



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 1.2

CLASE: PÚBLICO

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

INDICE

1. INTRODUCCIÓN	15
1.1. DESCRIPCIÓN GENERAL	15
1.2 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO	16
1.3 PARTICIPANTES DE LA ICPP	16
1.3.1 AUTORIDADES CERTIFICADORAS (AC)	16
1.3.2 AUTORIDAD DE REGISTRO (AR)	18
1.3.3 AUTORIDADES DE VALIDACIÓN (AV)	19
1.3.4 TITULARES DEL CERTIFICADO	20
1.3.5 PARTE USUARIA	20
1.3.6. OTROS PARTICIPANTES	21
1.3.6.1. PRESTADORES DE SERVICIOS DE SOPORTE (PSS)	21
1.4 USO DEL CERTIFICADO	22
1.4.1 USOS APROPIADOS DEL CERTIFICADO	22
1.4.2 USOS PROHIBIDOS DEL CERTIFICADO	22
1.5 ADMINISTRACIÓN DE LA POLÍTICA	23
1.5.1 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO	23
1.5.2 PERSONA DE CONTACTO	23
1.5.3 PERSONA QUE DETERMINA LA ADECUACIÓN DE LA DPC A LA POLÍTICA	23
1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA PC	24
1.6 DEFINICIONES Y ACRÓNIMOS	24
1.6.1 DEFINICIONES	24
1.6.2 ACRÓNIMOS	34
2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO	37
2.1 REPOSITORIOS	37
2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN	37
2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN	37
2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS	37
3. IDENTIFICACION Y AUTENTICACION	38
3.1 NOMBRES	39

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

3.1.1 TIPOS DE NOMBRES	39
3.1.2 NECESIDAD DE NOMBRES SIGNIFICATIVOS	39
3.1.3 ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES	39
3.1.4 REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES	39
3.1.5 UNICIDAD DE LOS NOMBRES	39
3.1.6. RECONOCIMIENTO PARA RESOLVER DIPUTA DE NOMBRE	39
3.1.7 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS	39
3.2 VALIDACIÓN INICIAL DE IDENTIDAD	39
3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA	39
3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA	39
3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA	40
3.2.4 INFORMACIÓN NO VERIFICADA DEL TITULAR DEL CERTIFICADO	40
3.2.5 VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)	40
3.2.6 CRITERIOS PARA INTEROPERABILIDAD	40
3.2.7. PROCEDIMIENTOS COMPLEMENTARIOS	40
3.2.8 PROCEDIMIENTOS ESPECÍFICOS	40
3.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE NUEVAS CLAVES	40
3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN	40
4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO	41
4.1. SOLICITUD DE CERTIFICADO	42
4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO	42
4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES	42
4.2 PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO	42
4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN	42
4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO	42
4.2.3 TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO	42
4.3 EMISIÓN DEL CERTIFICADO	42
4.3.1 ACCIONES DEL PCSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS	42
4.3.2 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO POR PARTE DEL PCSC SOBRE LA EMISIÓN DEL CERTIFICADO	43
4.4 ACEPTACIÓN DEL CERTIFICADO	43

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO	43
4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PCSC	43
4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR EL PCSC A OTRAS ENTIDADES	43
4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO	43
4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR O RESPONSABLE	43
4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LA PARTE USUARIA	43
4.6 RENOVACIÓN DEL CERTIFICADO	43
4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO	43
4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN	44
4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO	44
4.6.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO	44
4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO	44
4.6.6 PUBLICACIÓN POR EL PCSC DEL CERTIFICADO RENOVADO	44
4.6.7 NOTIFICACIÓN POR EL PCSC DE LA EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES	44
4.7 RE-EMISIÓN DE CLAVES DE CERTIFICADO (RE-KEY)	44
4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO	44
4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA	45
4.7.3 PROCESAMIENTO DE SOLICITUDES DE RE-EMISIÓN DE CLAVES DE CERTIFICADO	45
4.7.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO SOBRE LA RE-EMISIÓN DE UN NUEVO CERTIFICADO	45
4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE-EMITIDO	45
4.7.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS RE-EMITIDOS	45
4.7.7 NOTIFICACIÓN POR EL PCSC DE LA RE-EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES	45
4.8 MODIFICACIÓN DE CERTIFICADOS	45
4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO	45
4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO	45
4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO	45

