code100 S.A.
SERVICIOS DE CERTIFICACION DIGITAL

# POLÍTICA DE CERTIFICACIÓN F1

## VERSIÓN 1.2

**CLASE: PÚBLICO**

# CONTROL DOCUMENTAL

| **Documento** | |
|---|---|
| **Título: POLÍTICA DE CERTIFICACIÓN F1** | **Nombre del Archivo:** CODE100.Politica de Certificacion F1 v1.2.docx |
| **Código: CODE100 Politica de Certificacion F1 v1.2** | **Soporte Lógico:** Https://www.code100.com.py/firma-digital/index.php |
| **Fecha:** 28/08/2018 | **Ubicación Física:** CODE100 S.A |
| **Versión:** 1.2 | |

| **Registro de cambios** | | |
|---|---|---|
| Versión | Fecha | Motivo de cambio |
| Versión 1.0 | 07/02/2017 | Adecuación Resoluciones N° 1400 y 1401/2016 del MIC |
| Versión 1.0.1 | 05/06/2017 | Revisión de documento |
| Versión 1.1 | 05/02/2018 | Adecuación a observaciones de Auditoría |
| Version 1.2 | 28/08/2018 | Adecuación a observaciones de Auditoría |

| **Distribución del Documento** | |
|---|---|
| Nombre | Área |
| Ministerio de Industria y Comercio (MIC) | Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE) |
| CODE100 S.A. | Directorio CODE100 |
| Documento Público | www.code100.com.py |

| **Control del Documento** | | |
|---|---|---|
| Preparado por: | Revisado por: | Aceptado por: |
| | | |
| Alfredo de Alzaá | Manuel Riera | Director CODE100 |
| Pablo Casal | Aníbal Pardini | Director CODE100 |
| Pablo Casal | Aníbal Pardini | Director CODE100 |
| Pablo Casal | Manuel Riera | Director CODE100 |

## INDICE

# 1. INTRODUCCIÓN

## 1.1. DESCRIPCIÓN GENERAL

CODE100 S.A. en su calidad de Prestador de Servicios de Certificación (en adelante "PSC") brinda los servicios de certificación digital según lo establecido por la Ley Nro. 4017/10, Nro. 4610/12, Decreto Reglamentario Nro. 7369/11.

Dichas normativas establecen la validez jurídica de la Firma Electrónica, la Firma Digital, los mensajes de datos y el expediente electrónico y regula la utilización de estas herramientas, así como el funcionamiento de las Prestadoras de Servicios de Certificación, sus requisitos y obligaciones.
El Ministerio de Industria y Comercio como ente regulador debe:

- Administrar la Autoridad Certificación Raíz del Paraguay.
- Dictar las normas que regulen el Servicio de Certificación Digital en el País.
- Habilitar a los Prestadores de Servicios de Certificación.
- Auditar a los Prestadores de Servicios de Certificación.
- Revocar la habilitación de los Prestadores de Servicios de Certificación.
- Imponer sanciones a los Prestadores de Servicio de Certificación.

El Ministerio de Industria y Comercio tiene entre sus cometidos la administración de la Autoridad Certificadora Raíz del Paraguay. Dicha Autoridad Certificadora es la raíz de toda la Jerarquía de PKI, cuenta con un certificado autoafirmado y aceptado por los terceros que establezcan confianza en la PKI del Paraguay.

El Ministerio de Industria y Comercio como AA de la normativa vigente habilita la operación de los Prestadores de Servicios de Certificación (PSC) en la República del Paraguay, de esta manera los PSC habilitados pasan a ser parte de la cadena de confianza de la Infraestructura de Clave Pública del Paraguay.

El presente documento es la **Política de Certificación F1 de CODE100 S. A**. (en adelante "CP") con habilitación otorgada por el Ministerio Industria y Comercio (MIC), en su carácter de Autoridad de Aplicación de la Infraestructura de Clave Pública del Paraguay, aprobada por el Directorio y personal autorizado de CODE100 S.A., acorde a la CP de la Infraestructura de Clave Pública del Paraguay.

Esta CP es aplicable a:

- Prestador de Servicios de Certificación (PSC).
- Usuario Final.
- Parte que confía.

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.

Los tipos de certificados asociados a la presente Política son F1 y C1.

## 1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

| | |
|---|---|
| Nombre: | Política de Certificación F1 de CODE100 S.A. |
| Versión: | 1.2 |
| Fecha de aprobación: | 28/08/2018 |
| Ubicación de la CP: | http://www.code100.com.py/firma-digital/CODE100%20Politica%20de%20Certificacion%20F1%20v1.0.pdf |
| CPS relacionada: | Declaración de Prácticas de Certificación de CODE100 S.A. v3.0 |
| Lugar: | República del Paraguay |
| Tipos de certificados asociados | F1 y C1. |

## 1.3. PARTICIPANTES DE LA PKI

### 1.3.1. AUTORIDADES CERTIFICADORAS (CA)

Estipulado en la CPS de CODE100 S.A.

### 1.3.2. AUTORIDADES DE REGISTROS (RA)

Estipulado en la CPS de CODE100 S.A.

### 1.3.3. PRESTADORES DE SERVICIOS DE SOPORTE (PSS)

Estipulado en la CPS de CODE100 S.A.

### 1.3.4. SUSCRIPTORES

Estipulado en la CPS de CODE100 S.A.

### 1.3.5. PARTE QUE CONFÍA

Estipulado en la CPS de CODE100 S.A.

### 1.3.6. OTROS PARTICIPANTES

Sin estipulaciones.

## 1.4 USO DEL CERTIFICADO

### 1.4.1 USOS APROPIADOS DEL CERTIFICADO

Certificados del tipo F1 serán utilizados en aplicaciones como confirmación de identidad y firma de documentos electrónicos con verificación de integridad de sus informaciones.

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

Deben cumplir los siguientes estándares de hardware, algoritmos y parámetros criptográficos que serán utilizados en todos los procesos realizados en el ámbito de la Infraestructura de Claves Públicas del Paraguay (PKI Paraguay):

| **Generación de las Claves Asimétricas de Usuarios Finales** | |
|---|---|
| Normativa PKI Paraguay | DOC-PKI-04- ítem 6.1.5 |
| Algoritmo | RSA conforme al RFC 5639 |
| Tamaño de clave F1 o C1 | RSA 2048 0 4096 |

| **Utilización** | **Requisito obligatorio** | **Estándares** | **Norma** |
|---|---|---|---|
| Módulo criptográfico de generación de claves asimétricas para usuario final | Homologado por el MIC | FIPS 140-1 o FIPS 140-2 nivel 2 (para certificados tipo F1 o C1). | DOC-PKI-03 item 6.2.1<br>DOC-PKI-04 Ítem 6.2.1 |
| Módulo criptográfico para almacenamiento de la clave privada del titular del certificado | Homologado por el MIC | FIPS 140-1 o FIPS 140-2 (para certificados tipo F1 o C1). | DOC-PKI-04 ítem 6.8 |
| Parámetro de generación de claves asimétricas de usuario final | Homologado por el MIC | FIPS 140-1 o FIPS 140-2 (para certificados tipo F1 o C1). | DOC- PKI -04 ítem 6.1.6 |

Para determinar si es posible utilizar un certificado de firma digital del tipo F1 es necesario comprobar el valor de la extensión **'Key Usage'** del certificado en cuestión. Este campo deberá contener los siguientes datos:

| **Tipo** | **Descripción de Uso Apropiado** |
|---|---|
| Certificado de Firma Digital Tipo F1 | Firma digital y Autenticación<br>• No repudio (Non- Repudiation)<br>• Firma Digital (Digital Signature) |

| | |
|---|---|
| | • Cifrado de Clave (Key Encipherment) |

### 1.4.2. USOS PROHIBIDOS DEL CERTIFICADO

Los certificados emitidos deben ser utilizados dentro del marco de la normativa vigente que rige la materia.

Cualquier otro uso de los certificados no especificado en esta CP y en la normativa vigente, está fuera del alcance y responsabilidad de esta CP.

El uso indebido de los certificados será sancionado por el PSC CODE100 S.A., pudiendo llegar a la revocación de este.

## 1.5 ADMINISTRACIÓN DE LA POLÍTICA

### 1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre: CODE100 S.A.

Dirección: Iturbe 869, Asunción, Paraguay

Teléfono: (+59521) 444789

Dirección de correo electrónico: info@code100.com.py

Página Web: www.code100.com.py

### 1.5.2. PERSONA DE CONTACTO

Nombre: Representante Legal de CODE100 S.A

Dirección: Iturbe 869, Asunción, Paraguay

Teléfono: (+59521) 444789

Dirección de correo electrónico: info@code100.com.py

### 1.5.3. PERSONA QUE DETERMINA LA ADECUACIÓN DE LA CP A LA POLÍTICA

Director General de Firma Digital y Comercio Electrónico, será el encargado de determinar la adecuación de la presente Política de Certificación de tipo F2 (CP) de la PKI y la de CODE100 S. A.

### 1.5.4. PROCEDIMIENTOS DE APROBACIÓN DE LA CP

El MIC aprobará el contenido de la presente CP y sus posteriores enmiendas o modificaciones.

## 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 y responsabilidades de las partes con respecto a la emisión y gestión de los certificados. Éste acuerdo, requiere la aceptación explícita tanto del PSC, como del suscriptor, respectivamente.

**Agente de Registro Validador:** Persona responsable de la ejecución de actividades relacionadas con la RA, que realiza la validación de la identidad de quien solicita un certificado digital.

**Agente de Registro Verificador:** Persona responsable de la ejecución de actividades relacionadas con la RA, que realiza la verificación de la solicitud de certificado.

**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 digitalmente, en función del mensaje firmado por éste, y al cual se le vincula. Éste proceso no otorga certificación notarial ni fe pública.

**Autoridad de Aplicación (AA):** Ministerio de Industria y Comercio a través de la Dirección General de Firma Digital y Comercio Electrónico, dependiente de la Subsecretaría de Estado de Comercio. Órgano Regulador competente designado 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".

