POLÍTICA DE CERTIFICACIÓN F1

VERSIÓN 1.2

CLASE: PÚBLICO

INDICE

1. INTRODUCCIÓN 8
1.1 DESCRIPCIÓN GENERAL 8
1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO 8
1.3. PARTICIPANTES DE LA PKI 9
1.3.1. AUTORIDADES CERTIFICADORAS (CA) 9
1.3.2. AUTORIDADES DE REGISTROS (RA) 9
1.3.3. SUSCRIPTORES 9
1.3.4. PARTE QUE CONFÍA 9
1.3.5. OTROS PARTICIPANTES 10
1.3.5.1. PRESTADORES DE SERVICIO DE SOPORTE (PSS): 10
1.3.5.1. AUTORIDAD DE VALIDACIÓN (VA): 10
1.4. USO DEL CERTIFICADO 10
1.4.1 USOS APROPIADOS DEL CERTIFICADO 10
1.4.2. USOS PROHIBIDOS DEL CERTIFICADO 11
1.5 ADMINISTRACIÓN DE LA POLÍTICA 11
1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO 11
1.5.2. PERSONA DE CONTACTO 11
1.5.3. PERSONA QUE DETERMINA LA ADECUACIÓN DE LA CPS A LA POLÍTICA 11
1.5.4. PROCEDIMIENTOS DE APROBACIÓN DE LA CPS 11
1.6 DEFINICIONES Y ACRÓNIMOS 12
1.6.1 DEFINICIONES 12
1.6.2 ACRÓNIMOS 17

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO 19
2.1. REPOSITORIO 19
2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN 19
2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN 19
2.4 CONTROLES DE ACCESO 19

3. IDENTIFICACION Y AUTENTICACION 19
3.1. NOMBRE 19
3.1.1. TIPOS DE NOMBRES 19
3.1.2. NECESIDAD DE NOMBRES SIGNIFICATIVOS 19
3.1.3. ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES 19
3.1.4. REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES 19
3.1.5. UNICIDAD DE LOS NOMBRES 19
3.1.6. RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS 19
3.2. VALIDACIÓN INICIAL DE IDENTIDAD 19
3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA 19
3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA 19
3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA 19
3.2.4 INFORMACIÓN DEL SUSCRIPTOR NO VERIFICADA 19
3.2.5. VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO) 19
3.2.6. CRITERIOS PARA INTEROPERABILIDAD 19
3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RE EMISIÓN DE CLAVES 19
3.3.1 IDENTIFICACIÓN Y AUTENTICACIÓN PARA RE EMISIÓN DE CLAVES 19
3.3.2 IDENTIFICACIÓN Y AUTENTICACIÓN PARA LA RE EMISIÓN DE CLAVES DESPUÉS DE UNA REVOCACIÓN 20
3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN 20

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO 20
4.1. SOLICITUD DE CERTIFICADO 20
4.1.1. QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO 20
4.2. PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO 20
4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN 20
4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO 20
4.2.3. TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO 20
4.3. EMISIÓN DEL CERTIFICADO 20
4.3.1 ACCIONES DE LA CA DURANTE LA EMISIÓN DE LOS CERTIFICADOS 20
4.3.2 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DEL CERTIFICADO DIGITAL 20
4.4. ACEPTACIÓN DEL CERTIFICADO 20

4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO 20
4.4.2 PUBLICACIÓN DEL CERTIFICADO POR LA CA 20
4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA CA A OTRAS ENTIDADES 20
4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO 20
4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL SUSCRIPTOR 20
4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LA PARTE QUE CONFÍA 20
4.6 RENOVACIÓN DEL CERTIFICADO 20
4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO 21
4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN 21
4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO 21
4.6.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO 21
4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO 21
4.6.6 PUBLICACIÓN POR LA CA DEL CERTIFICADO 21
4.6.7 NOTIFICACIÓN POR LA CA DE LA EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES 21
4.7 RE-EMISIÓN DE CLAVES DE CERTIFICADO 21
4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO 21
4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA 21
4.7.3 PROCESAMIENTO DE SOLICITUDES DE RE-EMISIÓN DE CLAVES DE CERTIFICADO 21
4.7.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA RE-EMISIÓN DE UN NUEVO CERTIFICADO 21
4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE-EMITIDO 21
4.7.6 PUBLICACIÓN POR LA CA DE LOS CERTIFICADOS RE-EMITIDOS 21
4.7.7 NOTIFICACIÓN POR LA CA DE LA RE-EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES 21
4.8 MODIFICACIÓN DE CERTIFICADOS 21
4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO 21
4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO 21
4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO 21
4.8.4 NOTIFICACIÓN AL SUSCRIPTOR DE LA EMISIÓN DE UN NUEVO CERTIFICADO 21
4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO 21
4.8.6 PUBLICACIÓN POR LA CA DE LOS CERTIFICADOS MODIFICADOS 21
4.8.7 NOTIFICACIÓN POR LA CA DE EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES 21
4.9 REVOCACIÓN Y SUSPENSIÓN 22
4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN 22
4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN 22
4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN 22
4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN 22
4.9.5 TIEMPO DENTRO DEL CUAL LA CA DEBE PROCESAR LA SOLICITUD DE REVOCACIÓN 22
4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LAS PARTES QUE CONFÍAN 22
4.9.7 FRECUENCIA DE EMISIÓN DEL CRL 22
4.9.8 LATENCIA MÁXIMA PARA CRL 22
4.9.9 REQUISITOS DE VERIFICACIÓN DE CRL 22
4.9.10 DISPONIBILIDAD DE VERIFICACIÓN DE REVOCACIÓN / ESTADO EN LÍNEA 22
4.9.11 REQUERIMIENTOS PARA VERIFICAR LA REVOCACIÓN EN LÍNEA 22
4.9.12 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES 22
4.9.13 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA 22
4.9.14 CIRCUNSTANCIAS PARA SUSPENSIÓN 22
4.9.15 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN 22
4.9.16 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN 22
4.9.17 LÍMITES DE PERÍODO DE SUSPENSIÓN 22
4.10 SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADO 22
4.10.1 CARACTERÍSTICAS OPERACIONALES 22
4.10.2 DISPONIBILIDAD DEL SERVICIO 22
4.10.3 CARACTERÍSTICAS OPCIONALES 22
4.11 FIN DE LA SUSCRIPCIÓN 22
4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES 22
4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES 22
4.12.2 POLÍTICAS Y PRÁCTICAS DE RECUPERACIÓN Y ENCAPSULACIÓN DE CLAVES DE SESIÓN 22
5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES 23
5.1 CONTROLES FÍSICOS 23
5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO 23
5.1.2 ACCESO FÍSICO 23
5.1.2.1 NIVELES DE ACCESO FÍSICO 23