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

4.8.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO DE LA EMISIÓN DE UN NUEVO CERTIFICADO	45
4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO	46
4.8.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS MODIFICADOS	46
4.8.7 NOTIFICACIÓN POR EL PCSC DE EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES	46
4.9 REVOCACIÓN Y SUSPENSIÓN	46
4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN	46
4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN	46
4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN	46
4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN	46
4.9.5 TIEMPO DENTRO DEL CUAL EL PCSC DEBE PROCESAR LA SOLICITUD DE REVOCACIÓN	46
4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LA PARTE USUARIA	46
4.9.7 FRECUENCIA DE EMISIÓN DEL LCR	46
4.9.8 LATENCIA MÁXIMA PARA LCR	46
4.9.9 DISPONIBILIDAD PARA REVOCACIÓN / VERIFICACIÓN DE ESTADO EN LÍNEA	47
4.9.10 REQUISITOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA	47
4.9.11 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES	47
4.9.12 REQUERIMIENTOS ESPECIALES POR EL COMPROMISO DE LA CLAVE PRIVADA	47
4.9.13 CIRCUNSTANCIAS PARA SUSPENSIÓN	47
4.9.14 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN	47
4.9.15 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN	47
4.9.16 LÍMITES DE PERÍODO DE SUSPENSIÓN	47
4.10 SERVICIOS DE ESTADO DE CERTIFICADO	47
4.10.1 CARACTERÍSTICAS OPERACIONALES	47
4.10.2 DISPONIBILIDAD DEL SERVICIO	47
4.10.3 CARACTERÍSTICAS OPCIONALES	47
4.11 FIN DE LA SUSCRIPCIÓN	47
4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES	48
4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES	48

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

4.12.2 POLÍTICAS Y PRÁCTICAS DE RECUPERACIÓN Y ENCAPSULACIÓN DE CLAVES DE SESIÓN	48
5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES	49
5.1 CONTROLES FÍSICOS	49
5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO	49
5.1.2 ACCESO FÍSICO	49
5.1.2.1 NIVELES DE ACCESO FÍSICO	49
5.1.2.2. SISTEMAS FÍSICOS DE DETECCIÓN	49
5.1.2.3. SISTEMAS DE CONTROL DE ACCESO	49
5.1.2.4. MECANISMOS DE EMERGENCIA	49
5.1.3 ENERGÍA Y AIRE ACONDICIONADO	49
5.1.4 EXPOSICIONES AL AGUA	49
5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO	49
5.1.6 ALMACENAMIENTO DE MEDIOS	49
5.1.7 ELIMINACIÓN DE RESIDUOS	49
5.1.8 RESPALDO FUERA DE SITIO	50
5.2 CONTROLES PROCEDIMENTALES	50
5.2.1 ROLES DE CONFIANZA	50
5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA	50
5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL	50
5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES	50
5.3 CONTROLES DE PERSONAL	50
5.3.1 REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN	50
5.3.2 PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES	50
5.3.3 REQUERIMIENTOS DE CAPACITACIÓN	50
5.3.4 REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN	50
5.3.5 FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES	50
5.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS	50
5.3.7 REQUISITOS DE CONTRATACIÓN A TERCEROS	50
5.3.8 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL	51
5.4 PROCEDIMIENTO DE REGISTRO DE AUDITORÍA	51

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

5.4.1 TIPOS DE EVENTOS REGISTRADOS	51
5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)	51
5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA	51
5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA	51
5.4.5 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE REGISTRO (LOGS) DE AUDITORÍA	51
5.4.6 SISTEMA DE RECOLECCIÓN DE INFORMACIÓN DE AUDITORÍA (INTERNO VS EXTERNO)	51
5.4.7 NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO	51
5.4.8 EVALUACIÓN DE VULNERABILIDADES	51
5.5 ARCHIVOS DE REGISTROS	51
5.5.1 TIPOS DE REGISTROS ARCHIVADOS	51
5.5.2 PERIODOS DE RETENCIÓN PARA ARCHIVOS	51
5.5.3 PROTECCIÓN DE ARCHIVOS	51
5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO	52
5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS	52
5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO)	52
5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA	52
5.6 CAMBIO DE CLAVE	52
5.7 RECUPERACIÓN DE DESASTRES Y COMPROMISO	52
5.7.1 PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO	52
5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES	52
5.7.3 PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD	52
5.7.3.1. CERTIFICADO DE ENTIDAD ES REVOCADO	52
5.7.3.2. CLAVE DE ENTIDAD ESTÁ COMPROMETIDA	52
5.7.4 CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE	53
5.8 EXTINCIÓN DE UN PCSC	53
6. CONTROLES TÉCNICOS DE SEGURIDAD	54
6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES	54
6.1.1 GENERACIÓN DEL PAR DE CLAVES	54
6.1.2 ENTREGA DE LA CLAVE PRIVADA AL TITULAR	56

