional de Telecomunicaciones – Sector de normalización de las telecomunicaciones (ITU-T por sus siglas en inglés Internationa,l Telecomunication Union – Telecomunication Standardization Sector)
MIC	Ministerio de Industria y Comercio
O	Organización (por su sigla en inglés, Organization)
OCSP	Servicio de validación de certificados en línea (OCSP por sus siglas en inglés, Online Certificate Status Protocol).
OID	Identificador de Objeto (OID por sus siglas en inglés, Object Identifier).
OU	Unidad Organizacional (OU por sus siglas en inglés, Organization Unit)
PIN	Número de Identificación Personal, (por sus siglas en inglés, Personal Identification Number)
PKCS	Norma de criptografía de clave pública (PKCS por sus siglas en inglés, Public Key Cryptography Standard)
PKI	Infraestructura de Clave Pública (PKI por sus siglas en inglés, Public Key Infrastructure).
PSC	Prestador de Servicios de Certificación

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

PY	Paraguay
RA	Autoridad de Registro (RA por sus siglas en inglés, Registration Authority).
RFC	Petición de Comentarios (RFC por sus siglas en inglés, Request for Comments)
RSA	Sistema criptográfico de clave pública desarrollado por Rivers, Shamir y Adleman
RUC	Registro único del contribuyente
SN	Número de Serie (por sus siglas en inglés, Serial Number)
TLS	Capa de conexión segura (TLS por sus siglas en inglés, Transport Layer Security)
UPS	Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés, uninterruptible power supply)
URL	Localizador uniforme de recursos (URL por sus siglas en inglés, Uniform Resource Locator).
VA	Autoridad de validación (VA por sus siglas en inglés, Validation Vutorithy)

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

En los apartados siguientes se deben referir a los puntos correspondientes de la CPS del PSC responsable o se deben detallar los aspectos específicos para la CP si hubiere.

2.1. REPOSITORIOS

2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN

2.4 CONTROLES DE ACESSO

3. IDENTIFICACIÓN Y AUTENTICACIÓN

En los apartados siguientes se deben referir a los puntos correspondientes de la CPS del PSC responsable o se deben detallar los aspectos específicos para la CP si hubiere.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

3.1 NOMBRES

3.1.1 TIPOS DE NOMBRES

3.1.2. NECESIDAD DE NOMBRES SIGNIFICATIVOS

3.1.3. ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES

3.1.4 REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES

3.1.5. UNICIDADE DE NOMBRES

3.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

3.2 VALIDACIÓN INICIAL DE IDENTIDAD

3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA

3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FISÍCA

3.2.4 INFORMACIÓN DEL SUSCRIPTOR NO VERIFICADA

3.2.5 VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)

3.2.6 CRITERIOS PARA INTEROPERABILIDAD

3.2.7. CRITERIOS PARA INTEROPERABILIDAD

3.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RE EMISIÓN DE CLAVES

3.3.1 IDENTIFICACIÓN Y AUTENTICACIÓN PARA RE EMISIÓN DE CLAVES

3.3.2 IDENTIFICACIÓN Y AUTENTICACIÓN PARA LA RE EMISIÓN DE CLAVES DESPUÉS DE UNA REVOCACIÓN

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

En los apartados siguientes se deben referir a los puntos correspondientes de la CPS del PSC responsable o se deben detallar los aspectos específicos para la CP si hubiere.4.1 SOLICITUD DEL CERTIFICADO

4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

4.2. PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

4.2.3. TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO

4.3 EMISIÓN DEL CERTIFICADO

4.3.1 ACCIONES DE LA CA DURANTE LA EMISIÓN DE LOS CERTIFICADOS

4.3.2 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DEL CERTIFICADO DIGITAL

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR LA CA

4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA CA A OTRAS ENTIDADES

4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL SUSCRIPTOR

4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LA PARTE QUE CONFÍA

4.6 RENOVACIÓN DEL CERTIFICADO

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO

4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN

4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO

4.6.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO

4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO

4.6.6 PUBLICACIÓN POR LA CA DEL CERTIFICADO RENOVADO

4.6.7 NOTIFICACIÓN POR LA CA DE LA EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES

4.7 RE-EMISIÓN DE CLAVES DE CERTIFICADO

4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO

4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA

4.7.3 PROCESAMIENTO DE SOLICITUDES DE RE-EMISIÓN DE CLAVES DE CERTIFICADO

4.7.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA RE-EMISIÓN DE UN NUEVO CERTIFICADO

4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE-EMITIDO

4.7.6 PUBLICACIÓN POR LA CA DE LOS CERTIFICADOS RE-EMITIDOS

4.7.7 NOTIFICACIÓN POR LA CA DE LA RE-EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES

4.8 MODIFICACIÓN DE CERTIFICADOS

4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO

4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

4.8.4 NOTIFICACIÓN AL SUSCRIPTOR DE LA EMISIÓN DE UN NUEVO CERTIFICADO

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

4.8.6 PUBLICACIÓN POR LA CA DE LOS CERTIFICADOS MODIFICADOS

4.8.7 NOTIFICACIÓN POR LA CA DE EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES

4.9 REVOCACIÓN Y SUSPENSIÓN

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

4.9.2 QUIEN PUEDE SOLICITAR REVOCACIÓN

4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

4.9.5 TIEMPO DENTRO DEL CUAL LA CA DEBE PROCESAR LA SOLICITUD DE REVOCACIÓN

4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LAS PARTES QUE CONFÍAN

4.9.7 FRECUENCIA DE EMISIÓN DEL CRL

4.9.8 LATENCIA MÁXIMA PARA CRL

4.9.9 REQUISITOS DE VERIFICACIÓN DE CRL

4.9.10 DISPONIBILIDAD DE VERIFICACIÓN DE REVOCACIÓN/ ESTADO EN LÍNEA

4.9.11 REQUERIMIENTOS PARA VERIFICAR LA REVOCACIÓN EN LÍNEA

4.9.12 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES

4.9.13 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA

4.9.14 CIRCUNSTANCIAS PARA SUSPENSIÓN

4.9.15 QUIEN PUEDE SOLICITAR LA SUSPENSIÓN

4.9.16 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

4.9.17 LÍMITES DEL PERÍODO DE SUSPENSIÓN

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

4.10 SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADO

4.10.1 CARACTERÍSTICAS OPERACIONALES

4.10.2 DISPONIBILIDAD DEL SERVICIO

4.10.3 CARACTERÍSTICAS OPCIONALES

4.11 FIN DE LA SUSCRIPCIÓN

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.2 POLÍTICAS Y PRÁCTICAS DE RECUPERACIÓN Y ENCAPSULACIÓN DE CLAVES DE SESIÓN

5 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

En los apartados siguientes se deben referir a los puntos correspondientes de la CPS del PSC responsable o se deben detallar los aspectos específicos para la CP si hubiere.

