



**TETÃ REKUÁI**  
MOTENONDEHA  
MINISTERIO DEL  
**INTERIOR**



**PRESTADOR CUALIFICADO DE SERVICIOS CONFIANZA DE LA  
POLICÍA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES**

## **POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA**

**VERSIÓN 1.1**

**CLASE: PÚBLICO**

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## INDICE

1. INTRODUCCIÓN .....	17
1.1. DESCRIPCIÓN GENERAL.....	17
1.2 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO .....	18
1.3 PARTICIPANTES DE LA PKI.....	19
1.3.1 AUTORIDADES CERTIFICADORAS (AC) .....	19
1.3.2 AUTORIDAD DE REGISTRO (AR) .....	21
1.4 USO DEL CERTIFICADO .....	25
1.4.1 USOS APROPIADOS DEL CERTIFICADO .....	25
1.4.2 USOS PROHIBIDOS DEL CERTIFICADO .....	27
1.5 ADMINISTRACIÓN DE LA POLÍTICA .....	27
1.5.1 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO .....	27
1.5.2 PERSONA DE CONTACTO .....	27
1.5.3 PERSONA QUE DETERMINA LA ADECUACIÓN DE LA DPC A LA POLÍTICA.....	28
1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA PC .....	28
1.6 DEFINICIONES Y ACRÓNIMOS .....	28
1.6.1 DEFINICIONES.....	28
1.6.2 ACRÓNIMOS.....	38
2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO .....	42
2.1 REPOSITORIOS.....	42
2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN.....	42
2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN .....	43
2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS.....	43
3. IDENTIFICACION Y AUTENTICACION .....	44
3.1 NOMBRES.....	44

 <p><b>TETÁ REKUÁI</b> MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

3.1.1 TIPOS DE NOMBRES .....	44
Como establezca la DPC de la PNDI. ....	44
3.1.2 NECESIDAD DE NOMBRES SIGNIFICATIVOS .....	44
Como establezca la DPC de la PNDI. ....	44
3.1.3 ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES .....	44
Como establezca la DPC de la PNDI. ....	44
3.1.4 REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES.....	44
3.1.5 UNICIDAD DE LOS NOMBRES .....	44
3.1.7 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS .....	45
3.2 VALIDACIÓN INICIAL DE IDENTIDAD .....	45
3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA .....	45
3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA .....	45
3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA .....	45
3.2.4 INFORMACIÓN NO VERIFICADA DEL TITULAR DEL CERTIFICADO .....	45
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 NUEVAS CLAVES.....	46
3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN .....	46
4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO .....	47
4.1. SOLICITUD DE CERTIFICADO.....	47
4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO.....	47
4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES.....	47
4.2 PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO .....	47
4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN.....	47
4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO .....	47

 <p><b>TETÁ REKUÁI</b> MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

4.2.3 TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO .....	48
4.3 EMISIÓN DEL CERTIFICADO.....	48
4.3.1 ACCIONES DEL PCSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS .....	48
4.3.2 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO POR PARTE DEL PCSC SOBRE LA EMISIÓN DEL CERTIFICADO.....	48
4.4 ACEPTACIÓN DEL CERTIFICADO .....	48
4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO.....	48
4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PCSC .....	48
4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR EL PCSC A OTRAS ENTIDADES .....	49
4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO .....	49
4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR O RESPONSABLE	49
4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LA PARTE USUARIA .....	49
4.6 RENOVACIÓN DEL CERTIFICADO.....	49
4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO .....	49
4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN .....	49
4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO .....	50
4.6.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO	50
4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO ...	50
4.6.6 PUBLICACIÓN POR EL PCSC DEL CERTIFICADO RENOVADO.....	50
4.6.7 NOTIFICACIÓN POR EL PCSC DE LA EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES .....	50
4.7 RE-EMISIÓN DE CLAVES DE CERTIFICADO (RE-KEY).....	50
4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO .....	51
4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA.....	51

 <p><b>TETÁ REKUÁI</b> MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

4.7.3 PROCESAMIENTO DE SOLICITUDES DE RE-EMISIÓN DE CLAVES DE CERTIFICADO ....	51
4.7.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO SOBRE LA RE-EMISIÓN DE UN NUEVO CERTIFICADO .....	51
4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE- EMITIDO .....	51
4.7.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS RE-EMITIDOS.....	51
4.7.7 NOTIFICACIÓN POR EL PCSC DE LA RE-EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES .....	51
4.8 MODIFICACIÓN DE CERTIFICADOS.....	52
4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO.....	52
4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO.....	52
4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO.....	52
4.8.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO DE LA EMISIÓN DE UN NUEVO CERTIFICADO .....	52
4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO .....	52
4.8.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS MODIFICADOS .....	52
4.8.7 NOTIFICACIÓN POR EL PCSC DE EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES ....	53
4.9 REVOCACIÓN Y SUSPENSIÓN .....	53
4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN.....	53
4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN.....	53
4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN.....	53
4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN .....	53
4.9.5 TIEMPO DENTRO DEL CUAL EL PCSC DEBE PROCESAR LA SOLICITUD DE REVOCACIÓN .....	53
4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LA PARTE USUARIA....	53
4.9.7 FRECUENCIA DE EMISIÓN DEL LCR .....	54
4.9.8 LATENCIA MÁXIMA PARA LCR.....	54

 <p><b>TETÁ REKUÁI</b> MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

4.9.9	DISPONIBILIDAD PARA REVOCACIÓN / VERIFICACIÓN DE ESTADO EN LÍNEA.....	54
4.9.10	REQUISITOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA.....	54
4.9.11	OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES .....	54
4.9.12	REQUERIMIENTOS ESPECIALES POR EL COMPROMISO DE LA CLAVE PRIVADA .....	54
4.9.13	CIRCUNSTANCIAS PARA SUSPENSIÓN .....	54
4.9.14	QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN.....	54
4.9.15	PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN.....	55
4.9.16	LÍMITES DE PERÍODO DE SUSPENSIÓN .....	55
4.10	SERVICIOS DE ESTADO DE CERTIFICADO.....	55
4.10.1	CARACTERÍSTICAS OPERACIONALES .....	55
4.10.2	DISPONIBILIDAD DEL SERVICIO .....	55
4.10.3	CARACTERÍSTICAS OPCIONALES.....	55
4.11	FIN DE LA SUSCRIPCIÓN .....	55
4.12	CUSTODIA Y RECUPERACIÓN DE CLAVES.....	55
4.12.1	POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES .....	55
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 .....	58

 <p><b>TETÁ REKUÁI</b> MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

5.1.6 ALMACENAMIENTO DE MEDIOS.....	58
5.1.7 ELIMINACIÓN DE RESIDUOS.....	58
5.1.8 RESPALDO FUERA DE SITIO .....	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.....	59
5.3.1 REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN .....	59
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.....	60
5.4.1 TIPOS DE EVENTOS REGISTRADOS .....	60
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

 <p><b>TETÁ REKUÁI</b> MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

5.4.7 NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO.....	60
5.4.8 EVALUACIÓN DE VULNERABILIDADES .....	60
5.5 ARCHIVOS DE REGISTROS .....	61
5.5.1 TIPOS DE REGISTROS ARCHIVADOS .....	61
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
5.8 EXTINCIÓN DE UN PCSC .....	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 TITULAR .....	65
6.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO .....	65
6.1.4 ENTREGA DE LA CLAVE PÚBLICA DEL PCSC A LA PARTE USUARIA.....	65
6.1.5 TAMAÑO DE LA CLAVE .....	66



 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

6.1.6 GENERACIÓN DE PARÁMETROS DE CLAVES ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD. ....	66
6.1.7 PROPÓSITOS DE USOS DE CLAVE (CONFORME AL CAMPO KEY USAGE X509 V3) .....	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/(ESCROW) 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 MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA.....	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

 <p><b>TETÁ REKUÁI</b> MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR .....	70
6.5.3 CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO .....	71
Como Establezca la DPC de la PNDI .....	71
6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA .....	71
6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA .....	71
Los sistemas informáticos del PCSC 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. ....	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 LCR.....	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 FUENTES DE TIEMPO.....	73
7. PERFILES DE CERTIFICADOS, CRL Y OCSP .....	74
7.1 PERFIL DEL CERTIFICADO .....	74
7.1.1 NÚMERO DE VERSIÓN.....	82
7.1.2 EXTENSIONES DEL CERTIFICADO.....	82
7.1.3 IDENTIFICADORES DE OBJETO DE ALGORITMOS .....	86
7.1.4 FORMAS DEL NOMBRE.....	87
7.1.5 RESTRICCIONES DEL NOMBRE .....	88
7.1.6 IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO .....	89