**Autoridad Certificadora (CA):** Entidad que presta servicios de emisión, gestión, revocación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de una RA. En el marco de la PKI Paraguay, son Autoridades Certificadoras, 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.

**Autoridad Certificadora 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 al usuario final.

**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 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.

**Cifrado:** Es un proceso para aumentar y convertir la información de un mensaje o archivo a un formato más seguro. Se convierte mediante un proceso matemático a un formato codificado, es decir ininteligible.

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

**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 aberturas 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 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.

**Datos de activación:** Valores de los datos, distintos a las 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, validación y firma de los Certificados; el proceso de generación es una función de la RA, la validación y firma, 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.

**Grupo Electrógeno:** Máquina encargada de generar electricidad a partir de un motor de gasolina o diesel. La instalación de este equipo deberá ser de tal forma que al interrumpirse el suministro de energía eléctrica del proveedor, el mismo debe arrancar automáticamente tomando la carga de las instalaciones del data center de la AC, 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, 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):**Son un sistema de identificación para entidades físicas o virtuales, compuesto por una serie única de números enteros, que identifica inequívocamente un objeto de información.

**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.

**Par de claves:** Son las claves privada y pública de un cripto-sistema 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(CertificationRequestSyntax Standard):** Estándar desarrollado por RSA que define la sintaxis de una petición de certificado.

**Parte que confía:** Es toda persona física o jurídica que confía en un certificado y/o en las firmas digitales generadas a partir de un certificado, emitidos bajo 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)

**Periodo 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.

**Periodo de uso:** Refiere 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.

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

**Prestador de Servicios de Certificación (PSC):** Entidad habilitada ante 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 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 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.

**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.

## 1.6.2 ACRÓNIMOS

Tabla Nº1 – Acrónimos

| Acrónimos | Descripción |
|---|---|
| C | País (del inglés, Country) |
| CA | Autoridad Certificadora (CA por sus siglas en inglés Certificate Authority) |
| CAI | Autoridad de Certificación Intermedia (CAI por sus siglas en inglés Certificate Authority Intermediate) |
| CA Raíz | Autoridad Certificadora Raíz del Paraguay |
| CI | Cedula de Identidad |
| CN | Nombre Común (del inglés, Common Name) |
| CP | Política 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) |
| DGFD&CE | Dirección General de Firma Digital y Comercio Electrónico |

| | |
|---|---|
| | dependiente del Vice Ministro de Comercio |
| DNS | Servicio de nombre de dominio (DNS por sus siglas en inglés Domain Name Server |
| 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 su sigla en inglés Hardware Security module) |
| ISO | Organización Internacional para la Estandarización (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 International Telecomunication Union – Telecomunication Standarization Sector) |
| MIC | Ministerio de Industria y Comercio |
| O | Organización (del inglés Organization) |
| OCSP | Servicio de Validación de certificado 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) contraseña que protege el acceso a una tarjeta criptográfica |
| PKCS | Norma de criptografía de clave pública (PKCS por sus siglas en inglés Public Key Cryptography Standard) |

| | |
|---|---|
| PKI | Infraestructura de Clave Publica (PKI por su sigla en inglés Public Key Infraestructure) |
| PSC | Prestador de Servicios de Certificación |
| 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 (del inglés, Serial Number) |
| TLS | Transport Layer Security (seguridad de la capa de transporte) |
| 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 Authority) |

# 2. RESPONSABILIDADES DE PUBLICACION Y DEL REPOSITORIO

## 2.1. REPOSITORIOS

Estipulado en la CPS DE CODE100 S.A.

## 2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

Estipulado en la CPS DE CODE100 S.A.

## 2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN

Las enmiendas o modificaciones de la CP se publicarán de acuerdo con lo establecido en el punto 9.12 de este documento. Las actualizaciones del Acuerdo de Suscriptores serán publicadas cuando sufran modificaciones.

La información de estados de certificados, es publicada de acuerdo con a lo dispuesto en el punto 4.9.7 de este documento.

Las demás informaciones mencionadas en el punto anterior, serán actualizadas lo más pronto posible y con un máximo de un día hábil desde que se dispongan o surjan modificaciones.

## 2.4 CONTROLES DE ACCESO

Establecido en la CPS de CODE100 S.A.

# 3. IDENTIFICACION Y AUTENTICACION

Establecido en la CPS de CODE100 S.A.

## 3.1 NOMBRES

Estipulado en la CPS de CODE100 S.A.

### 3.1.1. TIPOS DE NOMBRES

El tipo de nombre admitido para los titulares de los certificados emitidos conforme a la presente CPS son el Nombre Distintivo (Distinguished Name) según lo establecido en el estándar ITU X.500, direcciones de correo electrónico, dirección de página web (URL), u otra información que permita la identificación única del titular.

**En el caso de la CA de PSC CODE100**

| **Campo** | **Ejemplo** | **Descripción** |
|---|---|---|
| Country (C) | PY | Código de país, está asignado de acuerdo al estándar ISO 3166 |
| Organization (O) | CODE100 S.A. | Denominación o Razón Social de la Persona Jurídica habilitada como PSC |

| | | |
|---|---|---|
| CommonName (CN) | CA –CODE100 | CA + Nombre de la CA |
| Serial Number<br>{OID: 2.5.4.5} | RUC80080610-7 | RUC Número de Cédula Tributaria correspondiente a CODE100 |

**En el caso del Suscriptor Persona Física**

| **Campo** | **Ejemplo** | **Descripción** |
|---|---|---|
| Country (C) | PY | Código de país es asignado de acuerdo al estándar ISO 3166 |
| Organization (O) | PERSONA FISICA | La Política identifica si se trata de un certificado para: Persona física o Persona jurídica o Aplicación. |
| OrganizationUnit (OU) | FIRMA F1 o CIFRADO C1 | La Política identifica si se trata de un certificado generado para firma o cifrado. Los valores posibles son FIRMA F1, CIFRADO C1. |
| CommonName (CN) | JUAN PEREZ GOMEZ | Nombre del suscriptor, según documento de identificación, en mayúsculas y sin tildes. |
| SerialNumber<br>{OID: 2.5.4.5} | CI9999999 | CI más Número de Cédula de Identidad para paraguayos o CIE más Cédula de identidad para extranjeros |
| Surname (SN)<br>{OID: 2.5.4.4} | PEREZ GOMEZ | Se registran los dos apellidos del suscriptor, en mayúsculas y sin tildes. |
| GivenName (G)<br>{OID:2.5.4.42} | JUAN | Se registra el nombre de suscriptor, en mayúsculas y sin Tildes |

**En el caso del Suscriptor Persona Jurídica**

| **Campo** | **Ejemplo** | **Descripción** |
|---|---|---|
| Country (C) | PY | Código de país es asignado de acuerdo al estándar ISO 3166 |
| Organization (O) | PERSONAJURIDICA | Identifica si se trata de un certificado para: Persona física o Persona jurídica o Aplicación. |

| | | |
|---|---|---|
| OrganizationUnit<br>(OU) | FIRMA F1 o CIFRADO C1 | La Política identifica si se trata de un certificado generado por software o hardware para firma o cifrado. Los valores posibles son FIRMA F1 o CIFRADO C1. |
| CommonName | EMPRESA S.A. | Razón Social de la entidad, según inscripción en el Registro Público, en mayúsculas y sin tildes. |
| SerialNumber<br>{OID: 2.5.4.5} | RUC99999999-9 | RUC Número de Cédula Tributaria correspondiente al suscriptor. Debe ser validada durante el proceso de registro |
| Subjectalternativename | CommonName= JUAN GARCIA<br>SerialNumber= CI999999<br>Title= DIRECTOR | Certificados de Firma de Personas Jurídicas.<br>Este campo debe incluirse con<br>Nombre del titular persona física , según documento de identificación, en mayúsculas,<br>CI más Número de Cédula de<br>Identidad para paraguayos o CIE más Cédula de identidad para extranjeros, Cargo en la institución. |

### 3.1.2 NECESIDAD DE NOMBRES SIGNIFICATIVOS

Estipulado en la CPS de CODE100 S.A.

### 3.1.3 ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES

Estipulado en la CPS de CODE100 S.A.

### 3.1.4 REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES

Estipulado en la CPS de CODE100 S.A.

### 3.1.5 UNICIDAD DE LOS NOMBRES

Estipulado en la CPS de CODE100 S.A.

### 3.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

Se prohíbe a los solicitantes de certificados de personas jurídicas que incluyan nombres en las solicitudes que puedan suponer infracción de derechos de terceros. En el

caso de personas jurídicas, no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente. Los procesos de tratamiento, reconocimiento, autenticación y rol de marcas registradas, serán ejecutados por CODE100 S.A. de acuerdo con la legislación vigente sobre la materia.

La PKI Paraguay no arbitrará, mediará o resolverá ninguna disputa concerniente a la propiedad de nombres de dominio, nombres de empresas o instituciones y marcas registradas.

Durante el proceso de verificación de identidad, corresponderá al solicitante del certificado demostrar su derecho a usar un nombre específico. El PSC CODE100 S.A. tiene el derecho de rechazar una solicitud de certificado a causa de conflicto de nombre.

## 3.2. VALIDACIÓN INICIAL DE IDENTIDAD

### 3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA

Estipulado en la CPS de CODE100 S.A.

### 3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

Estipulado en la CPS de CODE100 S.A.

### 3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA

Estipulado en la CPS de CODE100 S.A.

### 3.2.4 INFORMACIÓN DEL SUSCRIPTOR NO VERIFICADA

No aplica.

### 3.2.5. VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)

Estipulado en la CPS de CODE100 S.A.

### 3.2.6. CRITERIOS PARA INTEROPERABILIDAD

Estipulado en la CPS de CODE100 S.A.

