TETÃ REKUÁI
MOTENONDEHA

MINISTERIO DEL
INTERIOR

PRESTADOR DE SERVICIOS DE CERTIFICACIÓN DE LA POLICÍA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES

POLÍTICA DE CERTIFICACIÓN DE TIPO F2 Y C2 PARA PERSONA FÍSICA

VERSIÓN 1.0

CLASE: PÚBLICO

INDICE

1. INTRODUCCIÓN 17

1.1. DESCRIPCIÓN GENERAL 17

1.2 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO 19

1.3 PARTICIPANTES DE LA PKI 19

1.3.1 AUTORIDADES CERTIFICADORAS (CA) 19

1.3.2 AUTORIDAD DE REGISTRO (RA) 20

1.3.3 PRESTADORES DE SERVICIOS DE SOPORTE (PSS) 23

1.3.4 SUSCRIPTORES 23

1.3.5 PARTE QUE CONFÍA 24

1.3.6 OTROS PARTICIPANTES 24

1.4 USO DEL CERTIFICADO 24

1.4.1 USOS APROPIADOS DEL CERTIFICADO 24

1.4.2 USOS PROHIBIDOS DEL CERTIFICADO 26

1.5 ADMINISTRACIÓN DE LA POLÍTICA 26

1.5.1 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO 26

1.5.2 PERSONA DE CONTACTO 27

1.5.3 PERSONA QUE DETERMINA LA ADECUACIÓN DE LA CPS A LA POLÍTICA 27

1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA CPS 27

1.6 DEFINICIONES Y ACRÓNIMOS 28

1.6.1 DEFINICIONES 28

1.6.2 ACRÓNIMOS 39

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO 43

2.1 REPOSITORIOS 43

2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN 43

2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN 44
2.4 CONTROLES DE ACCESO 44
3. IDENTIFICACION Y AUTENTICACION 45
3.1 NOMBRES 45
3.1.1 TIPOS DE NOMBRES 45
Como establezca la CPS de la PNDI. 45
3.1.2 NECESIDAD DE NOMBRES SIGNIFICATIVOS 45
Como establezca la CPS de la PNDI. 45
3.1.3 ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES 45
Como establezca la CPS de la PNDI. 45
3.1.4 REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES 45
3.1.5 UNICIDAD DE LOS NOMBRES 45
3.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS 45
3.2 VALIDACIÓN INICIAL DE IDENTIDAD 46
3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA 46
3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA 46
3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA 46
3.2.4 INFORMACIÓN DEL SUSCRIPTOR NO VERIFICADA 46
3.2.5 VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO) 46
3.2.6 CRITERIOS PARA INTEROPERABILIDAD 46
3.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RE EMISIÓN DE CLAVES 47
3.3.1 IDENTIFICACIÓN Y AUTENTICACIÓN PARA RE EMISIÓN DE CLAVES 47
3.3.2 IDENTIFICACIÓN Y AUTENTICACIÓN PARA LA RE EMISIÓN DE CLAVES DESPUÉS DE UNA REVOCACIÓN 47
3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN 47

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO 48
4.1. SOLICITUD DE CERTIFICADO 48
4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO 48
4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES 48
4.2 PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO 48
4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN 48
4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO 48
4.2.3 TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO 49
4.3 EMISIÓN DEL CERTIFICADO 49
4.3.1 ACCIONES DE LA CA DURANTE LA EMISIÓN DE LOS CERTIFICADOS 49
4.3.2 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DEL CERTIFICADO DIGITAL 49
4.4 ACEPTACIÓN DEL CERTIFICADO 49
4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO 49
4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PSC 49
4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR EL PSC A OTRAS ENTIDADES 50
4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO 50
4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL SUSCRIPTOR 50
4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LA PARTE QUE CONFÍA 50
4.6 RENOVACIÓN DEL CERTIFICADO 50
4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO 50
4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN 50
4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO 51
4.6.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO 51
4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO ... 51
4.6.6 PUBLICACIÓN POR EL PSC DEL CERTIFICADO 51

4.6.7 NOTIFICACIÓN POR EL PSC DE LA EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES 51
4.7 RE-EMISIÓN DE CLAVES DE CERTIFICADO 51
4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO 51
4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA 52
4.7.3 PROCESAMIENTO DE SOLICITUDES DE RE-EMISIÓN DE CLAVES DE CERTIFICADO 52
4.7.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA RE-EMISIÓN DE UN NUEVO CERTIFICADO 52
4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE- EMITIDO..... 52
4.7.6 PUBLICACIÓN POR EL PSC DE LOS CERTIFICADOS RE-EMITIDOS 52
4.7.7 NOTIFICACIÓN POR EL PSC DE LA RE-EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES 52
4.8 MODIFICACIÓN DE CERTIFICADOS 52
4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO 53
4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO 53
4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO 53
4.8.4 NOTIFICACIÓN AL SUSCRIPTOR DE LA EMISIÓN DE UN NUEVO CERTIFICADO..... 53
4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO..... 53
4.8.6 PUBLICACIÓN POR EL PSC DE LOS CERTIFICADOS MODIFICADOS 53
4.8.7 NOTIFICACIÓN POR EL PSC DE EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES 53
4.9 REVOCACIÓN Y SUSPENSIÓN 54
4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN 54
4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN 54
4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN 54
4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN 54

4.9.5 TIEMPO DENTRO DEL CUAL EL PSC DEBE PROCESAR LA SOLICITUD DE REVOCACIÓN 54
4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LAS PARTES QUE CONFÍAN 54
4.9.7 FRECUENCIA DE EMISIÓN DEL CRL 54
4.9.8 LATENCIA MÁXIMA PARA CRL 54
4.9.9 REQUISITOS DE VERIFICACIÓN DE CRL 55
4.9.10 DISPONIBILIDAD DE VERIFICACIÓN DE REVOCACIÓN / ESTADO EN LÍNEA 55
4.9.11 REQUERIMIENTOS PARA VERIFICAR LA REVOCACIÓN EN LÍNEA 55
4.9.12 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES 55
4.9.13 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA 55
4.9.14 CIRCUNSTANCIAS PARA SUSPENSIÓN 55
4.9.15 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN 55
4.9.16 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN 55
4.9.17 LÍMITES DE PERÍODO DE SUSPENSIÓN 56
4.10 SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADO 56
4.10.1 CARACTERÍSTICAS OPERACIONALES 56
4.10.2 DISPONIBILIDAD DEL SERVICIO 56
4.10.3 CARACTERÍSTICAS OPCIONALES 56
4.11 FIN DE LA SUSCRIPCIÓN 56
4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES 56
4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES 56
4.12.2 POLÍTICAS Y PRÁCTICAS DE RECUPERACIÓN Y ENCAPSULACIÓN DE CLAVES DE SESIÓN 56
5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES 57
5.1 CONTROLES FÍSICOS 57

5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO 57
5.1.2 ACCESO FÍSICO 57
5.1.2.1 NIVELES DE ACCESO FÍSICO 57
5.1.3 ENERGÍA Y AIRE ACONDICIONADO 57
5.1.4 EXPOSICIONES AL AGUA 57
5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO 57
5.1.6 ALMACENAMIENTO DE MEDIOS 57
5.1.7 ELIMINACIÓN DE RESIDUOS 57
5.1.8 RESPALDO FUERA DE SITIO 58
5.1.9 INSTALACIONES TÉCNICAS DE LA RA 58
5.2 CONTROLES PROCEDIMENTALES 58
5.2.1 ROLES DE CONFIANZA 58
5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA 58
5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL 58
5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES 58
5.3 CONTROLES DE PERSONAL 58
5.3.1 REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN 58
5.3.2 PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES 59
5.3.3 REQUERIMIENTOS DE CAPACITACIÓN 59
5.3.4 REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN 59
5.3.5 FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES 59
5.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS 59
5.3.7 REQUISITOS DE CONTRATACIÓN A TERCEROS 59
5.3.8 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL 59
5.4 PROCEDIMIENTO DE REGISTRO DE AUDITORÍA 59

5.4.1 TIPOS DE EVENTOS REGISTRADOS 59
5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS) 60
5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA 60
5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA 60
5.4.5 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE REGISTRO (LOGS) DE AUDITORÍA ... 60
5.4.6 SISTEMA DE RECOLECCIÓN DE INFORMACIÓN DE AUDITORÍA (INTERNO VS EXTERNO) 60
5.4.7 NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO 60
5.4.8 EVALUACIÓN DE VULNERABILIDADES 60
5.5 ARCHIVOS DE REGISTROS 60
5.5.1 TIPOS DE REGISTROS ARCHIVADOS 60
5.5.2 PERIODOS DE RETENCIÓN PARA ARCHIVOS 61
5.5.3 PROTECCIÓN DE ARCHIVOS 61
5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO 61
5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS 61
5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO) 61
5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA 61
5.6 CAMBIO DE CLAVE 61
5.7 RECUPERACIÓN DE DESASTRES Y COMPROMISO 62
5.7.1 PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO 62
5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES 62
5.7.3 PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD 62
5.7.4 CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE 62
5.7.5 ACTIVIDADES DE LAS AUTORIDADES DE REGISTRO 62
5.8 EXTINCIÓN DE UN PSC 62