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

7.1.7	USO DE LA EXTENSIÓN RESTRICCIONES DE POLÍTICA (POLICY CONSTRAINTS) ...	89
7.1.8	SEMÁNTICA Y SINTAXIS DE LOS CALIFICADORES DE POLÍTICA (POLICY QUALIFIERS)	90
7.1.9	SEMÁNTICA DE PROCESAMIENTO PARA LA EXTENSIÓN DE POLÍTICAS DE CERTIFICADO (CERTIFICATE POLICIES) .....	90
7.2	PERFIL DE LA LCR .....	90
7.2.1	NÚMERO (S) DE VERSIÓN .....	90
7.2.2	CRL Y EXTENSIONES DE ENTRADAS DE CRL .....	90
7.3	PERFIL DE OCSP .....	91
7.3.1	NÚMERO (S) DE VERSIÓN .....	91
7.3.2	EXTENSIONES DE OCSP .....	91
8.	AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES .....	92
8.1	FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN .....	92
8.2	IDENTIFICACIÓN/CALIFICACIÓN DEL EVALUADOR .....	92
8.3	RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA .....	92
8.4	ASPECTOS CUBIERTOS POR LA EVALUACIÓN.....	92
8.5	ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA .....	92
8.6	COMUNICACIÓN DE RESULTADOS .....	92
9.	OTROS ASUNTOS LEGALES Y COMERCIALES .....	93
9.1	TARIFAS .....	93
9.1.1	TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS.....	93
9.1.2	TARIFAS DE ACCESO A CERTIFICADOS.....	93
9.1.3	TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN .....	93
9.1.4	TARIFAS POR OTROS SERVICIOS .....	93
9.1.5	POLÍTICAS DE REEMBOLSO .....	93
9.2	RESPONSABILIDAD FINANCIERA .....	94

 <p><b>TETÁ REKUÁI</b> MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

9.2.1 COBERTURA DE SEGURO.....	94
9.2.2 OTROS ACTIVOS .....	94
9.2.3 COBERTURA DE SEGURO O GARANTÍA PARA LAS PERSONAS FÍSICAS O JURÍDICAS TITULARES DE CERTIFICADOS.....	94
9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL .....	94
9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL.....	95
9.3.2 INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL	95
9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL.....	95
9.4.1 PLAN DE PRIVACIDAD.....	95
9.4.2 INFORMACIÓN TRATADA COMO PRIVADA.....	95
9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA .....	95
9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA .....	95
9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA .....	95
9.4.6 DIVULGACIÓN ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO .....	96
9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN .....	96
9.5 DERECHO DE PROPIEDAD INTELECTUAL.....	96
9.6 REPRESENTACIONES Y GARANTÍAS .....	96
9.6.1 REPRESENTACIONES Y GARANTÍAS DEL PCSC.....	96
9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA AR .....	97
9.6.3 REPRESENTACIONES Y GARANTÍAS DEL TITULAR DEL CERTIFICADO.....	97
9.6.4 REPRESENTACIONES Y GARANTÍAS DE LAS PARTES USUARIAS .....	97
9.6.5 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES .....	97
9.7 EXENCIÓN DE GARANTÍA .....	98
9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL .....	98

 <p><b>TETÁ REKUÁI</b> MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO: PC-PNDI-V1.1</b>	<b>FECHA: 07/02/2023</b>	

9.9	INDEMNIZACIONES .....	98
9.10	PLAZO Y FINALIZACIÓN .....	98
9.10.1	PLAZO .....	98
9.10.2	FINALIZACIÓN.....	98
9.10.3	EFFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA .....	98
9.11	NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES.....	98
9.12	ENMIENDAS.....	98
9.12.1	PROCEDIMIENTOS PARA ENMIENDAS .....	98
9.12.2	PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN .....	99
9.12.3	CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS .....	99
9.13	DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS .....	99
9.14	NORMATIVA APLICABLE.....	99
9.15	ADECUACIÓN A LA LEY APLICABLE.....	99
9.16	DISPOSICIONES VARIAS.....	99
9.16.1	ACUERDO COMPLETO .....	99
9.16.2	ASIGNACIÓN.....	99
9.16.3	DIVISIBILIDAD .....	99
9.16.4	APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DE DERECHOS).....	100
9.16.5	FUERZA MAYOR .....	100
9.17	OTRAS DISPOSICIONES.....	100
10.	DOCUMENTOS DE REFERENCIA .....	101

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## CONTROL DOCUMENTAL

DOCUMENTO	
<b>Título:</b> POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES	<b>Nombre del Archivo:</b> PC F2 PNDI v1.1
<b>Código:</b> PC-PNDI-V1.0	<b>Soporte Lógico:</b>  <a href="https://www.identificaciones.gov.py/firmadigital/PC/PC%20F2%20Y%20C2%20PNDI%20v1.0.pdf">https://www.identificaciones.gov.py/firmadigital/PC/PC%20F2%20Y%20C2%20PNDI%20v1.0.pdf</a>
<b>Fecha:</b> 07/02/2023	<b>Ubicación Física:</b> Policía Nacional - Departamento de Identificaciones (PNDI)
<b>Versión:</b> 1.1	

REGISTRO DE CAMBIOS		
Versión	Fecha	Motivo de cambio
1.0	13/09/19	Versión inicial
1.1	07/02/2023	Actualización de la Normativa

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

<b>DISTRIBUCIÓN DEL DOCUMENTO</b>	
<b>NOMBRE</b>	<b>ÁREA</b>
Ministerio de Industria y Comercio (MIC)	Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE)
Policía Nacional	Departamento de Identificaciones
Documento Público	<a href="https://www.identificaciones.gov.py/firmadigital/PC/PC%20F2%20Y%20C2%20PNDI%20v1.0.pdf">https://www.identificaciones.gov.py/firmadigital/PC/PC%20F2%20Y%20C2%20PNDI%20v1.0.pdf</a>

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

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

	Crio. Principal Inocencio Escobar	
--	-----------------------------------	--



 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

# 1. INTRODUCCIÓN

## 1.1. DESCRIPCIÓN GENERAL

Este documento establece los requisitos mínimos que obligatoriamente deberán ser observados por los Prestadores Cualificados de Servicios de Confianza (PCSC) en su carácter de Autoridad de Certificación Intermedia (ACI) y como integrantes de la Infraestructura de Clave Pública del Paraguay (ICPP), para la formulación y la elaboración de su política de certificación (PC)

Toda PC elaborada en el ámbito de la ICPP debe obligatoriamente adoptar la misma estructura empleada de este documento.

Esta PC es aplicable a los siguientes certificados:

- Certificado cualificado de firma electrónica

➤ F2

Los tipos de certificados "F" definen escalas de seguridad (1, 2 y 3), asociados con requisitos menos o más estrictos atendiendo al tipo de certificado. El nivel de seguridad estará caracterizado por los requisitos mínimos definidos para aspectos como: algoritmo y tamaño de la clave criptográfica, medios de almacenamiento de clave, proceso de generación del par de claves,

 <b>TETÁ REKUÁI</b> MOTENONDEHA MINISTERIO DEL INTERIOR	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

procedimiento de identificación del titular del certificado, frecuencia de emisión de la lista de certificados revocados (LCR) y el plazo de validez del certificado.

El par de claves criptográficas relacionadas a los tipos de certificado F2 deberá obligatoriamente ser generados y almacenados en módulos criptográficos tipo hardware en un:

- i) dispositivo Smart Card con capacidad de generación de claves;
- ii) token criptográfico u otro dispositivo equivalente, con capacidad de generación de
- iii) claves; o módulo de seguridad hardware (HSM)

Las claves privadas relacionadas a los certificados del tipo F1, F2, S1, S2 no podrán ser generadas ni gestionadas por los PCSC por lo que serán de exclusiva responsabilidad del titular del certificado o del responsable del mismo.