## 3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RE EMISIÓN DE CLAVES

### 3.3.1 IDENTIFICACIÓN Y AUTENTICACIÓN PARA RE EMISIÓN DE CLAVES

Estipulado en la CPS de CODE100 S.A.

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

Estipulado en la CPS de CODE100 S.A.

## 3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

Estipulado en la CPS de CODE100 S.A.

# 4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

## 4.1. SOLICITUD DE CERTIFICADO

### 4.1.1. QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

Estipulado en la CPS de CODE100 S.A.

### 4.1.1. QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

Estipulado en la CPS de CODE100 S.A.

### 4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

El proceso de solicitud de emisión de certificado debe ser iniciado exclusivamente por el Solicitante, quien debe acreditar fehacientemente su identidad.

Para poder efectuar la Solicitud de un certificado, el Solicitante debe:

- Ingresar al portal del Suscriptor.
- Cumplir con los requisitos mínimos de configuración de hardware y software.
- La aplicación, mostrara el formulario de Solicitud, éste deberá ser completado por el solicitante.
- Completados los datos de la Solicitud, el Solicitante deberá confirmarlos.
- El sistema a continuación desplegará las RA habilitadas, debiendo el Solicitante proceder a elegir libremente la más conveniente para realizar su identificación.
- Se realiza la generación del par de claves criptográficas asimétricas y el requerimiento de certificado digital en formato PKCS#10. La generación del par de claves correspondiente al certificado debe ser implementada en un dispositivo criptográfico provisto por el Solicitante, conforme con la lista de dispositivos criptográficos homologados por CODE100 S.A. publicada en

  http://www.code100.com.py/dispositivos-homologados.html
- Generadas las claves, la aplicación del PSC valida el requerimiento PKCS#10 y genera el PIN de revocación del certificado.
- Si la Solicitud es rechazada se le informa al Solicitante a sus datos de contacto.
- Cumpliendo el Solicitante podrá presentarse en la RA elegida o ser visitado por un Agente de Registro Validador, la aprobación de la Solicitud de

certificado digital estará sujeta a cubrir los requerimientos para la verificación de la identidad del Solicitante y los requisitos específicos en relación con las características del certificado digital solicitado.

- Cuando el Solicitante se presenta para su identificación ante el Agente de Registro Validador con toda la documentación exigida, procede a firmar el Acuerdo con Suscriptores.
- En caso de ser visitado por un Agente de Registro Verificador, este deberá validar que la generación del requerimiento del certificado de firma digital sea realizada en un dispositivo criptográfico homologado por CODE100 S.A.
- El Agente de Registro Verificador, podrá denegar o condicionar la aprobación de la solicitud del interesado hasta el efectivo cumplimiento de los requisitos y condiciones establecidos.
- La solicitud para la que no se haya completado el proceso de validación, caduca a los treinta (30) días de generada.
- Luego de aprobada de la Solicitud, la aplicación enviará un mail al Solicitante a los fines de hacerle saber que el certificado está listo para su descarga e instalación.

## 4.2. PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

### 4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Estipulado en la CPS de CODE100 S.A.

### 4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

Estipulado en la CPS de CODE100 S.A.

### 4.2.3. TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO

Se establece el plazo máximo de quince días hábiles para la emisión del certificado de tipo F1, contados a partir de haberse verificado la identidad del solicitante y admitida la solicitud.

En caso de que el PSC CODE100 S.A. supere el plazo máximo establecido para la emisión del certificado, deberá informar al solicitante de las causas que motivaron la demora y el nuevo plazo en el que se emitirá el certificado.

En caso que el interesado opte por desistir de su solicitud por el motivo expuesto en el PSC CODE100 S.A. tendrá previsto un procedimiento de reembolso de lo abonado.

## 4.3. EMISIÓN DEL CERTIFICADO

Estipulado en la CPS de CODE100 S.A.

### 4.3.1 ACCIONES DE LA CA DURANTE LA EMISIÓN DE LOS CERTIFICADOS

Estipulado en la CPS de CODE100 S.A.

### 4.3.2 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DEL CERTIFICADO DIGITAL

Estipulado en la CPS de CODE100 S.A.

## 4.4. ACEPTACIÓN DEL CERTIFICADO

### 4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

Estipulado en la CPS de CODE100 S.A.

### 4.4.2 PUBLICACIÓN DEL CERTIFICADO POR el PSC

Estipulado en la CPS de CODE100 S.A.

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

Estipulado en la CPS de CODE100 S.A.

## 4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

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

El uso de la clave privada correspondiente a la clave pública, contenida en el certificado, solamente debe ser permitido una vez que el suscriptor haya aceptado el certificado emitido, dicho uso, debe realizarse conforme a la normativa vigente, lo estipulado en esta CP y el acuerdo de suscriptores respectivo.

Los suscriptores deben proteger su clave privada del uso no autorizado y una vez expirado o revocado el certificado, su uso queda expresamente prohibido.

Notificar al PSC CODE100 S.A. sin dilación indebida:

- La pérdida, robo o extravío del dispositivo criptográfico,
- El compromiso potencial de su clave privada,
- La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación o por cualquier otra causa,
- Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera contener el suscriptor.

**CERTIFICADO DE PSC**

La Clave privada y el certificado del PSC podrá ser utilizado con el único propósito de:

- Firmar los certificados personas físicas y jurídicas para firma digital y para autenticación; y,
- Firmar las Listas de Certificados Revocados (CRL) correspondientes.

**CERTIFICADO DE PERSONA FÍSICA PARA FIRMA DIGITAL Y PARA CIFRADO**

El uso de los certificados emitidos por el PSC, debe ser acorde a lo dispuesto en el punto"6.1.7. Propósito de usos de clave (Campo keyusage x509 v3)" de la presente CP.

**CERTIFICADO DE PERSONA JURÍDICA PARA FIRMA DIGITAL Y PARA CIFRADO**

Los certificados de persona jurídica para firma digital serán usados de conformidad a lo establecido en la normativa vigente.

En el caso que el titular del certificado sea una persona jurídica, serán responsables por el uso sus representantes o personas designadas.

Cada persona jurídica deberá desarrollar y establecer los mecanismos de seguridad informática y de infraestructura física, así como los reglamentos, procedimientos o políticas que considere pertinentes para resguardar y delimitar el uso de dicho certificado en su organización.

El uso de los certificados emitidos por el PSC, debe ser acorde a lo dispuesto en el punto "6.1.7. Propósito de usos de clave (Campo keyusage x509 v3)"de la presente CP.

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

La parte que confía debe aceptar las estipulaciones establecidas en la presente CP, en todo lo que les resulte aplicable, como condición indispensable para confiar en el certificado.

Antes de cualquier acto de confianza la parte que confía debe evaluar en forma independiente:

- Que el certificado sea utilizado para un propósito apropiado, y que no esté prohibido o restringido por la presente CP. El PSC no es responsable de esta tarea.
- El estado del certificado y el estado de todos los certificados de las CA en la cadena que emitieron los certificados.

## 4.6 RENOVACIÓN DEL CERTIFICADO

La renovación del certificado no está permitida por esta CP, cuando un certificado requiera ser renovado debe solicitarse un nuevo certificado, de acuerdo con la sección 4.1 de esta CP.

### 4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADOS

No aplica.

### 4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN

No aplica.

### 4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO

No aplica.

### 4.6.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO

No aplica.

### 4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO

No aplica.

### 4.6.6 PUBLICACIÓN POR EL PSC DEL CERTIFICADO RENOVADO

No aplica.

### 4.6.7 NOTIFICACIÓN POR EL PSC DE LA EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES

No aplica.

## 4.7 RE-EMISIÓN DE CLAVES DE CERTIFICADO

Estipulado en la CPS de CODE100 S.A.

### 4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO

No aplica.

### 4.7.2 QUIEN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA

No aplica.

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

No aplica.

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

No aplica.

### 4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE-EMITIDO

No aplica.

### 4.7.6 PUBLICACIÓN POR EL PSC DE LOS CERTIFICADOS RE-EMITIDOS

No aplica.

### 4.7.7 NOTIFICACIÓN POR EL PSC DE LA RE-EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES

No aplica.

## 4.8 MODIFICACIÓN DE CERTIFICADOS

### 4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO
### 4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

No aplica.

### 4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

No aplica.

### 4.8.4 NOTIFICACIÓN AL SUSCRIPTOR DE LA EMISIÓN DE UN NUEVO CERTIFICADO

No aplica.

### 4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

No aplica.

### 4.8.6 PUBLICACIÓN POR EL PSC DE LOS CERTIFICADOS MODIFICADOS

No aplica.

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

No aplica.

## 4.9 REVOCACION Y SUSPENSION

### 4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

Estipulado en la CPS de CODE100 S.A.

### 4.9.2 QUIEN PUEDE SOLICITAR REVOCACIÓN

Estipulado en la CPS de CODE100 S.A.

### 4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

Los suscriptores podrán solicitar la revocación de su certificado ingresando a la aplicación del Certificador desde:

- http://www.code100.com.py/firma-digital/revocacion.html

Este sitio se encuentra disponible las 24 horas los 7 días de la semana, durante todo el año, lo que permite servicios de revocación en horarios no habituales de jornada laboral, como así también fines de semana y feriados.

El PSC CODE100 S.A. y sus RA vinculadas conservarán como documentación probatoria toda solicitud de revocación y el material probatorio vinculado. Se registraran en los registros informáticos del PSC CODE100 S.A. la revocación.

La revocación se reflejará en la próxima Lista de Certificados Revocados, cuando sea generada de acuerdo con lo especificado en el punto "4.9.7 Frecuencia de emisión de la CRL".

El PSC CODE100 S.A. debe evaluar la solicitud de revocación presentada y verificar que la misma ha sido presentada por el suscriptor del certificado, por una autoridad competente o un tercero de acuerdo con la sección "3.4 Requerimiento de revocación".