5.1 CONTROLES FÍSICOS

5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

5.1.2 ACCESO FÍSICO

5.1.2.1 NIVELES DE ACCESO FÍSICO

5.1.3 ENERGÍA Y AIRE ACONDICIONADO

5.1.4 EXPOSICIONES AL AGUA

5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

5.1.6 ALMACENAMIENTO DE MEDIOS

5.1.7 ELIMINACIÓN DE RESIDUOS

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

5. CONTROLES TÉCNICOS DE SEGURIDAD

La CP debe definir las medidas de seguridad, necesarias para proteger las claves de cifrado de los titulares de certificados emitidos bajo la CP. También se deben establecer otros controles técnicos de seguridad utilizados por el PSC y la RA a ella vinculada para la ejecución de sus funciones operativas.

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1. GENERACIÓN DEL PAR DE CLAVES

Compete a la CA Raíz el seguimiento de la evolución tecnológica y en caso necesario, actualizar las normas y los algoritmos criptográficos utilizados en la PKI-Paraguay.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Cuando el titular del certificado es una persona física, éste será responsable de generar el par de claves criptográficas. Cuando el titular del certificado es una persona jurídica, su representante (s) legal (s), será la persona responsable de la generación de pares de claves criptográficas y del uso del certificado.

En este ítem, la CP debe describir todos los requisitos y procedimientos referentes al proceso de generación de claves, aplicables al certificado que define.

El algoritmo a ser utilizado para las claves criptográficas de titulares de certificados, está definido en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

Para ser generada, la clave privada de la persona física o jurídica titular del certificado deberá ser grabada y cifrada por un algoritmo simétrico aprobado en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY,** en un medio de almacenamiento definido para cada tipo de certificado previsto por la CA raíz del Paraguay, conforme a lo estipulado en la Tabla N° 2.

La clave privada debe transportarse encriptada, utilizando los mismos algoritmos citados en el párrafo anterior, entre el dispositivo generador y el medio utilizado para su almacenamiento.

Los medios de almacenamiento de claves privadas, garantizarán, por medios técnicos y de procedimiento adecuados, como mínimo, que:

a) la clave privada es única y su confidencialidad es suficientemente asegurada;
b) la clave privada no puede, con seguridad razonable, ser deducida y debe estar protegida contra falsificaciones realizadas a través de la tecnología disponible en la actualidad; y
c) la clave privada puede ser eficazmente protegida por el legítimo titular contra su utilización por parte de terceros.

Esos medios de almacenamiento no deben modificar los datos que serán firmados ni debe impedir que esos datos sean presentados al firmante antes del proceso de firma.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Tabla N° 2 – Medio de almacenamiento de llaves criptográficas.

Tipo de certificado	Medio de almacenamiento
F1 y C1	repositorio protegido por contraseña y/o identificación biométrica, cifrado por software
F2 y C2	Hardware criptográfico homologado por la autoridad de aplicación.

6.1.2. ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR

Ítem no aplicable.

6.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

La CP debe detallar los procedimientos utilizados para la entrega de la clave pública del titular del certificado al PSC. En los casos en lo que hubiere solicitud de certificado por su titular o por una RA vinculada, deberá adoptarse el formato definido en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY**

6.1.4. ENTREGA DE LA CLAVE PÚBLICA DE LA CA A LAS PARTES QUE CONFÍAN

En este ítem, la CP debe definir las formas para la entrega del certificado del PSC y de todos los certificados de la cadena de certificación, para los usuarios de la PKI Paraguay, la cual podrá comprender, entre otras:

a) en el momento de entrega de un certificado para su titular, usando el formato definido en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY;**
b) un directorio;
c) una página WEB del PSC; y
d) Otros medios seguros aprobados por el MIC.

6.1.5. TAMAÑO DE LA CLAVE

Este ítem se debe definir el tamaño de las claves criptográficas asociadas a los certificados emitidos según la CP.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Los algoritmos y tamaños de clave a ser utilizados en los diferentes tipos de certificados de la PKI Paraguay, se definen en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

6.1.6. GENERACIÓN DE PARÁMETROS DE CLAVE ASIMETRICAS Y VERIFICACIÓN DE CALIDAD

La CP debe prever que los parámetros de generación de claves asimétricas de las entidades titulares de certificados, adoptará el estándar definido en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

Los parámetros de verificación de calidad, deberán ser verificados de acuerdo con las normas establecidas por el patrón definido en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

6.1.7. PROPÓSITOS DE USOS DE CLAVE (CAMPO KEY USAGE X509 V3)

En este ítem, la CP debe especificar los propósitos para los cuales, podrán ser utilizadas las claves criptográficas de los titulares de los certificados, así como las posibles restricciones aplicables, de conformidad con las aplicaciones definidas para los certificados correspondientes (ítem 1.3.4).

6.1.8. GENERACIÓN DE CLAVE POR HARWARE O SOFTWARE

El proceso de generación de claves criptográficas, definido por la CP, deberá ser realizado, para cada tipo de certificado previsto por la PKI Paraguay, conforme con la Tabla N° 3 a continuación:

Tabla N° 3 – Proceso de generación de claves criptográficas

Tipo de certificado	Proceso de generación de claves criptográficas
F1 yC1	Software
F2 y C2	Hardware

6.2. CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO Y PROTECCIÓN DE LA CLAVE PRIVADA

En los ítems siguientes, la CP debe definir los requisitos para la protección de las claves privadas de los titulares según la CP

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO

En este ítem, en su caso, deben ser especificados los estándares requeridos para los módulos de generación de las claves criptográficas, de conformidad con las normas establecidas en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA

Ítem no aplicable.

6.2.3 CUSTODIA/RECUPERACIÓN DE LA CLAVE PRIVADA

En este ítem, la CP debe indicar que no se permitirá, en el ámbito de la PKI Paraguay, almacenar clave privada del titular del certificado de firma digital (tipo F) emitido por el PSC.

6.2.4. RESPALDO/COPIA DE LA CLAVE PRIVADA

Con la excepción de las claves privadas vinculadas a los certificados de tipo F, que no pueden tener copia de seguridad, cualquier titular de un certificado de otro tipo puede, a su criterio, mantener una copia de su propia clave privada.

El PSC responsable por la CP no podrá mantener una copia de seguridad de la clave privada del titular del certificado de firma digital (Tipo F) por el emitido.

El PSC podrá mantener una copia de seguridad de la clave privada correspondiente al certificado de cifrado (Tipo C) por ella emitida a solicitud:

a) del Titular del certificado.
b) del Titular del certificado y empresa u organización cuándo el titular del certificado es su empleado o cliente

En cualquier caso, la copia de seguridad deberá ser almacenada cifrada por algoritmo simétrico adoptado por el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY**, y protegida con un nivel de seguridad no inferior para aquel definido para la clave original.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Además de las observaciones anteriores, la CP debe describir los requisitos y procedimientos aplicables al proceso de generación de una copia de seguridad.

6.2.5. ARCHIVADO DE LA CLAVE PRIVADA

En este ítem, en una CP que defina certificado de cifrado, deben ser descriptos, cuando sea el caso, los requisitos para el archivado de las claves privadas. Las claves deberán ser archivadas en un nivel de seguridad no inferior a aquella definida para la clave original. No deben ser archivadas las claves privadas de la firma digital.

Defínase archivado como el almacenamiento de la clave privada para su uso futuro, después del periodo de validez del certificado correspondiente.