## 1.2 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

<b>Nombre:</b>	Políticas de Certificación Tipo F2 Persona Física de la Policía Nacional - Departamento de Identificaciones
<b>Versión:</b>	1.0
<b>Fecha de aprobación:</b>	07 – Febrero - 2023

	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

Ubicación de la DPC:	<a href="https://www.identificaciones.gov.py/firmadigital/DPC/DPC%20F2%20Y%20C2%20PNDI%20v1.0.pdf">https://www.identificaciones.gov.py/firmadigital/DPC/DPC%20F2%20Y%20C2%20PNDI%20v1.0.pdf</a>
----------------------	---

## 1.3 PARTICIPANTES DE LA PKI

### 1.3.1 AUTORIDADES CERTIFICADORAS (AC)

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:

- AC Raíz-Py: En la cúspide de la Jerarquía de la Infraestructura de Clave Pública del Paraguay (ICPP), se ubica la AC Raíz-Py, la misma cuenta con un certificado auto emitido y aceptado por los terceros que confían en la ICPP. Emite certificados a los PCSC y a partir de allí, comienza la cadena de confianza. Los certificados electrónicos emitidos por la AC Raíz-Py se rigen y ajustan a su Declaración de Prácticas de Certificación (DPC), cuyo cumplimiento es de carácter obligatorio.
- ACI; Es una entidad habilitada por la AA, encargada de operar una AC en el marco de la ICPP, debe contar con un certificado emitido por la AC Raíz-Py y solo podrá emitir certificados a personas físicas o jurídicas que sean usuarios finales. En el ámbito de la ICPP un PCSC es considerada una ACI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

Un PCSC presta servicios de CREACIÓN, VERIFICACIÓN Y VALIDACIÓN DE FIRMAS ELECTRÓNICAS CUALIFICADAS y/o SELLO ELECTRÓNICO CUALIFICADO y CERTIFICADOS RELATIVOS A ESTOS SERVICIOS.

El PCSC además podrá ser habilitado para prestar servicios de GENERACIÓN O GESTIÓN DE DATOS DE CREACIÓN DE FIRMA ELECTRÓNICA y/o DATOS DE CREACIÓN DE SELLO ELECTRÓNICO EN NOMBRE DEL FIRMANTE O CREADOR DEL SELLO en los términos establecidos en el documento DOC-ICPP-07 [2].

Un PCSC habilitado para brindar servicios de GENERACIÓN O GESTIÓN DE DATOS DE CREACIÓN DE FIRMA ELECTRÓNICA y/o DATOS DE CREACIÓN DE SELLO ELECTRÓNICO EN NOMBRE DEL FIRMANTE O CREADOR DEL SELLO, debe utilizar sistemas y productos fiables, incluidos canales de comunicación electrónicos seguros, aplicar procedimientos y mecanismos técnicos y organizativos adecuados para garantizar que el entorno sea confiable y que los datos de creación de firma o sello se utilicen bajo el control exclusivo del titular del certificado. Además, deben custodiar y proteger los datos de creación de firma o sello frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

Las claves privadas de los firmantes y/o de los creadores de sellos almacenadas en dispositivos estandarizados conforme lo establecido en el documento DOC-ICPP- 06 [1], y las firmas electrónicas cualificadas o los sellos electrónicos

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

calificados hechas por la clave privada del firmante y/o creador del sello en otros sistemas son válidas de conformidad a la Ley N° 6822/2021.

### 1.3.2 AUTORIDAD DE REGISTRO (AR)

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 (AR) llevarán a cabo la identificación de los solicitantes de certificados conforme a las normas de esta PC y el acuerdo suscrito con el PCSC de la PNDI.

El PCSC de la PNDI cumple funciones de AR. 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 AC 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 PCSC de la PNDI estarán siempre bajo el control y supervisión de este.

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

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

El PCSC de la PNDI mantiene publicada en el sitio principal de internet las siguientes informaciones actualizadas:

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO: PC-PNDI-V1.1</b>	<b>FECHA: 07/02/2023</b>	

- Lista de todas las ARs habilitadas
- Lista de las ARs que se han inhabilitado por el PCSC, indicando la fecha de la
- inhabilitación.

La AR vinculada al PCSC 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 DPC, PC, 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;

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

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

### 1.3.3 AUTORIDADES DE VALIDACION (AV)

La AV puede ser una entidad del PCSC o delegada a un tercero cuyo funcionamiento deberá ser autorizado por la AC Raíz-Py con la habilitación correspondiente. Su función es suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una AR y certificados por el PCSC.

Las AVs delegadas son autoridades de validación vinculadas a un PCSC mediante un acuerdo operacional.

El PCSC deberá igualmente publicar información referente a:

- Lista de todas las AVs habilitadas
- Lista de las AVs que se han inhabilitado por el PCSC, indicando la fecha de la inhabilitación

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

<https://www.identificaciones.gov.py/firmadigital/av>

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

### 1.3.4 TITULARES DEL CERTIFICADO

Son las personas físicas o jurídicas que podrán ser titulares de los certificados emitidos por el PCSC según corresponda a un certificado cualificado de firma electrónica o de sello electrónico cualificado respectivamente conforme a esta PC.

### 1.3.5 PARTE USUARIA

Se entenderá por parte usuaria, toda persona física o jurídica que confía en el servicio de confianza. Es decir confía en el contenido, validez y aplicabilidad del certificado electrónico y claves emitidas en el marco de la ICPP.

### 1.3.6. OTROS PARTICIPANTES

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

Las PSS son entidades externas a las que recurre el PCSC de la PNDI o un AR vinculada para desempeñar actividades descritas en esta PC o en una DPC 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 PCSC de la PNDI se encuentran en la dirección de página web (URL):



 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

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

El PCSC deberá igualmente publicar información referente a:

- Lista de todas las PSSs habilitadas
- Lista de los PSSs que se han inhabilitado por el PCSC, indicando la fecha de la inhabilitación.

## 1.4 USO DEL CERTIFICADO

### 1.4.1 USOS APROPIADOS DEL CERTIFICADO

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

Para determinar si es posible utilizar un certificado de firma digital, autenticación y cifrado del tipo F2 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
------	------------------------------

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

<b>Certificado de Firma Digital tipo F2</b>	<b>Firma digital y Autenticación</b> <ul style="list-style-type: none"> <li>● No repudio (Non- Repudiation)</li> <li>● Firma Digital (Digital Signature)</li> <li>● Cifrado de Clave (Key Encipherment)</li> </ul>
---	--

**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.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 1.4.2 USOS PROHIBIDOS DEL CERTIFICADO

Los certificados emitidos por el PCSC 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 PC y en la normativa vigente, está fuera del alcance y responsabilidad de esta PC.

El uso indebido de los certificados será sancionado por el PCSC 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](mailto: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

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

**Dirección de correo electrónico:** [dpto.identificaciones@pn.gov.py](mailto:dpto.identificaciones@pn.gov.py)

### 1.5.3 PERSONA QUE DETERMINA LA ADECUACIÓN DE LA DPC 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 (PC).



### 1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA PC

El personal autorizado del PCSC de la PNDI, conforme con la reglamentación vigente, validará el contenido de la Política de Certificación (PC) 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

- **Agente de registro:** persona responsable de la realización de las actividades inherentes a la AR. Realiza la identificación de los solicitantes en la solicitud de emisión/revocación de certificados de firma electrónica cualificada o sello electrónico cualificado.
- **Autenticación:** proceso técnico que permite determinar la identidad de la persona física o jurídica.

	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

- **Autoridad de Aplicación:** Ministerio de Industria y Comercio a través de la Dirección General de Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.
- **Autoridad de Certificación:** entidad que presta servicios de emisión, gestión, revocación u otros servicios de confianza basados en certificados cualificados. En el marco de la ICPP, son Autoridades de Certificación, la AC Raíz-Py y el PCSC.
- **Autoridad de Certificación Raíz del Paraguay:** órgano técnico, cuya función principal es coordinar el funcionamiento de la ICPP. La AC Raíz-Py tiene los certificados de más alto nivel, posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza. Las funciones de la AC Raíz-Py son ejercidas por la AA.
- **Autoridad de Certificación Intermedia:** entidad cuyo certificado ha sido emitido por la AC Raíz-Py, es responsable de la emisión de certificados cualificados a personas físicas y jurídicas. Un Prestador cualificado de Servicios de Confianza es considerado una Autoridad de Certificación Intermedia.
- **Autoridad de Registro:** entidad responsable de tramitar las distintas solicitudes inherentes a certificados cualificados, identificar al solicitante y remitir las solicitudes al PCSC. La AR puede ser propia del PCSC o delegada a un tercero.
- **Autoridad de Validación:** entidad responsable de suministrar información sobre la vigencia de los certificados que a su vez hayan sido

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

registrados por una AR y certificados por la AC. La AV puede ser propia del PCSC o delegada a un tercero.