5.1.3 ENERGÍA Y AIRE ACONDICIONADO 23
5.1.4 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO 23
5.1.5 ALMACENAMIENTO DE MEDIOS 23
5.1.6 ELIMINACIÓN DE RESIDUOS 23
5.1.7 RESPALDO FUERA DE SITIO 23
5.1.8 INSTALACIONES TÉCNICAS DE LA RA 23
5.2 CONTROLES PROCEDIMENTALES 23
5.2.1 ROLES DE CONFIANZA 23
5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA 23
5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL 23
5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES 23
5.3 CONTROLES DE PERSONAL 23
5.3.1 REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN 23
5.3.2 PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES 23
5.3.3 REQUERIMIENTOS DE CAPACITACIÓN 23
5.3.4 REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN 23
5.3.5 FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES 23
5.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS 23
5.3.7 REQUISITOS DE CONTRATACIÓN A TERCEROS 23
5.3.8 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL 23
5.4 PROCEDIMIENTO DE REGISTRO DE AUDITORÍA 23
5.4.1 TIPOS DE EVENTOS REGISTRADOS 24
5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS) 24
5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA 24
5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA 24
5.4.5 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE REGISTRO (LOGS) DE AUDITORÍA 24
5.4.6 SISTEMA DE RECOLECCIÓN DE INFORMACIÓN DE AUDITORÍA (INTERNO VS EXTERNO) 24
5.4.7 NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO 24
5.4.8 EVALUACIÓN DE VULNERABILIDADES 24
5.5.1 TIPOS DE REGISTROS ARCHIVADOS 24
5.5.2 PERIODOS DE RETENCIÓN PARA ARCHIVOS 24
5.5.3 PROTECCIÓN DE ARCHIVOS 24
5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO 24
5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS 24
5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO) 24
5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA 24
5.6 CAMBIO DE CLAVE 24
5.7 RECUPERACIÓN DE DESASTRES Y COMPROMISO 24
5.7.1 PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO 24
5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES 24
5.7.3 PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD 24
5.7.4 CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE 24
5.7.5 ACTIVIDADES DE LAS AUTORIDADES DE REGISTRO 24
6. CONTROLES TÉCNICOS DE SEGURIDAD 25
6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES 25
6.1.1 GENERACIÓN DEL PAR DE CLAVES 25
6.1.2 ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR 25
6.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO 26
6.1.4 ENTREGA DE LA CLAVE PÚBLICA DE LA CA A LAS PARTES QUE CONFÍAN 26
6.1.5 TAMAÑO DE LA CLAVE 26
6.1.6 GENERACIÓN DE PARÁMETROS DE CLAVES ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD 26
6.1.7 PROPÓSITOS DE USOS DE CLAVE (CAMPO KEY USAGE X509 V3) 26
6.1.8 GENERACIÓN DE CLAVE POR HARDWARE O SOFTWARE 26
6.2 CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO Y PROTECCIÓN DE LA CLAVE PRIVADA 26
6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO 27
6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA 27
6.2.3 CUSTODIA/RECUPERACIÓN DE LA CLAVE PRIVADA 27
6.2.4 RESPALDO/COPIA DE LA CLAVE PRIVADA 27
6.2.5 ARCHIVADO DE LA CLAVE PRIVADA 27

6.2.6 TRANSFERENCIA DE CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRIPTOGRÁFICO 27
6.2.7 ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO 27
6.2.8 MÉTODO DE ACTIVACIÓN DE CLAVE PRIVADA 28
6.2.9 MÉTODOS DE DESACTIVACIÓN DE LA CLAVE PRIVADA 28
6.2.10 DESTRUCCIÓN DE CLAVE PRIVADA 28
6.2.11 CLASIFICACIÓN DEL MÓDULO CRIPTOGRÁFICO 28
6.3 OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES 28
6.3.1 ARCHIVO DE LA CLAVE PÚBLICA 28
6.3.2 PERÍODO OPERACIONAL DEL CERTIFICADO Y PERÍODO DE USO DEL PAR DE CLAVES 28
6.4 DATOS DE ACTIVACIÓN 28
6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN 28
6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN 29
6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN 29
6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR 29
6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS 29
6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR 29
6.5.3 CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO 29
6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA 30
6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA 30
6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD 30
6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA 30
6.6.4 CONTROLES EN LA GENERACIÓN DE CRL 30
6.7 CONTROLES DE SEGURIDAD DE RED 30
6.7.1 DIRECTRICES GENERALES 30
6.7.2 FIREWALL 30
6.7.3 SISTEMA DE DETECCIÓN DE INTRUSO (IDS) 30
6.7.4 REGISTRO DE ACCESO NO AUTORIZADO A LA RED 30
6.8 CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO 30

7. PERFILES DE CERTIFICADOS, CRL Y OCSP 31
7.1 Perfil del Certificado 31
7.1.1 NÚMERO DE VERSIÓN 41
7.1.2 EXTENSIONES DEL CERTIFICADO 41
7.1.3 IDENTIFICADORES DE OBJETO DE ALGORITMOS 43
7.1.4 FORMAS DEL NOMBRE 43
7.1.5 RESTRICCIONES DEL NOMBRE 43
7.1.6 IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO 43
7.1.7 USO DE LA EXTENSIÓN RESTRICCIONES DE POLÍTICA (POLICYCONSTRAINTS) 44
7.1.8 SEMÁNTICA Y SINTAXIS DE LOS CALIFICADORES DE POLÍTICA (POLICYQUALIFIERS) 44
7.1.9 SEMÁNTICA DE PROCESAMIENTO PARA LA EXTENSIÓN DE POLÍTICAS DE CERTIFICADO (CERTIFICATEPOLICIES) 44
7.2 Perfil de la CRL 44
7.2.1 Número (s) de versión 45
7.2.2 CRL y extensiones de entradas de CRL 45
7.3 PERFIL DE OCSP 45
7.3.1 NÚMERO (S) DE VERSIÓN 45
7.3.2 EXTENSIONES DE OCSP 45

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES 45
8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN 45
8.2 IDENTIFICACIÓN/CALIFICACIÓN DEL EVALUADOR 45
8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA 45
8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN 45
8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA 45
8.6 COMUNICACIÓN DE RESULTADOS 45

9. OTROS ASUNTOS LEGALES Y COMERCIALES 46
9.1 TARIFAS 46
9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS 46
9.1.2 TARIFAS DE ACCESO A CERTIFICADOS 46
9.1.3 TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN 46
9.1.4 TARIFAS POR OTROS SERVICIOS 46
9.1.5 POLÍTICAS DE REEMBOLSO 46

9.2 RESPONSABILIDAD FINANCIERA 46
9.2.1 COBERTURA DE SEGURO 46
9.2.2 OTROS ACTIVOS 46
9.2.3 COBERTURA DE SEGURO O GARANTÍA PARA USUARIOS FINALES 46
9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL 46
9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL 46
9.3.2 INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL 46
9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL 46
9.4.1 PLAN DE PRIVACIDAD 46
9.4.2 INFORMACIÓN TRATADA COMO PRIVADA 46
9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA 46
9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA 46
9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA 46
9.4.6 DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO 46
9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN 46
9.5 DERECHO DE PROPIEDAD INTELECTUAL 46
9.6 REPRESENTACIONES Y GARANTÍAS 46
9.6.1 REPRESENTACIONES Y GARANTÍAS DEL PSC 46
9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA RA 47
9.6.3 REPRESENTACIONES Y GARANTÍAS DEL SUSCRIPTOR 47
9.6.4 REPRESENTACIONES Y GARANTÍAS DE LAS PARTES QUE CONFÍAN 47
9.6.5 REPRESENTACIONES Y GARANTÍAS DEL REPOSITORIO 47
9.6.6 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES 47
9.7 EXENCIÓN DE GARANTÍA 47
9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL 47
9.8.1 LIMITACIONES DE LA RESPONSABILIDAD DEL PSC 47
9.9 INDEMNIZACIONES 47
9.10 PLAZO Y FINALIZACIÓN 47
9.10.1 PLAZO 47
9.10.2 FINALIZACIÓN 47
9.10.3 EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA 47
9.11 NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES 47
9.12 ENMIENDAS 47
9.12.1 PROCEDIMIENTOS PARA ENMIENDAS 47
9.12.2 PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN 47
9.12.3 CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS 47
9.13 DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS 47
9.14 NORMATIVA APLICABLE 47
9.15 ADECUACIÓN A LA LEY APLICABLE 47
9.16 DISPOSICIONES VARIAS 47
9.16.1 ACUERDO COMPLETO 47
9.16.2 ASIGNACIÓN 47
9.16.3 DIVISIBILIDAD 47
9.16.4 APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DE DERECHOS) 47
9.16.5 FUERZA MAYOR 47
9.17 OTRAS DISPOSICIONES 47
10. DOCUMENTOS DE REFERENCIA 48

Control documental

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 S.A.
Documento Público	https://www.code100.com.py/firma-digital/

CONTROL DEL DOCUMENTO		
Preparado por:	**Revisado por:**	**Aceptado por:**
Rocio Vazquez	Elizabeth Aguilar	Directivo CODE100 S.A.