En los casos que la solicitud de revocación provenga de una Autoridad Judicial Competente, el PSC CODE100 S.A. deberá evaluar la solicitud. Antes de comenzar con el proceso de revocación se deberá notificar al suscriptor lo cual no implicará aun la revocación efectiva del certificado.

Un certificado revocado será válido únicamente para la verificación de firmas generadas durante el periodo en que el referido certificado era válido.

### 4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

No se estipula periodo de gracia para revocación de certificados.

### 4.9.5 TIEMPO DENTRO DEL CUAL EL PSC DEBE PROCESAR LA SOLICITUD DE REVOCACIÓN

La recepción de la solicitud de revocación está disponible 7 días de la semana x 24 hs. a través de la aplicación del PSC desde:

- http://www.code100.com.py/firma-digital/revocacion.html

Esta solicitud será procesada de inmediato, sin intervención del PSC CODE100 S.A.

En caso de que el Suscriptor se presente personalmente ante el PSC CODE100 S.A., la solicitud de revocación será ingresada por el Agente de Registro y también será procesada de inmediato, dicho proceso no podrá superar las 12 horas.

### 4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LAS PARTES QUE CONFÍAN

Estipulado por la CPS de CODE100 S.A.

### 4.9.7 FRECUENCIA DE EMISIÓN DEL CRL

Estipulado en la CPS de CODE100 S.A.

### 4.9.8 LATENCIA MÁXIMA PARA CRL

Estipulado en la CPS de CODE100 S.A.

### 4.9.9 REQUISITOS DE VERIFICACIÓN DEL CRL

Estipulado en la CPS de CODE100 S.A.

### 4.9.10 DISPONIBILIDAD DE VERIFICACIÓN DE REVOCACIÓN/ ESTADO EN LÍNEA

Estipulado en la CPS de CODE100 S.A.

### 4.9.11 REQUERIMIENTOS PARA VERIFICAR LA REVOCACIÓN EN LÍNEA

Estipulado en la CPS de CODE100 S.A.

### 4.9.12 OTRAS FORMAS DE ADVERTENCIAS DE |REVOCACIÓN DISPONIBLES

Este Ítem no aplica.

### 4.9.13 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA

Estipulado en la CPS de CODE100 S.A.

### 4.9.14 CIRCUNSTANCIAS PARA SUSPENSIÓN

No aplica.

### 4.9.15 QUIEN PUEDE SOLICITAR LA SUSPENSIÓN

No aplica.

### 4.9.16 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

No aplica.

### 4.9.17 LÍMITES DEL PERÍODO DE SUSPENSIÓN

No aplica.

## 4.10 SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADO

### 4.10.1 CARACTERÍSTICAS OPERACIONALES

Estipulado en la CPS de CODE100 S.A.

### 4.10.2 DISPONIBILIDAD DEL SERVICIO

Estipulado en la CPS de CODE100 S.A.

### 4.10.3 CARACTERÍSTICAS OPCIONALES

Sin estipulaciones.

## 4.11 FIN DE LA SUSCRIPCIÓN

Estipulado en la CPS de CODE100 S.A.

## 4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

### 4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

Estipulado en la CPS de CODE100 S.A.

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

No aplica.

# 5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

## 5.1 CONTROLES FÍSICOS

### 5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

Estipulado en la CPS de CODE100 S.A.

### 5.1.2 ACCESO FÍSICO

Estipulado en la CPS de CODE100 S.A.

### 5.1.3 ENERGÍA Y AIRE ACONDICIONADO

Estipulado en la CPS de CODE100 S.A.

### 5.1.4 EXPOSICIONES AL AGUA

Estipulado en la CPS de CODE100 S.A.

### 5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

Estipulado en la CPS de CODE100 S.A.

### 5.1.6 ALMACENAMIENTO DE MEDIOS

Estipulado en la CPS de CODE100 S.A.

### 5.1.7 ELIMINACIÓN DE RESIDUOS

Estipulado en la CPS de CODE100 S.A.

### 5.1.8 RESPALDO FUERA DE SITIO

Estipulado en la CPS de CODE100 S.A.

### 5.1.9 INSTALACIONES TÉCNICAS DE LA RA

Estipulado en la CPS de CODE100 S.A.

## 5.2 CONTROLES PROCEDIMENTALES

### 5.2.1 ROLES DE CONFIANZA

Estipulado en la CPS de CODE100 S.A.

### 5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Estipulado en la CPS de CODE100 S.A.

### 5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Estipulado en la CPS de CODE100 S.A.

### 5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES

Estipulado en la CPS de CODE100 S.A.

## 5.3 CONTROLES DE PERSONAL

### 5.3.1 REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

Estipulado en la CPS de CODE100 S.A.

### 5.3.2 PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Estipulado en la CPS de CODE100 S.A.

### 5.3.3 REQUERIMIENTOS DE CAPACITACIÓN

Estipulado en la CPS de CODE100 S.A.

### 5.3.4 REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

Estipulado en la CPS de CODE100 S.A.

### 5.3.5 FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

Estipulado en la CPS de CODE100 S.A.

### 5.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS

Estipulado en la CPS de CODE100 S.A.

### 5.3.7 REQUISITOS DE CONTRATACIÓN A TERCEROS

Estipulado en la CPS de CODE100 S.A.

### 5.3.8 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

Estipulado en la CPS de CODE100 S.A.

## 5.4 PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

### 5.4.1 TIPOS DE EVENTOS REGISTRADOS

Estipulado en la CPS de CODE100 S.A.

### 5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)

Estipulado en la CPS de CODE100 S.A.

### 5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

Estipulado en la CPS de CODE100 S.A.

### 5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

Estipulado en la CPS de CODE100 S.A.

### 5.4.5 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE REGISTRO (LOGS) DE AUDITORÍA

Estipulado en la CPS de CODE100 S.A.

### 5.4.6 SISTEMA DE RECOLECCIÓN DE INFORMACIÓN DE AUDITORÍA (INTERNO VS EXTERNO)

Estipulado en la CPS de CODE100 S.A.

### 5.4.7 NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

Estipulado en la CPS de CODE100 S.A.

### 5.4.8 EVALUACIÓN DE VULNERABILIDADES

Estipulado en la CPS de CODE100 S.A.

## 5.5 ARCHIVOS DE REGISTROS

### 5.5.1 TIPOS DE REGISTROS ARCHIVADOS

Estipulado en la CPS de CODE100 S.A.

### 5.5.3 PROTECCIÓN DE ARCHIVOS

Estipulado en la CPS de CODE100 S.A.

### 5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO

Estipulado en la CPS de CODE100 S.A.

### 5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

Estipulado en la CPS de CODE100 S.A.

### 5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO)

Estipulado en la CPS de CODE100 S.A.

### 5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA

Estipulado en la CPS de CODE100 S.A.

## 5.6 CAMBIO DE CLAVE

Estipulado en la CPS de CODE100 S.A.

## 5.7 RECUPERACIÓN DE DESASTRES Y COMPROMISO

### 5.7.1 PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO

Estipulado en la CPS de CODE100 S.A.

### 5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES

Estipulado en la CPS de CODE100 S.A.

### 5.7.3 PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD

Estipulado en la CPS de CODE100 S.A.

### 5.7.4 CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Estipulado en la CPS de CODE100 S.A.

### 5.7.5 ACTIVIDADES DE LAS AUTORIDADES DE REGISTRO

Estipulado en la CPS de CODE100 S.A.

## 5.8 EXTINCIÓN DE UN PSC

Estipulado en la CPS de CODE100 S.A.

# 6. CONTROLES TÉCNICOS DE SEGURIDAD

En este apartado únicamente se describen los controles de seguridad técnica particulares del tipo de certificado tratado por el PSC CODE100 S.A. y las RA Vinculadas.

## 6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

El PSC CODE100 S.A. mantendrá controles para brindar seguridad razonable de que los pares de claves del PSC, se generan e instalan de acuerdo con el protocolo definido para la generación 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.

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 (es), será la persona responsable de la generación de pares de claves criptográficas y del uso del certificado.

El algoritmo a ser utilizado para las claves criptográficas de titulares de certificados, está definido en el documento NORMAS DE ALGORITMOS 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 ALGORITMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY, en un medio de almacenamiento definido para cada tipo de certificado previsto por la Autoridad de Aplicación, conforme a lo estipulado en la siguiente tabla:

| **Tipo de Certificado** | **Medio de Almacenamiento** |
|---|---|
| **F1** | Repositorio Protegido por contraseña y/o identificaron Biométrica, cifrado por software. |

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.

### 6.1.2 ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR

La clave privada de los certificados de firma digital tipo F1 es generada por el propio titular, por lo que en ningún caso será entregada al mismo.

### 6.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

Estipulado en la CPS de CODE100 S.A.

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

La clave pública del PSC CODE100 S.A. se encuentra incluida en el certificado de dicho PSC. El certificado del PSC CODE100 S.A. no se encuentra incluido en los certificados personales generados por el usuario final.

El certificado del PSC CODE100 S.A. debe ser obtenido del repositorio (ver apartado 2.1) que estará a disposición de los titulares de certificados y terceros aceptantes para realizar cualquier tipo de comprobación.

### 6.1.5 TAMAÑO DE LA CLAVE

Los algoritmos y tamaños de clave a ser utilizados en los certificados de firma digital tipo F1 emitidos por el PSC CODE100 S.A, se definen en el documento NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.

### 6.1.6 GENERACIÓN DE PARÁMETROS DE CLAVES ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD

Estipulado en la CPS de CODE100 S.A.

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

Los usos admitidos de la clave para los certificados de firma digital tipo F1 vienen dados por el valor de las extensiones Key Usage y Extended Key Usage de los mismos.

El contenido de dichas extensiones para los de firma digital tipo F1 se puede consultar en el apartado 7.1 del presente documento.

### 6.1.8 GENERACIÓN DE CLAVE POR HARDWARE O SOFTWARE

El proceso de generación de claves criptográficas, deberá ser realizado, para los certificados del tipo F1 en software.