- **Gestión de datos de creación de firma o sello electrónico:** El PCSC podrá, en nombre del firmante o creador de sello gestionar los datos de creación de firma o sello electrónico a los que hayan prestado sus servicios, este servicio deberá ser provisto por un PCSC siempre y cuando cuente con la debida habilitación.
- **Cadena de certificación:** lista ordenada de certificados que contiene un certificado del firmante o creador de sello y certificados de la AC, que termina en un certificado raíz. El emisor del certificado del firmante o creador de sello es el titular del certificado del PCSC y a su vez, el emisor del certificado del PCSC es el titular del certificado de AC Raíz-Py. El firmante, creador de sello o la parte usuaria debe verificar la validez de los certificados en la cadena de certificación.
- **Certificado cualificado de firma electrónica:** un certificado de firma electrónica que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 43 de la ley No 6822/2021.
- **Certificado cualificado de sello electrónico:** un certificado de sello electrónico que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 53 de la ley No 6822/2021.
- **Certificado cualificado tributario:** certificado expedido por un Prestador Cualificado de Servicios de Confianza, el cual podrá ser utilizado para todos los fines convencionales ante el Sistema Marangatu, Sistema

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

Integrado de Facturación Electrónica Nacional, otros Sistemas de Información administrados por la Subsecretaría de Estado de Tributación (SET) así como otros usos afines autorizados por la Autoridad de Aplicación.

- **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.
- **Contrato de prestación de servicio de confianza:** Acuerdo entre la AC Raíz-Py y el PCSC, o entre el PCSC y el titular o responsable del certificado que contiene información relativa al solicitante del certificado y además establece los derechos, obligaciones y responsabilidades de las partes con respecto a la prestación del servicio. Este contrato, requiere la aceptación explícita de las partes intervinientes.
- **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 ICPP, es la criptografía asimétrica. En ella, se emplean 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 electrónico, mientras que a la otra se le denomina privada y está bajo exclusivo control del titular o responsable del certificado.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

- **Compromiso:** violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.
- **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:** documento en el cual se determina la declaración de las prácticas que emplea una AC al emitir certificados y que define la infraestructura, políticas y procedimientos que utiliza la AC para satisfacer los requisitos especificados en la PC vigente.
- **Documento de identidad:** documento válido y vigente que permite acreditar la identidad de la persona, a los efectos del proceso de emisión, suspensión o revocación del certificado cualificado electrónico será considerada la cédula de identidad civil o el pasaporte del solicitante.
- **Emisor del certificado:** persona física o jurídica cuyo nombre aparece en el campo emisor de un certificado.
- **Emisión de certificado:** es la autorización de la emisión del certificado en el sistema del PCSC previa comprobación de la concordancia de los datos de solicitud del certificado con los contenidos en los documentos presentados.
- **Firma electrónica cualificada:** una firma electrónica que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica, la cual deberá estar vinculada al firmante de manera única, permitir la identificación del



 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

firmante, haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo y estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

- **Firmante:** una persona física que crea una firma electrónica.
- **Generador:** 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 AC, incluyendo los circuitos de iluminación, de los equipos informáticos, equipos de refrigeración, circuitos de monitoreo, prevención de incendios; en fin de todos los circuitos eléctricos críticos para el funcionamiento de las instalaciones tecnológicas.
- **Habilitación:** autorización que otorga el MIC, una vez cumplidos los requisitos y condiciones establecidos en la norma.
- **Identificador de Objeto:** 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.
- **Identificación del Titular de certificado:** comprende la etapa de la confirmación de la identidad de una persona física o jurídica, realizada a

	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

través de la presencia física del interesado o mediante otros medios que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, conforme a los supuestos establecidos en la Ley y en base a los documentos de identificación previstos en la presente DPC.

- **Infraestructura de Claves Públicas del Paraguay:** conjunto de personas, normas, leyes, políticas, procedimientos y sistemas informáticos necesarios para proporcionar una plataforma criptográfica de confianza que garantiza la presunción de validez legal para actos electrónicos firmados o cifrados con certificados electrónicos cualificados y claves criptográficas emitidas por esta infraestructura.
- **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.
- **Lista de Certificados Revocados:** lista emitida por una AC, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.
- **Lista de Confianza:** Lista publicada en el sitio web oficial de la AC Raíz - Py y que contiene información relativa a los Prestadores cualificados de servicios de confianza y a los servicios cualificados que éstos prestan conforme a la Ley No 6822/21.
- **Módulo criptográfico:** software o hardware criptográfico que genera y almacena claves criptográficas.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

- **Módulo de Seguridad de Hardware:** dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.
- **Normas Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la prestación de los servicios mencionados en la presente DPC.
- **Organismo de Evaluación de Conformidad:** organismo que desempeña actividades de evaluación de la conformidad a un prestador de servicios de confianza y de los servicios de confianza que este presta conforme a la Ley No 6822/2021.
- **Organismo de Supervisión:** organismo que concede y retira la cualificación a los prestadores de servicios de confianza y a los servicios de confianza que prestan además de las funciones establecidas en el artículo 17 de la Ley No 6822/2021.
- **Parte usuaria:** persona física o jurídica que confía en el servicio de confianza.
- **Perfil del certificado:** especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).
- **Política de Certificación:** documento en el cual la AC 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.

	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

- **Prestador Cualificado de Servicios de Confianza:** prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la habilitación.
- **Política de Seguridad:** es un conjunto de directrices destinadas a definir la protección del personal, seguridad física, lógica y de red, clasificación de la información, salvaguarda de activos de la información, gerenciamento de riesgos, plan de continuidad de negocio y análisis de registros de eventos de una AC.
- **Prestador de Servicios de Soporte:** entidad externa vinculada a un PCSC mediante un acuerdo operacional a la que recurre la AC o la AR y autorizada por la AC Raíz-Py para desempeñar actividades descritas en la DPC o en una PC.
- **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 AC con el fin de difundir su información pública.
- **Rol de confianza:** función crítica que desempeña personal de la AC, que si se realiza insatisfactoriamente puede tener un impacto adverso sobre el grado de confianza proporcionado por la AC.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

- **Servicio OCSP:** permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la AC sobre el estado de un certificado.
- **Solicitante de Certificado:** persona física o jurídica que solicita la emisión de un certificado a una AC.
- **Solicitud de Firma de Certificado:** petición de certificado electrónico que se envía a la AC, mediante la información contenida en el CSR, la AC, puede emitir el certificado electrónico una vez realizadas las comprobaciones que correspondan.
- **Solicitud de certificado:** documento que se instrumenta mediante un formato autorizado de solicitud de certificado o como parte de documento específico denominado Contrato de Prestación de Servicios de Confianza, suscripto por el solicitante en nombre propio en el caso de certificados cualificados de firma electrónica para persona física, o bien en nombre del titular en el caso de certificados cualificados de sello electrónico para persona jurídica.
- **Solicitud de revocación:** documento que se instrumenta mediante un formato autorizado de solicitud para la revocación de un certificado.
- **Verificación y validación de firma o sello:** determinación y validación de que la firma o sello electrónico fue creado durante el periodo operacional de un certificado válido, por la clave privada correspondiente a la clave pública que se encuentra en el certificado y que el mensaje no ha sido alterado desde que su creación.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	



- **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
AA	Autoridad de Aplicación
AGR	Agente de Registro
P	País (C por su sigla en Inglés, Country)
AC	Autoridad de Certificación (CA por sus siglas en inglés, Certificate Authority)
ACI	Autoridad de Certificación Intermedia (CAI por sus siglas en inglés, Certificate Authority Intermediate)
AC Raíz-Py	Autoridad Certificadora Raíz del Paraguay
CI	Cédula de identidad civil
NC	Nombre Común (CN por sus siglas en inglés, Common Name)

 <p><b>TETÁ REKUÁI</b> MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO: PC-PNDI-V1.1</b>	<b>FECHA: 07/02/2023</b>	

PC	Políticas de Certificación (CP por sus siglas en inglés, Certificate Policy)
DPC	Declaración de Prácticas de Certificación (DPC por sus siglas en inglés, Certification Practice Statement)
LCR	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)
DGCE	Dirección General de Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.
HSM	Módulo de Seguridad Criptográfico basado en Hardware (HSM por sus siglas en inglés, Hardware Security Module)
ISO	Organización Internacional para la Estandarización (por sus siglas en inglés International Organization for Standardization)
MIC	Ministerio de Industria y Comercio

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

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)
PAS	Pasaporte
ICPP	Infraestructura de Clave Pública del Paraguay
PCSC	Prestador cualificado de servicios de confianza
PSS	Prestador de Servicios de Soporte
PY	Paraguay
AR	Autoridad de Registro (RA por sus siglas en inglés Registration Authority)
RFC	Petición de Comentarios (RFC por sus siglas en inglés Request for Comments)
RUC	Registro único del contribuyente



 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

URL	Localizador uniforme de recursos (URL por sus siglas en inglés Uniform Resource Locator)
AV	Autoridad de Validación (VA por sus siglas en inglés Validation Authority)

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

### 2.1 REPOSITORIOS

El PCSC de la PNDI, es responsable de las funciones de repositorio para su AC.