6. CONTROLES TÉCNICOS DE SEGURIDAD 63
6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES 63
6.1.1 GENERACIÓN DEL PAR DE CLAVES 63
6.1.2 ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR 64
6.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO 65
6.1.4 ENTREGA DE LA CLAVE PÚBLICA DE LA CA A LAS PARTES QUE CONFÍAN 65
6.1.5 TAMAÑO DE LA CLAVE 65
6.1.6 GENERACIÓN DE PARÁMETROS DE CLAVES ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD. 66
6.1.7 PROPÓSITOS DE USOS DE CLAVE (CAMPO KEY USAGE X509 V3) 66
6.1.8 GENERACIÓN DE CLAVE POR HARDWARE O SOFTWARE 66
6.2 CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO Y PROTECCIÓN DE LA CLAVE PRIVADA 67
6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO 67
6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA 67
6.2.3 CUSTODIA/RECUPERACIÓN DE LA CLAVE PRIVADA 67
6.2.4 RESPALDO/COPIA DE LA CLAVE PRIVADA 67
6.2.5 ARCHIVADO DE LA CLAVE PRIVADA 67
6.2.6 TRANSFERENCIA DE CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRIPTOGRÁFICO 68
6.2.7 ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO 68
6.2.8 MÉTODO DE ACTIVACIÓN DE CLAVE PRIVADA 68
6.2.9 MÉTODOS DE DESACTIVACIÓN DE LA CLAVE PRIVADA 68
6.2.10 DESTRUCCIÓN DE CLAVE PRIVADA 69
6.2.11 CLASIFICACIÓN DEL MÓDULO CRIPTOGRÁFICO 69
6.3 OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES 69

6.3.1 ARCHIVO DE LA CLAVE PÚBLICA 69
6.3.2 PERÍODO OPERACIONAL DEL CERTIFICADO Y PERÍODO DE USO DEL PAR DE CLAVES 69
6.4 DATOS DE ACTIVACIÓN 70
6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN 70
6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN 70
6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN 70
6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR 70
6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS 70
6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR 71
6.5.3 CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO 71
Como Establezca la CPS de la PNDI 71
6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA 71
6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA 71
6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD 71
6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA 71
6.6.4 CONTROLES EN LA GENERACIÓN DE CRL 72
6.7 CONTROLES DE SEGURIDAD DE RED 72
6.7.1 DIRECTRICES GENERALES 72
6.7.2 FIREWALL 72
6.7.3 SISTEMA DE DETECCIÓN DE INTRUSO (IDS) 72
6.7.4 REGISTRO DE ACCESO NO AUTORIZADO A LA RED 72
6.8 CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO 72
7. PERFILES DE CERTIFICADOS, CRL Y OCSP 73
7.1 PERFIL DEL CERTIFICADO 73

7.1.1 NÚMERO DE VERSIÓN 91
7.1.2 EXTENSIONES DEL CERTIFICADO 91
7.1.3 IDENTIFICADORES DE OBJETO DE ALGORITMOS 92
7.1.4 FORMAS DEL NOMBRE 92
7.1.5 RESTRICCIONES DEL NOMBRE 92
7.1.6 IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO 93
7.1.7 USO DE LA EXTENSIÓN RESTRICCIONES DE POLÍTICA (POLICYCONSTRAINTS) ... 93
7.1.8 SEMÁNTICA Y SINTAXIS DE LOS CALIFICADORES DE POLÍTICA (POLICY QUALIFIERS) 93
7.1.9 SEMÁNTICA DE PROCESAMIENTO PARA LA EXTENSIÓN DE POLÍTICAS DE CERTIFICADO (CERTIFICATEPOLICIES) 93
7.2 PERFIL DE LA CRL 93
7.2.1 NÚMERO (S) DE VERSIÓN 93
7.2.2 CRL Y EXTENSIONES DE ENTRADAS DE CRL 93
7.3 PERFIL DE OCSP 94
7.3.1 NÚMERO (S) DE VERSIÓN 94
7.3.2 EXTENSIONES DE OCSP 94
8. AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES 95
8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN 95
8.2 IDENTIFICACIÓN/CALIFICACIÓN DEL EVALUADOR 95
8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA 95
8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN 95
8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA 95
8.6 COMUNICACIÓN DE RESULTADOS 95
9. OTROS ASUNTOS LEGALES Y COMERCIALES 96
9.1 TARIFAS 96

9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS 96
9.1.2 TARIFAS DE ACCESO A CERTIFICADOS 96
9.1.3 TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN 96
9.1.4 TARIFAS POR OTROS SERVICIOS 96
9.1.5 POLÍTICAS DE REEMBOLSO 96
9.2 RESPONSABILIDAD FINANCIERA 97
9.2.1 COBERTURA DE SEGURO 97
9.2.2 OTROS ACTIVOS 97
9.2.3 COBERTURA DE SEGURO O GARANTÍA PARA USUARIOS FINALES 97
9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL 97
9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL 97
9.3.2 INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL 98
9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL 98
9.4.1 PLAN DE PRIVACIDAD 98
9.4.2 INFORMACIÓN TRATADA COMO PRIVADA 98
9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA 98
9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA 98
9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA 98
9.4.6 DIVULGACIÓN ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO 98
9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN 99
9.5 DERECHO DE PROPIEDAD INTELECTUAL 99
9.6 REPRESENTACIONES Y GARANTÍAS 99
9.6.1 REPRESENTACIONES Y GARANTÍAS DEL PSC 99
9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA RA 99
9.6.3 REPRESENTACIONES Y GARANTÍAS DEL SUSCRIPTOR 99

9.6.4 REPRESENTACIONES Y GARANTÍAS DE LAS PARTES QUE CONFÍAN 99
9.6.5 REPRESENTACIONES Y GARANTÍAS DEL REPOSITORIO 99
9.6.6 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES 99
9.7 EXENCIÓN DE GARANTÍA 100
9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL 100
9.9 INDEMNIZACIONES 100
9.10 PLAZO Y FINALIZACIÓN 100
9.10.1 PLAZO 100
9.10.2 FINALIZACIÓN 100
9.10.3 EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA 100
9.11 NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES 100
9.12 ENMIENDAS 100
9.12.1 PROCEDIMIENTOS PARA ENMIENDAS 100
9.12.2 PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN 101
9.12.3 CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS 101
9.13 DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS 101
9.14 NORMATIVA APLICABLE 101
9.15 ADECUACIÓN A LA LEY APLICABLE 101
9.16 DISPOSICIONES VARIAS 101
9.16.1 ACUERDO COMPLETO 101
9.16.2 ASIGNACIÓN 101
9.16.3 DIVISIBILIDAD 101
9.16.4 APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DE DERECHOS) 102
9.16.5 FUERZA MAYOR 102
9.17 OTRAS DISPOSICIONES 102

10. DOCUMENTOS DE REFERENCIA 103

CONTROL DOCUMENTAL

DOCUMENTO	
Título: POLÍTICA DE CERTIFICACIÓN DE TIPO F2 Y C2 PARA PERSONA FÍSICA del PSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES	**Nombre del Archivo:** CP F2 Y C2 PNDI v1.0
Código: CP-PNDI-V1.0	**Soporte Lógico:** https://www.identificaciones.gov.py/firmadigital/CP/CP%20F2%20PNDI%20v.1.0.pdf
Fecha: 13/09/2019	**Ubicación Física:** Policía Nacional - Departamento de Identificaciones (PNDI)
Versión: 1.0	

REGISTRO DE CAMBIOS		
Versión	**Fecha**	**Motivo de cambio**
1.0	13/09/19	Versión inicial

DISTRIBUCIÓN DEL DOCUMENTO	
NOMBRE	**ÁREA**
Ministerio de Industria y Comercio (MIC)	Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE)
Policía Nacional	Departamento de Identificaciones
Documento Público	https://www.identificaciones.gov.py/firmadigital/CP/CP%20F2%20PNDI%20v.1.0.pdf

CONTROL DEL DOCUMENTO		
Preparado por:	**Revisado por:**	**Aceptado por:**
Consorcio CDE	**MDI:** Dr. Abog. Blas Dubrez Lic. Victor Uribe Lic. Ricardo Bogarín Lic. Mariza Chávez **PNDI:** Suboficial Inspector Emilio Centurión Crio. Principal D.E.A.A.P Christian Ramírez Oficial Inspector Dr. Abog. Julián Giménez Crio. Principal Inocencio Escobar	Ministerio del Interior

1. INTRODUCCIÓN

1.1. DESCRIPCIÓN GENERAL

El PSC de la Policía Nacional – Departamento de Identificaciones, quien ejerce funciones de Autoridad Certificadora atribuidas al Ministerio del Interior se constituye en un Prestador de Servicios de Certificación (en adelante PSC de la PNDI) habilitado por el Ministerio de Industria y Comercio (MIC) y brinda los servicios de certificación digital según lo establecido por la Ley Nro. 4017/10, Nro. 4610/12, Decreto Reglamentario Nro. 7369/11 y Decreto Modificatorio N° 2063/2019 que amplia y establece la nueva estructura orgánica y funcional del Ministerio del Interior.