6.2.6. TRANSFERENCIA DE CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRIPTOGRÁFICO

En este ítem de la CP, deben ser descriptos los requisitos de transferencia de la clave privada del PSC responsable de un módulo criptográfico a otro. La RFC 2510 podrá ser utilizada para ese fin.

6.2.7. ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

El PSC no podrá mantener almacenada la clave privada del titular de certificado de firma digital por ella emitida.

En este ítem, en una CP que defina certificado de cifrado, debe indicar, que el PSC podrá mantener almacenada una copia de la clave privada por ella emitida por solicitud:

a) del Titular del certificado;
b) del Titular del certificado y empresa u organización cuándo el titular del certificado es su empleado o cliente.

En cualquier caso, la clave privada deberá ser almacenada cifrada por un algoritmo simétrico definido en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

6.2.8. MÉTODO DE ACTIVACIÓN DE CLAVE PRIVADA

En este ítem de la CP, deben ser descriptos los requisitos y procedimientos necesarios para la activación de la clave privada del titular el certificado. Deben ser definidos los agentes autorizados a activar esa clave, el método de confirmación de identidad de esos agentes (contraseñas, tokens o biometría) y las acciones necesarias para la activación.

6.2.9. MÉTODOS DE DESACTIVACIÓN DE LA CLAVE PRIVADA

En este ítem de la CP, deben ser descriptos los requisitos y procedimientos necesarios para la desactivación de la clave privada del titular del certificado. Deben ser definidos los agentes autorizados a activar esa clave, el método de confirmación de identidad de esos agentes y las acciones necesarias.

6.2.10. DESTRUCCIÓN DE CLAVE PRIVADA

En este ítem de la CP, deben ser descriptos los requisitos y procedimientos necesarios para la destrucción de la clave privada del titular del certificado y de sus copias de seguridad si las hubiere. Deben ser definidos los agentes autorizados, el método de confirmación de identidad de esos agentes y las acciones necesarias, tal como la destrucción física, la sobre-escritura o la eliminación de los medios de almacenamiento.

6.2.11. CLASIFICACIÓN DEL MÓDULO CRIPTOGRÁFICO

En este ítem la CP debe indicar la capacidad del módulo criptográfico utilizado en los dispositivos. Conforme a lo que dicta el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

6.3.1. ARCHIVO DE LA CLAVE PÚBLICA

La CP debe prever que las claves públicas de los titulares de los certificados de firma digital (Tipo F), así como las CRL emitidas, serán almacenadas por el PSC emisor, después de la expiración de los certificados correspondientes, permanentemente, para la verificación de firmas generadas durante su periodo de validez.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

6.3.2. PERÍODO OPERACIONAL DEL CERTIFICADO Y PERÍODO DE USO DEL PAR DE CLAVES

En caso que la CP se refiera a certificado de firma digital, ella debe prever que las claves privadas de sus titulares, deberán ser utilizadas únicamente durante el periodo de validez correspondiente. Las correspondientes claves públicas podrán ser utilizadas durante todo el periodo de tiempo determinado por la normativa vigente, para la verificación de firmas generadas durante el plazo de validez de los respectivos certificados.

En caso que la CP se refiera a certificado de cifrado, ella debe definir los periodos de usos de las claves correspondientes.

La tabla 4 define los períodos máximos de validez admitidos para cada tipo de certificado previsto por la PKI Paraguay.

Tabla 4 – Período de validez de los certificados

Tipo de certificado	Periodo máximo de validez del certificado (en años)
F1 y C1	1
F2 y C2	2

6.4 DATOS DE ACTIVACIÓN

En los siguientes ítems de la CP, deben ser descriptos los requerimientos de seguridad referentes a los datos de activación. Los datos de activación, distintos a las claves criptográficas, son aquellos requeridos para la operación de algunos módulos criptográficos.

6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

La CP debe garantizar que los datos de activación de la clave privada del titular del certificado, si se utiliza, serán únicos y aleatorios.

6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

La CP debe garantizar que los datos de activación de la clave privada del titular del certificado, si se utiliza, serán protegidos contra el uso no autorizado.

Abog. Rocys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

En este ítem, cuando fuera el caso, deben ser definidos otros aspectos referentes a los datos de activación. Entre esos otros aspectos, pueden ser considerados algunos de aquellos tratados, en relación a las claves, en los ítems 6.1 al 6.3.

6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

La CP debe describir los requisitos de seguridad computacional del equipamiento donde será generado el par de claves criptográficas de los titulares de certificados, observando los requerimientos generales previstos en la CPS.

6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

Ítem no aplicable.

6.5.3. CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO

Ítem no aplicable.

6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

En caso que el PSC exija un software específico para la utilización de certificados emitidos según la CP, en los puntos siguientes deben ser descriptos los controles implementados en el desarrollo y la gestión de la seguridad referentes a ese software.

6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA

En este ítem de la CP, deben ser abordados aspectos tales como: seguridad del ambiente y del personal de desarrollo, prácticas de ingeniería del software adoptadas, metodología de desarrollo de software, entre otros.

6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

En este ítem, deben ser descriptos los procedimientos y las herramientas utilizadas para garantizar que el software y su ambiente operacional, implementan los niveles de seguridad apropiados.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

En este ítem, la CP debe informar, cuando esté disponible, el nivel de seguridad atribuido al ciclo de vida del software, basado en criterios tales como: *Trusted Software Development Methodology* (TSDM) ou o *Capability Maturity Model* do *Software Engineering Institute* (CMM-SEI).

6.6.4. CONTROLES EN LA GENERACIÓN DE CRL

Ítem no aplicable.

6.7 CONTROLES DE SEGURIDAD DE RED

En el caso que el ambiente de utilización del certificado, definido por la CP, exija controles específicos de seguridad de red, estos controles deben de ser descriptos en este ítem de la CP, de acuerdo a las normas, criterios, prácticas y procedimientos de la PKI Paraguay

6.7.1. DIRECTRICES GENERALES

6.7.2. FIREWALL

6.7.3. SISTEMA DE DETECIIÓN DE INTRUSO (IDS)

6.7.4. REGISTRO DE ACCESO NO AUTORIZADO A LA RED

6.8. CONTROLES DE INGENIERIA DEL MÓDULO CRIPTOGRÁFICO

En este ítem de la CP debe describirse los requisitos aplicables al módulo criptográfico utilizado para el almacenamiento de la clave privada del titular del certificado. Podrán ser indicados normas de referencia, observados en el documento NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

7. PERFILES DE CERTIFICADOS, CRL Y OCSP

En los siguientes ítems deben ser descriptos los formatos de los certificados y de la CRL según la CP. Deben ser incluidas informaciones sobre las normas adoptadas, sus perfiles, versiones y extensiones. Los requisitos mínimos establecidos en los siguientes ítems deben ser obligatoriamente considerados en todos los tipos de certificados admitidos en el ámbito de la PKI Paraguay.

7.1. PERFIL DEL CERTIFICADO

Todos los certificados emitidos por los PSC, según sus respectivas CP, deberán estar conformes al formato definido por la norma ITU X.509 o ISO/IEC 9594-8.