DOCUMENTO	
Título: **POLÍTICA DE CERTIFICACIÓN F1**	Nombre del Archivo:CODE100.Politica de Certificacion F1 v1.3.docx
Código: **CODE100.Politica de Certificacion F1 v1.3**	SOPORTE LÓGICO: https://www.code100.com.py/firma-digital/
FECHA: 14/02/2020	Ubicación Física: CODE100 S.A
Versión: 1.3	

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
Versión 1.2	28/08/2018	Adecuación a observaciones de Auditoría
Versión 1.3	14/02/2020	Adecuación Resolución N° 1434/2019 del MIC

1. INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL

La infraestructura de Clave Pública del Paraguay es una plataforma criptográfica confiable que garantiza la presunción de validez legal para actos y negocios electrónicos firmados o cifrados con certificados digitales y claves emitidas en el marco de la PKI Paraguay.

Está CP describe la Política de Certificación del PSC CODE100 S. A. para **certificados de Firma Digital Tipo F1** en el marco de la PKI Paraguay.

La estructura de esta CPS se basa en lo estipulado en la **Resolución MIC N° 1434/2019 ANEXO I: DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA POLÍTICA DE CERTIFICACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC)**

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

Tipos de certificados de firma digital

I. F1

II. F2

Tipos de certificados de cifrado

I. C1

II. C2

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

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

1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Nombre:	Política de Certificación F1 de CODE100 S.A.
Versión:	1.3
OID:	1.3.6.1.4.1.55152.1.1.2
Fecha de aprobación:	14/02/2020
Ubicación de la CPS:	https://www.code100.com.py/firma-digital/

1.3. PARTICIPANTES DE LA PKI

1.3.1. AUTORIDADES CERTIFICADORAS (CA)

Esta CP se refiere exclusivamente al PSC CODE100 S. A. dentro del ámbito de la PKI Paraguay.

Las prácticas y procedimientos de certificación del PSC CODE100 S. A. se describen en su Declaración de Prácticas de Certificación.

1.3.2. AUTORIDADES DE REGISTROS (RA)

Los datos referentes a las RA habilitadas por CODE100 S.A. para los procesos de recepción validación y direccionamiento de solicitudes de emisión o de revocación de los certificados digitales, y de identificación de sus solicitantes. se encuentran en la dirección de página web (URL) http://www.code100.com.py/autoridad-de-registro

El PSC CODE100 S.A. mantiene publicada en el sitio las siguientes informaciones actualizadas:

- Identificación y vinculación de todas las RA habilitadas, con informaciones sobre las CP que implementan.
- Para cada RA habilitada, las direcciones de sus instalaciones técnicas, cuyo funcionamiento haya sido autorizado por la CA Raíz.
- Para cada RA habilitada, el tipo de vínculo con eventuales locales provisorios autorizados por la CA Raíz, con fecha de creación y cierre de actividades;
- Identificación y vínculo de las RA deshabilitadas dentro de la cadena PKI Paraguay, con su respectiva fecha de cese de actividades;
- Instalaciones técnicas de la RA habilitada que ha dejado de operar, con su respectiva fecha de cierre de actividades;
- Acuerdos operacionales celebrados entre las RA vinculadas con otra RA dentro de la PKI Paraguay, si fuera el caso.

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

1.3.3. SUSCRIPTORES

Es suscriptor toda persona física o jurídica a quien se emite un certificado digital dentro de la jerarquía PKI Paraguay. Es obligación de todo suscriptor el conocimiento de la presente CPS, así como de la normativa vigente.

En el caso de un certificado emitido para maquina o aplicación, el titular será persona física o jurídica que solicita el certificado.

1.3.4. PARTE QUE CONFÍA

Se entenderá por parte que confía, toda persona física o jurídica, diferente al titular del certificado que decide aceptar y confiar en el contenido, la validez y la aplicabilidad de un certificado digital y los claves emitidos dentro de la jerarquía PKI Paraguay

Una parte que confía puede o no ser un suscriptor.

1.3.5. OTROS PARTICIPANTES

1.3.5.1. PRESTADORES DE SERVICIO DE SOPORTE (PSS):

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

a) Disponibilización de infraestructura física y lógica;

b) Disponibilización de recursos humanos especializados;

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

Los PSS de CODE100 S.A. se publicarán en el sitio:

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

El PSC CODE100 S.A. mantiene las informaciones, arriba citadas, siempre actualizadas.

1.3.5.1. AUTORIDAD DE VALIDACIÓN (VA):

La VA puede ser una entidad propia o externa al PSC CODE100 S.A. 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.

Toda información referente a la VA se encuentran disponibles en la web: https://www.code100.com.py/autoridad-de-validacion

1.4. USO DEL CERTIFICADO

1.4.1 USOS APROPIADOS DEL CERTIFICADO

Este ítem enumera las aplicaciones para las cuales los certificados definidos en esta CP son adecuados.

Las aplicaciones y otros programas que permiten el uso de un certificado digital de cierto tipo contemplado por la PKI Paraguay deben aceptar cualquier certificado del mismo tipo, o superior, emitido por cualquier PSC acreditado por CA Raíz.

El PSC CODE100 S. A. tiene en cuenta el nivel de seguridad proporcionado para el certificado definido por esta CP en la definición de aplicaciones para el certificado. Este nivel de seguridad se caracteriza por los requisitos definidos para aspectos tales como: tamaño de clave criptográfica, medios de almacenamiento de claves, proceso de generación de pares de claves, procedimientos de identificación del titular del certificado, frecuencia de emisión de la correspondiente Lista de Certificados Revocados y extensión del período de validez del certificado.

Los certificados emitidos por PSC CODE100 S. A. dentro del alcance de esta CP se pueden usar en aplicaciones como la verificación de identidad y la firma de documentos electrónicos con la verificación de la integridad de su información.

Los certificados de los tipos F1, F2 se utilizarán en aplicaciones como la confirmación de identidad y la firma de documentos electrónicos con la verificación de la integridad de su información.

Los certificados de los tipos C1, C2 se utilizarán en aplicaciones como el cifrado de documentos, bases de datos, mensajes y otra información electrónica, para garantizar su confidencialidad.

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: Benjamín Constant 973, Edificio Arasá 2, Oficina 12

Teléfono: *(+59521) 445 601/2*

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: Benjamín Constant 973, Edificio Arasá 2, Oficina 12

Teléfono: *(+59521) 445 601/2*

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

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

La entidad competente para determinar la adecuación de esta CPS a las diferentes políticas de certificación de CODE100 S.A. es el personal autorizado por el representante legal conforme a los estatutos de CODE100 S.A.