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

El Ministerio de Industria y Comercio en su carácter de Autoridad de Aplicación de las leyes referidas realiza las siguientes funciones:

- Administra la Autoridad de Certificación Raíz del Paraguay;
- Dicta las normas que regulen el Servicio de Certificación Digital en el país;
- Habilita a los Prestadores de Servicios de Certificación;
- Audita a los Prestadores de Servicios de Certificación;
- Revoca la habilitación de los Prestadores de Servicios de Certificación; y

- Impone sanciones a los Prestadores de Servicio de Certificación.

El Ministerio de Industria y Comercio en su carácter de Autoridad Certificadora Raíz del Paraguay constituye el primer nivel de la cadena de confianza o sea es la raíz de toda la Jerarquía de PKI y cuenta con un certificado autoafirmado y aceptado por los terceros que establezcan confianza en la PKI del Paraguay.

El Ministerio de Industria y Comercio como AA de la normativa vigente habilita la operación como Prestador de Servicios de Certificación (PSC) en la República del Paraguay al Ministerio del Interior, cuya operativa será ejecutada por la Policía

Nacional - Departamento de Identificaciones. Para tal efecto le emitió su certificado y de esta manera pasa a ser parte de la cadena de confianza en segundo nivel de la Infraestructura de Clave Pública del Paraguay.

El presente documento describe la Política de Certificación (CP) del PSC de la PNDI que estipula el funcionamiento y operaciones como Prestador de Servicios de Certificación dentro de la PKI del Paraguay.

El tipo de certificados digital previsto en esta CP para los usuarios de la PKI Paraguay es el certificado de firma digital del Tipo F2 y C2 para persona física cuya correspondiente clave privada es almacenada en un dispositivo criptográfico en módulo hardware.

El tipo de certificados indicados define una escala de requisitos de seguridad más rigurosos y pueden ser emitidos por el PSC de la PNDI, para personas físicas.

1.2 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Nombre:	Políticas de Certificación Tipo F2 y C2 Persona Física de la Policía Nacional - Departamento de Identificaciones
Versión:	1.0
Fecha de aprobación:	-------
Ubicación de la CPS:	https://www.identificaciones.gov.py/firmadigital/CPS/CPS%20F2%20PNDI%20v1.0.pdf

1.3 PARTICIPANTES DE LA PKI

1.3.1 AUTORIDADES CERTIFICADORAS (CA)

Son las entidades autorizadas a emitir certificados de clave pública dentro de la PKI Paraguay. Así mismo, efectúan la revocación de los mencionados certificados y la generación de claves públicas y privadas, cuando así lo establecen sus prácticas y políticas. Estos se denominan:

- Autoridad Certificadora Raíz del Paraguay (CA Raíz): emite certificados a los PSC bajo la jerarquía del Certificado Raíz. El certificado raíz es un certificado auto firmado, en el que se inicia la cadena de confianza. Subordinados al Certificado Raíz, se encuentran los certificados emitidos

al PSC. En el Paraguay, la cadena de certificación tiene como máximo dos niveles, en el primer nivel se encuentra la CA Raíz, en el segundo nivel, uno o varios PSC, estos solo podrán emitir certificados digitales a usuarios finales. Se constituye como CA Raíz del Paraguay el MIC.

- Prestador de Servicios de Certificación (PSC): es la persona jurídica que emite certificados digitales a los usuarios finales. El PSC de la PNDI presta servicios de certificación digital habiendo sido habilitado por el MIC luego de presentar la solicitud de habilitación y ajustándose al procedimiento establecido para el efecto. El PSC de la PNDI es parte de la cadena de confianza de la PKI Paraguay y cuenta con un certificado digital firmado y emitido por la CA Raíz, generando de esta manera, una estructura jerárquica. El PSC de la PNDI emite certificados digitales a los usuarios finales.

1.3.2 AUTORIDAD DE REGISTRO (RA)

Son las personas, políticas, procedimientos y sistemas informáticos encargados de la validación y verificación de la identidad de los solicitantes de certificados digitales y si procede, de los atributos asociados a los mismos. Las Autoridades de Registro (RA) llevarán a cabo la identificación de los solicitantes de certificados conforme a las normas de esta CP y el acuerdo suscrito con el PSC de la PNDI.

El PSC de la PNDI cumple funciones de RA. Además, podrá mediante un contrato de prestación de servicio establecer Autoridades de Registros vinculadas a él, siempre y cuando las mismas estén autorizadas por la CA Raíz, en todo el

territorio de la república, cumpliendo las normas y procedimientos establecidos en el documento “Características Mínimas de Seguridad para las Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay” y la normativa vigente, previa comunicación y autorización de la AA. Los RA vinculados al PSC de la PNDI estarán siempre bajo el control y supervisión de este.

Los datos referentes a las RA habilitadas por el PSC de la PNDI se encuentran en la dirección de página web (URL):

https://www.identificaciones.gov.py/firmadigital/ras

El PSC de la PNDI mantiene publicada en el sitio principal de internet 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 los RA vinculados con otra RA dentro de la PKI Paraguay, si fuera el caso.

La RA vinculada al PSC de la PNDI se encarga de garantizar y cumplir con las siguientes tareas:

- Que el trámite se realice de forma presencial por parte de las personas implicadas en la solicitud, custodia y uso del certificado solicitado, en todas las modalidades del certificado;
- Que los documentos aportados para la identificación y acreditación de la capacidad de representación sean auténticos y suficientes para llevar a cabo este trámite;
- Que las consultas y dudas que les sean formuladas sean atendidas;
- Poner a disposición del solicitante y de todas las personas que intervienen en el trámite de solicitud, la CPS, CP, tasas y aranceles del servicio, así como toda información relacionada con el proceso de emisión y de revocación: causas, obligaciones y procedimiento a seguir;
- Informar a los solicitantes, de las condiciones precisas para la utilización del certificado y de sus limitaciones de uso;
- Verificar que el titular de los datos ha prestado su consentimiento para el tratamiento de sus datos personales, den conocimiento de la finalidad que se les va a dar;

- Procesar toda la documentación presentada por el solicitante y enviar la solicitud de certificado al PSC de la PNDI de forma segura y firmada digitalmente.

1.3.3 PRESTADORES DE SERVICIOS DE SOPORTE (PSS)

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

- Disponibilidad de infraestructura física y lógica;
- Disponibilidad de recursos humanos especializados;
- Disponibilidad de infraestructura física y lógica y de recursos humanos especializados.

Las informaciones actualizadas de las PSS a la que recurre el PSC de la PNDI se encuentran en la dirección de página web (URL):

https://www.identificaciones.gov.py/firmadigital/pss

1.3.4 SUSCRIPTORES

En relación con el PSC de la PNDI, es suscriptor toda persona física a quien se emite un certificado digital en el marco de la jerarquía PKI Paraguay. Es obligación de todo suscriptor el conocimiento de la presente CP y su correspondiente CPS, así como de la normativa vigente.

1.3.5 PARTE QUE CONFÍA

Es toda persona física que confía en un certificado y/o en las firmas digitales generadas a partir de un certificado, emitidos dentro de la jerarquía PKI Paraguay.

Una parte que confía puede o no ser un suscriptor.

1.3.6 OTROS PARTICIPANTES

No estipulado.

1.4 USO DEL CERTIFICADO

1.4.1 USOS APROPIADOS DEL CERTIFICADO

Los certificados regulados por la presente CP tipo F2 sólo deben ser utilizados en aplicaciones como confirmación de identidad y firma de documentos electrónicos con verificación de identidad de sus informaciones.

Los certificados regulados por la presente CP tipo C2 serán utilizados en aplicaciones como cifrado de documentos, base de datos, mensajes y otras informaciones electrónicas con la finalidad de asegurar su confidencialidad.

Para determinar si es posible utilizar un certificado de firma digital, autenticación y cifrado del tipo F2 y C2 es necesario comprobar el valor de la extensión 'Key Usage' de los certificados en cuestión. Este campo deberá contener los siguientes datos:

TIPO	DESCRIPCIÓN DE USO APROPIADO
Certificado de Firma Digital tipo F2	**Firma digital y Autenticación** ● No repudio (Non- Repudiation) ● Firma Digital (Digital Signature) ● Cifrado de Clave (Key Encipherment)

TIPO	DESCRIPCIÓN DE USO APROPIADO
Certificado de Cifrado tipo C2	**Cifrado** ● Cifrado de Datos (Data Encipherment) ● Cifrado de Clave (Key Encipherment)

Firma Digital (Digital Signature): se activa cuando la clave pública del suscriptor se usa para la verificación de firmas digitales, distintas de firmas en certificados.

No repudio (Non repudiation): se activa cuando la clave pública del suscriptor es utilizada para verificar las firmas digitales, distintas de las firmas en certificados, proporciona un servicio de no repudio que protege contra el hecho que el firmante falsamente niegue alguna acción. En las últimas ediciones de X.509 han cambiado el nombre del no repudio a contenido aprobado (Content commitment).

Cifrado de Clave (Key encipherment): se activa cuando la clave pública del suscriptor es utilizada para cifrar otras claves usadas en proceso de autenticación. No se encriptan los datos. Las claves privadas o secretas, es decir, para la clave de transporte. Por ejemplo, cuando una clave pública RSA es utilizada para encriptar la clave simétrica o una clave privada asimétrica.