CERTIFICADO DE PERSONA FÍSICA

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

Tabla N° 5 – Estructura del campo subject certificado de persona física.

CAMPO	EJEMPLO	DESCRIPCIÓN
C (Country) {OID: 2.5.4.6}	PY	Este campo debe contener el codigo del país asignado de acuerdo al ISO 3166.
O (Organization) {OID: 2.5.4.10}	PERSONA FISICA	En este campo se identifica el tipo de certificado. En este caso se identifica que corresponde a un certificado de persona física y se debe indicar PERSONA FISICA, en mayúscula y sin tilde.
OU (Organization Unit) {OID: 2.5.4.11}	FIRMA F1	En este campo se indica el propósito del uso del certificado digital y el módulo (software/hardware) en el que fue almacenada la clave privada del titular del certificado. Según lo estipulado en el punto 1.1 y 1.4.1 podrán ser : • FIRMA F1 ; • FIRMA F2; • CIFRADO C1; o • CIFRADO C2.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

CN (Common Name) {OID: 2.5.4.3}	LUCAS ALCARAZ RIOS	Este campo debe contener el/los nombre y apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.
Serial Number {OID: 2.5.4.5}	CI2304024	Este campo debe contener las siglas CI, seguidas del número de cédula de Identidad del titular del certificado, según documento de identificación.
SN (Surname) {OID: 2.5.4.4}	LUCAS	Este campo debe contener el/los nombre/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.
G (GivenName) {OID:2.5.4.42	ALCARZ RIOS	Este campo debe contener el/los apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.

Descripción de los campos más relevantes del perfil de certificado de persona física:

Tabla N° 6 Estructura de los principales campos del certificado de persona física.

PRINCIPAL CERTIFICADO DE PERSONA FÌSICA		
CAMPO	EJEMPLO	DESCRIPCIÓN
Version(versión)	V3	Los certificados deben ser X.509 versión 3 (V3).
Serial number (Número de serie)	18 6f 57 dd 38 6c 47 ad 54 5d 0c 9a 22 f4 96 60	Este campo indica el número de serie del certificado digital. Valor único emitido dentro del ámbito de cada PSC.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Signature Algorithm (Algoritmo de firma)	sha256RSA	El Algoritmo de firma debe ser como mínimo SHA256RSAencryption.
signature hash algorithm (algoritmo hash de firma)	sha256	El Algoritmo de firma debe ser como mínimo SHA256.
Issuer (emisor)	CN = CA-MUESTRA S. A. O = MUESTRA S. A. C = PY SERIALNUMBER = RUC80090099-4	Este campo indica los datos de identificación del PSC que emitió el certificado.
Valid from (Válido desde)	viernes, 07 de noviembre de 2016 15:16:58	En caso de certificados tipos C2 y F2, deben ser menor o igual a 2 (dos) años de validez. En caso de certificados tipos C1 y F1, deben ser menor o igual a 1 (un) año de validez.
Valid to (Válido hasta)	lunes, 07 de noviembre de 2017 15:16:58	
Subject (sujeto)	C = PY O = PERSONA FISICA OU= FIRMA F1 CN = LUCAS ALCARAZ RIOS SERIALNUMBER = CI2304024 G = LUCAS SN = ALACRAZ RIOS	Este campo indica los datos de identificación del titular del certificado emitido por un PSC.
Subject Public Key (Clave pública del sujeto)	30 82 01 0a 02 82 01 01 00 b4 46 43 e2 4a 52 1e b4 87 bc 8c f0 a0 f9 df 1f 68 1d 08 e5 00 fe 20 6b fe 3d 2c 5b 48 ad 46 7d 22 65 03 27 10 0c 86 e1 f7 31 dd 23 37 0b ad 08 cc b9 cd 96 03 64 8e 58 c0 fb 8d f9 5e fa 26 df 07 a1 b4 81 f6 ec a5 e7 5e 50 67 61 31 97 bc 76 94 7f 3e be 28 be 0b a8 03 11 57 64 58 f2 70 da 22 b3 f2 ee 28 18 29 57 1c 59 ce 46 ec f9 4c 2d a9 89 89 65 97 b1 19 fb b1 ab 2a e1 09 65 ed 8c c6 6c 46 db 8c 3e a6 50 9d 9f ff ee 51 8c 33 5c 15 aa 6b 88	Este campo indica la clave pública del titular del certificado. Codificado de acuerdo con el RFC 5280.y con un largo de clave mínima de 2048 bits y algoritmo RSA Encryption.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

	8e 8e 7c fa af 1d 9d 48 9f 12 2d b1 98 ff b6 88 ac 09 e0 b5 f9 fc 5a b6 32 32 26 d1 00 72 95 7e d9 5b 5a d8 90 84 86 65 49 32 08 b9 a8 3e 2f 0d db bf 2c 4d 48 e0 6f 52 71 19 5f 86 32 ba dc 87 9d 5f 38 66 80 a7 a7 48 3d 9f 10 09 82 28 47 9b 00 00 cb 1c 90 a1 63 af 86 71 9e 75 24 e5 a2 63 a6 d5 e9 8b 0e 96 44 fb fa a3 f1 b5 02 03 01 fa 01	

Tabla N° 7 – Estructura de las extensiones del certificado de persona física

EXTENCIONES CERTIFICADO DE PERSONA FÌSICA			
CAMPO	EJEMPLO	DESCRIPCIÓN	CRÍTICO
Subject Key Identifier (Identificador de la clave del Sujeto)	ac dc d4 d3 cf 0c 20 ce bb 20 29 1b 93 1a 10 bb b2 36 3f a7	Este campo debe contener el hash SHA-1 de la clave pública del titular del certificado. Este Campo es usado por el software de validación para ayudar a identificar un certificado que contiene una determinada clave pública.	NO
Authority Key Identifier(Identificador de la clave de la entidad emisora)	Id. de clave=03 7c 7c 9f 6d 5a 72 a5 91 91 b4 db ec 91 fb 03 5f 7c 7c 9d	El campo key identifier debe contener el hash SHA-1 de la clave pública del PSC emisor del certificado. Este campo es usado por los diversos software de validación para ayudar a identificar a la autoridad certificadora que emitió el certificado en la cadena de Confianza.	NO

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Authority Information Access(Acceso a información de la entidad emisora)	[1]Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://www.muestra.com.py/crt/archivo.crt [2]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://www.muestra.com.py/oscp	Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado del PSC. Además, para indicar la dirección donde puede accederse al servicio de OCSP, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no. La primera entrada debe contener el método de acceso i d-ad-calssuer, utilizando uno de los siguientes protocolos de acceso: HTTPS o LDAP, para la recuperación de la cadena de certificación. La segunda entrada puede contener el método de acceso id-ad-ocsp con el respectivo respondedor OCSP utilizando uno de los siguientes protocolos de acceso HTTPS o LDAP.	NO