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

6.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO	57
6.1.4 ENTREGA DE LA CLAVE PÚBLICA DEL PCSC A LA PARTE USUARIA	57
6.1.5 TAMAÑO DE LA CLAVE	58
6.1.6 GENERACIÓN DE PARÁMETROS DE CLAVES ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD.	58
6.1.7 PROPÓSITOS DE USOS DE CLAVE (CONFORME AL CAMPO KEY USAGE X509 V3)	58
6.2 CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO Y PROTECCIÓN DE LA CLAVE PRIVADA	58
6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO.	58
6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA	59
6.2.3 CUSTODIA/(ESCROW) DE LA CLAVE PRIVADA	59
6.2.4 RESPALDO/COPIA DE LA CLAVE PRIVADA	59
6.2.5 ARCHIVADO DE LA CLAVE PRIVADA	59
6.2.6 TRANSFERENCIA DE CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRIPTOGRÁFICO	59
6.2.7 ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO	60
6.2.8 MÉTODO DE ACTIVACIÓN DE CLAVE PRIVADA	60
6.2.9 MÉTODOS DE DESACTIVACIÓN DE LA CLAVE PRIVADA	60
6.2.10 MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA	60
6.3 OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES	61
6.3.1 ARCHIVO DE LA CLAVE PÚBLICA	61
6.3.2 PERÍODO OPERACIONAL DEL CERTIFICADO Y PERÍODO DE USO DEL PAR DE CLAVES	61
6.4 DATOS DE ACTIVACIÓN	61
6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN	62
6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN	62
6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN	62
6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR	62
6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS	62
6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR	62
6.5.3 CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO	63
6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA	63

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA	63
6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD	63
6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA	63
6.6.4 CONTROLES EN LA GENERACIÓN DE LCR	63
6.7 CONTROLES DE SEGURIDAD DE RED	63
6.7.1 DIRECTRICES GENERALES	63
6.7.2 FIREWALL	63
6.7.3 SISTEMA DE DETECCIÓN DE INTRUSO (IDS)	63
6.7.4 REGISTRO DE ACCESO NO AUTORIZADO A LA RED	63
6.8 FUENTES DE TIEMPO	63
7. PERFILES DE CERTIFICADOS, CRL Y OCSP	65
7.1 PERFIL DEL CERTIFICADO	65
7.1.1 NÚMERO DE VERSIÓN	65
7.1.2 EXTENSIONES DEL CERTIFICADO	65
7.1.3 IDENTIFICADORES DE OBJETO DE ALGORITMOS	69
7.1.4 FORMAS DEL NOMBRE	69
7.1.5 RESTRICCIONES DEL NOMBRE	70
7.1.6 IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO	72
7.1.7 USO DE LA EXTENSIÓN RESTRICCIONES DE POLÍTICA (POLICY CONSTRAINTS)	72
7.1.8 SEMÁNTICA Y SINTAXIS DE LOS CALIFICADORES DE POLÍTICA (POLICY QUALIFIERS)	72
7.1.9 SEMÁNTICA DE PROCESAMIENTO PARA LA EXTENSIÓN DE POLÍTICAS DE CERTIFICADO (CERTIFICATE POLICIES)	72
7.2 PERFIL DE LA LCR	73
7.2.1 NÚMERO (S) DE VERSIÓN	73
7.2.2 LCR Y EXTENSIONES DE ENTRADAS DE LCR	73
7.3 PERFIL DE OCSP	74
7.3.1 NÚMERO (S) DE VERSIÓN	74
7.3.2 EXTENSIONES DE OCSP	74
8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES	75
8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN	75

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

8.2 IDENTIFICACIÓN/CALIFICACIÓN DEL EVALUADOR	75
8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA	75
8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN	75
8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA	75
8.6 COMUNICACIÓN DE RESULTADOS	75
9. OTROS ASUNTOS LEGALES Y COMERCIALES	76
9.1 TARIFAS	76
9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS	76
9.1.2 TARIFAS DE ACCESO A CERTIFICADOS	76
9.1.3 TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN	76
9.1.4 TARIFAS POR OTROS SERVICIOS	76
9.1.5 POLÍTICAS DE REEMBOLSO	76
9.2 RESPONSABILIDAD FINANCIERA	76
9.2.1 COBERTURA DE SEGURO	76
9.2.2 OTROS ACTIVOS	76
9.2.3 COBERTURA DE SEGURO O GARANTÍA PARA LAS PERSONAS FÍSICAS O JURÍDICAS TITULARES DE CERTIFICADOS	76
9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL	76
9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL	77
9.3.2 INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL	77
9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL	77
9.4.1 PLAN DE PRIVACIDAD	77
9.4.2 INFORMACIÓN TRATADA COMO PRIVADA	77
9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA	77
9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA	77
9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA	77
9.4.6 DIVULGACIÓN ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO	77
9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN	77
9.5 DERECHO DE PROPIEDAD INTELECTUAL	78
9.6 REPRESENTACIONES Y GARANTÍAS	78