1.4.2 USOS PROHIBIDOS DEL CERTIFICADO

Los certificados emitidos por el PSC de la PNDI 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 de la PNDI, pudiendo llegar a la revocación de este.

1.5 ADMINISTRACIÓN DE LA POLÍTICA

1.5.1 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre: Policía Nacional - Departamento de Identificaciones.

Dirección: Avda. Guido Boggiani esquina R.I.2 Ytororó Teléfono: (+595) (021) 605-618/9

Dirección de correo electrónico: dpto.identificaciones@pn.gov.py

Página Web: https://www.identificaciones.gov.py

1.5.2 PERSONA DE CONTACTO

Nombre: Jefe del Departamento de Identificaciones

Dirección: Avda. Guido Boggiani esquina R.I.2 Ytororó

Teléfono: (+595) (021) 605-618/9

Dirección de correo electrónico: dpto.identificaciones@pn.gov.py

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

El Director General de Firma Digital y Comercio Electrónico del MIC, será el encargado de determinar la adecuación de la presente Política de Certificación (CP).

1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA CPS

El personal autorizado del PSC de la PNDI, conforme con la reglamentación vigente, validará el contenido de la Política de Certificación (CP) y sus posteriores enmiendas o modificaciones, y luego será puesta a consideración de la Dirección General de Firma Digital y Comercio Electrónico y autoridades pertinentes del Ministerio de Industria y Comercio para su aprobación.

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 la validación de la identidad de quien solicita un certificado digital.

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

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

Autenticación: proceso técnico que permite determinar la identidad de la persona que firma 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 N° 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 allí, 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 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 sólo 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 almacena claves criptográficas.

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

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

Par de claves: son las claves privada y pública de un 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 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 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 contenida en el CSR, la CA, puede emitir el certificado digital una vez realizadas las comprobaciones que correspondan.

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

Usuario final: persona física 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

ACRÓNIMOS	DESCRIPCIÓN
C	País (del inglés, Country)
CA	Autoridad Certificadora (CA por sus siglas en inglés Certificate Authority)
CAI	Autoridad de Certificación Intermedia (CAI por sus siglas en inglés Certificate Authority Intermediate)
CA Raíz	Autoridad Certificadora Raíz del Paraguay
CI	Cédula de Identidad
CN	Nombre Común (del inglés, Common Name)
CP	Política de Certificación (CP por sus siglas en inglés Certificate Policy)
CPS	Declaración de Prácticas de Certificación (CPS por sus siglas en inglés Certification Practice Statement)
CRL	Lista de Certificados Revocados (CRL por sus siglas en inglés Certificate Revocation List)
CSR	Solicitud de firma de Certificado (CSR por sus siglas en inglés Certificate Signing Request)

DGFDYCE	Dirección General de Firma Digital y Comercio Electrónico dependiente del Vice Ministro de Comercio
DNS	Servicio de nombre de dominio (DNS por sus siglas en inglés Domain Name Server
PNDI	Policía Nacional - Departamento de Identificaciones
FIPS	Estándares Federales de Procesamiento de la Información (FIPS por sus siglas en inglés Federal Information Processing Standards)
HSM	Módulo de seguridad criptográfico basado en Hardware (HSM por su sigla en inglés Hardware Security module)
ISO	Organización Internacional para la Estandarización (por sus siglas en inglés International Organization for Standardization)
ITU-T	Unión Internacional de Telecomunicaciones - Sector de Normalización de las Telecomunicaciones (ITU-T por sus siglas en inglés International Telecomunication Union – Telecomunication Standarization Sector)
MIC	Ministerio de Industria y Comercio
O	Organización (del inglés Organization)
OCSP	Servicio de Validación de certificado en línea (OCSP por sus siglas en inglés Online Certificate Status Protocol)

OID	Identificador de Objeto (OID por sus siglas en inglés Object Identifier)
OU	Unidad Organizacional (OU, por sus siglas en inglés Organization Unit)
PIN	Número de Identificación Personal (por sus siglas en inglés Personal Identification Number) contraseña que protege el acceso a una tarjeta criptográfica
PKCS	Norma de criptografía de clave pública (PKCS por sus siglas en inglés Public Key Cryptography Standard)
PKI	Infraestructura de Clave Pública (PKI por su sigla en inglés Public Key Infraestructure)
PSC	Prestador de Servicios de Certificación
PY	Paraguay
RA	Autoridad de Registro (RA por sus siglas en inglés Registration Authority)
RFC	Petición de Comentarios (RFC por sus siglas en inglés Request for Comments)
RSA	Sistema criptográfico de clave pública desarrollado por Rivers, Shamir y Adleman

RUC	Registro único del contribuyente
SN	Número de Serie (del inglés, Serial Number)
TLS	Transport Layer Security (seguridad de la capa de transporte)
UPS	Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés Uninterruptible Power Supply)
URL	Localizador uniforme de recursos (URL por sus siglas en inglés Uniform Resource Locator)
VA	Autoridad de Validación (VA por sus siglas en inglés Validation Authority)

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

2.1 REPOSITORIOS

El PSC de la PNDI, es responsable de las funciones de repositorio para su CA.

Los repositorios de información y la publicación de la lista de certificados revocados son administrados en forma directa por el PSC de la PNDI.

El PSC de la PNDI aplica los recursos necesarios para garantizar la seguridad e integridad de los datos almacenados en él.

El repositorio público del PSC de la PNDI está disponible en un 99% anual, durante 24 horas al día, 7 días a la semana. Es un servicio Web de acceso libre y no contiene ninguna información de naturaleza confidencial.

Las informaciones del repositorio son publicadas en la página web:

https://www.identificaciones.gov.py

El acceso se realiza vía HTTPS.

2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

Como establezca la CPS de la PNDI.

2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN

Como establezca la CPS de la PNDI.

2.4 CONTROLES DE ACCESO

Como establezca la CPS de la PNDI.

3. IDENTIFICACION Y AUTENTICACION

3.1 NOMBRES

3.1.1 TIPOS DE NOMBRES

Como establezca la CPS de la PNDI.

3.1.2 NECESIDAD DE NOMBRES SIGNIFICATIVOS

Como establezca la CPS de la PNDI.

3.1.3 ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES

Como establezca la CPS de la PNDI.

3.1.4 REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES

Como establezca la CPS de la PNDI.

3.1.5 UNICIDAD DE LOS NOMBRES

Como establezca la CPS de la PNDI.

3.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

No aplica. Solo emitirá certificados a personas físicas, según el art. 3 del Decreto 2063/19.

3.2 VALIDACIÓN INICIAL DE IDENTIDAD

Como establezca la CPS de la PNDI.

3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA

Como establezca la CPS de la PNDI.

3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

No Aplica.

3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA

Como establezca la CPS de la PNDI.

3.2.4 INFORMACIÓN DEL SUSCRIPTOR NO VERIFICADA

No aplica.

3.2.5 VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)

Como establezca la CPS de la PNDI.

3.2.6 CRITERIOS PARA INTEROPERABILIDAD

Como establezca la CPS de la PNDI.

3.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RE EMISIÓN DE CLAVES

3.3.1 IDENTIFICACIÓN Y AUTENTICACIÓN PARA RE EMISIÓN DE CLAVES

No aplica.

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

No aplica.

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

Como establezca la CPS de la PNDI.

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1. SOLICITUD DE CERTIFICADO

4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

Como establezca la CPS de la PNDI.

4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

Como establezca la CPS de la PNDI.

4.2 PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Como establezca la CPS de la PNDI.

4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

Como establezca la CPS de la PNDI.

4.2.3 TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO

Como establezca la CPS de la PNDI.

4.3 EMISIÓN DEL CERTIFICADO

4.3.1 ACCIONES DE LA CA DURANTE LA EMISIÓN DE LOS CERTIFICADOS

Como establezca la CPS de la PNDI.

4.3.2 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DEL CERTIFICADO DIGITAL

Como establezca la CPS de la PNDI.

4.4 ACEPTACIÓN DEL CERTIFICADO

4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

Como establezca la CPS de la PNDI.

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PSC

Como establezca la CPS de la PNDI.

4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR EL PSC A OTRAS ENTIDADES

Como establezca la CPS de la PNDI.

4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

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

Como establezca la CPS de la PNDI.

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

Como establezca la CPS de la PNDI.

4.6 RENOVACIÓN DEL CERTIFICADO

Como establezca la CPS de la PNDI

4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO

No aplica.

4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN

No aplica.

4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO

No aplica.

4.6.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO

No aplica.

4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO

No aplica.

4.6.6 PUBLICACIÓN POR EL PSC DEL CERTIFICADO

No aplica.

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

No aplica.

4.7 RE-EMISIÓN DE CLAVES DE CERTIFICADO

Como establezca la CPS de la PNDI.

4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO

No aplica.

4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA

No aplica.

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

No aplica.

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

No aplica.

4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE- EMITIDO

No aplica.

4.7.6 PUBLICACIÓN POR EL PSC DE LOS CERTIFICADOS RE-EMITIDOS

No aplica.

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

No aplica.

4.8 MODIFICACIÓN DE CERTIFICADOS

Como establezca la CPS de la PNDI.