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

CRL Distribution Points (Puntos de distribución de CRL)	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://www.muestra.com.py/crl/archivo.crl	Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no.	NO
Key Usage(Uso de la clave)	Sin repudio, Firma digital, Cifrado de clave.	En certificados tipo F1 o F2 I solamente pueden ser activados los siguientes bits: • **digitalSignature;** • **NonRepudiation** (renombrado recientemente con el nombre de **contentCommitmen**); y • **keyEncipherment** En certificados tipo C1 o C2 solamente pueden ser activados los siguientes bits: • **keyEncipherment;** y • **dataEncipherment.**	SI
Extended Key Usage (uso extendido de la clave)	Correo seguro (1.3.6.1.5.5.7.3.4)	Referencia otros propósitos de la clave, adicionales al uso y debe ser consistente con la extensión **keyUsage**	SI

Abog. Rocxs Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Subject Altenative Name (nombre alternativo del sujeto)	Rfc822Name=lucasalacraz@hmail.com DirectoryName O= BLANCO S. A. OU= AREA TECNICA SerialNumber=RUC80090099-4 T= DIRECTOR TECNICO	Campo no obligatorio. Los datos a incluir en esta extensión deben ser representados mediante la utilización de los siguientes campos: • **Rfc822Name=** [*email del titular del certificado*] • **DirectoryName= 2.5.4.10:**[*nombre de la organización en el que presta servicio el titular del certificado*] • **DirectoryName= 2.5.4.11:**[*nombre de la unidad de la organización en el que presta servicio el titular del certificado*] • **DirectoryName =2.5.4.5: RUC** [*número de cédula tributaria correspondiente a la organización en el que presta servicio el titular del certificado*] • **DirectoryName= 2.5.4.1:** [*Cargo o Titulo del titular del certificado]* Los otros campos que compone la extensión "Subject Alternative Name" podrán ser	NO

Abog. Raddys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

		utilizados en la forma y con los propósitos definidos por la RFC 5280, siempre y cuanto estén aprobados por la CA Raíz.	
Certificate Policies (Política del certificado)	[1]Directiva de certificados: Identificador de directiva= [OID CP del PSC]. [1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.muestra.com.py/repositorio [1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=[Texto de aviso en español] [1,3]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso==[Texto de aviso en ingles]	Debe contener el OID de la CP correspondiente y la dirección WEB de la CPS del PSC que emite el certificado.	NO

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

CERTIFICADO DE PERSONA JURÍDICA

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

Tabla N° 8 - – Estructura del campo subject certificado de persona jurídica.

CAMPO	EJEMPLO	DESCRIPCIÓN
C (Country) {OID: 2.5.4.6}	PY	Este campo debe contener el condigo del país asignado de acuerdo al ISO 3166.
O (Organization) {OID: 2.5.4.10}	PERSONA JURIDICA	En este campo se identifica el tipo de certificado. En este caso se identifica que corresponde a un certificado de persona física y debe ser PERSONA JURIDICA en mayúscula y sin tilde.
OU (Organization Unit) {OID: 2.5.4.11}	FIRMA F2	En este campo se indica el propósito del uso del certificado digital y el módulo (software/hardware) en el que fue almacenada la clave privada del titular del certificado. Según lo estipulado en el punto 1.1 y 1.4.1 podrán ser : • FIRMA F1; • FIRMA F2; • CIFRADO C1; o • CIFRADO C2.
CN (Common Name) {OID: 2.5.4.3}	YASY S. A.	Este campo debe contener las siglas RUC seguido del número de cédula tributaria correspondiente al titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.
Serial Number {OID: 2.5.4.5}	RUC80070078-2	Este campo debe contener las siglas RUC, seguidas del número de cédula tributaria, según el documento de identificación.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Descripción de los campos más relevantes del perfil de certificado de persona jurídica:

Tabla N° 9 – Estructura de los principales campos del certificado de persona jurídica

PRINCIPAL CERTIFICADO DE PERSONA JURÍDICA		
CAMPO	EJEMPLO	DESCRIPCIÓN
Version(versión)	V3	Los certificados deben ser X.509 versión 3 (V3).
Serial number (Número de serie)	6f 18 6f 57 dd 38 47 6c ad 5d 54 0c 9a 22 f4 60 96	Este campo indica el número de serie del certificado digital. Valor único emitido dentro del ámbito de cada CA.
Signature Algorithm (Algoritmo de firma)	sha256RSA	El Algoritmo de firma debe ser como mínimo SHA256RSAencryption.
signature hash algorithm (algoritmo hash de firma)	sha256	El Algoritmo de firma debe ser como mínimo SHA256.
Issuer (emisor)	CN = CA-MUESTRA S. A. O = MUESTRA S. A. C = PY SERIALNUMBER = RUC80090099-4	Este campo indica los datos de identificación del PSC que emitió el certificado.
Valid from (Válido desde)	viernes, 10 de noviembre de 2016 13:17:59	En caso de certificados tipos C2 y F2, debe ser menor o igual a 2 (dos) años de validez. En caso de certificados tipos C1 y F1, debe ser menor o igual a 1 (un) año de validez.
Valid to (Válido hasta)	lunes, 10 de noviembre de 2018 13:17:59	
Subject (sujeto)	C = PY O = PERSONA FISICA OU= FIRMA F1 CN = YASY S. A. SERIALNUMBER = RUC80070078-2	Este campo indica los datos de identificación del titular del certificado emitido por un PSC.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Subject Public Key (Clave pública del sujeto)	30 82 01 0a 02 82 01 01 00 b4 46 43 e2 4a 52 1e b4 87 bc 8c f0 a0 f9 df 1f 68 1d 08 e5 00 fe 20 6b fe 3d 2c 5b 48 ad 46 7d 22 65 03 27 10 0c 86 e1 f7 31 dd 23 37 0b ad 08 cc b9 cd 96 03 64 8e 58 c0 fb 8d f9 5e fa 26 df 07 a1 b4 81 f6 ec a5 e7 5e 50 67 61 31 97 bc 76 94 7f 3e be 28 be 0b a8 03 11 57 64 58 f2 70 da 22 b3 f2 ee 28 18 29 57 1c 59 ce 46 ec f9 4c 2d a9 89 89 65 97 b1 19 fb b1 ab 2a e1 09 65 ed 8c c6 6c 46 db 8c 3e a6 50 9d 9f ff ee 51 8c 33 5c 15 aa 6b 88 8e 8e 7c fa af 1d 9d 48 9f 12 2d b1 98 ff b6 88 ac 09 e0 b5 f9 fc 5a b6 32 32 26 d1 00 72 95 7e d9 5b 5a d8 90 84 86 65 49 32 08 b9 a8 3e 2f 0d db bf 2c 4d 48 e0 6f 52 71 19 5f 86 32 ba dc 87 9d 5f 38 66 80 a7 a7 48 3d 9f 10 09 82 28 47 9b 00 00 cb 1c 90 a1 63 af 86 71 9e 75 24 e5 a2 63 a6 d5 e9 8b 0e 96 44 fb fa a3 f1 b5 02 03 01 fa 01	Este campo indica la clave pública del titular del certificado. Codificado de acuerdo con el RFC 5280.y con un largo de clave mínima de 2048 bits y algoritmo RSA Encryption.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Tabla N° 10 – Estructura de las extensiones del certificado de persona jurídica