1.5.4. PROCEDIMIENTOS DE APROBACIÓN DE LA CPS

Esta CP está aprobada por el MIC.

Los procedimientos de aprobación para esta CPS de CODE100 S. A. se establecen a criterio de la Dirección General de Firma Digital y Comercio Electrónico del MIC.

1.6 DEFINICIONES Y ACRÓNIMOS

1.6.1 DEFINICIONES

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

Agente de Registro Validador: Persona responsable de la ejecución de actividades relacionadas con la RA, que realiza el proceso de validación de la solicitud del certificado de firma digital.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

en la protección que brinda a la clave privada y asegura la confianza en los certificados digitales emitidos por la CA.

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

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

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

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

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

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

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

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

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

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

datos que produzcan el mismo código de verificación al usar el mismo algoritmo.

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

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

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 documento 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 almacenas 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 criptosistema asimétrico. La clave privada y la clave pública están relacionadas matemáticamente y poseen ciertas propiedades, entre ellas que es imposible deducir la clave privada de la clave pública conocida.

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

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

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

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

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

Período de uso: 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 por la AA, encargada de operar una CA en el marco de la PKI Paraguay. El PSC debe contar con un certificado digital emitido por la CA Raíz del Paraguay y solo podrá emitir certificados a usuarios finales.

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

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

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

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

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

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

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

Acrónimo	Descripción
C	País (C por sus siglas en inglés, Country)
CA	Autoridad Certificadora (CA por sus siglas en inglés Certificate Authority)
CAI	Autoridad de Certificación Intermedia (Certificate Authority Intermediate)
CA Raíz	Raíz Autoridad Certificadora Raíz del Paraguay
CI	Cédula de identidad
CN	Nombre común (CN por sus siglas en inglés, Common Name)
CP	Políticas de Certificación (CP por sus siglas en inglés Certificate Policy)
CPS	Declaración de Prácticas de Certificación (CPS por sus siglas en inglés Certification Practice Statement)
CRL	Lista de certificados revocados (CRL por sus siglas en inglés Certificate Revocation List)
CSR	Solicitud de firma de Certificado (CSR por sus siglas en inglés Certificate Signing Request)
DGFD&CE	Dirección General de Firma Digital y Comercio Electrónico dependiente de la Subsecretaría de Estado 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 (ISO por sus siglas en inglés International Organization for Standardization)
ITU-T	Unión Internacional de Telecomunicaciones – Sector de Normalización de las telecomunicaciones (ITU-T por sus siglas en inglés International Telecomunication Union – Telecomunication Standardization Sector)

MIC	Ministerio de Industria y Comercio
O	Organización (por su sigla en inglés, Organization)
OCSP	Servicio de validación de certificados en línea (OCSP por sus siglas en inglés Online Certificate Status Protocol)
OID	Identificador de Objeto (OID por sus siglas en inglés Object Identifier)
OU	Unidad Organizacional (OU, por sus siglas en inglés Organization Unit)
PIN	Número de Identificación Personal (por su sigla en inglés Personal Identification Number)
PKCS	Norma de criptografía de clave pública (PKCS por sus sigla en inglés Public Key Cryptography Standard)
PKI	Infraestructura de Clave Pública (PKI por sus siglas en inglés Public Key Infrastructure).
PSC	Prestador de Servicios de Certificación
PY	Paraguay
RA	RA (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)
(sacar ssl y sms)TLS	Capa de conexión segura (TLS por sus sigls en inglés, Transport Layer Security)
UPS	Sistemas de alimentación ininterrumpida (UPS por sus sigla 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 sigla en inglés Validation Authority)

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

Los ítems siguientes son referidos en los puntos correspondientes de la CPS de CODE100 S. A.

2.1. REPOSITORIO
2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN
2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN
2.4 CONTROLES DE ACCESO

3. IDENTIFICACION Y AUTENTICACION

Los ítems siguientes son referidos en los puntos correspondientes de la CPS de CODE100 S.A.

3.1. NOMBRE

3.1.1. TIPOS DE NOMBRES
3.1.2. NECESIDAD DE NOMBRES SIGNIFICATIVOS
3.1.3. ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES
3.1.4. REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES
3.1.5. UNICIDAD DE LOS NOMBRES
3.1.6. RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS
3.2. VALIDACIÓN INICIAL DE IDENTIDAD
3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA
3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA
3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA
3.2.4 INFORMACIÓN DEL SUSCRIPTOR NO VERIFICADA
3.2.5. VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)
3.2.6. CRITERIOS PARA INTEROPERABILIDAD

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

3.3.1 IDENTIFICACIÓN Y AUTENTICACIÓN PARA RE EMISIÓN DE CLAVES

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

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

Los ítems siguientes son referidos en los puntos correspondientes de la CPS de CODE100 S. A.

4.1. SOLICITUD DE CERTIFICADO

4.1.1. QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

4.2. PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

4.2.3. TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO

4.3. EMISIÓN DEL CERTIFICADO

4.3.1 ACCIONES DE LA CA DURANTE LA EMISIÓN DE LOS CERTIFICADOS

4.3.2 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DEL CERTIFICADO DIGITAL

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR LA CA

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

4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

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

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

4.6 RENOVACIÓN DEL CERTIFICADO

4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO

4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN

4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO

4.6.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO

4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO

4.6.6 PUBLICACIÓN POR LA CA DEL CERTIFICADO

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

4.7 RE-EMISIÓN DE CLAVES DE CERTIFICADO

4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO

4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA

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

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

4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE-EMITIDO

4.7.6 PUBLICACIÓN POR LA CA DE LOS CERTIFICADOS RE-EMITIDOS

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

4.8 MODIFICACIÓN DE CERTIFICADOS

4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO

4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

4.8.4 NOTIFICACIÓN AL SUSCRIPTOR DE LA EMISIÓN DE UN NUEVO CERTIFICADO

4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

4.8.6 PUBLICACIÓN POR LA CA DE LOS CERTIFICADOS MODIFICADOS

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

4.9 REVOCACIÓN Y SUSPENSIÓN

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN

4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

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

4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LAS PARTES QUE CONFÍAN

4.9.7 FRECUENCIA DE EMISIÓN DEL CRL

4.9.8 LATENCIA MÁXIMA PARA CRL

4.9.9 REQUISITOS DE VERIFICACIÓN DE CRL

4.9.10 DISPONIBILIDAD DE VERIFICACIÓN DE REVOCACIÓN / ESTADO EN LÍNEA

4.9.11 REQUERIMIENTOS PARA VERIFICAR LA REVOCACIÓN EN LÍNEA

4.9.12 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES

4.9.13 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA

4.9.14 CIRCUNSTANCIAS PARA SUSPENSIÓN

4.9.15 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

4.9.16 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

4.9.17 LÍMITES DE PERÍODO DE SUSPENSIÓN

4.10 SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADO

4.10.1 CARACTERÍSTICAS OPERACIONALES

4.10.2 DISPONIBILIDAD DEL SERVICIO

4.10.3 CARACTERÍSTICAS OPCIONALES

4.11 FIN DE LA SUSCRIPCIÓN

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

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

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

Los ítems siguientes son referidos en los puntos correspondientes de la CPS de CODE100 S. A.