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

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

El repositorio público del PCSC 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 DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN

Como establezca la DPC de la PNDI.

## 2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 3. IDENTIFICACION Y AUTENTICACION

### 3.1 NOMBRES

#### 3.1.1 TIPOS DE NOMBRES

Como establezca la DPC de la PNDI.

#### 3.1.2 NECESIDAD DE NOMBRES SIGNIFICATIVOS

Como establezca la DPC de la PNDI.

#### 3.1.3 ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES

Como establezca la DPC de la PNDI.

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

Como establezca la DPC de la PNDI.

#### 3.1.5 UNICIDAD DE LOS NOMBRES

Como establezca la DPC de la PNDI.

#### 3.1.6. RECONOCIMIENTO PARA RESOLVER DIPUTA DE NOMBRE

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

### **3.1.7 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 DPC de la PNDI.

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

Como establezca la DPC 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 DPC de la PNDI.

#### **3.2.4 INFORMACIÓN NO VERIFICADA DEL TITULAR DEL CERTIFICADO**

No aplica.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

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

Como establezca la DPC de la PNDI.

### **3.2.6 CRITERIOS PARA INTEROPERABILIDAD**

Como establezca la DPC de la PNDI.

### **3.2.7. PROCEDIMIENTOS COMPLEMENTARIOS**

Como establezca la DPC de la PNDI.

### **3.2.8 PROCEDIMIENTOS ESPECÍFICOS**

Como establezca la DPC de la PNDI.

## **3.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE NUEVAS CLAVES**

## **3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN**

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 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 DPC de la PNDI.

#### 4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

Como establezca la DPC 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 DPC de la PNDI.

#### 4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

### **4.2.3 TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO**

Como establezca la DPC de la PNDI.

## **4.3 EMISIÓN DEL CERTIFICADO**

### **4.3.1 ACCIONES DEL PCSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS**

Como establezca la DPC de la PNDI.

### **4.3.2 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO POR PARTE DEL PCSC SOBRE LA EMISIÓN DEL CERTIFICADO**

Como establezca la DPC de la PNDI.

## **4.4 ACEPTACIÓN DEL CERTIFICADO**

### **4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO**

Como establezca la DPC de la PNDI.

### **4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PCSC**

Como establezca la DPC de la PNDI.



 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

#### **4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR EL PCSC A OTRAS ENTIDADES**

Como establezca la DPC 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 TITULAR O RESPONSABLE**

Como establezca la DPC de la PNDI.

##### **4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LA PARTE USUARIA**

Como establezca la DPC de la PNDI.

#### **4.6 RENOVACIÓN DEL CERTIFICADO**

Como establezca la DPC de la PNDI

##### **4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO**

Como establezca la DPC de la PNDI

##### **4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN**

Como establezca la DPC de la PNDI

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

#### **4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO**

Como establezca la DPC de la PNDI

#### **4.6.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO**

Como establezca la DPC de la PNDI

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

Como establezca la DPC de la PNDI

#### **4.6.6 PUBLICACIÓN POR EL PCSC DEL CERTIFICADO RENOVADO**

Como establezca la DPC de la PNDI

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

No aplica.

#### **4.7 RE-EMISIÓN DE CLAVES DE CERTIFICADO (RE-KEY)**

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

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

Como establezca la DPC de la PNDI

#### **4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA**

Como establezca la DPC de la PNDI

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

Como establezca la DPC de la PNDI

#### **4.7.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO SOBRE LA RE-EMISIÓN DE UN NUEVO CERTIFICADO**

Como establezca la DPC de la PNDI

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

Como establezca la DPC de la PNDI

#### **4.7.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS RE-EMITIDOS**

Como establezca la DPC de la PNDI

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

Como establezca la DPC de la PNDI

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 4.8 MODIFICACIÓN DE CERTIFICADOS

Como establezca la DPC de la PNDI.

### 4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO

Como establezca la DPC de la PNDI

### 4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

Como establezca la DPC de la PNDI

### 4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

Como establezca la DPC de la PNDI

### 4.8.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO DE LA EMISIÓN DE UN NUEVO CERTIFICADO

Como establezca la DPC de la PNDI

### 4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

Como establezca la DPC de la PNDI

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

No aplica.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

#### **4.8.7 NOTIFICACIÓN POR EL PCSC DE EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES**

No aplica.

### **4.9 REVOCACIÓN Y SUSPENSIÓN**

#### **4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN**

Como establezca la DPC de la PNDI.

#### **4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN**

Como establezca la DPC de la PNDI.

#### **4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN**

Como establezca la DPC de la PNDI.

#### **4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN**

Como establezca la DPC de la PNDI.

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

Como establezca la DPC de la PNDI.

#### **4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LA PARTE USUARIA**

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

#### **4.9.7 FRECUENCIA DE EMISIÓN DEL LCR**

Como establezca la DPC de la PNDI.

#### **4.9.8 LATENCIA MÁXIMA PARA LCR**

Como establezca la DPC de la PNDI.

#### **4.9.9 DISPONIBILIDAD PARA REVOCACIÓN / VERIFICACIÓN DE ESTADO EN LÍNEA**

Como establezca la DPC de la PNDI.

#### **4.9.10 REQUISITOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA**

Como establezca la DPC de la PNDI.

#### **4.9.11 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES**

Como establezca la DPC de la PNDI.

#### **4.9.12 REQUERIMIENTOS ESPECIALES POR EL COMPROMISO DE LA CLAVE PRIVADA**

Como establezca la DPC de la PNDI.

#### **4.9.13 CIRCUNSTANCIAS PARA SUSPENSIÓN**

Como establezca la DPC de la PNDI.

#### **4.9.14 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN**

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

#### **4.9.15 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN**

Como establezca la DPC de la PNDI.

#### **4.9.16 LÍMITES DE PERÍODO DE SUSPENSIÓN**

Como establezca la DPC de la PNDI.

### **4.10 SERVICIOS DE ESTADO DE CERTIFICADO**

#### **4.10.1 CARACTERÍSTICAS OPERACIONALES**

Como establezca la DPC de la PNDI.

#### **4.10.2 DISPONIBILIDAD DEL SERVICIO**

Como establezca la DPC de la PNDI.

#### **4.10.3 CARACTERÍSTICAS OPCIONALES**

No aplica.

#### **4.11 FIN DE LA SUSCRIPCIÓN**

Como establezca la DPC 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 DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO: PC-PNDI-V1.1</b>	<b>FECHA: 07/02/2023</b>	

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

No aplica.



 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 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 DPC de la PNDI.

#### 5.1.2 ACCESO FÍSICO

Como establezca la DPC de la PNDI.

##### 5.1.2.1 NIVELES DE ACCESO FÍSICO

Como establezca la DPC de la PNDI.

##### 5.1.2.2. SISTEMAS FÍSICOS DE DETECCIÓN

Como establezca la DPC de la PNDI.

##### 5.1.2.3. SISTEMAS DE CONTROL DE ACCESO

Como establezca la DPC de la PNDI.

##### 5.1.2.4. MECANISMOS DE EMERGENCIA

Como establezca la DPC de la PNDI.

#### 5.1.3 ENERGÍA Y AIRE ACONDICIONADO

Como establezca la DPC de la PNDI.

#### 5.1.4 EXPOSICIONES AL AGUA

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

### **5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO**

Como establezca la DPC de la PNDI.

### **5.1.6 ALMACENAMIENTO DE MEDIOS**

Como establezca la DPC de la PNDI.

### **5.1.7 ELIMINACIÓN DE RESIDUOS**

Como establezca la DPC de la PNDI.

### **5.1.8 RESPALDO FUERA DE SITIO**

Como establezca la DPC de la PNDI.

## **5.2 CONTROLES PROCEDIMENTALES**

Como establezca la DPC de la PNDI.

### **5.2.1 ROLES DE CONFIANZA**

Como establezca la DPC de la PNDI.

### **5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA**

Como establezca la DPC de la PNDI.

### **5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL**

Como establezca la DPC de la PNDI.

### **5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES**

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 5.3 CONTROLES DE PERSONAL

### 5.3.1 REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

Como establezca la DPC de la PNDI.

### 5.3.2 PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Como establezca la DPC de la PNDI.

### 5.3.3 REQUERIMIENTOS DE CAPACITACIÓN

Como establezca la DPC de la PNDI.