EXTENCIONES CERTIFICADO DE PERSONA JURÍDICA			
CAMPO	EJEMPLO	DESCRIPCIÓN	CRÍTICO
Subject Key Identifier (Identificador de la clave del Sujeto)	ac dc d4 d3 cf 0c 20 ce bb 20 29 1b 93 1a 10 bb b2 36 3f a7	Este campo debe contener el hash SHA-1 de la clave pública del titular del certificado. Este Campo es usado por el software de validación para ayudar a identificar un certificado que contiene una determinada clave pública.	NO
Authority Key Identifier(Identificador de la clave de la entidad emisora)	Id. de clave=03 7c 7c 9f 6d 5a 72 a5 91 91 b4 db ec 91 fb 03 5f 7c 7c 9d	El campo key identifier debe contener el hash SHA-1 de la clave pública del PSC emisor del certificado. Este campo es usado por los diversos software de validación para ayudar a identificar a la autoridad certificadora que emitió el certificado en la cadena de Confianza.	NO
Authority Information Access(Acceso a información de la entidad emisora)	[1]Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección	Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado de la CA. Además, para indicar la dirección donde puede	NO

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

	URL=http://www.muestra.com.py/crt/archivo.crt [2]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://www.muestra.com.py/oscp	accederse al servicio de OCSP, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no. La primera entrada debe contener el método de acceso i d-ad-calssuer, utilizando uno de los siguientes protocolos de acceso: HTTPS o LDAP, para la recuperación de la cadena de certificación. La segunda entrada puede contener el método de acceso id-ad-ocsp con el respectivo respondedor OCSP utilizando uno de los siguientes protocolos de acceso HTTPS o LDAP.	
CRL Distribution Points (Puntos de distribución de CRL)	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://www.muestra.com.py/crl/archivo.crl	Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado, de tal forma que se pueda validar si el certificado en	NO

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

		cuestión ha sido revocado o no.	
Key Usage(Uso de la clave)	Sin repudio, Firma digital, Cifrado de clave.	En certificados tipo F1 o F2 I solamente pueden ser activados los siguientes bits: • **digitalSignature;** • **NonRepudiation** (renombrado recientemente con el nombre de **contentCommitmen**); y • **keyEnciphermen t** En certificados tipo C1 o C2 solamente pueden ser activados los siguientes bits: • **keyEnciphermen t;** y • **dataEncipherme nt.**	SI
Extended Key Usage (uso extendido de la clave)	Correo seguro (1.3.6.1.5.5.7.3.4)	Referencia otros propósitos de la clave, adicionales al uso y debe ser consistente con la extensión **keyUsage**	SI
Subject Alternate Names (nombre alternativo del sujeto)	**Rfc822Name=** yasysa@yasy.com.py **DirectoryName** CN=PIERINA OJEDA SerialNumber: CI3452365 T=REPRESENTANTE LEGAL	Los datos a incluir en la extensión deben ser representados mediante la utilización de los siguientes campos: **no obligatorio:** • **Rfc822Name** =[*email del titular del certificado*]	NO

Abog. Rodolfo Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

		• DirectoryName= 2.5.4.12: [*cargo que ocupa en la organización el responsable del certificado*] obligatorio: • DirectoryName= 2.5.4.3: [*nombre y apellido del responsable del certificado*] • DirectoryName= 2.5.4.5: CI [*número de cédula de identidad correspondiente al responsable del certificado*] Los otros campos que compone la extensión"Subject Alternative Name" podrán ser utilizados en la forma y con los propósitos definidos por la RFC 5280, siempre y cuanto estén aprobados por la CA Raíz.	
Certificate Policies (Política del certificado)	[1]Directiva de certificados: Identificador de directiva= [OID CP del PSC]. [1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador:	Debe contener el OID de la CP correspondiente y la dirección WEB de la CPS del PSC que emite el certificado.	NO

Abog. Rolys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

	http://www.muestra.com.py/repositorio [1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=[Texto de aviso en español] [1,3]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso==[Texto de aviso en ingles]		

CERTIFICADO DE MÁQUINA O APLICACIÓN

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

Tabla N° 11 – Estructura del campo subject de certificado de máquina o aplicación.

CAMPO	EJEMPLO	DESCRIPCIÓN
C (Country) {OID: 2.5.4.6}	PY	Este campo debe contener el condigo del país asignado de acuerdo al ISO 3166.
O (Organization) {OID: 2.5.4.10}	APLICACION	En este campo se identifica el tipo de certificado. En este caso se identifica que corresponde a un certificado de maquina o aplicación y puede ser MAQUINA O APLICACIÓN en mayúscula y sin tilde.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

OU (Organization Unit) {OID: 2.5.4.11}	FIRMA F1	En este campo se indica el propósito del uso del certificado digital y el módulo (software/hardware) en el que fue almacenada la clave privada del titular del certificado. Según lo estipulado en el punto 1.1 y 1.4.1 podrán ser : • FIRMA F1; • FIRMA F2; • CIFRADO C1; o • CIFRADO C2.
CN (Common Name) {OID: 2.5.4.3}	KEYTWO	Este campo debe contener la URL correspondiente o el nombre de la aplicación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.
Serial Number {OID: 2.5.4.5}	MCI4543456	Este campo debe contener según sea el titular: **Persona Física:** • las siglas MCI, seguidas del número de cédula de Identidad del titular del certificado, según documento de identificación. **Persona Jurídica:** • siglas MRUC, seguidas del número de cédula tributaria, según el documento de identificación.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Descripción de los campos más relevantes del perfil de certificado de maquina o aplicación:

Tabla N° 12 Estructura de los principales campos del certificado de máquina o aplicación

PRINCIPAL CERTIFICADO DE MÁQUINA O APLICACIÓN		
CAMPO	EJEMPLO	DESCRIPCIÓN
Version(versión)	V3	Los certificados deben ser X.509 versión 3 (V3).
Serial number (Número de serie)	18 dd 6f 57 38 6c 47 ad 9a 5d 0c 59 22 f4 60 96	Este campo indica el número de serie del certificado digital. Valor único emitido dentro del ámbito de cada CA.
Signature Algorithm (Algoritmo de firma)	sha256RSA	El Algoritmo de firma debe ser como mínimo SHA256RSAencryption.
signature hash algorithm (algoritmo hash de firma)	sha256	El Algoritmo de firma debe ser como mínimo SHA256.
Issuer (emisor)	CN = CA-MUESTRA S. A. O = MUESTRA S. A. C = PY SERIALNUMBER = RUC80090099-4	Este campo indica los datos de identificación del PSC que emitió el certificado.
Valid from (Válido desde)	viernes, 11 de noviembre de 2016 19:16:57	En caso de certificados tipos C2 y F2, debe ser menor o igual a 2 (dos) años de validez. En caso de certificados tipos C1 y F1, debe ser menor o igual a 1 (un) año de validez.
Valid to (Válido hasta)	lunes, 11 de noviembre de 2017 19:16:57	
Subject (sujeto)	C = PY O = APLICACION OU= FIRMA F1 CN = KEYTWO SERIALNUMBER = RUC80070078-2	Este campo indica los datos de identificación del titular del certificado emitido por un PSC.