4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO

No aplica.

4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

No aplica.

4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

No aplica.

4.8.4 NOTIFICACIÓN AL SUSCRIPTOR DE LA EMISIÓN DE UN NUEVO CERTIFICADO

No aplica.

4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

No aplica.

4.8.6 PUBLICACIÓN POR EL PSC DE LOS CERTIFICADOS MODIFICADOS

No aplica.

4.8.7 NOTIFICACIÓN POR EL PSC DE EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES

No aplica.

4.9 REVOCACIÓN Y SUSPENSIÓN

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

Como establezca la CPS de la PNDI.

4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN

Como establezca la CPS de la PNDI.

4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

Como establezca la CPS de la PNDI.

4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

Como establezca la CPS de la PNDI.

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

Como establezca la CPS de la PNDI.

4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LAS PARTES QUE CONFÍAN

Como establezca la CPS de la PNDI.

4.9.7 FRECUENCIA DE EMISIÓN DEL CRL

Como establezca la CPS de la PNDI.

4.9.8 LATENCIA MÁXIMA PARA CRL

Como establezca la CPS de la PNDI.

4.9.9 REQUISITOS DE VERIFICACIÓN DE CRL

Como establezca la CPS de la PNDI.

4.9.10 DISPONIBILIDAD DE VERIFICACIÓN DE REVOCACIÓN / ESTADO EN LÍNEA

Como establezca la CPS de la PNDI.

4.9.11 REQUERIMIENTOS PARA VERIFICAR LA REVOCACIÓN EN LÍNEA

Como establezca la CPS de la PNDI.

4.9.12 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES

Como establezca la CPS de la PNDI.

4.9.13 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA

Como establezca la CPS de la PNDI.

4.9.14 CIRCUNSTANCIAS PARA SUSPENSIÓN

No aplica.

4.9.15 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

No aplica.

4.9.16 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

No aplica.

4.9.17 LÍMITES DE PERÍODO DE SUSPENSIÓN

No aplica.

4.10 SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADO

4.10.1 CARACTERÍSTICAS OPERACIONALES

Como establezca la CPS de la PNDI.

4.10.2 DISPONIBILIDAD DEL SERVICIO

Como establezca la CPS de la PNDI.

4.10.3 CARACTERÍSTICAS OPCIONALES

No aplica.

4.11 FIN DE LA SUSCRIPCIÓN

Como establezca la CPS de la PNDI.

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

Como establezca la CPS de la PNDI.

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

No aplica.

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

5.1 CONTROLES FÍSICOS

5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

Como establezca la CPS de la PNDI.

5.1.2 ACCESO FÍSICO

Como establezca la CPS de la PNDI.

5.1.2.1 NIVELES DE ACCESO FÍSICO

Como establezca la CPS de la PNDI.

5.1.3 ENERGÍA Y AIRE ACONDICIONADO

Como establezca la CPS de la PNDI.

5.1.4 EXPOSICIONES AL AGUA

Como establezca la CPS de la PNDI.

5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

Como establezca la CPS de la PNDI.

5.1.6 ALMACENAMIENTO DE MEDIOS

Como establezca la CPS de la PNDI.

5.1.7 ELIMINACIÓN DE RESIDUOS

Como establezca la CPS de la PNDI.

5.1.8 RESPALDO FUERA DE SITIO

Como establezca la CPS de la PNDI.

5.1.9 INSTALACIONES TÉCNICAS DE LA RA

Como establezca la CPS de la PNDI.

5.2 CONTROLES PROCEDIMENTALES

Como establezca la CPS de la PNDI.

5.2.1 ROLES DE CONFIANZA

Como establezca la CPS de la PNDI.

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Como establezca la CPS de la PNDI.

5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Como establezca la CPS de la PNDI.

5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES

Como establezca la CPS de la PNDI.

5.3 CONTROLES DE PERSONAL

5.3.1 REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

Como establezca la CPS de la PNDI.

5.3.2 PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Como establezca la CPS de la PNDI.

5.3.3 REQUERIMIENTOS DE CAPACITACIÓN

Como establezca la CPS de la PNDI.

5.3.4 REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

Como establezca la CPS de la PNDI.

5.3.5 FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

Como establezca la CPS de la PNDI.

5.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS

Como establezca la CPS de la PNDI.

5.3.7 REQUISITOS DE CONTRATACIÓN A TERCEROS

Como establezca la CPS de la PNDI

5.3.8 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

Como establezca la CPS de la PNDI

5.4 PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

5.4.1 TIPOS DE EVENTOS REGISTRADOS

Como establezca la CPS de la PNDI.

5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)

Como establezca la CPS de la PNDI.

5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

Como establezca la CPS de la PNDI.

5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

Como establezca la CPS de la PNDI.

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

Como establezca la CPS de la PNDI.

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

Como establezca la CPS de la PNDI.

5.4.7 NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

Como establezca la CPS de la PNDI.

5.4.8 EVALUACIÓN DE VULNERABILIDADES

Como establezca la CPS de la PNDI.

5.5 ARCHIVOS DE REGISTROS

5.5.1 TIPOS DE REGISTROS ARCHIVADOS

Como establezca la CPS de la PNDI.

5.5.2 PERIODOS DE RETENCIÓN PARA ARCHIVOS

Como establezca la CPS de la PNDI.

5.5.3 PROTECCIÓN DE ARCHIVOS

Como establezca la CPS de la PNDI.

5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO

Como establezca la CPS de la PNDI.

5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

No aplica.

5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO)

Como establezca la CPS de la PNDI.

5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA

Como establezca la CPS de la PNDI.

5.6 CAMBIO DE CLAVE

Como establezca la CPS de la PNDI.

5.7 RECUPERACIÓN DE DESASTRES Y COMPROMISO

5.7.1 PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO

Como establezca la CPS de la PNDI.

5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES

Como establezca la CPS de la PNDI.

5.7.3 PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD

Como establezca la CPS de la PNDI.

5.7.4 CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Como establezca la CPS de la PNDI.

5.7.5 ACTIVIDADES DE LAS AUTORIDADES DE REGISTRO

Como establezca la CPS de la PNDI.

5.8 EXTINCIÓN DE UN PSC

Como establezca la CPS de la PNDI.

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.

La generación de claves criptográficas se realiza utilizando una tarjeta inteligente o en general un dispositivo criptográfico de seguridad tipo hardware, todos con una capacidad de generación de claves y protegido por contraseña y / o identificación biométrica. El algoritmo que se utilizará para generar las claves criptográficas de los titulares de certificados adopta el estándar RSA conforme al RFC 5639 cuyo tamaño de clave para el certificado del Tipo F2 y C2 podrá ser RSA 2048 o RSA 4096.

Para ser generada, la clave privada de la persona física titular del certificado del Tipo F2 es grabada y cifrada por un algoritmo simétrico y tamaño de clave que pueden ser 3DES – 112 bits o AES – 128 o 256 bits en modo de operación CBC o GCM, en un medio de almacenamiento tipo hardware criptográfico homologado por el MIC.

La clave privada es transportada en forma 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, garantizan, 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 está 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

Este punto no aplica porque la clave privada de los certificados 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 al PSC del PNDI 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 para los certificados del Tipo F2 y C2 a través de un medio electrónico seguro.

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

La clave pública del PSC del PNDI es entregada a las partes que confían utilizando el formato del estándar PKCS#7.

El certificado del PSC de la PNDI se encuentra disponible para su descarga en su repositorio público.

La forma para la entrega de un certificado emitido por el PSC de la PNDI podrá comprender, entre otras:

- En el momento de entrega de un certificado para su titular, usando el formato del estándar PKCS#7;
- Una página WEB del PSC de la PNDI; y
- Otros medios seguros aprobados por el MIC.

6.1.5 TAMAÑO DE LA CLAVE

Los tamaños de clave a ser utilizados en los certificados de tipo F2 y C2 emitidos por el PSC de la PNDI podrán tener un tamaño de RSA 2048 o RSA 4096.

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

Los parámetros de generación de claves asimétricas para los suscriptores del PSC de la PNDI cumplen con el estándar FIPS 140-2 nivel 3 para certificados tipo F2 y C2.

El proceso para verificación de parámetros de generación de claves asimétricas cumple con el estándar FIPS 140-2 nivel 3.

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

Los usos admitidos de la clave para los certificados tipo F2 y C2 vienen dados por el valor de las extensiones Key Usage y Extended Key Usage de los mismos.

El contenido de dichas extensiones para los de firma digital y autenticación tipo F2 y Cifrado tipo C2 se puede consultar en el apartado 7.1 de la presente CP.

6.1.8 GENERACIÓN DE CLAVE POR HARDWARE O SOFTWARE

El proceso de generación de claves criptográficas es realizado, para los certificados del tipo F2 y C2 en un módulo criptográfico de hardware que cumple, con el estándar FIPS 140-2 nivel 3

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

6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO.

El módulo criptográfico de generación de claves asimétricas de un suscriptor del PSC del PNDI adopta el estándar FIPS 140-2 nivel 3.

6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA

No aplica.

6.2.3 CUSTODIA/RECUPERACIÓN DE LA CLAVE PRIVADA

El PSC de la PNDI no almacena ni copia las claves privadas de los titulares de certificados por el emitido.