### 5.3.4 REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

Como establezca la DPC de la PNDI.

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

Como establezca la DPC de la PNDI.

### 5.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS

Como establezca la DPC de la PNDI.

### 5.3.7 REQUISITOS DE CONTRATACIÓN A TERCEROS

Como establezca la DPC de la PNDI

### 5.3.8 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

Como establezca la DPC de la PNDI

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 5.4 PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

### 5.4.1 TIPOS DE EVENTOS REGISTRADOS

Como establezca la DPC de la PNDI.

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

Como establezca la DPC de la PNDI.

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

Como establezca la DPC de la PNDI.

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

Como establezca la DPC de la PNDI.

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

Como establezca la DPC de la PNDI.

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

Como establezca la DPC de la PNDI.

### 5.4.7 NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

Como establezca la DPC de la PNDI.

### 5.4.8 EVALUACIÓN DE VULNERABILIDADES

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 5.5 ARCHIVOS DE REGISTROS

### 5.5.1 TIPOS DE REGISTROS ARCHIVADOS

Como establezca la DPC de la PNDI.

### 5.5.2 PERIODOS DE RETENCIÓN PARA ARCHIVOS

Como establezca la DPC de la PNDI.

### 5.5.3 PROTECCIÓN DE ARCHIVOS

Como establezca la DPC de la PNDI.

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

Como establezca la DPC 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 DPC de la PNDI.

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

Como establezca la DPC de la PNDI.

## 5.6 CAMBIO DE CLAVE

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 5.7 RECUPERACIÓN DE DESASTRES Y COMPROMISO

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

Como establezca la DPC de la PNDI.

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

Como establezca la DPC de la PNDI.

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

Como establezca la DPC de la PNDI.

#### 5.7.3.1. CERTIFICADO DE ENTIDAD ES REVOCADO

Como establezca la DPC de la PNDI.

#### 5.7.3.2. CLAVE DE ENTIDAD ESTÁ COMPROMETIDA

Como establezca la DPC de la PNDI.

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

Como establezca la DPC de la PNDI.

## 5.8 EXTINCIÓN DE UN PCSC

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 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 AC 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 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.

 <b>TETÁ REKUÁI</b> MOTENONDEHA MINISTERIO DEL INTERIOR	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

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.

<b>TIPO DE CERTIFICADO</b>	<b>MEDIO DE ALMACENAMIENTO</b>
F2	<ul style="list-style-type: none"> <li>• Hardware criptográfico certificado por el MIC (Tarjeta inteligente o token con capacidad de generación de claves)</li> <li>• Hardware criptográfico certificado por el MIC (HSM)</li> </ul>



 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

### 6.1.2 ENTREGA DE LA CLAVE PRIVADA AL TITULAR

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 PCSC 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 a través de un medio electrónico seguro.

### 6.1.4 ENTREGA DE LA CLAVE PÚBLICA DEL PCSC A LA PARTE USUARIA

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

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

La forma para la entrega de un certificado emitido por el PCSC 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 PCSC de la PNDI; y
- Otros medios seguros aprobados por el MIC.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

### 6.1.5 TAMAÑO DE LA CLAVE

Los tamaños de clave a ser utilizados en los certificados de tipo F2 emitidos por el PCSC 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 PCSC de la PNDI cumplen con el estándar FIPS 140-2 nivel 3 para certificados tipo F2.

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 (CONFORME AL CAMPO KEY USAGE X509 V3)

Los usos admitidos de la clave para los certificados tipo F2 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 se puede consultar en el apartado 7.1 de la presente PC.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 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 PCSC 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/(ESCROW) DE LA CLAVE PRIVADA

El PCSC 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 PCSC 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 PCSC de la PNDI nunca archiva claves privadas de sus suscriptores para certificados de Tipo F2 emitido bajo esta PC.

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

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

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 PCSC de la PNDI nunca transfiere claves privadas de sus suscriptores para certificados emitidos bajo esta PC.

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 PCSC 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.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

### 6.2.10 MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA

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

## 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 LCR emitidas, son almacenadas por el PCSC 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 es como máximo de 2 (dos) años desde el momento de emisión del mismo.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 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, 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

Como establezca la DPC de la PNDI

## 6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

### 6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

Como establezca la DPC de la PNDI

### 6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

Como establezca la DPC de la PNDI

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

### 6.5.3 CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO

Como Establezca la DPC de la PNDI

## 6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

### 6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA

Los sistemas informáticos del PCSC 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 PCSC de la PNDI comprueba los niveles de seguridad configurados periódicamente para la verificación del correcto funcionamiento del sistema.

En caso de incidencias, el PCSC 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

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

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 6.6.4 CONTROLES EN LA GENERACIÓN DE LCR

Antes de su publicación, todas las LCRs generadas por el PCSC, deben ser comprobadas la consistencia de su contenido, comparándolo con el contenido esperado en relación al número de LCR, la fecha / hora de emisión y otras informaciones relevantes.

## 6.7 CONTROLES DE SEGURIDAD DE RED

En el caso que el ambiente de utilización del certificado definido por la PC exija controles específicos de seguridad de red, estos controles deben de ser descritos en este ítem de la PC, de acuerdo con las normas, criterios, prácticas y procedimientos de la ICPP.

### 6.7.1 DIRECTRICES GENERALES

Como establezca la DPC de la PNDI

### 6.7.2 FIREWALL

Como establezca la DPC de la PNDI

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

Como establezca la DPC de la PNDI

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

Como establezca la DPC de la PNDI



 <p><b>TETÁ REKUÁI</b> MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 6.8 FUENTES DE TIEMPO

Todos los sistemas deben estar sincronizados en fecha y hora utilizando una fuente confiable de tiempo ajustados a la fecha y hora oficial paraguaya.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 7. PERFILES DE CERTIFICADOS, CRL Y OCSP

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

### 7.1 PERFIL DEL CERTIFICADO

El certificado digital del PCSC 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.

 <b>TETÁ REKUÁI</b> MOTENONDEHA MINISTERIO DEL INTERIOR	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

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 {OID: 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) {OID: 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) {OID: 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 PCSC de la PNDI. Este campo indica el número de serie del certificado digital.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

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 PCSC 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 (Subscriber 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 PCSC 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.

 <b>TETÁ REKUÁI</b> MOTENONDEHA MINISTERIO DEL INTERIOR	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

	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 contener el hash SHA-1 de la clave pública del titular del certificado. Este Campo es usado por	NO

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

		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 PCSC 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	[1] Acceso a información de autoridad	Este Campo es usado para indicar las	NO

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

<p>Access (Acceso a la información de la entidad emisora)</p>	<p>Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2)</p> <p>Nombre alternativo: Dirección URL= <a href="https://www.identificaciones.gov.py/firmadigital/PCSCCA.crt">https://www.identificaciones.gov.py/firmadigital/PCSCCA.crt</a></p> <p>[2] Acceso a información de autoridad</p> <p>Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)</p> <p>Nombre alternativo: Dirección URL= <a href="https://ocsp.identificaciones.gov.py/ocsp">https://ocsp.identificaciones.gov.py/ocsp</a></p>	<p>direcciones donde puede ser encontrado el certificado del PCSC de la PNDI.</p> <p>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.</p> <p>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</p>
---	--	---

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

		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= <a href="https://www.identificaciones.gov.py/firmadigital/crl/SignatureCRL.crl">https://www.identificaciones.gov.py/firmadigital/crl/SignatureCRL.crl</a>	Este Campo es usado para indicar las direcciones donde puede ser encontrado el LCR correspondientes al PCSC 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:	SI



 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

		<ul style="list-style-type: none"> <li>•digitalSignature;</li> <li>•NonRepudiation (renombrado recientemente con el nombre de contentCommitmen); y</li> <li>•keyEncipherment</li> </ul>	
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)	Id. De certificador de directiva= DPC Certificador: <a href="https://www.identificaciones.gov.py/firmadigital/DPC/DPC%20F2%20PNDI%20v1.0.pdf">https://www.identificaciones.gov.py/firmadigital/DPC/DPC%20F2%20PNDI%20v1.0.pdf</a> [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 almacenada en un módulo de hardware y son	Contiene la dirección WEB de la DPC del PCSC de la PNDI que emite el certificado.	NO

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

	<p>utilizadas para autenticar a su titular y generar firmas digitales.</p> <p>[1,3] Información de certificador de directiva:</p> <p>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</p>		
--	---	--	--

### 7.1.1 NÚMERO DE VERSIÓN


Los certificados emitidos por el PCSC 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:

La ICPP define las siguientes extensiones como obligatorias:

- a) **Identificador de la clave de la Autoridad Certificadora "Authority Key Identifier", no crítica:** El campo *key Identifier* debe contener el hash SHA-1 de la clave pública del PCSC;
- b) **Identificador de la clave del titular del certificado "Subject Key Identifier", no crítica:** debe contener el hash SHA-1 de la clave pública del titular del certificado;

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

**c) Uso de Claves "KeyUsage", crítica:**

c.1.1) **para certificados cualificados de firma electrónica:** debe contener los bits *digitalSignature*, *keyEncipherment* y *nonRepudiation* activados;

c.1.2) **para certificados cualificados de sello electrónico:** debe contener los bits *digitalSignature*, *keyEncipherment* y *nonRepudiation* activados;

c.1.3) **para certificados cualificados tributarios:** debe contener los bits *digitalSignature*, *keyEncipherment* o *keyAgreement* y *nonRepudiation* activados.