5.1 CONTROLES FÍSICOS

5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

5.1.2 ACCESO FÍSICO

5.1.2.1 NIVELES DE ACCESO FÍSICO

5.1.3 ENERGÍA Y AIRE ACONDICIONADO

5.1.4 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

5.1.5 ALMACENAMIENTO DE MEDIOS

5.1.6 ELIMINACIÓN DE RESIDUOS

5.1.7 RESPALDO FUERA DE SITIO

5.1.8 INSTALACIONES TÉCNICAS DE LA RA

5.2 CONTROLES PROCEDIMENTALES

5.2.1 ROLES DE CONFIANZA

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES

5.3 CONTROLES DE PERSONAL

5.3.1 REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

5.3.2 PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

5.3.3 REQUERIMIENTOS DE CAPACITACIÓN

5.3.4 REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

5.3.5 FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

5.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS

5.3.7 REQUISITOS DE CONTRATACIÓN A TERCEROS

5.3.8 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

5.4 PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

5.4.1 TIPOS DE EVENTOS REGISTRADOS

5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)

5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

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

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

5.4.7 NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

5.4.8 EVALUACIÓN DE VULNERABILIDADES

5.5 ARCHIVOS DE REGISTROS

5.5.1 TIPOS DE REGISTROS ARCHIVADOS

5.5.2 PERIODOS DE RETENCIÓN PARA ARCHIVOS

5.5.3 PROTECCIÓN DE ARCHIVOS

5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO

5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO)

5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA

5.6 CAMBIO DE CLAVE

5.7 RECUPERACIÓN DE DESASTRES Y COMPROMISO

5.7.1 PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO

5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES

5.7.3 PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD

5.7.4 CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

5.7.5 ACTIVIDADES DE LAS AUTORIDADES DE REGISTRO

5.8 EXTINCIÓN DE UN PSC

6. CONTROLES TÉCNICOS DE SEGURIDAD

6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1 GENERACIÓN DEL PAR DE CLAVES

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

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

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 CA raíz del Paraguay, conforme a lo estipulado en la siguiente tabla:

Tipo de certificado	Medio de almacenamiento
F1	repositorio protegido por contraseña y/o identificación 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:

- La clave privada es única y su confidencialidad es suficientemente asegurada;
- 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
- 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 F2 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

La clave pública generada bajo control del usuario final es entregada a CODE100 S.A. mediante el envío de una solicitud de firma de certificado (CSR) que concuerda con la especificación del PKCS#10, firmado digitalmente con la clave privada correspondiente a la clave pública que se solicita certificar. En el caso que el par de claves del usuario final sea generado por el PSC, este requisito no es aplicable.

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

El certificado del PSC CODE100 S.A. así como el certificado de la ACRAIZ, que forman la cadena de certificación se encuentran disponibles en el repositorio público del PSC CODE100 S.A. (https://www.code100.com.py/firma-digital/)
Los certificados de las entidades finales se encuentran disponibles en el sitio de consultas y descargas de certificados del PSC CODE100 S.A.
(https://ca1.code100.com.py/ServicioDescargas.aspx)

6.1.5 TAMAÑO DE LA CLAVE

El tamaño de clave para certificados de tipo F2 es de 2048 bits, como se define en el definen en el documento **NORMAS DE ALGORITMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY**

6.1.6 GENERACIÓN DE PARÁMETROS DE CLAVES ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD

- Se prevé que los parámetros de generación de claves asimétricas de las entidades titulares de certificados adoptaran el patrón definido en el documento **NORMAS Y ALGORITMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**
- Los parámetros de verificación de calidad, son verificados de acuerdo con las normas establecidas por el patrón definido en el documento **NORMAS DE ALGORITMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

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

La clave privada de las entidades titulares de certificados tipo F1 se utilizará para Firma Digital, No repudio, y Cifrado de Clave.

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 un repositorio protegido por contraseña y/o identificación biométrica, cifrado por 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 F2, es el FIPS 140-2 nivel 1 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 F2 no se encuentran bajo control multi-persona. 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 F2 la realizan los propios titulares de la misma.

6.2.4 RESPALDO/COPIA DE LA CLAVE PRIVADA

Con la excepción de las claves privadas vinculadas a los certificados de tipo F, que no pueden tener copia de seguridad, cualquier titular de un certificado de otro tipo puede, a su criterio, mantener una copia de su propia clave privada.
El PSC CODE100 S.A. no podrá mantener una copia de seguridad de la clave privada del titular del certificado de firma digital (Tipo F)
En cualquier caso, la copia de seguridad deberá ser almacenada cifrada por algoritmo simétrico adoptado por el documento **NORMAS DE ALGORITMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY**, y protegida con un nivel de seguridad no inferior para aquel definido para la clave original.

6.2.5 ARCHIVADO DE LA CLAVE PRIVADA

Las claves son archivadas en un nivel de seguridad no inferior a aquella definida para la clave original. No son archivadas las claves privadas del titular de certificado de firma digital.

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

6.2.6 TRANSFERENCIA DE CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRIPTOGRÁFICO

La clave privada del PSC CODE100 S.A. puede ser exportada del módulo criptográfico únicamente para propósitos de respaldo.

6.2.7 ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

El PSC CODE100 S.A. no mantiene almacenada la clave privada del titular de certificado de firma digital por ella emitida.

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 (contraseñas, tokens o biometría).

6.2.9 MÉTODOS DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Sin estipulaciones.

6.2.10 DESTRUCCIÓN DE CLAVE PRIVADA

La destrucción de la clave privada la podrá efectuar el titular de la misma mediante el uso de al menos un factor de seguridad (contraseñas, tokens o biometría).

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 ALGORITMOS 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 sus titulares deberán ser utilizadas únicamente durante el periodo de validez correspondiente. Las correspondientes claves públicas podrán ser utilizadas durante todo el periodo de tiempo determinado por la normativa vigente, para la verificación de firmas generadas durante el plazo de validez de los respectivos certificados.

TIPO DE CERTIFICADO	PERIODO DE VALIDEZ (En años)
F1	1

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

Los datos de activación de la clave privada del titular del certificado, si se utilizan, están protegidos, mediante contraseña y/o PIN, contra uso no autorizado.

6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Sin estipulaciones.

6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

Cada computador del PSC CODE100 S.A., relacionado directamente con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificado, deberá implementar, entre otras, las siguientes características:

a) Control de acceso a los servicios y perfiles del PSC;
b) Clara segregación de tareas y atribuciones relacionadas con cada rol de confianza del PSC;
c) Uso de criptografía para seguridad de base de datos, cuando sea requerido por la clasificación de su información;
d) Generación y almacenamiento de registros de auditoría del PSC;
e) Mecanismos internos de seguridad para garantizar la integridad de datos y procesos críticos; y
f) Mecanismos para copias de seguridad (backup).

Estas características deberán ser implementadas por el sistema operativo o por medio de combinación de este con el sistema de certificación y con mecanismos de seguridad física.

6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

Ítem no aplicable.

6.5.3 CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO

Ítem no aplicable.

6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA

El PSC CODE100 S.A. utiliza los modelos espiral y SCRUM en el desarrollo de sistemas, de acuerdo con la mejor idoneidad de estos modelos para el proyecto en desarrollo. Las fases que se llevan a cabo son: requisitos, análisis, diseño, codificación y prueba para cada interacción del sistema utilizando Orientación a objetos.

Para respaldar este modelo, El PSC CODE100 S.A. utiliza la gestión configuración, gestión de cambios, pruebas formales y otros procesos.