6.2.4 RESPALDO/COPIA DE LA CLAVE PRIVADA

El PSC de la PNDI no mantiene una copia de seguridad de la clave privada del titular del certificado por el emitido.

6.2.5 ARCHIVADO DE LA CLAVE PRIVADA

El PSC de la PNDI nunca archiva claves privadas de sus suscriptores para certificados de Tipo F2 y C2 emitido bajo esta CP.

La clave privada permanece dentro de los límites del dispositivo criptográfico donde fue generada.

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

El PSC de la PNDI nunca transfiere claves privadas de sus suscriptores para certificados emitidos bajo esta CP.

La clave privada permanece dentro de los límites del dispositivo criptográfico donde fue generada.

6.2.7 ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

El PSC de la PNDI no almacena las claves privadas de sus suscriptores para certificados emitidos bajo esta Política. La clave privada permanece dentro de los límites del dispositivo criptográfico donde fue generada.

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.

En general el titular de certificado puede definir procedimientos necesarios para la activación de su clave privada.

6.2.9 MÉTODOS DE DESACTIVACIÓN DE LA CLAVE PRIVADA

El titular de certificado puede definir procedimientos necesarios para la desactivación de su clave privada.

6.2.10 DESTRUCCIÓN DE CLAVE PRIVADA

El titular de certificado puede definir procedimientos necesarios para la destrucción de su clave privada.

6.2.11 CLASIFICACIÓN DEL MÓDULO CRIPTOGRÁFICO

Los módulos criptográficos de los certificados emitidos por el PSC de la PNDI cumplen con el estándar FIPS 140-2 nivel 3.

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, así como las CRL emitidas, son almacenadas por el PSC de la PNDI emisor, después de la expiración de los certificados correspondientes, permanentemente, para la verificación de firmas generadas durante su periodo de validez.

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

Las claves privadas de los certificados de firma digital deberán ser utilizadas por sus titulares únicamente durante el periodo de validez correspondiente.

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

El periodo de validez de los certificados de firma digital de tipo F2 y cifrado del tipo C2 es como máximo de 2 (dos) años desde el momento de emisión del mismo.

6.4 DATOS DE ACTIVACIÓN

6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Para certificados de firma digital y autenticación tipo F2 y cifrado tipo C2, la generación y almacenamiento del par de claves son realizados en dispositivos criptográficos hardware con capacidad de generación de claves. Los datos de activación de la clave privada del titular del certificado son únicos.

6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación de la clave privada del titular del certificado están protegidos contra el uso no autorizado.

6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

No aplica.

6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

Como establezca la CPS de la PNDI

6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

Como establezca la CPS de la PNDI

6.5.3 CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO

Como Establezca la CPS de la PNDI

6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA

Los sistemas informáticos del PSC de la PNDI son homologados por personal técnico al momento de su implementación, para asegurar que los programas que se ponen en producción respondan a las características de diseño declaradas por el proveedor y oportunamente aceptadas cuando fueron seleccionados.

6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

El PSC de la PNDI comprueba los niveles de seguridad configurados periódicamente para la verificación del correcto funcionamiento del sistema.

En caso de incidencias, el PSC de la PNDI se referirá al Plan de Continuidad del Negocio y Recuperación ante desastres.

6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

No aplica.

6.6.4 CONTROLES EN LA GENERACIÓN DE CRL

No aplica.

6.7 CONTROLES DE SEGURIDAD DE RED

6.7.1 DIRECTRICES GENERALES

No aplica.

6.7.2 FIREWALL

No aplica.

6.7.3 SISTEMA DE DETECCIÓN DE INTRUSO (IDS)

No aplica.

6.7.4 REGISTRO DE ACCESO NO AUTORIZADO A LA RED

No aplica.

6.8 CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO

El módulo criptográfico utilizado para almacenar la clave privada del titular del certificado está conforme al estándar FIPS 140-2 nivel 3.

7. PERFILES DE CERTIFICADOS, CRL Y OCSP

En los siguientes puntos la CP, son descriptos los aspectos de los formatos de los certificados y las CRL emitidos por el PSC de la PNDI. Se incluyen informaciones sobre las normas adoptadas, sus perfiles, versiones y extensiones.

7.1 PERFIL DEL CERTIFICADO

El certificado digital del PSC de la PNDI cumple con el formato definido por la norma ITU X.509 V.3 *Information technology Open systems interconnection TheDirectory: Public- key and attribute certificate frameworks.*

A continuación, se detalla el formato del certificado Tipo F2 de persona física utilizado para autenticación y firma digital.

La estructura del certificado, referente a la extensión subject del certificado Tipo F2 de persona física, es la que se describe en la siguiente tabla:

CAMPO	EJEMPLO	DESCRIPCIÓN
C (Country) {OID: 2.5.4.6}	PY	Este campo contiene 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 FÍSICA, en mayúscula y sin tilde.

OU (OrganizationUnit) {OID: 2.5.4.11}	FIRMA F2	En este campo se indica el propósito del uso del certificado digital y el módulo (software/hardware) en el que fue almacenada la clave privada del titular del certificado. En el caso de este tipo de certificado es FIRMA F2 por utilizarse un módulo de hardware.
CN (CommonName) {OID: 2.5.4.3}	JUAN PEREZ GOMEZ	Este campo contiene el/los nombre/s y apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes. Podrán ser incluidos la letra Ñ, diéresis y apostrofes si corresponde.
Serial Number {01D: 2.5.4.5}	CI2304025	Este campo contiene las siglas CI, seguidas del número de cédula de Identidad del titular del certificado, según documento de identificación.
(GivenName) {01D:2.5.4.42}	JUAN	Este campo contiene el/los nombre/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes. Podrán ser incluidas la letra Ñ, diéresis y apostrofes si corresponde.
SN (Surname) {01D: 2.5.4.4}	PEREZ GÓMEZ	Este campo contiene el/los apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes. Podrán ser incluidos la letra Ñ, diéresis y apostrofes si corresponde.

CAMPO	EJEMPLO	VALOR O RESTRICCIONES
Versión (Versión)	V3	Los certificados son X.509 versión 3 (V3).
Número de serie (Serial number)	18 6f 57 dd 38 6c 47 ad 54 5d 0c 9a 22 f4 96 60	Valor único emitido dentro del ámbito del PSC de la PNDI. Este campo indica el número de serie del certificado digital.

Algoritmo de firma (Signaturealgorithm)	sha256RSA	El Algoritmo de firma es como mínimo SHA 256 RSA encryption.
Signaturehash algorithm (algoritmo hash de firma)	sha256	El Algoritmo de firma es como mínimo SHA256.
Emisor (Issuer DN)	CN = CA-MINISTERIO DEL INTERIOR O = MINISTERIO DEL INTERIOR C = PY SERIALNUMBER=RUC80001140-6	Este campo indica los datos de identificación del PSC de la PNDI que emitió el certificado.
Válido desde (Valid from)	lunes, 17 de junio de 2019 15:16:58	Para certificados del Tipo F2 puede ser menor o igual a 2 (dos) años de validez.
Válido hasta (Valid to)	jueves, 17 de junio de 2021 15:16:58	
Sujeto (Suscriber DN)	C = PY O = PERSONA FÍSICA OU= FIRMA F2 CN = JUAN PEREZ GOMEZ SERIALNUMBER=CI2304025 G = JUAN SN = PEREZ GOMEZ	Este campo indica los datos de Identificación del titular de un certificado emitido por un PSC de la PNDI.
Clave pública del sujeto (Subject Public 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	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.

	ec f9 4c 2d a9 89 89 65 97 b1 19 fb b1 ab 2a e1 09 65 ed 8c c6 6c 46 db 8c 3e a6 50 9d 9f ff ee 51 8c 33 5c15 aa 6b 88 8e 7c fa af 1d 9d 48 9f 12 2d b1 98 ff b6 88 ac 09 e0 b5 f9 fc 5a b6 32 32 26 d1 00 72 95 7e d9 5b 5a d8 90 84 86 65 49 32 08 b9 a8 3e 2f 0d db bf 2c 4d 48 e0 6f 52 71 19 5f 86 32 ba dc 87 9d 5f 38 66 80 a7 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	

La estructura del certificado, referente a los campos más relevantes del certificado Tipo F2 de persona física, es la que se describe en la siguiente tabla:

La estructura del certificado, referente a las extensiones del certificado Tipo F2 de persona física, es la que se describe en la siguiente tabla:

CAMPO	EJEMPLO	DESCRIPCION	CRITICO
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 contiene el hash SHA-1 de la clave pública del titular del certificado. Este Campo es usado por	NO

		el software de validación para ayudar a identificar un certificado que contiene una determinada clave pública.	
Authority Key Identifier (Identificador de la clave de la entidad emisora)	Id. de clave=04 7c 7c 9f 6d 5a 72 a5 91 91 b4 db ec 91 fb 03 5f 7c 7c 9d	El campo key identifier contiene el hash SHA-1 de la clave pública del PSC de la PNDI emisor del certificado. Este campo es usado por los diversos softwares de validación para ayudar a identificar a la autoridad certificadora que emitió el certificado en la cadena de Confianza.	NO
Authority Information Access	[1] Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2)	Este Campo es usado para indicar las direcciones donde	NO