**d) Uso extendido de la clave "Extended Key Usage", no crítico:**

d.1) **para certificados cualificados de firma electrónica:** al menos uno de los propósitos *client authentication OID= 1.3.6.1.5.5.7.3.2* o *E-mail protection OID = 1.3.6.1.5.5.7.3.4* debe estar activado y pudiendo implementar otros propósitos instituidos, siempre que sean verificables y previstos por el PCSC en su PC de acuerdo con el RFC 5280;

d.2) **para certificados cualificados de sello electrónico:** al menos uno de los propósitos *client authentication OID= 1.3.6.1.5.5.7.3.2* o *E-mail protection OID = 1.3.6.1.5.5.7.3.4* debe estar activado y pudiendo implementar otros propósitos instituidos, siempre que sean verificables y previstos por el PCSC en su PC de acuerdo con el RFC 5280;

d.3) **para certificados cualificados tributarios:** el propósito *client authentication OID = 1.3.6.1.5.5.7.3.2* debe estar activado. Puede contener el propósito *server authentication OID = 1.3.6.1.5.5.7.3.1*.

d.4) **para certificados de firma de respuesta OCSP:** solamente el propósito *OCSPSigning OID = 1.3.6.1.5.5.7.3.9* debe estar presente;

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

**e) Directivas del Certificado "Certificate Policies", no crítica:**

**e.1) para certificados cualificados de firma electrónica:**

e.1.1) el campo ***policyIdentifier*** debe contener los OIDs de la PC implementada por el PCSC titular del certificado, para la emisión de certificados de personas físicas;

e.1.2) el campo ***policyQualifiers***

e.1.2.1) el campo ***CPS Pointer*** debe contener la dirección web de la DPC del PCSC que emite el certificado.

e.1.2.2) el campo ***User Notice*** debe decir: "**certificado cualificado de firma electrónica tipo [siglas: F2 (claves en dispositivo cualificado) o F3 (clave en dispositivo cualificado centralizado) según tipo de certificado]** sujeta a las condiciones de uso expuestas en la DPC del [*nombre del PCSC*]"

**f) Restricciones Básicas "*Basic Constraints*", crítica:**

f.1) el campo ***Subject Type*** debe contener Entidad Final= True f.2) el campo ***PathLenConstraint*** debe tener valor cero;

**g) Puntos de distribución de las LCR "CRL Distribution Points", no crítica:**



g.1) el campo ***Distribution Point 1*** debe contener la primera dirección web donde se obtiene la LCR correspondiente al certificado; y

g.2) el campo ***Distribution Point 2*** debe contener la segunda dirección web donde se obtiene la LCR correspondiente al certificado.

**h) Acceso a la Información de la Autoridad Certificadora "Authority Information Access", no crítica:**

h.1) Primer acceso

h.1.1) en el campo ***Access Method 1*** debe contener el identificador de método de acceso a la información de revocación (OCSP); y

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

h.1.2) en el campo **Access Location 1** debe contener la dirección Web del servicio del OCSP, utilizando uno de los siguientes protocolos de acceso: HTTP, HTTPS o LDAP.

h.2) Segundo acceso

h.2.1) en el campo **Access Method 2** debe contener el identificador de método de acceso del certificado del PCSC; y

h.2.2) en el campo **Access Location 2** debe contener la dirección web donde se encuentra alojado el certificado del PCSC, utilizando uno de los siguientes protocolos de acceso: HTTP, HTTPS o LDAP.

i) **Nombre Alternativo del Sujeto "Subject Alternative Name", no crítica**, en los siguientes formatos:

**i.1) Para CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA:**

**i.1.1) Campo NO obligatorio: Rfc822Name= [email del titular del certificado]; i.1.2) 1 (un) campo otherName, obligatorio, que contiene:**

**1. DirectoryName OID=2.5.4.13:** *debe contener el siguiente mensaje:*

**1.1) para certificado del tipo F2: ["FIRMA ELECTRÓNICA CUALIFICADA"]**

**1.2) para certificado del tipo F3: ["FIRMA ELECTRÓNICA CUALIFICADA CENTRALIZADA"]**

**i.1.2) 4 (cuatro) campos otherName, NO obligatorios, que contienen:**

**1. DirectoryName OID= 2.5.4.10:** *[nombre de la organización en el que presta servicio el titular del certificado];*

**2. DirectoryName OID= 2.5.4.11:** *[nombre de la unidad de la organización en el que presta servicio el titular del certificado];*

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

3. **DirectoryName OID=2.5.4.5: RUC** [siglas **RUC** seguido del *número de RUC correspondiente a la organización en el que presta servicio el titular del certificado o el número de RUC del titular del certificado si no se registran los datos de la organización en la que presta servicio*];
4. **DirectoryName OID=2.5.4.12:** [*posición o función designada al titular del certificado en la organización en el que presta servicio o título académico del titular del certificado*];

i.3.3) 2 (dos) campos otherName, NO obligatorios, que contienen:

1. **DirectoryName OID= 2.5.4.11:** [*nombre de la unidad de la organización en el que presta servicio el titular del certificado*]; y
  2. **DirectoryName OID=2.5.4.12:** [*posición o función designada al titular del certificado en la organización en el que presta servicio* ];
- Los campos otherName definidos por la ICPP deben cumplir con las siguientes

especificaciones:

- a) El conjunto de información definido en cada campo otherName debe almacenarse como una cadena de tipo **ASN.1 OCTET STRING o PRINTABLE STRING**; y
- b) Solo se pueden utilizar los caracteres de la A a la Z, del 0 al 9, observando lo establecido en el ítem 7.1.5 del presente documento.

Otros campos que componen la extensión "**Subject Alternative Name**" podrán ser utilizados en la forma y con los propósitos definidos por la RFC 5280 siempre y cuando estén aprobados por la AC Raíz-Py.

### 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

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

- 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

El nombre del titular del certificado, que consta en el campo “*Subject*”, deberá adoptar el “*Distinguished Name*” (DN) del estándar ITU X.500/ISO 9594 de la siguiente forma para:

#### a) **Certificado cualificado de firma electrónica:**

**i) OID=2.5.4.6 C= PY;**

**ii) OID=2.5.4.10 O=CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA;**

**iii) OID=2.5.4.11 OU= [podrá ser: F2 o F3, conforme lo estipulado en el punto 1.1 y 1.4.1 de este documento];**

**iv) OID: 2.5.4.3 CN= [nombre/s y apellido/s del titular del certificado en mayúsculas y sin tilde, conforme documento de identidad presentado];**

y

**v) OID:2.5.4.5. Serial Number= [conforme al formato descrito en el ítem 3.1.4.2 del documento DOC-ICPP-03 [3]];**

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

6. **vi) OID: 2.5.4.4 SN=** [ *apellido/s del titular del certificado en mayúsculas y sin tilde, conforme documento de identidad presentado*]; y

7. **vii) OID:2.5.4.42 G=** [ *nombre/s del titular del certificado en mayúsculas y sin tilde, conforme documento de identidad presentado*];

### 7.1.5 RESTRICCIONES DEL NOMBRE

Los certificados emitidos bajo esta política cuentan con DN conforme a las recomendaciones X.509 que son únicos y no ambiguos.

Los nombres deberán escribirse tal y como figuran en el documento de identidad presentado.