6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

El PSC CODE100 S.A. verifica los niveles de seguridad configurados mensualmente y a través de herramientas del propio sistema operativo. Los controles se realizan emitiendo comandos del sistema y comparación con configuraciones aprobadas. En caso de divergencia, son tomadas las medidas para la recuperación de la situación, de acuerdo con la naturaleza y la investigación de la causa del problema, para evitar su recurrencia.

El PSC CODE100 S.A. utiliza una metodología formal de gestión de configuración para la instalación y el mantenimiento continuo del sistema.

6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

El PSC CODE100 S.A implementa controles de seguridad en torno a los sistemas involucrados en el ciclo de vida de certificados

6.6.4 CONTROLES EN LA GENERACIÓN DE CRL

Antes de su publicación, todas las CRL generadas por el PSC, es comprobada la consistencia de su contenido, comparándolo con el contenido esperado en relación al número el CRL, la fecha / hora de emisión otras informaciones relevantes.

6.7 CONTROLES DE SEGURIDAD DE RED

Ítem no aplicable.

6.7.1 DIRECTRICES GENERALES

6.7.2 FIREWALL

6.7.3 SISTEMA DE DETECCIÓN DE INTRUSO (IDS)

6.7.4 REGISTRO DE ACCESO NO AUTORIZADO A LA RED

6.8 CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO

Según el ítem 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 debe cumplir 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"

Certificado de Persona Física

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

Tabla Nº 5 Estructura del campo subject certificado de persona física.

CAMPO	EJEMPLO	DESCRIPCIÓN
C (Country) {OID: 2.5.4.6}	PY	Este campo debe contener el código del país asignado de acuerdo al ISO 3166.
O (Organization) {OID: 2.5.4.10}	PERSONA FISICA	En este campo se identifica el tipo de certificado. En este caso se identifica que corresponde a un certificado de persona física y se debe indicar PERSONA FISICA, en mayúscula y sin tilde.
OU (OrganizationUnit) {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.
CN (CommonName) {OID: 2.5.4.3}	JUAN 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.

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

Tabla Nº 6 Estructura de los principales campos del certificado de persona física.

Campo	Ejemplo	Valor o restricciones
Versión (Version)	V3	Los certificados deben ser 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. Este campo indica el número de serie del certificado digital. Valor único emitido dentro del ámbito de cada PSC.
Algoritmo de firma (Signaturealgorithm)	sha256RSA	El Algoritmo de firma debe ser como mínimo SHA 256 RSA.
Signaturehash algorithm (algoritmo hash de firma)	sha256	El Algoritmo de firma debe ser como mínimo SHA256.
Emisor (Issuer DN)	CN = CA-CODE100 S. A. O = CODE100 S. A. C = PY SERIALNUMBER=RUC80080610-7	Nombre de la CA Ver sección "7.1.4 Formas de Nombre" Este campo indica los datos de identificación del PSC que emitió el certificado.
Válido desde (Validfrom)	viernes, 07 de noviembre de 2016 15:16:58	. En caso de certificados tipos C1 y F1, deben ser menor o igual a 1 (un) año de validez
Válido hasta (Validto)	lunes, 07 de noviembre de 2017 15:16:58	
Sujeto (Suscriber DN)	C = PY O = PERSONA FISICA OU= FIRMA F1 CN = JUAN PEREZ GOMEZ SERIALNUMBER = CI2304024 G = JUAN SN = PEREZ GOMEZ	Este campo indica los datos de identificación del titular del certificado emitido por un PSC.
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	Este campo indica la clave pública del titular del certificado. Codificado de acuerdo con el RFC 5280.y con un largo de clave mínima de 2048 bits y algoritmo RSA Encryption.

	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 7 – Estructura de las extensiones del certificado de persona física

EXTENSIONES CERTIFICADO DE PERSONA FÌSICA			
CAMPO	EJEMPLO	DESCRIPCIÓN	CRÍTICO
Subject Key Identifier (Identificador de la clave del Sujeto)	ac dc d4 d3 cf 0c 20 ce bb 20 29 1b 93 1a 10 bb b2 36 3f a7	Este campo debe contener el hash SHA-1 de la clave pública del titular del certificado. Este Campo es usado por el software de validación para ayudar a identificar un certificado que contiene una determinada clave pública.	NO
Authority Key Identifier(Identificador de la clave de la entidad emisora)	Id. de clave=03 7c 7c 9f 6d 5a 72 a5 91 91 b4 db ec 91 fb 03 5f 7c 7c 9d	El campo keyidentifier debe contener el hash SHA-1 de la clave pública del PSC emisor del certificado. Este campo es usado por los diversos software de validación para ayudar a identificar a la autoridad certificadora que emitió el certificado en la cadena de Confianza.	NO
AuthorityInformation Access(Acceso a información de la entidad emisora)	[1]Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://www.code100.com.py/crt/archivo.crt [2]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://www.code100.com.py/oscp	Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado del PSC. Además, para indicar la dirección donde puede accederse al servicio de OCSP, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no. La primera entrada debe contener el método de acceso i d-ad-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 DistributionPoints (Puntos de distribución de CRL)	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo:	Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no.	NO

	Dirección URL=http://www.code100.com.py/crl/archivo.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 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)	Referencia otros propósitos de la clave, adicionales al uso y debe ser consistente con la extensión keyUsage	SI
SubjectAltenativeName (nombre alternativo del sujeto)	Rfc822Name=lucasalacraz@hmail.com DirectoryName O= BLANCO S. A. OU= AREA TECNICA SerialNumber=RUC80090099-4 T= DIRECTOR TECNICO	Campo no obligatorio. Los datos a incluir en esta extensión deben ser representados mediante la utilización de los siguientes campos: • Rfc822Name= [*email del titular del certificado*] • DirectoryName=2.5.4.10:[*nombre de la organización en el que presta servicio el titular del certificado*] • DirectoryName=2.5.4.11:[*nombre de la unidad de la organización en el que presta servicio el titular del certificado*] • DirectoryName =2.5.4.5: RUC [número de cédula tributaria correspondiente a la organización en el que presta servicio el titular del certificado, o el numero de cédula tributaria del titular del certificado] • DirectoryName=2.5.4.1: [*Cargo o Titulo del titular del certificado]* 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= [OID CP del PSC]. [1,1]Información de certificador de directiva:	Debe contener el OID de la CP correspondiente y la dirección WEB de la CPS del PSC que emite el certificado.	NO

	Id. de certificador de directiva=CPS Certificador: http://www.code100.com.py/repositorio [1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=[Texto de aviso en español] [1,3]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso==[Texto de aviso en inglés]		

Certificado de Personas Jurídicas

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

CAMPO	EJEMPLO	DESCRIPCIÓN
C (Country) {OID: 2.5.4.6}	PY	Este campo debe contener el código del país asignado de acuerdo al ISO 3166.
O (Organization) {OID: 2.5.4.10}	PERSONA JURIDICA	En este campo se identifica el tipo de certificado. En este caso se identifica que corresponde a un certificado de persona física y se debe indicar PERSONA FISICA, en mayúscula y sin tilde.
OU (OrganizationUnit) {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.
CN (CommonName) {OID: 2.5.4.3}	SU EMPRESA S.A.	Razón Social de la entidad, según inscripción en el Registro Público, en mayúsculas y sin tildes.
Serial Number {OID: 2.5.4.5}	RUC= 80070078-2	Este campo debe contener las siglas RUC, seguidas del número de cédula tributaria, según el documento de identificación.