(Acceso a la información de la entidad emisora)	Nombre alternativo: Dirección URL= https://www.identificaciones.gov.py/firmadigital/PSCCA.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= https://ocsp.identificaciones.gov.py/ocsp	puede ser encontrado el certificado del PSC de la PNDI. 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.	
CRL Distribution Points (Puntos de distribución de CRL)	[1] Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL= https://www.identificaciones.gov.py/firmadigital/crl/SignatureCRL.crl	Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes al PSC de la PNDI 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 F2 solamente pueden ser activados los siguientes bits: •digitalSignature;	SI

		•NonRepudiation (renombrado recientemente con el nombre de contentCommitmen); y •keyEncipherment	
Extended Key Usage (uso extendido de la clave)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2) Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	Referencia otros propósitos de la clave, adicionales al uso y debe ser consistente con la extensión keyUsage	SI
Certificate Policies (Política del certificado)	[1] Política de Certificado= [1,1] Información de certificador de directiva: Id. De certificador de directiva= CPS Certificador: https://www.identificaciones.gov.py/firmadigital/CPS/CPS F2 PNDI v1.0.pdf [1,2] Información de certificador de directiva: Id de certificador de directiva=Aviso de usuario Certificador: Texto de aviso= Este es un certificado Tipo F2 de persona física cuya clave privada está	Contiene la dirección WEB de la CPS del PSC de la PNDI que emite el certificado.	NO

	almacenada en un módulo de hardware y son utilizadas para autenticar a su titular y generar firmas digitales. [1,3] Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso= This is a Type F2 certificate of physical person whose private key is stored in a hardware module and used to authenticate the holder and generate digital signatures		

La estructura del certificado, referente a la extensión subject del certificado Tipo C2 de persona física, es la que se describe en la siguiente tabla:

CAMPO	EJEMPLO	DESCRIPCIÓN
C (Country) {OID: 2.5.4.6}	PY	Este campo contiene 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 FÍSICA, en mayúscula y sin tilde.

CAMPO	EJEMPLO	DESCRIPCIÓN
OU (OrganizationUnit) {OID: 2.5.4.11}	CIFRADO C2	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. En el caso de este tipo de certificado es CIFRADO C2 por utilizarse un módulo de hardware.
CN (CommonName) {OID: 2.5.4.3}	JUAN PEREZ GOMEZ	Este campo contiene el/los nombre y apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.
Serial Number {01D: 2.5.4.5}	CI2304025	Este campo contiene las siglas CI, seguidas del número de cédula de Identidad del titular del certificado, según documento de identificación.
(GivenName) {01D:2.5.4.42}	JUAN	Este campo contiene el/los nombre/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidas diéresis y apostrofes si corresponde.
SN (Surname) {01D: 2.5.4.4}	PEREZ GÓMEZ	Este campo contiene el/los apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de

CAMPO	EJEMPLO	DESCRIPCIÓN
		la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.

La estructura del certificado, referente a los campos más relevantes del certificado Tipo C2 de persona física, es la que se describe en la siguiente tabla:

CAMPO	EJEMPLO	VALOR O RESTRICCIONES
Versión (Versión)	V3	Los certificados son X.509 versión 3 (V3).
Número de serie (Serial number)	18 6f 57 dd 38 6c 47 ad 54 5d 0c 9a 22 f4 96 60	Valor único emitido dentro del ámbito del PSC de la PNDI. Este campo indica el número de serie del certificado digital.
Algoritmo de firma (Signaturealgorithm)	sha256RSA	El Algoritmo de firma es como mínimo SHA256RSAencryption.
Signaturehash algorithm (algoritmo hash de firma)	sha256	El Algoritmo de firma es como mínimo SHA256.
Emisor (Issuer DN)	CN = CA-MINISTERIO DEL INTERIOR O = MINISTERIO DEL INTERIOR C = PY SERIALNUMBER= 80001140-6	Este campo indica los datos de identificación del PSC de la PNDI que emitió el certificado.

CAMPO	EJEMPLO	VALOR O RESTRICCIONES
Válido desde (Valid from)	lunes, 17 de junio de 2019 15:16:58	Para certificados del Tipo C2 puede ser menor o igual a 2 (dos) años de validez.
Válido hasta (Valid to)	jueves, 17 de junio de 2021 15:16:58	
Subject (Sujeto)	C = PY O = PERSONA FÍSICA OU= CIFRADO C2 CN = JUAN PEREZ GOMEZ SERIALNUMBER=CI2304025 G = JUAN SN = PEREZ GOMEZ	Este campo indica los datos de Identificación del titular de un certificado emitido por un PSC de la PNDI.
Clave pública del sujeto (Subject Public 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	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.

CAMPO	EJEMPLO	VALOR O RESTRICCIONES
	df 07 a1 b4 81 f6 ec a5 e7 5e 50 67 61 31 97 bc 76 94 7f 3e be 28 be 0b a8 03 11 57 64 58 f2 70 da 22 b3 f2 ee 28 18 29 57 1c 59 ce 46 ec f9 4c 2d a9 89 89 65 97 b1 19 fb b1 ab 2a e1 09 65 ed 8c c6 6c 46 db 8c 3e a6 50 9d 9f ff ee 51 8c 33 5c15 aa 6b 88 8e 7c fa af 1d 9d 48 9f 12 2d b1 98 ff b6 88 ac 09 e0 b5 f9 fc 5a b6 32 32 26 d1 00 72 95 7e d9 5b 5a d8 90 84 86 65 49 32 08 b9 a8 3e 2f 0d db bf 2c 4d 48 e0 6f 52 71 19 5f 86 32 ba dc 87 9d 5f 38 66 80 a7 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	

CAMPO	EJEMPLO	VALOR O RESTRICCIONES
	a6 d5 e9 8b 0e 96 44 fb fa a3 f1 b5 02 03 01 fa 01	

La estructura del certificado, referente a las extensiones del certificado Tipo C2 de persona física, es la que se describe en la siguiente tabla:

CAMPO	EJEMPLO	DESCRIPCION	CRITICO
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 contiene el hash SHA-1 de la clave pública del titular del certificado. Este Campo es usado por el software de validación para ayudar a identificar un certificado que contiene una determinada clave pública.	NO
Authority Key Identifier (Identificador de la clave	Id. de clave=04 7c 7c 9f 6d 5a 72 a5 91 91 b4 db ec 91 fb 03 5f 7c 7c 9d	El campo key identifier contiene el hash SHA-1 de la clave pública del PSC de la PNDI emisor del certificado. Este campo es usado por los diversos softwares de validación para ayudar a	NO

CAMPO	EJEMPLO	DESCRIPCION	CRITICO
de la entidad emisora)		identificar a la autoridad certificadora que emitió el certificado en la cadena de Confianza.	
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= https://www.identificaciones.gov.py/firmadigital/PSCCA.crt [2] Acceso a información de autoridad Método de acceso=Protocolo de	Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado del PSC de la PNDI. 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	NO

CAMPO	EJEMPLO	DESCRIPCION	CRITICO
	estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL= https://ocsp.identificaciones.gov.py/ocsp	entrada puede contener el método de acceso id-ad-ocsp con el respectivo respondedor OCSP utilizando uno de los siguientes protocolos de acceso HTTPS o LDAP.	
CRL Distribution Points (Puntos de distribución de CRL)	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL= https://www.identificaciones.gov.py/firmadigital/crl/SignatureCRL.crl	Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes al PSC de la PNDI 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)	• Data Encipherment • keyEncipherment	En certificados tipo C1 y C2 solamente pueden ser activados los siguientes bits: - keyEncipherment	SI

CAMPO	EJEMPLO	DESCRIPCION	CRITICO
		- Data Encipherment	
Extended Key Usage (uso extendido de la clave)	Client Authentication (1.3.6.1.5.5.7.3.2) Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	Referencia otros propósitos de la clave, adicionales al uso y debe ser consistente con la extensión keyUsage	SI
Certificate Policies (Política del certificado)	[1]Política de Certificado= [1,1]Información de certificador de directiva: https://www.identificaciones.gov.py/firmadigital/CP/CP%20F2%20PNDI%20v.1.0.pdf Id. De certificador de directiva= CPS Certificador: https://www.identificaciones.gov.py/firmadigital/CPS/CPS%20F2%20PNDI%20v1.0.pdf	Contiene el OID de esta CP y la dirección WEB de la CPS del PSC de la PNDI que emite el certificado.	NO

CAMPO	EJEMPLO	DESCRIPCION	CRITICO
	[1,2]Información de certificador de directiva: Id de certificador de directiva=Aviso de usuario Certificador: Texto de aviso= Este es un certificado Tipo C2 de persona física cuya clave privada está almacenada en un módulo de hardware y son utilizadas para autenticar a su titular y generar firmas digitales. [1,3]Información de certificador de directiva: Id. De certificador de directiva=Aviso de usuario Certificador: Texto de aviso= This is a Type C2 certificate of physical person whose		

CAMPO	EJEMPLO	DESCRIPCION	CRITICO
	private key is stored in a hardware module and used to authenticate the holder and generate digital signatures		

7.1.1 NÚMERO DE VERSIÓN

Los certificados emitidos por el PSC de la PNDI soportan y utilizan la versión 3 (tres) del estándar ITU X.509, de acuerdo con el perfil establecido en la RFC 5280.