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

### 6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO

El estándar requerido para los módulos criptográficos con certificados del tipo F1, es el FIPS 140-1 o FIPS 140-2 o superior.

Los estándares requeridos para los módulos de generación de las claves criptográficas, son especificados en el documento NORMAS DE ALGORITMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.

### 6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA

Las claves privadas de los certificados del tipo F1 no se encuentran bajo control multipersona. El control de dicha clave privada recae enteramente sobre el titular.

### 6.2.3 CUSTODIA/RECUPERACIÓN DE LA CLAVE PRIVADA

La custodia de la clave privada del certificado de firma digital (tipo F1) la realizan los propios titulares de la misma.

### 6.2.4 RESPALDO/COPIA DE LA CLAVE PRIVADA

Cualquier entidad titular de certificado, podrá, a su criterio, mantener una copia de su propia clave privada.

CODE100 S.A mantiene una copia de seguridad de su propia clave privada.

CODE100 S.A no podrá mantener copia de seguridad de la clave privada del titular de certificado de firma digital por ella emitida para garantizar el no repudio.

### 6.2.5 ARCHIVADO DE LA CLAVE PRIVADA

Estipulado en la CPS de CODE100 S.A.

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

Estipulado en la CPS de CODE100 S.A.

### 6.2.7 ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

CODE100 S.A. no podrá almacenar la clave privada del titular de certificados de firma digital.

### 6.2.8 MÉTODO DE ACTIVACIÓN DE CLAVE PRIVADA

La activación de la clave privada la podrá efectuar el titular de la misma mediante el uso de al menos un factor de seguridad.

### 6.2.9 MÉTODOS DE DESACTIVACIÓN DE LA CLAVE PRIVADA

No estipulado.

### 6.2.10 DESTRUCCIÓN DE CLAVE PRIVADA

Cada titular del certificado debe definir los procedimientos necesarios para la destrucción de su clave privada de sus copias de seguridad si los hubiere.

### 6.2.11 CLASIFICACIÓN DEL MÓDULO CRIPTOGRÁFICO

La capacidad del módulo criptográfico utilizado en los dispositivos se realiza 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

Las claves públicas de los titulares de los certificados de firma digital (tipo F1), así como las CRL emitidas, serán almacenadas por el PSC CODE100 S.A., después de la expiración de los certificados correspondientes, permanentemente, para la verificación de firmas generadas durante su periodo de validez.

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

Las claves privadas de los certificados de firma digital deberán ser utilizadas por sus titulares 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.

El periodo de validez de los certificados de firma digital de tipo F1 es como máximo de un (1) año desde el momento de emisión del mismo.

# 6.4 DATOS DE ACTIVACIÓN

## 6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Para certificados de firma digital tipo F1, la generación y almacenamiento del par de claves son realizados en software, con capacidad de generación de claves, siendo activados y protegidos por contraseña y/o identificación biométrica

## 6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Estipulado en la CPS de CODE100 S.A.

## 6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Estipulado en la CPS de CODE100 S.A.

# 6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

## 6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

Estipulado en la CPS de CODE100 S.A.

## 6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

Estipulado en la CPS de CODE100 S.A.

## 6.5.3 CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO

Estipulado en la CPS de CODE100 S.A.

# 6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

## 6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA

Estipulado en la CPS de CODE100 S.A.

## 6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

Estipulado en la CPS de CODE100 S.A.

## 6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Estipulado en la CPS de CODE100 S.A.

## 6.6.4 CONTROLES EN LA GENERACIÓN DE CRL

Estipulado en la CPS de CODE100 S.A.

## 6.7 CONTROLES DE SEGURIDAD DE RED

Estipulado en la CPS de CODE100 S.A.

### 6.7.1 DIRECTRICES GENERALES

Estipulado en la CPS de CODE100 S.A.

### 6.7.2 FIREWALL

Estipulado en la CPS de CODE100 S.A.

### 6.7.3 SISTEMA DE DETECCIÓN DE INTRUSO (IDS)

Estipulado en la CPS de CODE100 S.A.

### 6.7.4 REGISTRO DE ACCESO NO AUTORIZADO A LA RED

6 Estipulado en la CPS de CODE100 S.A.

## 6.8 CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO

Los módulos criptográficos utilizados para el almacenamiento de la clave privada del titular del certificado son homologados por la AA, y sus requisitos se describen en el punto 6.2.1.

# 7. PERFILES DE CERTIFICADOS, CRL Y OCSP

Todos los certificados emitidos bajo la presente CP respetan la especificación ITU-T X.509 (ISO/IEC 9594-8) "Information Technology – The Directory: Public key and atribute certificate frameworks".

## 7.1 PERFIL DEL CERTIFICADO

El certificado digital cumple con:

- ITU-T X.509 V.3 Information technology Open systems interconnection The Directory: Public-key and attribute certificate frameworks
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- ETSI TS 101 862 V.1.3.3 Qualified Certificates Profile
- RFC 3739 "Internet X.509 Public Key Infrastructure-Qualified Certificates Profile
- ISO 3166-1 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países".
- RFC – 3279 '' Internet X.509 Public Key Infrastructure Algorithm Identifier"

A continuación, se detalla el contenido de las extensiones más significativas de los certificados de firma digital del tipo F1 emitidos por CODE100 S.A.

## CERTIFICADO DE PERSONA FÍSICA DEL TIPO F1

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

Tabla Nº 5 Estructura del campo subject certificado de persona física de tipo F1

| CAMPO | EJEMPLO | DESCRIPCIÓN |
|---|---|---|
| C (Country)<br>{OID: 2.5.4.6} | PY | Código de país es asignado de acuerdo al estándar ISO 3166 |
| O (Organization)<br>{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 (OrganizationUnit)<br>{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; CIFRADO C1. |
| CN (CommonName)<br>{OID: 2.5.4.3} | JUAN ANDRES PEREZ GOMEZ | 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 | CI4256897 | CI más Número de Cédula de Identidad del titular del certificado, según documento de identificación |
| GivenName (G)<br>{OID: 2.5.4.42} | JUAN ANDRES | 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. |
| Surname (SN)<br>{OID: 2.5.4.4} | PEREZ GOMEZ | 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. |

La estructura del certificado, referente a la extensión nombre alternativo del sujeto del certificado, es la que se describe como ejemplo en la siguiente tabla:

Tabla Nº 6 Estructura de los campos del certificado de persona física de tipo F1 referente a la extensión **nombre alternativo del sujeto.**

| Campo | Ejemplo | Valor o restricciones |
|---|---|---|
| Rfc822Name | Juanperez85@gmail.com | Email del titular del certificado. Campo no obligatorio. |
| DirectoryName {OID: 2.5.4.10} | O = BELCORP S.R.L. | Nombre de la organización en el que presta servicio el titular del certificado. Campo no obligatorio. |
| DirectoryName {OID: 2.5.4.11} | OU = ADMINISTRACION Y FINANZAS | Nombre de la unidad de la organización en el que presta servicio el titular del certificado. Campo no obligatorio. |
| DirectoryName {OID: 2.5.4.5} | Serial Number = RUC80081052-5 | RUC más Número de cédula tributaria correspondiente a la organización en el que presta servicio el titular del certificado. |
| DirectoryName {OID: 2.5.4.12} | T = DIRECTOR ADMINISTRATIVO | Cargo o Titulo del titular del certificado. Campo no obligatorio. |

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 cuando estén aprobados por la CA Raíz.

### Descripción de los campos más relevantes del perfil de Certificado de Persona Física de Tipo F1

Tabla Nº 7 Estructura de los principales campos del certificado de persona física de tipo F1.

| Campo | Ejemplo | Valor o restricciones |
|---|---|---|
| Versión (Version) | V3 | Los certificados son X.509 versión 3 (V3). |
| Número de serie (Serial number) | 18 6f 57 dd 38 6c 47 ad 54 5d 0c 9a 22 f4 96 60 | Valor único emitido dentro del ámbito de cada CA.<br>Este campo indica el número de serie del certificado digital. Valor único emitido dentro del ámbito del PSC. |

| | | |
|---|---|---|
| Algoritmo de firma (Signaturealgorithm) | sha256RSA | El Algoritmo de firma es SHA 256 RSA. |
| Signaturehash algorithm (algoritmo hash de firma) | sha256 | El Algoritmo de firma es SHA256. |
| Emisor (Issuer DN) | CN = CA-CODE100 S. A.<br>O = CODE100 S. A.<br>C = PY<br>SERIALNUMBER=RUC80080610-7 | Nombre del PSC CODE100 S.A. Ver sección "7.1.4 Formas de Nombre"<br>Este campo indica los datos de identificación del PSC CODE100 S.A. quien es emisor del certificado. |
| Válido desde (Validfrom) | viernes, 07 de noviembre de 2018 15:16:58 | En caso de certificados tipos C1 y F1, tienen 1 (un) año de validez. |
| Válido hasta (Validto) | lunes, 07 de noviembre de 2019 15:16:58 | |
| Sujeto (Suscriber DN) | C = PY<br>O = PERSONA FISICA<br>OU= FIRMA F1<br>CN = JUAN ANDRES PEREZ GOMEZ<br>SERIALNUMBER = CI2304024<br>G = JUAN ANDRES<br>SN = PEREZ GOMEZ | Este campo indica los datos de identificación del titular del certificado emitido por el PSC CODE100 S.A. |
| Clave pública del sujeto (SubjectPublic Key) | 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 ffee 51 8c 33 5c 15 aa | Este campo indica la clave pública del titular del certificado. Codificado de acuerdo con el RFC 5280, con un largo de clave mínima de 2048 bits y algoritmo RSA Encryption. |

| | | |
|---|---|---|
| | 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 dbbf 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 Nº 8 – Estructura de las extensiones del certificado de persona física de tipo F1

| **EXTENSIONES CERTIFICADO DE PERSONA FÍSICA DE TIPO F1** | | | |
|---|---|---|---|
| **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 contiene 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 keyidentifier contiene 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 |
| AuthorityInformationAccess(Acceso a información de la entidad emisora) | [1]Acceso a información de autoridad<br>Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2)<br>Nombre alternativo: Dirección | 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. | NO |