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

9.6.1 REPRESENTACIONES Y GARANTÍAS DEL PCSC	78
9.6.1.1 AUTORIZACIÓN PARA CERTIFICADO	78
9.6.1.2. PRECISIÓN DE LA INFORMACIÓN	78
9.6.1.3. IDENTIFICACIÓN DEL SOLICITANTE DE CERTIFICADO	78
9.6.1.4 CONSENTIMIENTO DE LOS TITULARES DE CERTIFICADO	78
9.6.1.5. SERVICIO	78
9.6.1.6. REVOCACIÓN	78
9.6.1.7. EXISTENCIA LEGAL	78
9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA AR	78
9.6.3 REPRESENTACIONES Y GARANTÍAS DEL TITULAR DEL CERTIFICADO	78
9.6.4 REPRESENTACIONES Y GARANTÍAS DE LAS PARTES USUARIAS	78
9.6.5 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES	78
9.7 EXENCIÓN DE GARANTÍA	79
9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL	79
9.9 INDEMNIZACIONES	79
9.10 PLAZO Y FINALIZACIÓN	79
9.10.1 PLAZO	79
9.10.2 FINALIZACIÓN	79
9.10.3 EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA	79
9.11 NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES	79
9.12 ENMIENDAS	79
9.12.1 PROCEDIMIENTOS PARA ENMIENDAS	79
9.12.2 PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN	80
9.12.3 CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS	80
9.13 DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS	80
9.14 NORMATIVA APLICABLE	80
9.15 ADECUACIÓN A LA LEY APLICABLE	80
9.16 DISPOSICIONES VARIAS	80
9.16.1 ACUERDO COMPLETO	80
9.16.2 ASIGNACIÓN	81
9.16.3 DIVISIBILIDAD	81

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

9.16.4 APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DE DERECHOS)	81
9.16.5 FUERZA MAYOR	81
9.17 OTRAS DISPOSICIONES	81
10. DOCUMENTOS DE REFERENCIA	82
10.1. REFERENCIAS EXTERNAS	82
10.2. REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP	83

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

CONTROL DOCUMENTAL

DOCUMENTO	
Título: POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES	Nombre del Archivo: PC F2 PNDI v1.2
Código: PC-PNDI-V1.2	Soporte Lógico: https://www.identificaciones.gov.py/firmadigital/PC/PC%20F2%20PNDI%20v1.1.pdf
Fecha: 11/07/2023	Ubicación Física: Policía Nacional - Departamento de Identificaciones (PNDI)
Versión: 1.2	

REGISTRO DE CAMBIOS		
Versión	Fecha	Motivo de cambio
1.0	13/09/19	Versión inicial
1.1	07/02/2023	Actualización de la Normativa
1.2		Ítem 6.3.2. Periodo Operacional de Certificado y Periodo de Uso.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.1	FECHA: 07/02/2023	Versión: 1.1	

DISTRIBUCIÓN DEL DOCUMENTO	
NOMBRE	ÁREA
Ministerio de Industria y Comercio (MIC)	Dirección General de Comercio Electrónico (DGCE)
Policía Nacional	Departamento de Identificaciones
Documento Público	https://www.identificaciones.gov.py/firmadigital/PC/PC%20F2%20PNDI%20v1.1.pdf

CONTROL DEL DOCUMENTO		
Preparado por:	Revisado por:	Aceptado por:
Consorcio CDE	Consorcio CDE	Ministerio del Interior

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

1. INTRODUCCIÓN

1.1. DESCRIPCIÓN GENERAL

Este documento establece los requisitos mínimos que deben ser cumplidos por el Prestador Cualificado de Servicios de Confianza (PCSC) de la Policía Nacional del Departamento de Identificaciones (PNDI) en su carácter de Autoridad de Certificación Intermedia (ACI) y miembro de la Infraestructura de Clave Pública del Paraguay (ICPP), quién ejerce funciones de Autoridad Certificadora atribuidas al Ministerio de Interior en adelante PCSC de la PNDI.

Toda PC elaborada en al 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

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

almacenamiento de clave, proceso de generación del par de claves, 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 son generados y almacenados en un dispositivo criptográfico (smart card) con capacidad de generación de claves, de tipo hardware.

Las claves privadas relacionadas a los certificados del tipo F2 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

Nombre:	Políticas de Certificación Tipo F2 Persona Física de la Policía Nacional - Departamento de Identificaciones
Versión:	1.2
Fecha de aprobación:	11 – Julio - 2023
Ubicación de la DPC:	https://www.identificaciones.gov.py/firmadigital/DPC/DPC%20F2%20PNDI%20v1.1.pdf

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

1.3 PARTICIPANTES DE LA ICPP

1.3.1 AUTORIDADES CERTIFICADORAS (AC)

Son las entidades autorizadas a emitir certificados de clave pública dentro de la ICPP. 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.

Un PCSC presta servicios de CREACIÓN, VERIFICACIÓN Y VALIDACIÓN DE FIRMAS ELECTRÓNICAS CUALIFICADAS.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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 cualificados 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 de electrónicos 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.