Abog. Roalys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Subject Public Key (Clave pública del sujeto)	30 82 01 0a 02 82 01 01 00 b4 46 43 e2 4a 52 1e b4 87 bc 8c f0 a0 f9 df 1f 68 1d 08 e5 00 fe 20 6b fe 3d 2c 5b 48 ad 46 7d 22 65 03 27 10 0c 86 e1 f7 31 dd 23 37 0b ad 08 cc b9 cd 96 03 64 8e 58 c0 fb 8d f9 5e fa 26 df 07 a1 b4 81 f6 ec a5 e7 5e 50 67 61 31 97 bc 76 94 7f 3e be 28 be 0b a8 03 11 57 64 58 f2 70 da 22 b3 f2 ee 28 18 29 57 1c 59 ce 46 ec f9 4c 2d a9 89 89 65 97 b1 19 fb b1 ab 2a e1 09 65 ed 8c c6 6c 46 db 8c 3e a6 50 9d 9f ff ee 51 8c 33 5c 15 aa 6b 88 8e 8e 7c fa af 1d 9d 48 9f 12 2d b1 98 ff b6 88 ac 09 e0 b5 f9 fc 5a b6 32 32 26 d1 00 72 95 7e d9 5b 5a d8 90 84 86 65 49 32 08 b9 a8 3e 2f 0d db bf 2c 4d 48 e0 6f 52 71 19 5f 86 32 ba dc 87 9d 5f 38 66 80 a7 a7 48 3d 9f 10 09 82 28 47 9b 00 00 cb 1c 90 a1 63 af 86 71 9e 75 24 a2 e5 63 a6 d5 e9 8b 0e 96 44 fb fa a3 f1 b5 02 03 01 01 fa	Este campo indica la clave pública del titular del certificado. Codificado de acuerdo con el RFC 5280.y con un largo de clave mínima de 2048 bits y algoritmo RSA Encryption.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Tabla N° 13 – Estructura de las extensiones del certificado de máquina o aplicación

EXTENCIONES CERTIFICADO DE MÁQUINA O APLICACIÓN			
CAMPO	EJEMPLO	DESCRIPCIÓN	CRÍTICO
Subject Key Identifier (Identificador de la clave del Sujeto)	ac dc d4 d3 cf 0c 36 20 bb 20 29 1b 93 1a 10 bb b2 3f a7 ce	Este campo debe contener el hash SHA-1 de la clave pública del titular del certificado. Este Campo es usado por el software de validación para ayudar a identificar un certificado que contiene una determinada clave pública.	NO
Authority Key Identifier(Identificador de la clave de la entidad emisora)	Id. de clave=03 7c 7c 9f 5a 72 a5 91 91 b4 db ec 91 fb 5f 7c 7c 9d 03 6d	El campo key identifier debe contener el hash SHA-1 de la clave pública del PSC emisor del certificado. Este campo es usado por los diversos software de validación para ayudar a identificar a la autoridad certificadora que emitió el certificado en la cadena de Confianza.	NO
Authority Information Access(Acceso a información de la entidad emisora)	[1]Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://www.muestra.com.py/crt/archivo.crt [2]Acceso a información de autoridad	Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado de la CA. Además, para indicar la dirección donde puede accederse al servicio de OCSP, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no.	NO

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

	Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://www.muestra.com.py/oscp	La primera entrada debe contener el método de acceso i d-ad-calssuer, utilizando uno de los siguientes protocolos de acceso: HTTPS o LDAP, para la recuperación de la cadena de certificación. La segunda entrada puede contener el método de acceso id-ad-ocsp con el respectivo respondedor OCSP utilizando uno de los siguientes protocolos de acceso HTTPS o LDAP.	
CRL Distribution Points (Puntos de distribución de CRL)	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://www.muestra.com.py/crl/archivo.crl	Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no.	NO
Key Usage(Uso de la clave)	Sin repudio, Firma digital, Cifrado de clave.	En certificados tipo F1 o F2 l solamente pueden ser activados los siguientes bits: • **digitalSignature;** • **NonRepudiation** (renombrado recientemente con el nombre de **contentCommitmen**) ; y	SI

Abog. Rodolfo Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

		• keyEncipherment En certificados tipo C1 o C2 solamente pueden ser activados los siguientes bits: • keyEncipherment; y • dataEncipherment.	
Extended Key Usage (uso extendido de la clave)	Correo seguro (1.3.6.1.5.5.7.3.4)	Referencia otros propósitos de la clave, adicionales al uso y debe ser consistente con la extensión keyUsage	SI
Subject Alternate Names (nombre alternativo del sujeto)	Rfc822Name=yasysa@yasy.com.py DirectoryName O=YASY S. A. CN=PIERINA OJEDA SERIALNUMBER=CI3452365 T=REPRESENTANTE LEGAL	Los datos a incluir en la extensión deben ser representados mediante la utilización de los siguientes campos: no obligatorio • Rfc822Name= [*email del responsable del certificado*] Este campo debe contener según sea el titular: Persona Física: obligatorio • DirectoryName =2.5.4.3: [*nombre y apellido del responsable del certificado*] Persona Jurídica obligatorio • DirectoryName=2.5.4.10:[*nombre de la organización titular del certificado*]	NO

Abog. Rodys Roión A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

		• DirectoryName =2.5.4.3: [*nombre y apellido del responsable del certificado*] • DirectoryName =2.5.4.5: CI [*número de cédula de identidad correspondiente al responsable del certificado*] no obligatorio • DirectoryName= 2.5.4.12: [*cargo que ocupa en la organización el responsable del certificado*] Los otros campos que compone la extensión "Subject Alternative Name" podrán ser utilizados en la forma y con los propósitos definidos por la RFC 5280 siempre y cuanto estén aprobados por la CA Raíz.	

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Certificate Policies (Política del certificado)	[1]Directiva de certificados: Identificador de directiva= [OID CP del PSC]. [1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.muestra.com.py/repositorio [1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=[Texto de aviso en español] [1,3]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso==[Texto de aviso en ingles]	Debe contener el OID de la CP correspondiente y la dirección WEB de la CPS del PSC que emite el certificado.	NO

7.1.1. NÚMERO DE VERSIÓN

Todos los certificados emitidos por el PSC, según sus respectivas CP, deberán implementar la versión 3 (tres) del certificado definido en la norma ITU X.509 de acuerdo al perfil establecido en la RFC 5280.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

7.1.2. EXTENSIONES DEL CERTIFICADO

Las extensiones utilizadas de forma genérica en los certificados son:

- **KeyUsage.** Calificada como crítica;
- **ExtendedKeyUsage.** Calificada como crítica;
- **CertificatePolicies.** Calificada como no crítica;
- **SubjectAlternativeName.** Calificada como no crítica;
- Authority Information Access Calificada como no crítica. y
- CRLDistributionPoint. Calificada como no crítica.