| | | | |
|---|---|---|---|
| | URL=http://ca1.code100.com.py/firma-digital/cer/CA-CODE100.cer<br>[2]Acceso a información de autoridad<br>Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2)<br>Nombre alternativo:<br>Dirección URL=http://ca2.code100.com.py/firma-digital/cer/CA-CODE100.cer<br>[3]Acceso a información de autoridad<br>Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)<br>Nombre alternativo:<br>Dirección URL=http://ca1.code100.com.py/ocsp<br>[4]Acceso a información de autoridad<br>Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)<br>Nombre alternativo:<br>Dirección URL=http://ca2.code100.com.py/ocsp | La primera entrada contiene el método de acceso i d-ad-caIssuer, utilizando uno de los siguientes protocolos de acceso: HTTPS o LDAP, para la recuperación de la cadena de certificación. La segunda entrada contiene el método de acceso id-ad-ocsp con el respectivo respondedor OCSP utilizando uno de los siguientes protocolos de acceso HTTPS o LDAP. | |
| CRL DistributionPoints (Puntos de distribución de CRL) | [1]Punto de distribución CRL<br>Nombre del punto de distribución:<br>Nombre completo:<br>Dirección URL=http://ca1.code100.com.py/firma-digital/crl/CA-CODE100.crl<br>Dirección | Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes al PSC CODE100 S.A. quien emitió el certificado, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no. | NO |

| | | | |
|---|---|---|---|
| | URL=http://ca2.code100.com.py/firma-digital/crl/CA-CODE100.crl | | |
| Key Usage (Uso de la clave) | Sin repudio, Firma digital, Cifrado de clave. | En certificados tipo F1 solamente pueden ser activados los siguientes bits: digitalSignature; NonRepudiation (renombrado recientemente con el nombre de contentCommitmen); y keyEncipherment<br><br>En certificados tipo C1 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) Autenticación del cliente (1.3.6.1.5.5.7.3.2) | Referencia otros propósitos de la clave, adicionales al uso y debe ser consistente con la extensión keyUsage | SI |
| SubjectAltenativeName (nombre alternativo del sujeto) | Rfc822Name=juanperez@gmail.com DirectoryName O= BELCORP S.R.L. SerialNumber= RUC80081052-5 T=DIRECTOR ADMINISTRATIVO | Campo no obligatorio. Los datos a incluir en esta extensión deben ser representados mediante la utilización de los siguientes campos:<br>• Rfc822Name= [ email del titular del certificado]<br>• DirectoryName=2.5.4.10:[ nombre de la organización en el que presta servicio el titular del certificado]<br>• DirectoryName =2.5.4.5: RUC [número de cédula tributaria correspondiente a la organización en el que presta servicio el titular del certificado]<br>• DirectoryName=2.5.4.1: [Cargo o Titulo del titular del certificado] | NO |

| | | | |
|---|---|---|---|
| | | Los otros campos que compone la extensión "SubjectAlternativeName" 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:<br>Identificador de directiva=1.3.6.1.4.1.44234.1.1.1.6<br>[1,1]Información de certificador de directiva:<br>Id. de certificador de directiva=CPS<br>Certificador:<br>http://www.code100.com.py/firma-digital/CODE100%20Politica%20de%20Certificacion%20F1%20v1.0.pdf<br>[1,2]Información de certificador de directiva:<br>Id. de certificador de directiva=Aviso de usuario<br>Certificador:<br>Texto de aviso=Politica de certificacion F1 de Code100 S.A.<br>[1,3]Información de certificador de directiva:<br>Id. de certificador de directiva=Aviso de usuario<br>Certificador:<br>Texto de aviso=Code 100 S.A. Certificate Policy F1 | Contiene el OID de la CP correspondiente y la dirección WEB de la CPS del PSC que emite el certificado. | NO |

## CERTIFICADO DE PERSONAS JURÍDICAS DEL TIPO F1

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

Tabla Nº 9 Estructura del campo subject certificado de persona jurídica de tipo F1

| CAMPO | EJEMPLO | DESCRIPCIÓN |
|---|---|---|
| C (Country)<br>{OID: 2.5.4.6} | PY | Código del país asignado de acuerdo al ISO 3166. |
| O (Organization)<br>{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 jurídica y se debe indicar PERSONA JURIDICA, en mayúscula y sin tilde. |
| OU (OrganizationUnit)<br>{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; CIFRADO C1. |
| CN (CommonName)<br>{OID: 2.5.4.3} | BELCORP S.R.L. | Este campo debe contener la razón social del titular del certificado, según documento identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde. |
| Serial Number<br>{OID: 2.5.4.5} | RUC80081052-5 | RUC más número de cédula tributaria del titular del certificado, según documento de identificación. |

La estructura del certificado, referente a la extensión **nombre alternativo del sujeto** del certificado, es la que se describe como ejemplo en la siguiente tabla:

Tabla Nº 10 Estructura de los campos del certificado de persona jurídica de tipo F1 referente a la extensión **nombre alternativo del sujeto**

| CAMPO | EJEMPLO | DESCRIPCIÓN |
|---|---|---|
| Rfc822Name | info@belcorpsrl.com | Email del titular del certificado. Campo no obligatorio. |
| DirectoryName<br>{OID: 2.5.4.3} | CN=RICARDO ANDRES PORTILLO BOGADO | Nombre y apellido del responsable del certificado. Campo obligatorio. |
| DirectoryName<br>{OID: 2.5.4.5} | SERIAL NUMBER=CI 3256478 | CI más Número de cédula de identidad correspondiente al responsable del certificado. Campo obligatorio. |

| | | |
|---|---|---|
| DirectoryName {OID: 2.5.4.12} | T=REPRESENTANTE LEGAL | Cargo que ocupa en la organización el responsable del certificado. Campo no obligatorio. |

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 cuando estén aprobados por la CA Raíz.

### Descripción de los campos más relevantes del perfil de Certificado de Persona Jurídica de Tipo F1:

Tabla Nº 11 – Estructura de los principales campos del certificado de persona jurídica de tipo F1

| Campo | Ejemplo | Valor o restricciones |
|---|---|---|
| Versión (Version) | V3 | Los certificados son X.509 versión 3 (V3). |
| Número de serie (Serial number) | 18 6f 57 dd 38 6c 47 ad 54 5d 0c 9a 22 f4 96 60 | Valor único emitido dentro del ámbito del PSC CODE100 S.A.<br>Este campo indica el número de serie del certificado digital. Valor único emitido dentro del ámbito del PSC CODE100 S.A. |
| Algoritmo de firma (Signaturealgorithm) | sha256RSA | El Algoritmo de firma es SHA 256 RSA. |
| Signaturehash algorithm (algoritmo hash de firma) | sha256 | El Algoritmo de firma es SHA256. |
| Emisor (Issuer DN) | CN=CA-CODE100 S. A.<br>C=PY<br>O=CODE100 S. A.<br>SERIALNUMBER=RUC80080610-7 | Nombre del PSC CODE100 S.A. Ver sección "7.1.4 Formas de Nombre"<br>Este campo indica los datos de identificación del PSC CODE100 S.A. quien emitió el certificado. |
| Válido desde (Validfrom) | viernes, 07 de noviembre de 2018 15:16:58 | En caso de certificados tipos C2 y F2, la validez es de 1 (un) año. |
| Válido hasta (Validto) | lunes, 07 de noviembre de 2019 15:16:58 | |
| Sujeto (Suscriber DN) | OU= FIRMA F1<br>SERIALNUMBER = RUC80081052-5 | Este campo indica los datos de identificación del titular del certificado emitido por el PSC CODE100 S.A. |

| | | |
|---|---|---|
| | C = PY<br>O = PERSONA JURIDICA<br>CN = BELCORP S.R.L. | |
| Clave pública del sujeto (SubjectPublic Key) | 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 ffee 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 dbbf 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, con un largo de clave mínima de 2048 bits y algoritmo RSA Encryption. |

Tabla Nº 12 – Estructura de las extensiones del certificado de persona jurídica de tipo F1

| **EXTENSIONES CERTIFICADO DE PERSONA JURIDICA DE TIPO F1** | | | |
|---|---|---|---|
| **CAMPO** | **EJEMPLO** | **DESCRIPCIÓN** | **CRÍTICO** |
| Subject Key Identifier (Identificador de | ac dc d4 d3 cf 0c 20 ce bb 20 29 1b 93 1a 10 bb b2 36 3f a7 | Este campo contiene el hash SHA-1 de la clave pública del titular del certificado. Este Campo | NO |

| | | | |
|---|---|---|---|
| la clave del Sujeto) | | es usado por el software de validación para ayudar a identificar un certificado que contiene una determinada clave pública. | |
| 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 keyidentifier contiene el hash SHA-1 de la clave pública del PSC CODE100 S.A. 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 |
| AuthorityInformation Access(Acceso a información de la entidad emisora) | [1]Acceso a información de autoridad<br>Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2)<br>Nombre alternativo:<br>Dirección URL=http://ca1.code100.com.py/firma-digital/cer/CA-CODE100.cer<br>[2]Acceso a información de autoridad<br>Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2)<br>Nombre alternativo:<br>Dirección URL=http://ca2.code100.com.py/firma-digital/cer/CA-CODE100.cer<br>[3]Acceso a información de autoridad<br>Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) | Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado del PSC.<br>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.<br>La primera entrada debe contener el método de acceso i d-ad-caIssuer, 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 |