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:

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

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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;
- Procesar toda la documentación presentada por el solicitante y enviar la solicitud de certificado al PCSC de la PNDI de forma segura y con firma electrónica del agente.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

1.3.3 AUTORIDADES DE VALIDACIÓN (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/autoridad-de-validacion-av/>

1.3.4 TITULARES DEL CERTIFICADO

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

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

1.3.5 PARTE USUARIA

Se entenderá por parte usuaria, toda persona física 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 una AR vinculada para desempeñar actividades descritas en esta PC o en una DPC y se clasifican en tres categorías, conforme al tipo de actividades prestadas:

- 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):

<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.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

1.4 USO DEL CERTIFICADO

1.4.1 USOS APROPIADOS DEL CERTIFICADO

Las aplicaciones y otros programas que soporten el uso de un certificado electrónico de cierto tipo contemplado por la ICPP deben aceptar cualquier certificado del mismo tipo, o superior, emitido por cualquier PCSC habilitado por la AC Raíz-Py.

En la definición de aplicaciones para el tipo de certificado definido por la PC, el PCSC responsable debe tener en cuenta el nivel de seguridad previsto para ese tipo de certificado conforme a lo estipulado en el ítem 1.1.

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

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.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

1.5 ADMINISTRACIÓN DE LA POLÍTICA

1.5.1 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre: Policía Nacional - Departamento de Identificaciones.

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

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

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

1.5.2 PERSONA DE CONTACTO

Nombre: Jefe del Departamento de Identificaciones

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

Teléfono: (+595) (021) 605-618/9

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

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

Nombre: Jefe del Departamento de Identificaciones.

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

Teléfono: (+595) (021) 605-618/9

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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

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 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.
- **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

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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 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

	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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 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.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

- **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 firmante, haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza,

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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 través de la presencia física del interesado o mediante otros medios que aporten una seguridad equivalente en términos de fiabilidad a la presencia

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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.
- **Módulo de Seguridad de Hardware:** dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

- **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.
- **PrestadorCualificadodeServiciosdeConfianza:** prestadordeservicios deconfianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la habilitación.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

- **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, gerenciamiento 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.
- **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.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

- **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.
- **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.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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)
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)

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.1	FECHA: 07/02/2023	Versión: 1.1	

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
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)

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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
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)

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

Conforme a lo establecido en la DPC de la PNDI.

2.1 REPOSITORIOS

2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN

2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

3. IDENTIFICACION Y AUTENTICACION

En los apartados siguientes se encuentran referidos conforme a la DPC de la PNDI

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

3.1 NOMBRES

3.1.1 TIPOS DE NOMBRES

3.1.2 NECESIDAD DE NOMBRES SIGNIFICATIVOS

3.1.3 ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES

3.1.4 REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES

3.1.5 UNICIDAD DE LOS NOMBRES

3.1.6. RECONOCIMIENTO PARA RESOLVER DIPUTA DE NOMBRE

3.1.7 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

3.2 VALIDACIÓN INICIAL DE IDENTIDAD

3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA

3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA

3.2.4 INFORMACIÓN NO VERIFICADA DEL TITULAR DEL CERTIFICADO

3.2.5 VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)

3.2.6 CRITERIOS PARA INTEROPERABILIDAD

3.2.7. PROCEDIMIENTOS COMPLEMENTARIOS

3.2.8 PROCEDIMIENTOS ESPECÍFICOS

3.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE NUEVAS CLAVES

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

En los apartados siguientes se encuentran referidos conforme a la DPC de la PNDI

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

4.1. SOLICITUD DE CERTIFICADO

4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

4.2 PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

4.2.3 TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO

4.3 EMISIÓN DEL CERTIFICADO

4.3.1 ACCIONES DEL PCSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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

4.4 ACEPTACIÓN DEL CERTIFICADO

4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PCSC

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

4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR O RESPONSABLE

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

4.6 RENOVACIÓN DEL CERTIFICADO

4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN

4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO

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

4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO

4.6.6 PUBLICACIÓN POR EL PCSC DEL CERTIFICADO RENOVADO

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

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

4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA

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

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

4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE- EMITIDO

4.7.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS RE-EMITIDOS

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

4.8 MODIFICACIÓN DE CERTIFICADOS

4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO

4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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

4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

4.8.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS MODIFICADOS

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

4.9 REVOCACIÓN Y SUSPENSIÓN

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN

4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

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

4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LA PARTE USUARIA

4.9.7 FRECUENCIA DE EMISIÓN DEL LCR

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

4.9.8 LATENCIA MÁXIMA PARA LCR

4.9.9 DISPONIBILIDAD PARA REVOCACIÓN / VERIFICACIÓN DE ESTADO EN LÍNEA

4.9.10 REQUISITOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA

4.9.11 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES

4.9.12 REQUERIMIENTOS ESPECIALES POR EL COMPROMISO DE LA CLAVE PRIVADA

4.9.13 CIRCUNSTANCIAS PARA SUSPENSIÓN

4.9.14 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

4.9.15 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

4.9.16 LÍMITES DE PERÍODO DE SUSPENSIÓN

4.10 SERVICIOS DE ESTADO DE CERTIFICADO

4.10.1 CARACTERÍSTICAS OPERACIONALES

4.10.2 DISPONIBILIDAD DEL SERVICIO

4.10.3 CARACTERÍSTICAS OPCIONALES

4.11 FIN DE LA SUSCRIPCIÓN

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

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

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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