El contenido de las extensiones más significativas de los certificados emitidos 7.1

7.1.3. IDENTIFICADORES DE OBJETO DE ALGORÍTMOS

En este ítem de la CP debe ser indicado el OID (Object Identifier) del algoritmo criptográfico utilizado para la firma de certificado. De acuerdo al algoritmo admitido en el ámbito de la PKI Paraguay, conforme a lo estipulado en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

7.1.4. FORMAS DEL NOMBRE

Los nombres del titular del certificado, que consta en el campo *"Subject"* y el número de identificación, que consta el campo "Serial Number", deberán adoptar el *"Distinguished Name"* (DN) del estándar ITU X.500/ISO 9594.

7.1.5. RESTRICCIONES DEL NOMBRE

En este ítem de la CPS, deben ser descriptas las retenciones aplicables para los nombres de los titulares de certificados.

La PKI Paraguay, establece que los nombres deberán ser escritos en mayúsculas.

El código de país es de dos caracteres y se asigna de acuerdo al estándar ISO 3166-1"Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países".

7.1.6. IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO

En este ítem debe ser informado el OID atribuido a la CP. Todo certificado emitido según la CP deberá tener en la extensión "Certificate Policies", el OID correspondiente.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

7.1.7. USO DE LA EXTENSIÓN RESTRICCIONES DE POLÍTICA (POLICY CONSTRAINTS)

Este Ítem no aplica.

7.1.8. SEMÁNTICA Y SINTAXIS DE LOS CALIFICADORES DE POLÍTICA (POLICY QUALIFIERS)

En los certificados emitidos según la CP el campo policyQualifiers de la extensión "Certificate Policies" debe contener la dirección Web (URL) de la CPS del PSC responsable.

7.1.9. SEMÁNTICA DE PROCESAMIENTO PARA LA EXTENSIÓN DE POLÍTICAS DE CERTIFICADO (CERTIFICATE POLICIES)

Extensiones críticas deben ser interpretadas conforme a la RFC 5280.

7.2. PERFIL DE LA CRL

7.2.1 NÚMERO (S) DE VERSIÓN

Las CRL generadas por el PSC responsable según la CP deberán implementar la versión 2 del CRL definido en el estándar ITU X.509, de acuerdo con el perfil establecido en el RFC 5280.

7.2.2 CRL Y EXTENSIONES DE ENTRADAS DE CRL

En este ítem, la CP debe describir todas las extensiones de CRL utilizadas y su criticidad.

La PKI Paraguay define como obligatorias las siguientes extensiones de CRL:

a) **"Authority Key Identifier", no critica**: debe contener el hash SHA-1 de clave pública de la PSC que firma la CRL; y
b) **"CRL number" no critica**: debe contener el número secuencial para cada CRL emitida.

7.3 PERFIL DE OCSP

No aplica.

7.3.1 NÚMERO (S) DE VERSIÓN

No aplica.

7.3.2 EXTENSIONES DE OCSP

No aplica.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

En los apartados siguientes se deben referir a los puntos correspondientes de la CPS de del PSC responsable o se debe detallar los aspectos específicos para la CP si hubiere

8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

8.2 IDENTIFICACIÓN/CALIFICACIÓN DEL EVALUADOR

8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA

8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN

8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA.

8.6 COMUNICACIÓN DE RESULTADOS

9. OTROS ASUNTOS LEGALES Y COMERCIALES

En los apartados siguientes se deben referir a los puntos correspondientes de la CPS del PSC responsable o se debe detallar los aspectos específicos para la CP si hubiere.

9.1 TARIFAS

9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

9.1.2 TARIFAS DE ACCESO A CERTIFICADOS

9.1.3 TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN

9.1.4 TARIFAS POR OTROS SERVICIOS

9.1.5 POLÍTICAS DE REEMBOLSO

9.2 RESPONSABILIDAD FINANCIERA

9.2.1 COBERTURA DE SEGURO

9.2.2 OTROS ACTIVOS

9.2.3 COBERTURA DE SEGURO O GARANTÍA PARA USUARIOS FINALES

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

9.3.2 INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL

9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL

9.4.1 PLAN DE PRIVACIDAD

9.4.2 INFORMACIÓN TRATADA COMO PRIVADA

9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

9.4.6 DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO

9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

9.5 DERECHO DE PROPIEDAD INTELECTUAL

9.6 REPRESENTACIONES Y GARANTÍAS

9.6.1 REPRESENTACIONES Y GARANTÍAS DE LA CA

9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA RA

9.6.3 REPRESENTACIONES Y GARANTÍAS DEL SUSCRIPTOR

9.6.4 REPRESENTACIONES Y GARANTÍAS DE LAS PARTES QUE CONFÍAN

9.6.5 REPRESENTACIONES Y GARANTÍAS DEL REPOSITORIO

9.6.6 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES

9.7 EXENCIÓN DE GARANTÍA

9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL

9.9 INDEMNIZACIONES

9.10 PLAZO Y FINALIZACIÓN

9.10.1 PLAZO

9.10.2 FINALIZACIÓN

Abog. Rocys Roión A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

9.10.3. EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

9.11. NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

9.12. ENMIENDAS

9.12.1. PROCEDIMIENTOS PARA ENMIENDAS

9.12.2. PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

9.12.3. CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

9.13 DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

9.14 NORMATIVA APLICABLE

9.15 ADECUACIÓN A LA LEY APLICABLE

9.16 DISPOSICIONES VARIAS

9.16.1 ACUERDO COMPLETO

9.16.2 ASIGNACIÓN

9.16.3 DIVISIBILIDAD

9.16.4 APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DE DERECHOS)

9.16.5 FUERZA MAYOR

9.17 OTRAS DISPOSICIONES

10. DOCUMENTOS DE REFERENCIA

Los siguientes documentos referenciados son aplicados para la confección de las políticas de certificación.

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- RFC 3739 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile.
- RFC2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".
- RFC 3647: "Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework".
- ISO 3166 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países.
- Ley Nro. 4017/2010 ''De validez jurídica de la firma electrónica, la firma digital, mensaje de datos y el expediente electrónico''

Abog. Rocio Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

ANEXO 1

Tabla Comparativa de requisitos mínimos por tipo de certificado.

Tabla Nº 14 – Tabla comparativa de requisitos mínimos por tipo de certificado.

Tipo de certificado	Clave criptográfica			Validez máxima del certificado (años)	Frecuencia de emisión del CRL (horas)	Tiempo límite de revocación (horas)
	Tamaño (bits)	Proceso de generación	Medio de almacenamiento			
F1 y C1	RSA 2048	Software	1. Repositorio protegido por contraseña y/o identificación biométrica, cifrado por software. 2. Tarjeta inteligente o token, ambos sin capacidad de generación de clave y protegido por contraseña y/o identificación biométrica.	1	12	12
F2 y C2	RSA 2048, 4096	Hardware	1. Tarjeta inteligente, HSM o token, con capacidad de generación de clave y protegidos por contraseña y/o identificación biométrica y homologado por la autoridad de aplicación.	2	12	12

Abog. Rodys Roión A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

GUSTAVO ANIBAL TOLEDO IRRAZABAL FIRMA

Firmado digitalmente por GUSTAVO ANIBAL TOLEDO IRRAZABAL FIRMA
Fecha: 2016.11.17 14:47:49 -03'00'