| | | | |
|---|---|---|---|
| | Nombre alternativo:<br>Dirección URL=http://ca1.code100.com.py/ocsp<br>[4]Acceso a información de autoridad<br>Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)<br>Nombre alternativo:<br>Dirección URL=http://ca2.code100.com.py/ocsp | | |
| CRL DistributionPoints (Puntos de distribución de CRL) | [1]Punto de distribución CRL<br>Nombre del punto de distribución:<br>Nombre completo:<br>Dirección URL=http://ca1.code100.com.py/firma-digital/crl/CA-CODE100.crl<br>Dirección URL=http://ca2.code100.com.py/firma-digital/crl/CA-CODE100.crl | Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a los certificados emitidos por CODE100 S.A., 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 solamente pueden ser activados los siguientes bits: digitalSignature; NonRepudiation (renombrado recientemente con el nombre de contentCommitmen); y keyEncipherment<br><br>En certificados tipo C1 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)<br>Autenticación de cliente | Referencia otros propósitos de la clave, adicionales al uso y debe ser consistente con la extensión keyUsage | SI |

| | | | |
|---|---|---|---|
| | (1.3.6.1.5.5.7.3.2) | | |
| SubjectAltenative Name (nombre alternativo del sujeto) | DirectoryName CN=RICARDO ANDRES PORTILLO BOGADO SerialNumber= CI 3256478 T=REPRESENTANTE LEGAL | Campo no obligatorio. Los datos a incluir en esta extensión deben ser representados mediante la utilización de los siguientes campos:<br>• Rfc822Name= [ email del titular del certificado]<br>• DirectoryName=2.5.4.10:[ nombre de la organización en el que presta servicio el titular del certificado]<br>• DirectoryName =2.5.4.5: RUC [número de cédula tributaria correspondiente a la organización en el que presta servicio el titular del certificado]<br>• DirectoryName=2.5.4.1: [Cargo o Titulo del titular del certificado]<br>Los otros campos que compone la extensión "SubjectAlternativeName" podrán ser utilizados en la forma y con los propósitos definidos por la RFC 5280, siempre y cuanto estén aprobados por la CA Raíz. | NO |
| Certificate Policies (Política del certificado) | [1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.44234.1.1.1.6<br>[1,1]Información de certificador de directiva:<br>Id. de certificador de directiva=CPS Certificador: http://www.code100.com.py/firma-digital/CODE100%20Politica%20de%20Certificacion%20F1%20v1.0.pdf | Contiene el OID de la CP correspondiente y la dirección WEB de la CPS del PSC que emite el certificado. | NO |

| | | | |
|---|---|---|---|
| | [1,2]Información de certificador de directiva:<br>Id. de certificador de directiva=Aviso de usuario<br>Certificador:<br>Texto de aviso=Politica de certificacion F1 de Code100 S.A.<br>[1,3]Información de certificador de directiva:<br>Id. de certificador de directiva=Aviso de usuario<br>Certificador:<br>Texto de aviso=Code 100 S.A. Certificate Policy F1. | | |

## 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 Nº 13 – Estructura del campo subject de certificado de máquina o aplicación.

| CAMPO | EJEMPLO | DESCRIPCIÓN |
|---|---|---|
| C (Country)<br>{OID: 2.5.4.6} | PY | Código del país asignado de acuerdo al ISO 3166. |
| O (Organization)<br>{OID: 2.5.4.10} | APLICACIÓN | En este campo se identifica el tipo de certificado. En este caso se identifica que corresponde a un certificado de máquina o aplicación y puede ser MAQUINA O APLICACION, en mayúscula y sin tilde. |
| OU (Organization Unit)<br>{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; o CIFRADO C1. |

| | | |
|---|---|---|
| CN (Common Name)<br>{OID: 2.5.4.3} | SU APLICACION | 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<br>{OID: 2.5.4.5} | MRUC4785-3 | Este campo debe contener según sea el titular:<br>Persona Física:<br>• Las siglas MCI, seguidas del número de cédula de Identidad del titular del certificado, según documento de identificación.<br><br>Persona Jurídica:<br>• Las siglas MRUC, seguidas del número de cédula tributaria, según el documento de identificación. |

La estructura del certificado, referente a la extensión nombre alternativo del sujeto del certificado, es la que se describe como ejemplo en la siguiente tabla:

Tabla Nº 14 – Estructura de las extensiones del certificado de máquina o aplicación

| **EXTENSIONES CERTIFICADO DE MAQUINA O APLICACIÓN** | | | |
|---|---|---|---|
| **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 contiene 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 contiene 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<br>Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2)<br>Nombre alternativo:<br>Dirección URL=http://www.code100.com.py/crt/archivo.crt<br>[2]Acceso a información de autoridad<br>Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)<br>Nombre alternativo:<br>Dirección URL=http://www.code100.com.py/oscp | Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado del PSC.<br>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.<br>La primera entrada debe contener el método de acceso i d-ad-caIssuer, 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 |
| CRL Distribution Points (Puntos de distribución de CRL) | [1]Punto de distribución CRL<br>Nombre del punto de distribución:<br>Nombre completo:<br>Dirección URL=http://www.code100.com.py/crl/archivo.crl | Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a los certificados emitidos por el PSC CODE100 S.A., 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 solamente pueden ser activados los siguientes bits:digitalSignature;NonRepudiation (renombrado recientemente con el nombre de contentCommitmen); y keyEncipherment<br><br>En certificados tipo C1 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)<br>Autenticación de Cliente (1.3.6.1.5.5.7.3.2) | Referencia otros propósitos de la clave, adicionales al uso y debe ser consistente con la extensión keyUsage | SI |
| Subject Altenative Name (nombre alternativo del sujeto) | Rfc822Name=suapp@suaplicacion.com.py<br>DirectoryName<br>O=SUEMPRESA S. A.<br>CN=NARDI MAITE TORRES MANCUELLO<br>SERIALNUMBER= CI2319493<br>T=REPRESENTANTE LEGAL | Los datos a incluir en la extensión deben ser representados mediante la utilización de los siguientes campos:<br>No obligatorio<br>• Rfc822Name= [email del responsable del certificado]<br><br>Este campo debe contener según sea el titular:<br>Persona Física:<br>Obligatorio<br>• DirectoryName =2.5.4.3: [nombre y apellido del responsable del certificado]<br><br>Persona Jurídica<br>Obligatorio<br>• DirectoryName=2.5.4.10:[nombre de la organización titular del certificado]<br>• DirectoryName =2.5.4.3: [nombre y apellido del responsable del certificado]<br>• DirectoryName =2.5.4.5:<br><br>• CI [número de cédula de identidad correspondiente al responsable del certificado]<br><br>No obligatorio<br>• DirectoryName=2.5.4.12: [cargo que ocupa en la organización el responsable del certificado]<br><br>Los otros campos que compone la extensión "Subject Alternative Name" podrán ser utilizados en la forma y con los propósitos definidos | NO |

| | | | |
|---|---|---|---|
| | | por la RFC 5280 siempre y cuanto estén aprobados por la CA Raíz. | |
| Certificate Policies (Política del certificado) | [1]Directiva de certificados:<br>Identificador de directiva= [OID CP del PSC].<br>[1,1]Información de certificador de directiva:<br>Id. de certificador de directiva=CPS<br>Certificador:<br>http://www.code100.com.py/repositorio<br>[1,2]Información de certificador de directiva:<br>Id. de certificador de directiva=Aviso de usuario<br>Certificador:<br>Texto de aviso=[Texto de aviso en español]<br>[1,3]Información de certificador de directiva:<br>Id. de certificador de directiva=Aviso de usuario<br>Certificador:<br>Texto de aviso==[Texto de aviso en inglés] | 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

Estipulado en la CPS.

## 7.1.2 EXTENSIONES DEL CERTIFICADO

### Key Usage

El "keyusage" indica el uso del certificado de acuerdo con el RFC 5280 "Internet X.509Public Key Infrastructure Certificate and CRL Profile". Ver sección "1.4.1 Usos apropiados del certificado". Es una extensión crítica.

### Extensión de política de certificados

En la extensión de "certificatepolicies" (Directivas del Certificado) detalla el nombre del dominio elegido por el PSC CODE100 S.A y el directorio creado para el repositorio de dicho documentos. Es una extensión no crítica.

### Nombre alternativo del sujeto

La extensión "subjectAlternativeName" es utilizada para Certificados de Firma de Personas Físicas, Físicas con Datos Laborales y Jurídicas.

Para Certificados de Personas Físicas este campo debe incluir el email del titular persona física.

Para Certificados de Personas Jurídicas este campo debe incluir el email del titular persona jurídica, el nombre del titular persona física, según documento de identificación, en mayúsculas, CI (Número de Cédula de Identidad Paraguaya) y cargo en la institución.

Para Certificados de Personas Físicas con Datos Laborales este campo debe incluir el email del titular persona física, el nombre de la empresa a la que pertenece el titular, según documento de identificación de la misma y en mayúsculas, el RUC de la empresa a la que pertenece y el cargo en la institución.

El uso de esta extensión es "no crítico" y únicamente está permitido el uso del nombre DNS, en concordancia con la sección "4.1.2. Proceso de inscripción y responsabilidades".

En los certificados de personas jurídicas públicas o privadas deben incluirse los datos identificatorios de la persona física a cargo de la custodia de la clave privada del mismo. Los datos a incluir en la extensión deben ser representados mediante la utilización de campos de tipo "otherName" y son:

- **Nombre y apellido:** debe ser utilizado y contener el OID de "commonName" (OID 2.5.4.3: Nombre común) y debe respetar lo especificado para el atributo "commonName" de los certificados de personas físicas
- **Tipo y número de documento:** debe ser utilizado, y contener el OID de "serialNumber" (OID 2.5.4.5: Nro de serie) y debe respetar lo especificado para el atributo "serialNumber" de los certificados de personas físicas
- **Posición o función del suscriptor (Title):** Cuando corresponda será utilizado para indicar la relación que lo vincula con la persona jurídica titular del certificado, debe contener el OID de "title" (OID 2.5.4.12: Cargo o título).

### Restricciones básicas

Debe tener el valor ''cero", para indicar que el mismo no permite más sub-niveles en la ruta del certificado y en el caso del certificado de persona física o jurídica, este campo no debe especificarse. Es una extensión crítica.