En los apartados siguientes se encuentran referidos conforme a la DPC de la PNDI

5.1 CONTROLES FÍSICOS

5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

5.1.2 ACCESO FÍSICO

5.1.2.1 NIVELES DE ACCESO FÍSICO

5.1.2.2. SISTEMAS FÍSICOS DE DETECCIÓN

5.1.2.3. SISTEMAS DE CONTROL DE ACCESO

5.1.2.4. MECANISMOS DE EMERGENCIA

5.1.3 ENERGÍA Y AIRE ACONDICIONADO

5.1.4 EXPOSICIONES AL AGUA

5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

5.1.6 ALMACENAMIENTO DE MEDIOS

5.1.7 ELIMINACIÓN DE RESIDUOS

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

5.1.8 RESPALDO FUERA DE SITIO

5.2 CONTROLES PROCEDIMENTALES

5.2.1 ROLES DE CONFIANZA

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES

5.3 CONTROLES DE PERSONAL

5.3.1 REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

5.3.2 PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

5.3.3 REQUERIMIENTOS DE CAPACITACIÓN

5.3.4 REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

5.3.5 FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

5.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS

5.3.7 REQUISITOS DE CONTRATACIÓN A TERCEROS

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

5.3.8 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

5.4 PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

5.4.1 TIPOS DE EVENTOS REGISTRADOS

5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)

5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

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

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

5.4.7 NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

5.4.8 EVALUACIÓN DE VULNERABILIDADES

5.5 ARCHIVOS DE REGISTROS

5.5.1 TIPOS DE REGISTROS ARCHIVADOS

5.5.2 PERIODOS DE RETENCIÓN PARA ARCHIVOS

5.5.3 PROTECCIÓN DE ARCHIVOS

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO

5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO)

5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA

5.6 CAMBIO DE CLAVE

5.7 RECUPERACIÓN DE DESASTRES Y COMPROMISO

5.7.1 PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO

5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES

5.7.3 PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD

5.7.3.1. CERTIFICADO DE ENTIDAD ES REVOCADO

5.7.3.2. CLAVE DE ENTIDAD ESTÁ COMPROMETIDA

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

5.7.4 CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

5.8 EXTINCIÓN DE UN PCSC

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

6. CONTROLES TÉCNICOS DE SEGURIDAD

En esta sección se definen las medidas de seguridad implementadas por el PCSC de la PNDI para proteger sus claves criptográficas y sus datos de activación, así como la gestión de las claves criptográficas de los titulares de certificados. También serán definidos otros controles técnicos de seguridad utilizados por el PCSC de la PNDI. y por sus AR vinculadas en la ejecución de sus funciones operacionales.

6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1 GENERACIÓN DEL PAR DE CLAVES

Cuando el titular del certificado sea

- una persona física, éste será el responsable de generar el par de claves criptográficas, salvo en caso de su gestión en nombre del firmante, en donde las claves privadas asociadas a los certificados son generadas y custodiadas por el módulo de activación de firma del PCSC, de forma que el acceso a dichas claves se realiza por medios que garantizan, con un alto nivel de confianza, el control exclusivo por parte del firmante.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

El algoritmo para utilizar para las claves criptográficas de titulares de certificados está definido conforme al documento DOC-ICPP-06 [3].

Para ser generada, la clave privada del titular del certificado es grabada y cifrada por un algoritmo simétrico conforme al documento DOC-ICPP-06 [3], en un medio de almacenamiento definido para cada tipo de certificado previsto en la ICPP.

La clave privada deberá viajar cifrada, utilizando los mismos algoritmos mencionados en el párrafo anterior, entre el dispositivo generador y el medio utilizado para su almacenamiento.

Los medios de almacenamiento de claves privadas cumplirán los siguientes requisitos garantizando como mínimo, por medios técnicos y de procedimiento adecuados, que:

- a) la confidencialidad de las claves privadas utilizadas para la creación de firmas electrónicas o sellos electrónicos, esté garantizada razonablemente.
- b) las claves privadas utilizadas para la creación de firma electrónica o sello electrónico sólo puedan aparecer una vez en la práctica.
- c) exista la seguridad razonable de que claves privadas utilizadas para la creación de firma electrónica o sello electrónico no pueden ser hallados por deducción y de que la firma o sello está protegido con seguridad contra la falsificación mediante las tecnologías disponibles en el momento.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

d) las claves privadas utilizadas para la creación de firma electrónica o sello electrónico puedan ser protegidas por el firmante legítimo de forma fiable frente a su utilización por otros.

Estos medios de almacenamiento de claves privadas no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestre al firmante antes de firmar.

