



TETÃ REKUÁI
MOTENONDEHA
MINISTERIO DEL
INTERIOR



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

**DECLARACIÓN DE PRÁCTICAS DE
CERTIFICACIÓN DE TIPO F2 PARA PERSONA
FÍSICA**

VERSIÓN 1.2

CLASE: PÚBLICO

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

INDICE

1.1	DESCRIPCIÓN GENERAL.....	13
1.2.	NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO.....	14
1.3.	PARTICIPANTES DE LA ICPP	14
1.3.1.	AUTORIDADES CERTIFICADORAS (AC)	14
1.3.2.	AUTORIDAD DE REGISTRO (AR)	15
1.3.3.	AUTORIDADES DE VALIDACIÓN (AV)	15
1.3.4.	TITULARES DEL CERTIFICADO	16
1.3.5.	PARTE USUARIA.....	16
1.3.6.	OTROS PARTICIPANTES.....	16
1.3.6.1	PRESTADORES DE SERVICIOS DE SOPORTE (PSS)	16
1.4.	USO DEL CERTIFICADO	17
1.4.1.	USOS APROPIADOS DEL CERTIFICADO	17
1.4.2.	USOS PROHIBIDOS DEL CERTIFICADO	18
1.5.	ADMINISTRACIÓN DE LA POLÍTICA.....	19
1.5.1.	ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO	19
1.5.2.	PERSONA DE CONTACTO	19
1.5.3.	PERSONA QUE DETERMINA LA ADECUACIÓN DE LA DPC A LA PC	19
1.5.4.	PROCEDIMIENTOS DE APROBACIÓN DE LA DPC.....	19
1.6.	DEFINICIONES Y ACRÓNIMOS	20
1.6.1.	DEFINICIONES	20
1.6.2.	ACRÓNIMOS.....	29
2.	RESPONSABILIDADES DE PUBLICACIÓN Y DELREPOSITORIO	33
3.	IDENTIFICACION Y AUTENTICACION.....	39
3.1.1.	TIPOS DE NOMBRES.....	39

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

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	40
3.1.6.	PROCEDIMIENTO PARA RESOLVER DISPUTA DE NOMBRE.....	40
3.1.7.	RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS	41
3.2.1	MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA.....	42
3.2.2	AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA	42
3.2.2.1.	DISPOSICIONES GENERALES.....	42
3.2.2.2	DOCUMENTOS REQUERIDOS PARA IDENTIFICAR UNA PERSONA JURIDICA.....	42
3.2.2.3.	INFORMACIÓN CONTENIDA EN UN CERTIFICADO CUALIFICADO DE SELLO ELECTRÓNICO.....	43
3.2.3	AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA.....	43
3.2.3.1.	PROCEDIMIENTO PARA LA IDENTIFICACIÓN DE UNA PERSONA FÍSICA	43
3.2.3.2.	INFORMACIÓN CONTENIDA EN UN CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA	44
3.2.3.3.	INFORMACIÓN CONTENIDA EN UN CERTIFICADO CUALIFICADO TRIBUTARIO	45
3.2.4	INFORMACIÓN NO VERIFICADA DEL TITULAR DEL CERTIFICADO..	45
3.2.5	VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO).....	45
3.2.6	CRITERIOS PARA INTEROPERABILIDAD	46
3.2.7	PROCEDIMIENTOS COMPLEMENTARIOS	46
3.2.8	PROCEDIMIENTOS ESPECÍFICOS	47
4.	REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO	49
4.1.1	QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO	50
4.1.2	PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES.....	50
4.1.2.1.	RESPONSABILIDADES Y OBLIGACIONES DEL PCSC DE LA PNDI....	50