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

Tabla Nº 9 – Estructura de los principales campos del certificado de persona jurídica

Campo	Ejemplo	Valor o restricciones

Versión (Version)	V3	Los certificados deben ser 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. Este campo indica el número de serie del certificado digital. Valor único emitido dentro del ámbito de cada PSC.
Algoritmo de firma (Signaturealgorithm)	sha256RSA	El Algoritmo de firma debe ser como mínimo SHA 256 RSA.
Signaturehash algorithm (algoritmo hash de firma)	sha256	El Algoritmo de firma debe ser como mínimo SHA256.
Emisor (Issuer DN)	CN = CA-CODE100 S. A. O = CODE100 S. A. C = PY SERIALNUMBER=RUC80080610-7	Nombre de la CA Ver sección "7.1.4 Formas de Nombre" Este campo indica los datos de identificación del PSC que emitió el certificado.
Válido desde (Validfrom)	viernes, 07 de noviembre de 2016 15:16:58	En caso de certificados tipos C1 y F1, debe ser menor o igual a 1 (un) año de validez.
Válido hasta (Validto)	lunes, 07 de noviembre de 2017 15:16:58	
Sujeto (Suscriber DN)	C = PY O = PERSONA JURIDICA OU= FIRMA F1 CN = SU EMPRESA S.A. SERIALNUMBER = RUC80050048-2	Este campo indica los datos de identificación del titular del certificado emitido por un PSC.
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.y con un largo de clave mínima de 2048 bits y algoritmo RSA Encryption.

Tabla Nº 10 – Estructura de las extensiones del certificado de persona jurídica

EXTENSIONES CERTIFICADO DE PERSONA JURIDICA			
CAMPO	EJEMPLO	DESCRIPCIÓN	CRÍTICO
Subject Key Identifier (Identificador de la clave del Sujeto)	ac dc d4 d3 cf 0c 20 ce bb 20 29 1b 93 1a 10 bb b2 36 3f a7	Este campo debe contener el hash SHA-1 de la clave pública del titular del certificado. Este Campo es usado por el software de validación para ayudar a identificar un certificado que contiene una determinada clave pública.	NO
Authority Key Identifier(Identificador de la clave de la entidad emisora)	Id. de clave=03 7c 7c 9f 6d 5a 72 a5 91 91 b4 db ec 91 fb 03 5f 7c 7c 9d	El campo keyidentifier debe contener el hash SHA-1 de la clave pública del PSC emisor del certificado. Este campo es usado por los diversos software de validación para ayudar a identificar a la autoridad certificadora que emitió el certificado en la cadena de Confianza.	NO
AuthorityInformation Access(Acceso a información de la entidad emisora)	[1]Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://www.code100.com.py/crt/archivo.crt [2]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://www.code100.com.py/oscp	Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado del PSC. Además, para indicar la dirección donde puede accederse al servicio de OCSP, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no. La primera entrada debe contener el método de acceso i d-ad-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 DistributionPoints (Puntos de distribución de CRL)	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: 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 la CA que emitió el certificado, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no.	NO
Key Usage(Uso de la clave)	Sin repudio, Firma digital, Cifrado de clave.	En certificados tipo F1 solamente pueden ser activados los siguientes bits: digitalSignature; NonRepudiation (renombrado recientemente con el nombre de contentCommitmen); y keyEncipherment 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)	Referencia otros propósitos de la clave, adicionales al uso y debe ser consistente con la extensión keyUsage	SI
SubjectAltenativeName (nombre alternativo del sujeto)	DirectoryName CN=JUAN PEREZ SerialNumber: CI2319493 T=REPRESENTANTE LEGAL	Los datos a incluir en la extensión deben ser representados mediante la utilización de los siguientes campos: no obligatorio: · Rfc822Name=[email del titular del certificado] · DirectoryName=2.5.4.12: [cargo que ocupa en la organización el responsable del certificado] obligatorio: · DirectoryName=2.5.4.3: [nombre y apellido del responsable del certificado] · DirectoryName=2.5.4.5: CI [número de cédula de identidad correspondiente al responsable del certificado] Los otros campos que compone la extensión"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= [OID CP del PSC]. [1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.muestra.com.py/repositorio [1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=[Texto de aviso en español] [1,3]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso==[Texto de aviso en inglés]	Debe contener el OID de la CP correspondiente y la dirección WEB de la CPS del PSC que emite el certificado.	NO

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

CAMPO	EJEMPLO	DESCRIPCIÓN
C (Country) {OID: 2.5.4.6}	PY	Este campo debe contener el código del país asignado de acuerdo al ISO 3166.
O (Organization) {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 persona física y se debe indicar PERSONA FISICA, en mayúscula y sin tilde.
OU (Organization Unit) {OID: 2.5.4.11}	FIRMA F1	En este campo se indica el propósito del uso del certificado digital y el módulo (software/hardware) en el que fue almacenada la clave privada del titular del certificado. Según lo estipulado en el punto 1.1 y 1.4.1 podrán ser : FIRMA F1; CIFRADO C1.
CN (Common Name) {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 {OID: 2.5.4.5}	MCI4543456	Este campo debe contener según sea el titular: Persona Física: ● las siglas MCI, seguidas del número de cédula de Identidad del titular del certificado, según documento de identificación. Persona Jurídica: ● siglas MRUC, seguidas del número de cédula tributaria, según el documento de identificación. seguidas del número de cédula de Identidad del titular del certificado, según documento de identificación.

Tabla Nº 13 – 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 debe contener el hash SHA-1 de la clave pública del titular del certificado. Este Campo es usado por el software de validación para ayudar a identificar un certificado que contiene una determinada clave pública.	NO

Authority Key Identifier(Identificador de la clave de la entidad emisora)	Id. de clave=03 7c 7c 9f 6d 5a 72 a5 91 91 b4 db ec 91 fb 03 5f 7c 7c 9d	El campo key identifier debe contener el hash SHA-1 de la clave pública del PSC emisor del certificado. Este campo es usado por los diversos software de validación para ayudar a identificar a la autoridad certificadora que emitió el certificado en la cadena de Confianza.	NO
Authority Information Access(Acceso a información de la entidad emisora)	[1]Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://www.code100.com.py/crt/archivo.crt [2]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://www.code100.com.py/oscp	Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado del PSC. Además, para indicar la dirección donde puede accederse al servicio de OCSP, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no. La primera entrada debe contener el método de acceso i d-ad-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 Nombre del punto de distribución: Nombre completo: 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 la CA que emitió el certificado, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no.	NO
Key Usage(Uso de la clave)	Sin repudio, Firma digital, Cifrado de clave.	En certificados tipo F1 solamente pueden ser activados los siguientes bits:digitalSignature;NonRepudiation (renombrado recientemente con el nombre de contentCommitmen); y keyEncipherment 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)	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 DirectoryName O=SUEMPRESA S. A. CN=JUAN PEREZ GOMEZ SERIALNUMBER= CI2319493 T=REPRESENTANTE LEGAL	Los datos a incluir en la extensión deben ser representados mediante la utilización de los siguientes campos: no obligatorio · Rfc822Name= [email del responsable del certificado] Este campo debe contener según sea el titular: Persona Física: obligatorio · DirectoryName =2.5.4.3: [nombre y apellido del responsable del certificado]	NO

		Persona Jurídica obligatorio ▪ DirectoryName=2.5.4.10:[nombre de la organización titular del certificado] ▪ DirectoryName =2.5.4.3: [nombre y apellido del responsable del certificado] ▪ DirectoryName =2.5.4.5: CI [número de cédula de identidad correspondiente al responsable del certificado] no obligatorio ▪ DirectoryName=2.5.4.12: [cargo que ocupa en la organización el responsable del certificado] Los otros campos que compone la extensión "Subject Alternative Name" podrán ser utilizados en la forma y con los propósitos definidos por la RFC 5280 siempre y cuanto estén aprobados por la CA Raíz.	
Certificate Policies (Política del certificado)	[1]Directiva de certificados: Identificador de directiva=[OID CP del PSC]. [1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.code100.com.py/repositorio [1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=[Texto de aviso en español] [1,3]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso==[Texto de aviso en 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

Todos los certificados emitidos dentro de la PKI Paraguay deben corresponder al estándarX.509 versión 3.