La generación o la gestión de las claves privadas de firma electrónica en nombre del firmante sólo podrán correr a cargo de un PCSC, en los términos establecidos en el documento DOC-ICPP-07 [2]

TIPO DE CERTIFICADO	MEDIO DE ALMACENAMIENTO
F2	● Hardware criptográfico certificado por el MIC (Tarjeta inteligente o token con capacidad de generación de claves) ● Hardware criptográfico certificado por el MIC (HSM)

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

6.1.2 ENTREGA DE LA CLAVE PRIVADA AL TITULAR

Para el caso de claves privadas asociadas a certificados de los tipos F2 la clave es generada en el dispositivo criptográfico al momento de la emisión y el titular es responsable de este.

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 de la PNDI. mediante el envío de una solicitud de firma de certificado (CSR) que concuerda con la especificación del PKCS#10, firmado electrónicamente 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 de la 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:

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

- a) en el momento de disponibilización de un certificado a su titular, usando el formato definido en el documento DOC-ICPP-06 [1];
- b) un directorio;
- c) una página WEB del PCSC; y
- d) otros medios seguros aprobados por la ACRaíz-Py

6.1.5 TAMAÑO DE LA CLAVE

Los algoritmos y tamaños de clave a ser utilizados en los diferentes tipos de certificados emitidos en el marco de la ICPP, se definen en el documento DOC-ICPP-06 [1].

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

Los parámetros de generación y verificación de calidad de claves asimétricas de las personas físicas de certificados emitidos por el PCSC de la PNDI adoptan el estándar definido en el documento DOC-ICPP-06 [3].

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

Conforme a lo establecido en la DPC del PCSC de la PNDI

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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 del titular del certificado es de conformidad con las normas establecidas en el documento DOC-ICPP-06 [1].

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 los titulares de certificados para certificados de Tipo F2 emitido bajo esta PC.

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

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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 titulares de certificados 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 titulares de certificados 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.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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, después de la expiración de los certificados correspondientes por un periodo de 10 (diez) años desde su última emisión, para la verificación de firmas o sellos generados 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 electronica 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 electronica cualificada de tipo F2 es como máximo de 4 (cuatro) años desde el momento de emisión del mismo.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

6.4 DATOS DE ACTIVACIÓN

Los datos de activación son distintos a las claves criptográficas y se definen como aquellas claves requeridas para la operación de algunos módulos criptográficos.

6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Para certificados de firma electrónica cualificada tipo F2 certificados la generación y almacenamiento del par de claves son realizados en dispositivos criptográficos hardware con capacidad de generación de claves siendo activados y protegidos por contraseñas y/o PIN.

6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

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

6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Conforme a lo establecido en la DPC de la PNDI.

6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

Conforme a lo establecido en la DPC de la PNDI.

6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

No aplica.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

6.5.3 CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO

No aplica.

6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

Conforme a lo establecido en la DPC del PCSC de la PNDI

6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA

6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

6.6.4 CONTROLES EN LA GENERACIÓN DE LCR

6.7 CONTROLES DE SEGURIDAD DE RED

6.7.1 DIRECTRICES GENERALES

6.7.2 FIREWALL

6.7.3 SISTEMA DE DETECCIÓN DE INTRUSO (IDS)

6.7.4 REGISTRO DE ACCESO NO AUTORIZADO A LA RED

6.8 FUENTES DE TIEMPO

Todos los sistemas del PCSC de la PNDI, tanto como los servidores como las de las estaciones de trabajo, están sincronizados en fecha y hora utilizando una

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

fuentes confiables de tiempo (servidor INTN "intn.gov.py") ajustados a la fecha y hora oficial paraguaya

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

7. PERFILES DE CERTIFICADOS, CRL Y OCSP

En los siguientes puntos la PC, son descritos 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

Todos los certificados emitidos por el PCSC de la PNDI, se ajustan al formato definido por la norma ITU X.509 o ISO/IEC 9594-8, según el perfil establecido en RFC 5280.

7.1.1 NÚMERO DE VERSIÓN

Todos los certificados emitidos por el PCSC de la PNDI implementan 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:

- 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;
- 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;
- Uso de Claves "KeyUsage", crítica:**

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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

d) Uso extendido de la clave "Extended Key Usage", 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;

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:

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

- 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
- 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"]

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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];
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.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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 ICPP deben usar el siguiente algoritmo:

Identificador de objeto (OID) de algoritmo criptográfico

- Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
- Identificador de objeto (OID) de clave pública
- RSAEncryption (1.2.840.113549.1.1.1)

7.1.4 FORMAS DEL NOMBRE

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];

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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]];

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:

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

Caracteres	Código (hexadecimal)
Blanco	20
!	21
"	22
#	23
\$	24
%	25
&	26
'	27
(	28
)	29
*	2a
+	2B
,	2C
-	2D
.	2E
/	2F
:	3a
;	3B

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

=	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.