### Uso extendido de la clave

La extensión permite configurar los propósitos de la clave. La extensión no es crítica.

#### Puntos de distribución de los CRL

La extensión "CRL DistributionPoints" (Puntos de Distribución) contiene las direcciones URL de la localización donde las partes que confían pueden obtener el CRL para verificar el estado del certificado. La extensión no es crítica.

#### Identificador de clave de Autoridad

El método para la generación del identificador está basado en la clave pública del PSC del certificado, de acuerdo a lo descrito por el RFC 5280 "Internet X.509 Public KeyInfraestructura Certificate and CRL Profile". La extensión no es crítica.

#### Identificador de la clave del sujeto

El método para la generación del identificador de clave está basado en la clave pública del sujeto del certificado y es calculado de acuerdo con uno de los métodos descritos en el RFC5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". La extensión no es crítica.

#### QcStatements

El "QcStatements" debe ser definido acorde al estándar ETSI-TS 101 862 V.1.3.3 "Qualified Certificate Profile". La extensión no es crítica.

## 7.1.3 IDENTIFICADORES DE OBJETO DE ALGORITMOS

Estipulado en la CPS de CODE100 S.A

## 7.1.4 FORMAS DEL NOMBRE

Estipulado en la CPS de CODE100 S.A

## 7.1.5 RESTRICCIONES DEL NOMBRE

Estipulado en la CPS de CODE100 S.A

### 7.1.6 IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO

Estipulado en la CPS de CODE100 S.A

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

Sin estipulaciones.

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

El calificador de la política está incluido en la extensión de "certificatepolicies" y contiene una referencia al URL con la CP aplicable y a los acuerdos de partes que confían.

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

Sin estipulaciones.

## 7.2 PERFIL DE LA CRL

Estipulado en la CPS de CODE100 S.A

### 7.2.1 NÚMERO (S) DE VERSIÓN

Estipulado en la CPS de CODE100 S.A

### 7.2.2 CRL Y EXTENSIONES DE ENTRADAS DE CRL

#### 7.2.2.1 NÚMERO CRL (CRL NUMBER)

Estipulado en la CPS de CODE100 S.A

#### 7.2.2.2 IDENTIFICADOR DE CLAVE DE AUTORIDAD

Estipulado en la CPS de CODE100 S.A

## 7.3 PERFIL DE OCSP

### 7.3.1 NÚMERO (S) DE VERSIÓN

Estipulado en la CPS de CODE100 S.A

### 7.3.2 EXTENSIONES DE OCSP

Sin estipulaciones.

# 8. AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

## 8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

Estipulado en la CPS de CODE100 S.A

## 8.2 IDENTIDAD/CALIDADES DEL EVALUADOR

Estipulado en la CPS de CODE100 S.A

## 8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA

Estipulado en la CPS de CODE100 S.A

## 8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN

Estipulado en la CPS de CODE100 S.A

## 8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA

Estipulado en la CPS de CODE100 S.A

## 8.6 COMUNICACIÓN DE RESULTADOS

Estipulado en la CPS de CODE100 S.A

# 9. OTROS ASUNTOS LEGALES Y COMERCIALES

## 9.1 TARIFAS

Estipulado en la CPS de CODE100 S.A.

### 9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

Estipulado en la CPS de CODE100 S.A.

### 9.1.2 TARIFAS DE ACCESO A CERTIFICADOS

Estipulado en la CPS de CODE100 S.A.

### 9.1.3 TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN

Estipulado en la CPS de CODE100 S.A.

### 9.1.4 TARIFAS POR OTROS SERVICIOS

Estipulado en la CPS de CODE100 S.A.

### 9.1.5 POLÍTICAS DE REEMBOLSO

Estipulado en la CPS de CODE100 S.A.

## 9.2 RESPONSABILIDAD FINANCIERA

### 9.2.1 COBERTURA DE SEGURO

Estipulado en la CPS de CODE100 S.A.

### 9.2.2 OTROS ACTIVOS

Estipulado en la CPS de CODE100 S.A.

### 9.2.3 COBERTURA DE SEGURO O GARANTÍA PARA USUARIOS FINALES

No estipulado.

## 9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

Estipulado en la CPS de CODE100 S.A.

### 9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

Estipulado en la CPS de CODE100 S.A.

### 9.3.2 INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL

Estipulado en la CPS de CODE100 S.A.

## 9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL

### 9.4.1 PLAN DE PRIVACIDAD

Estipulado en la CPS de CODE100 S.A.

### 9.4.2 INFORMACIÓN TRATADA COMO PRIVADA

Estipulado en la CPS de CODE100 S.A.

### 9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

Estipulado en la CPS de CODE100 S.A.

### 9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

Estipulado en la CPS de CODE100 S.A.

### 9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

Estipulado en la CPS de CODE100 S.A.

### 9.4.6 DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO

Estipulado en la CPS de CODE100 S.A.

### 9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

Estipulado en la CPS de CODE100 S.A.

## 9.5 DERECHO DE PROPIEDAD INTELECTUAL

CODE100 S.A. es propietaria exclusiva de todos los derechos de propiedad intelectual de la presente CP, acuerdos, declaraciones, procedimientos y documentos auxiliares referidos al PSC, así como la documentación y contenidos del sitio web del PSC que se encuentra en:

- http://www.code100.com.py/firma-digital

Asimismo, es titular del derecho de propiedad intelectual de las aplicaciones informáticas propias, excepto los sistemas operativos de soporte informáticos no desarrollados por CODE100 S.A. que cuentan con sus respectivas licencias de uso.

CODE100 S.A. es única y exclusiva propietaria de la presente CP, y sus documentos relacionados reservándose todos los derechos de autor establecidos en la legislación vigente de derechos de propiedad intelectual.

## 9.6 REPRESENTACIONES Y GARANTÍAS

### 9.6.1 REPRESENTACIONES Y GARANTÍAS DEL PSC

Estipulado en la CPS de CODE100 S.A.

### 9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA RA

Estipulado en la CPS de CODE100 S.A.

### 9.6.3 REPRESENTACIONES Y GARANTÍAS DEL SUSCRIPTOR

Estipulado en la CPS de CODE100 S.A.

### 9.6.4 REPRESENTACIONES Y GARANTÍAS DE LAS PARTES QUE CONFÍAN

Las partes que confían requieren conocer suficiente información para tomar la decisión de aceptar el certificado de acuerdo con lo que establece la CP del PSC de CODE100 S.A.

### 9.6.5 REPRESENTACIONES Y GARANTÍAS DEL REPOSITORIO.

Estipulado en la CPS de CODE100 S.A.

### 9.6.6 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES

Estipulado en la CPS de CODE100 S.A.

## 9.7 EXENCIÓN DE GARANTÍA

Estipulado en la CPS de CODE100 S.A.

## 9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL

Estipulado en la CPS de CODE100 S.A.

## 9.9 INDEMNIZACIONES

Estipulado en la CPS de CODE100 S.A.

## 9.10 PLAZO Y FINALIZACIÓN

### 9.10.1 PLAZO

La CP empieza a ser efectiva una vez publicada en su sitio de internet, previa aprobación del MIC, y los nuevos certificados deben ser emitidos cumpliendo las políticas determinadas en la nueva versión de la CP

### 9.10.2 FINALIZACIÓN

La CP de CODE100 S. A. estará en vigor mientras no se derogue expresamente por la emisión de una nueva versión, en ese caso, también se retirará del repositorio público del PSC CODE100 S.A.

### 9.10.3 EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

La finalización de la vigencia de la presente CP de CODE100 S.A, puede ser por derogación expresa, enmiendas o modificaciones; todos los certificados emitidos bajo esa declaración seguirán vigentes hasta que expiren o sean revocados, salvo que la nueva versión de la CP contemple aspectos críticos, en cuyo caso todos los certificados deberán ser revocados inmediatamente.

## 9.11 NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

Estipulado en la CPS de CODE100 S.A.

## 9.12 ENMIENDAS

### 9.12.1 PROCEDIMIENTOS PARA ENMIENDAS

Estipulado en la CPS de CODE100 S.A.

### 9.12.2 PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

Estipulado en la CPS de CODE100 S.A.

### 9.12.3 CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

Sin estipulaciones.

## 9.13 DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

Estipulado en la CPS de CODE100 S.A.

## 9.14 NORMATIVA APLICABLE

Estipulado en la CPS de CODE100 S.A.

## 9.15 ADECUACIÓN A LA LEY APLICABLE

La presente CP se adecua a legislación vigente aplicable a la materia.

## 9.15 ADECUACIÓN A LA LEY APLICABLE

No aplica.

### 9.16.2 ASIGNACIÓN

No aplica.

### 9.16.3 DIVISIBILIDAD

Estipulado en la CPS de CODE100 S.A.

### 9.16.4 APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DE DERECHOS)

No aplica.

### 9.16.5 FUERZA MAYOR

Estipulado en la CPS de CODE100 S.A.

## 9.17 OTRAS DISPOSICIONES

Estipulado en la CPS de CODE100 S.A.

# 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"
- Ley Nro. 4610/2012 que modifica y amplía la Ley Nro. 4017/2010
- Decreto Reglamentario Nro. 7369/2011.
- Resolución N° 1401/2016 del MIC "Por la cual se autoriza en carácter experimental, por el término de doce meses, la emisión de certificados de firma digital en módulo software para persona física".
- CP y CPS de la CA raíz del Paraguay.
- Directivas Obligatorias Para La Formulación Y Elaboración De La Práctica De Certificación De Los Prestadores De Servicios De Certificación (PSC) V1.0
- Directivas Obligatorias Para La Formulación Y Elaboración De La Política De Certificación De Los Prestadores De Servicios De Certificación (PSC) V1.0
- Características Mínimas De Seguridad Para La Autoridades De Registro De La Infraestructura De Claves Públicas Del Paraguay V 1.0
- Normas De Algoritmos Criptográficos PKI-Paraguay V1.0