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 la CA y el directorio creado para el repositorio de dicho documentos. Es una extensión crítica.

Nombre alternativo del sujeto

La extensión "subjectAlternativeName" es utilizada para Certificados de Firma de Personas Físicas y Jurídicas. Para Certificados de Personas Físicas este campo debe incluir el Mail del titular persona física. Para Certificados de Personas Jurídicas este campo debe incluir el Nombre del titular persona física, según documento de identificación, en mayúsculas, CI más Número de Cédula de Identidad para paraguayos o CIE más Cédula de identidad para extranjeros y Cargo en la institución. Opcionalmente también puede incluir el mail. Para Certificados de Personas Físicas puede incluir el mail. 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 "QualifiedCertificateProfile". La extensión no es crítica.

7.1.3 IDENTIFICADORES DE OBJETO DE ALGORITMOS

Los certificados generados dentro de la PKI Paraguay deben usar el siguiente algoritmo:

Identificador de objeto (OID) de algoritmo criptográfico

- sha256WithRSAEncryption (1.2.840.113549.1.1.11)

Identificador de objeto (OID) de clave pública

- RSAEncryption (1.2.840.113549.1.1.1)

7.1.4 FORMAS DEL NOMBRE

Los nombres dentro de la PKI Paraguay cumple las regulaciones de la sección "3.1.1 Tipos de nombre".

7.1.5 RESTRICCIONES DEL NOMBRE

Los nombres se escriben en mayúsculas y sin tildes, únicamente se acepta el carácter "Ñ" como un caso especial para los nombres de personas físicas y jurídicas.

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

7.1.6 IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO

Sin estipulaciones.

7.1.7 USO DE LA EXTENSIÓN RESTRICCIONES DE POLÍTICA (POLICYCONSTRAINTS)

Sin estipulaciones.

7.1.8 SEMÁNTICA Y SINTAXIS DE LOS CALIFICADORES DE POLÍTICA (POLICYQUALIFIERS)

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 (CERTIFICATEPOLICIES)

Sin estipulaciones.

7.2 Perfil de la CRL

Las listas de revocación de certificados cumplen con el RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" y contienen los elementos básicos especificados en el siguiente cuadro:

Campo	**Valor o restricciones**
Versión (Version)	Ver sección "7.2.1 Numero (s) de versión"
Algoritmo de firma (SignatureAlgorithm)	Algoritmo usado para la firma del CRL, puede ser como mínimo SHA256WithRSAEncryption
Emisor (Issuer)	Entidad que emite y firma la CRL.
Fecha efectiva (Effective Date)	Fecha de emisión de la CRL.
Siguiente actualización (NextUpdate)	Fecha para la cual es emitida la siguiente CRL. La frecuencia de emisión del CRL está acorde con lo requerido en la sección "4.9.7 Frecuencia de emisión de la CRL"
Certificados revocados (CertificateRevoked)	Lista de certificados revocados, incluyendo el número de serie del certificado revocado y la fecha de revocación.
Extensiones	
Número CRL (CRL Number)	Orden secuencial de emisión de CRL
Identificador de clave de Autoridad (Authority Key Identifier)	Identificador de la clave pública de CA.
Punto de distribución del CRL (DistribuitionPoints)	Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado.

7.2.1 Número (s) de versión

Las CRL generadas se implementan con la versión 2 del CRL definido en el estándar ITU X.509, de acuerdo con el perfil establecido en el RFC 5280.

7.2.2 CRL y extensiones de entradas de CRL

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

a) "Authority Key Identifier", no critica: debe contener el hash SHA-1 de clave pública de la PSC que firma la CRL; y

b) "CRL number" no critica: debe contener el número secuencial para cada CRL emitida.

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 Key Infraestructura Certificate and CRL Profile". La extensión no es crítica.

Puntos de distribución de las 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.

7.3 PERFIL DE OCSP

Conforme a lo estipulado en la CPS

7.3.1 NÚMERO (S) DE VERSIÓN

Conforme a lo estipulado en la CPS

7.3.2 EXTENSIONES DE OCSP

Conforme a lo estipulado en la CPS

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

Los ítems siguientes son referidos en los puntos correspondientes de la CPS de CODE100 S. A.

8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN
8.2 IDENTIFICACIÓN/CALIFICACIÓN DEL EVALUADOR
8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA
8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN
8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA
8.6 COMUNICACIÓN DE RESULTADOS

9. OTROS ASUNTOS LEGALES Y COMERCIALES

Los ítems siguientes son referidos en los puntos correspondientes de la CPS de CODE100 S. A.

9.1 TARIFAS

9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

9.1.2 TARIFAS DE ACCESO A CERTIFICADOS

9.1.3 TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN

9.1.4 TARIFAS POR OTROS SERVICIOS

9.1.5 POLÍTICAS DE REEMBOLSO

9.2 RESPONSABILIDAD FINANCIERA

9.2.1 COBERTURA DE SEGURO

9.2.2 OTROS ACTIVOS

9.2.3 COBERTURA DE SEGURO O GARANTÍA PARA USUARIOS FINALES

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

9.3.2 INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL

9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL

9.4.1 PLAN DE PRIVACIDAD

9.4.2 INFORMACIÓN TRATADA COMO PRIVADA

9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

9.4.6 DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO

9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

9.5 DERECHO DE PROPIEDAD INTELECTUAL

9.6 REPRESENTACIONES Y GARANTÍAS

9.6.1 REPRESENTACIONES Y GARANTÍAS DEL PSC

9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA RA
9.6.3 REPRESENTACIONES Y GARANTÍAS DEL SUSCRIPTOR
9.6.4 REPRESENTACIONES Y GARANTÍAS DE LAS PARTES QUE CONFÍAN
9.6.5 REPRESENTACIONES Y GARANTÍAS DEL REPOSITORIO
9.6.6 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES

9.7 EXENCIÓN DE GARANTÍA
9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL
9.8.1 LIMITACIONES DE LA RESPONSABILIDAD DEL PSC

9.9 INDEMNIZACIONES
9.10 PLAZO Y FINALIZACIÓN
9.10.1 PLAZO
9.10.2 FINALIZACIÓN
9.10.3 EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

9.11 NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES
9.12 ENMIENDAS
9.12.1 PROCEDIMIENTOS PARA ENMIENDAS
9.12.2 PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN
9.12.3 CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

9.13 DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS
9.14 NORMATIVA APLICABLE
9.15 ADECUACIÓN A LA LEY APLICABLE
9.16 DISPOSICIONES VARIAS
9.16.1 ACUERDO COMPLETO
9.16.2 ASIGNACIÓN
9.16.3 DIVISIBILIDAD
9.16.4 APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DE DERECHOS)
9.16.5 FUERZA MAYOR
9.17 OTRAS DISPOSICIONES

10. DOCUMENTOS DE REFERENCIA

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

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