La ICPP establece las siguientes restricciones de nombres, aplicables a todos los certificados:

- a) no se deben utilizar tildes ni diéresis; y
- b) además de los caracteres alfanuméricos, sólo se podrán utilizar los siguientes caracteres especiales:

<b>Caracteres</b>	<b>Código (hexadecimal)</b>
Blanco	20
!	21
"	22
#	23



 <b>TETÁ REKUÁI</b> MOTENONDEHA MINISTERIO DEL INTERIOR	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

\$	24
%	25
&	26
'	27
(	28
)	29
*	2a
+	2B
,	2C
-	2D
.	2E
/	2F
:	3a
;	3B
=	3D
?	3F
@	40
\	5C

### **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 (POLICY CONSTRAINTS)**

No aplica.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

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

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

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

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

## 7.2 PERFIL DE LA LCR

Como establece la DPC de la PNDI.

### 7.2.1 NÚMERO (S) DE VERSIÓN

Las LCRs generadas por el PCSC responsable según la PC deberán implementar la versión 2 de la LCRs definida en el estándar ITU X.509, de acuerdo con el perfil establecido en el RFC 5280.

### 7.2.2 CRL Y EXTENSIONES DE ENTRADAS DE CRL

La ACRaíz-Py define las siguientes extensiones de LCR como obligatorias:

- a) Identificador de la clave de la Autoridad Certificadora "Authority Key Identifier" no crítica: debe contener el hash SHA-1 de la clave pública del PCSC que firma o sella la LCR;

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

b) Número de LCR “CRL Number” no crítica: debe contener un número secuencial para cada LCR emitida por el PCSC; y

c) Puntos de Distribución del Emisor “Issuing Distribution Point” crítico: debe contener la dirección Web donde se obtiene la LCR correspondiente al certificado.

## 7.3 PERFIL DE OCSP

Las Respuestas OCSP deberán ser firmadas o selladas utilizando el algoritmo definido en el documento DOC-ICPP-06 [1].

### 7.3.1 NÚMERO (S) DE VERSIÓN

Los servicios de respuesta de OCSP del PCSC 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.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## **8. AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES**

Como establezca la DPC de la PNDI.

### **8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN**

Como establezca la DPC de la PNDI.

### **8.2 IDENTIFICACIÓN/CALIFICACIÓN DEL EVALUADOR**

Como establezca la DPC de la PNDI.

### **8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA**

Como establezca la DPC de la PNDI.

### **8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN**

Como establezca la DPC de la PNDI.

### **8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA**

Como establezca la DPC de la PNDI.

### **8.6 COMUNICACIÓN DE RESULTADOS**

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 9. OTROS ASUNTOS LEGALES Y COMERCIALES

### 9.1 TARIFAS

Como establezca la DPC 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 DPC de la PNDI.

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

Como establezca la DPC de la PNDI.

#### 9.1.4 TARIFAS POR OTROS SERVICIOS

Como establezca la DPC de la PNDI.

#### 9.1.5 POLÍTICAS DE REEMBOLSO

La Política de Reembolso del PCSC 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 PCSC de la PNDI dentro de los 10 (diez) días posteriores a su fecha de

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

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 PCSC, 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 PCSC de la PNDI no aceptará ningún reclamo.

## 9.2 RESPONSABILIDAD FINANCIERA

Como establezca la DPC de la PNDI.

### 9.2.1 COBERTURA DE SEGURO

Como establezca la DPC de la PNDI.

### 9.2.2 OTROS ACTIVOS

Como establezca la DPC de la PNDI.

### 9.2.3 COBERTURA DE SEGURO O GARANTÍA PARA LAS PERSONAS FÍSICAS O JURÍDICAS TITULARES DE CERTIFICADOS

Como establezca la DPC de la PNDI.

## 9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

### **9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL**

Como establezca la DPC de la PNDI.

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

Como establezca la DPC de la PNDI.

## **9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL**

### **9.4.1 PLAN DE PRIVACIDAD**

Como establezca la DPC de la PNDI.

### **9.4.2 INFORMACIÓN TRATADA COMO PRIVADA**

Como establezca la DPC de la PNDI.

### **9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA**

Como establezca la DPC de la PNDI.

### **9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA**

Como establezca la DPC de la PNDI.

### **9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA**

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 9.4.6 DIVULGACIÓN ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO

Como establezca la DPC de la PNDI.

## 9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

Como establezca la DPC de la PNDI.

### 9.4.8. INFORMACIÓN A TERCEROS

Como establezca la DPC de la PNDI.

## 9.5 DERECHO DE PROPIEDAD INTELECTUAL

Como establezca la DPC de la PNDI.

## 9.6 REPRESENTACIONES Y GARANTÍAS

### 9.6.1 REPRESENTACIONES Y GARANTÍAS DEL PCSC

Como establezca la DPC de la PNDI.

#### 9.6.1.1 AUTORIZACIÓN PARA CERTIFICADO

Como establezca la DPC de la PNDI.

#### 9.6.1.2. PRECISIÓN DE LA INFORMACIÓN

Como establezca la DPC de la PNDI.

#### 9.6.1.3. IDENTIFICACIÓN DEL SOLICITANTE DE CERTIFICADO

Como establezca la DPC de la PNDI.



 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

#### **9.6.1.4 CONSENTIMIENTO DE LOS TITULARES DE CERTIFICADO**

Como establezca la DPC de la PNDI.

#### **9.6.1.5. SERVICIO**

Como establezca la DPC de la PNDI.

#### **9.6.1.6. REVOCACIÓN**

Como establezca la DPC de la PNDI.

#### **9.6.1.7. EXISTENCIA LEGAL**

Como establezca la DPC de la PNDI.

#### **9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA AR**

Como establezca la DPC de la PNDI.

#### **9.6.3 REPRESENTACIONES Y GARANTÍAS DEL TITULAR DEL CERTIFICADO**

Como establezca la DPC de la PNDI.

#### **9.6.4 REPRESENTACIONES Y GARANTÍAS DE LAS PARTES USUARIAS**

Como establezca la DPC de la PNDI.

#### **9.6.5 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES**

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 9.7 EXENCIÓN DE GARANTÍA

Como establezca la DPC de la PNDI.

## 9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL

Como establezca la DPC de la PNDI.

## 9.9 INDEMNIZACIONES

Como establezca la DPC de la PNDI.

## 9.10 PLAZO Y FINALIZACIÓN

### 9.10.1 PLAZO

Como establezca la DPC de la PNDI.

### 9.10.2 FINALIZACIÓN

Como establezca la DPC de la PNDI.

### 9.10.3 EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

Como establezca la DPC de la PNDI.

## 9.11 NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

Como establezca la DPC de la PNDI.

## 9.12 ENMIENDAS

### 9.12.1 PROCEDIMIENTOS PARA ENMIENDAS

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 9.12.2 PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

Como establezca la DPC de la PNDI.

## 9.12.3 CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

Como establezca la DPC de la PNDI.

## 9.13 DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

Como establezca la DPC de la PNDI.

## 9.14 NORMATIVA APLICABLE

Como establezca la DPC de la PNDI.

## 9.15 ADECUACIÓN A LA LEY APLICABLE

Como establezca la DPC de la PNDI.

## 9.16 DISPOSICIONES VARIAS

### 9.16.1 ACUERDO COMPLETO

Como establezca la DPC de la PNDI.

### 9.16.2 ASIGNACIÓN

Como establezca la DPC de la PNDI.

### 9.16.3 DIVISIBILIDAD

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

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

Como establezca la DPC de la PNDI.

### **9.16.5 FUERZA MAYOR**

Como establezca la DPC de la PNDI.

### **9.17 OTRAS DISPOSICIONES**

Como establezca la DPC de la PNDI.

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO: PC-PNDI-V1.1</b>	<b>FECHA: 07/02/2023</b>	

## 10. DOCUMENTOS DE REFERENCIA

### 10.1. REFERENCIAS EXTERNAS

Los siguientes documentos referenciados son aplicados para la confección de esta Política de certificación:

- RFC 5280: "Internet X.509 Public Key Infrastructure.Certificate and Certificate Revocation List (CRL) Profile".
- • RFC 6960: "X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP".
- • TU X.500/ISO 9594: "Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services".
- • ITU X.509/ISO/IEC9594-8:"-Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks".
- • Principles and Criteria for Certification Authorities.
- • WebTrustSM/TM Principles and Criteria for Registration Authorities.
- • Ley No 6822/2021 "De los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos."

 <p>TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR</p>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY</b>		
	<b>POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES</b>		
	<b>CODIGO:</b> PC-PNDI-V1.1	<b>FECHA:</b> 07/02/2023	

## 10.2. REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	Normas de algoritmos criptográficos de la ICPP.	DOC-ICPP-06
[2]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación del PCSC que genera o gestiona datos de creación de firma electrónica y/o de sello electrónico.	
[3]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación de los prestadores cualificados de servicios de confianza de la ICPP.	