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.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

7.2 PERFIL DE LA LCR

Las Listas de Certificados Revocados LCR son firmadas y selladas utilizando el algoritmo definido en el documento DOC-ICPP-06 [3]

7.2.1 NÚMERO (S) DE VERSIÓN

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

7.2.2 LCR Y EXTENSIONES DE ENTRADAS DE LCR

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

- 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;
- Número de LCR "CRL Number" no crítica: debe contener un número secuencial para cada LCR emitida por el PCSC; y
- Puntos de Distribución del Emisor "Issuing Distribution Point" crítico: debe contener la dirección Web donde se obtiene la LCR correspondiente al certificado.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

Conforme a lo establecido en la DPC de la PNDI.

8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

8.2 IDENTIFICACIÓN/CALIFICACIÓN DEL EVALUADOR

8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA

8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN

8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA

8.6 COMUNICACIÓN DE RESULTADOS

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

9. OTROS ASUNTOS LEGALES Y COMERCIALES

Conforme a lo establecido en la DPC de la PNDI.

9.1 TARIFAS

9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

9.1.2 TARIFAS DE ACCESO A CERTIFICADOS

9.1.3 TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN

9.1.4 TARIFAS POR OTROS SERVICIOS

9.1.5 POLÍTICAS DE REEMBOLSO

9.2 RESPONSABILIDAD FINANCIERA

9.2.1 COBERTURA DE SEGURO

9.2.2 OTROS ACTIVOS

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

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

9.3.2 INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL

9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL

9.4.1 PLAN DE PRIVACIDAD

9.4.2 INFORMACIÓN TRATADA COMO PRIVADA

9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

9.4.6 DIVULGACIÓN ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO

9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

9.4.8. INFORMACIÓN A TERCEROS

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

9.5 DERECHO DE PROPIEDAD INTELECTUAL

9.6 REPRESENTACIONES Y GARANTÍAS

9.6.1 REPRESENTACIONES Y GARANTÍAS DEL PCSC

9.6.1.1 AUTORIZACIÓN PARA CERTIFICADO

9.6.1.2. PRECISIÓN DE LA INFORMACIÓN

9.6.1.3. IDENTIFICACIÓN DEL SOLICITANTE DE CERTIFICADO

9.6.1.4 CONSENTIMIENTO DE LOS TITULARES DE CERTIFICADO

9.6.1.5. SERVICIO

9.6.1.6. REVOCACIÓN

9.6.1.7. EXISTENCIA LEGAL

9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA AR

9.6.3 REPRESENTACIONES Y GARANTÍAS DEL TITULAR DEL CERTIFICADO

9.6.4 REPRESENTACIONES Y GARANTÍAS DE LAS PARTES USUARIAS

9.6.5 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

9.7 EXENCIÓN DE GARANTÍA

9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL

9.9 INDEMNIZACIONES

9.10 PLAZO Y FINALIZACIÓN

9.10.1 PLAZO

Esta PC entra en vigencia a partir de la fecha establecida en el instrumento que la aprueba y expedido por la AA.

9.10.2 FINALIZACIÓN

Esta PC permanecerá en vigencia indefinidamente, manteniéndose vigente y eficaz hasta que sea revocada o sustituida, expresa o tácitamente.

9.10.3 EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

Finalizada la vigencia de esta PC, por sustitución o revocación, esta se mantendrá válida para todos los efectos legales.

9.11 NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

9.12 ENMIENDAS

9.12.1 PROCEDIMIENTOS PARA ENMIENDAS

Los cambios efectuados en la PC y DPC del PCSC de la PNDI deben ser revisados y aprobados por AC Raíz-Py, antes de ser implementados. Las modificaciones deben documentarse y mantenerse actualizadas a través de versiones.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

9.12.2 PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

Toda enmienda o modificación de la DPC y las PC implementadas por el PCSC de la PNDI se publicarán en su sitio principal de internet.

9.12.3 CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

9.13 DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

9.14 NORMATIVA APLICABLE

9.15 ADECUACIÓN A LA LEY APLICABLE

9.16 DISPOSICIONES VARIAS

9.16.1 ACUERDO COMPLETO

Los titulares y partes usuarias que confían en los certificados asumen en su totalidad el contenido de la presente PC.

Esta PC representa las obligaciones y deberes aplicables al PCSC de la PNDI. y autoridades vinculadas.

En caso de conflicto entre esta PC y otras resoluciones del AC Raiz-Py, prevalecerá siempre la última editada.

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

9.16.2 ASIGNACIÓN

9.16.3 DIVISIBILIDAD

9.16.4 APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DE DERECHOS)

9.16.5 FUERZA MAYOR

9.17 OTRAS DISPOSICIONES

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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."

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.2	FECHA: 11/07/2023	Versión: 1.2	

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.	DOC-ICPP-07
[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.	DOC-ICPP-03

 TETÁ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	POLÍTICA DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES			
	CODIGO: PC-PNDI-V1.1	FECHA: 07/02/2023	Versión: 1.1	