7.1.2 EXTENSIONES DEL CERTIFICADO

Las extensiones utilizadas de forma genérica en los certificados son:

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

El contenido de las extensiones más significativas de los certificados emitidos por el PSC de la PNDI se describe en el punto 7.1

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 del titular del certificado, que consta en el campo "Subject" y el número de identificación, que consta el campo "Serial Number", adoptan el "Distinguished Name" (DN) del estándar ITU X.500/1S0 9594.

7.1.5 RESTRICCIONES DEL NOMBRE

Los nombres contenidos en los certificados están restringidos a distinguished name X.509, que son únicos y no ambiguos.

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. Podrán ser incluidos diéresis y apostrofes si corresponde.

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

Los OID asignados a las políticas de certificación contenidas en este documento se indican en el apartado 1.2.

7.1.7 USO DE LA EXTENSIÓN RESTRICCIONES DE POLÍTICA (POLICYCONSTRAINTS)

No aplica.

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

En el certificado emitido por el PSC de la PNDI, la extensión "Certificate Policies", contiene la URL de la CPS del PSC de la PNDI.

7.1.9 SEMÁNTICA DE PROCESAMIENTO PARA LA EXTENSIÓN DE POLÍTICAS DE CERTIFICADO (CERTIFICATEPOLICIES)

En el certificado emitido por el PSC de la PNDI es una extensión crítica y deben ser interpretadas conforme a la RFC 5280.

7.2 PERFIL DE LA CRL

Como establezca la CPS de la PNDI.

7.2.1 NÚMERO (S) DE VERSIÓN

Como establezca la CPS de la PNDI.

7.2.2 CRL Y EXTENSIONES DE ENTRADAS DE CRL

Como establezca la CPS de la PNDI.

7.3 PERFIL DE OCSP

7.3.1 NÚMERO (S) DE VERSIÓN

Los servicios de respuesta de OCSP del PSC de la PNDI implementan la versión 1 del estándar ITU X 509, de acuerdo al perfil establecido en el RFC 6960.

7.3.2 EXTENSIONES DE OCSP

Si se implementan, debe cumplir con RFC 6960.

8. AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

Como establezca la CPS de la PNDI.

8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

Como establezca la CPS de la PNDI.

8.2 IDENTIFICACIÓN/CALIFICACIÓN DEL EVALUADOR

Como establezca la CPS de la PNDI.

8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA

Como establezca la CPS de la PNDI.

8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN

Como establezca la CPS de la PNDI.

8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA

Como establezca la CPS de la PNDI.

8.6 COMUNICACIÓN DE RESULTADOS

Como establezca la CPS de la PNDI.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 TARIFAS

Como establezca la CPS de la PNDI.

9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

Las tarifas de emisión y revocación de cada certificado se estipulan por resolución ministerial y se encuentran detalladas en la dirección https://www.identificaciones.gov.py/firmadigital

9.1.2 TARIFAS DE ACCESO A CERTIFICADOS

Como establezca la CPS de la PNDI.

9.1.3 TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN

Como establezca la CPS de la PNDI.

9.1.4 TARIFAS POR OTROS SERVICIOS

Como establezca la CPS de la PNDI.

9.1.5 POLÍTICAS DE REEMBOLSO

La Política de Reembolso del PSC de la PNDI comprende los Certificados Digitales que emite bajo sus Políticas de Certificación.

Ante los siguientes casos:

- El solicitante presenta un reclamo sobre un certificado digital emitido por el PSC de la PNDI dentro de los 10 (diez) días posteriores a su fecha de

emisión, argumentando la existencia de una falla en el certificado y/o el dispositivo de almacenamiento.

- De comprobarse fallas u errores en origen atribuibles al PSC, el mismo otorgará la emisión de un nuevo certificado y/o el dispositivo de almacenamiento, de forma gratuita.
- Cumplido los 10 (diez) días desde la fecha de emisión del certificado, el PSC de la PNDI no aceptará ningún reclamo.

9.2 RESPONSABILIDAD FINANCIERA

Como establezca la CPS de la PNDI.

9.2.1 COBERTURA DE SEGURO

Como establezca la CPS de la PNDI.

9.2.2 OTROS ACTIVOS

Como establezca la CPS de la PNDI.

9.2.3 COBERTURA DE SEGURO O GARANTÍA PARA USUARIOS FINALES

Como establezca la CPS de la PNDI.

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

Como establezca la CPS de la PNDI.

9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

Como establezca la CPS de la PNDI.

9.3.2 INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL

Como establezca la CPS de la PNDI.

9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL

9.4.1 PLAN DE PRIVACIDAD

Como establezca la CPS de la PNDI.

9.4.2 INFORMACIÓN TRATADA COMO PRIVADA

Como establezca la CPS de la PNDI.

9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

Como establezca la CPS de la PNDI.

9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

Como establezca la CPS de la PNDI.

9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

Como establezca la CPS de la PNDI.

9.4.6 DIVULGACIÓN ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO

Como establezca la CPS de la PNDI.

9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

Como establezca la CPS de la PNDI.

9.5 DERECHO DE PROPIEDAD INTELECTUAL

Como establezca la CPS de la PNDI.

9.6 REPRESENTACIONES Y GARANTÍAS

9.6.1 REPRESENTACIONES Y GARANTÍAS DEL PSC

Como establezca la CPS de la PNDI.

9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA RA

Como establezca la CPS de la PNDI.

9.6.3 REPRESENTACIONES Y GARANTÍAS DEL SUSCRIPTOR

Como establezca la CPS de la PNDI.

9.6.4 REPRESENTACIONES Y GARANTÍAS DE LAS PARTES QUE CONFÍAN

Como establezca la CPS de la PNDI.

9.6.5 REPRESENTACIONES Y GARANTÍAS DEL REPOSITORIO

Como establezca la CPS de la PNDI.

9.6.6 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES

Como establezca la CPS de la PNDI.

9.7 EXENCIÓN DE GARANTÍA

Como establezca la CPS de la PNDI.

9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL

Como establezca la CPS de la PNDI.

9.9 INDEMNIZACIONES

Como establezca la CPS de la PNDI.

9.10 PLAZO Y FINALIZACIÓN

9.10.1 PLAZO

Como establezca la CPS de la PNDI.

9.10.2 FINALIZACIÓN

Como establezca la CPS de la PNDI.

9.10.3 EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

Como establezca la CPS de la PNDI.

9.11 NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

Como establezca la CPS de la PNDI.

9.12 ENMIENDAS

9.12.1 PROCEDIMIENTOS PARA ENMIENDAS

Como establezca la CPS de la PNDI.

9.12.2 PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

Como establezca la CPS de la PNDI.

9.12.3 CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

Como establezca la CPS de la PNDI.

9.13 DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

Como establezca la CPS de la PNDI.

9.14 NORMATIVA APLICABLE

Como establezca la CPS de la PNDI.

9.15 ADECUACIÓN A LA LEY APLICABLE

Como establezca la CPS de la PNDI.

9.16 DISPOSICIONES VARIAS

9.16.1 ACUERDO COMPLETO

Como establezca la CPS de la PNDI.

9.16.2 ASIGNACIÓN

Como establezca la CPS de la PNDI.

9.16.3 DIVISIBILIDAD

Como establezca la CPS de la PNDI.

9.16.4 APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DE DERECHOS)

Como establezca la CPS de la PNDI.

9.16.5 FUERZA MAYOR

Como establezca la CPS de la PNDI.

9.17 OTRAS DISPOSICIONES

Como establezca la CPS de la PNDI.

10. DOCUMENTOS DE REFERENCIA

Los siguientes documentos referenciados son aplicados para la confección de esta Política 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.
- RFC 2560 “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° 1400/2016 del MIC “por la cual se aprueba y pone en vigencia, las Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación y Declaración de Prácticas de Certificación de los Prestadores de Servicios de Certificación habilitados en la República del Paraguay”.

- Resolución N° 1399/2016.- por la cual se aprueba y pone en vigencia la nueva versión de la Política de Certificación y de la Declaración de Prácticas de Certificación de la Autoridad de Certificación Raíz del Paraguay, y se abrogan las resoluciones N° 1.430/2013 y 401/2014.
- Resolución N° 501/16.- por la cual se aprueba y pone en vigencia la Guía de Estándares tecnológico y lineamientos de seguridad para la habilitación y auditoria a Prestadores de Servicios de Certificación.
- Resolución N° 1105/15.- Por el cual se establece y aprueba el Sistema de Auditoria al cual se someterán los Prestadores de Servicios de Prestadores habilitados y se dejan sin efecto los artículos 3º, 4º y 6º de la Resolución Nº164/14
- Resolución N° 1430/17.- por la cual se modifica parcialmente el anexo de la resolución N° 1.105 de fecha 29 de setiembre de 2015“por la cual se establece y aprueba el Sistema de Auditoria al cual se someterán los Prestadores de Servicios de Certificación habilitados y se dejan sin efecto los artículos 3°, 4° y 6° de la resolución N° 164/14.

- Decreto Reglamentario Nro. 2063/2019.