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

4.1.2.2. RESPONSABILIDADES Y OBLIGACIONES DE LA ARDEL PCSC DE LA PNDI	59
4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN	60
4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO	60
4.2.3 TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO	60
4.3.1 ACCIONES DEL PCSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS	60
4.3.2 NOTIFICACIONES AL TITULAR DEL CERTIFICADO POR PARTE DEL PCSC SOBRE LA EMISIÓN DEL CERTIFICADO	61
4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO	61
4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PCSC	62
4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR EL PCSC A OTRAS ENTIDADES	62
4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR RESPONSABLE	62
4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LA PARTE USUARIA	64
4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADOS	64
4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN	64
4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO	64
4.6.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO	65
4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO	65
4.6.6 PUBLICACIÓN POR EL PCSC DEL CERTIFICADO RENOVADO	65
4.6.7 NOTIFICACIÓN POR EL PCSC DE LA EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES	65
4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO	65

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA.....	65
4.7.3 PROCESAMIENTO DE SOLICITUDES DE RE-EMISIÓN DE CLAVES DE CERTIFICADO	65
4.7.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA RE-EMISIÓN DE UN NUEVO CERTIFICADO	66
4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE-EMITIDO.....	66
4.7.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS RE- EMITIDOS.....	66
4.7.7 NOTIFICACIÓN POR EL PCSC DE LA RE- EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES	66
4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO.....	66
4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO	66
4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO	66
4.8.4 NOTIFICACIÓN AL SUSCRIPTOR DE LA EMISIÓN DE UN NUEVO CERTIFICADO	66
4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO	67
4.8.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS MODIFICADOS	67
4.8.7 NOTIFICACIÓN POR LA AC DE EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES	67
4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN	67
4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN	68
4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN.....	69
4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN	70
4.9.5 TIEMPO DENTRO DEL CUAL EL PCSC DEBE PROCESAR LA SOLICITUD DE REVOCACIÓN	70
4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LA PARTE USUARIA.....	70
4.9.7 FRECUENCIA DE EMISIÓN DE LA LCR.....	71

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

4.9.8	LATENCIA MÁXIMA PARA LCR	71
4.9.9	DISPONIBILIDAD PARA REVOCACIÓN / VERIFICACIÓN DE ESTADO EN LÍNEA.....	72
4.9.10	REQUISITOS DE VERIFICACIÓN DE LA LCR	72
4.9.11	OTRAS FORMAS DE ADVERTENCIA DE REVOCACIÓN DISPONIBLES	73
4.9.12	REQUERIMIENTOS ESPECIALES POR COMPROMISO DE LA CLAVE PRIVADA.....	73
4.9.13	CIRCUNSTANCIAS PARA SUSPENSIÓN.....	74
4.9.14	QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN	74
4.9.15	PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN	74
4.9.16	LÍMITES DEL PERÍODO DE SUSPENSIÓN	74
4.10.1	CARACTERÍSTICAS OPERACIONALES	74
4.10.2	DISPONIBILIDAD DEL SERVICIO	75
4.10.3	CARACTERÍSTICAS OPCIONALES.....	75
4.12.1	POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES	75
4.12.2	POLÍTICAS Y PRÁCTICAS DE RECUPERACIÓN Y ENCAPSULACIÓN DE CLAVES	76
5.	CONTROLES DE SEGURIDAD FÍSICA, DEGESTIÓN Y DE OPERACIONES.	77
5.1.1	LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO.....	77
5.1.2	ACCESO FÍSICO	78
5.1.2.1	NIVELES DE ACCESO FÍSICO.....	78
5.1.2.2	SISTEMAS FÍSICOS DE DETECCIÓN:	81
5.1.2.3	SISTEMA DE CONTROL DE ACCESO:	82
5.1.2.4	MECANISMOS DE EMERGENCIA:.....	82
5.1.3	ENERGÍA Y AIRE ACONDICIONADO	83
5.1.4	EXPOSICIONES AL AGUA	85
5.1.5	PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO.....	85
5.1.6	ALMACENAMIENTO DE MEDIOS	86
5.1.7	ELIMINACIÓN DE RESIDUOS.....	86

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO:DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

5.1.8	RESPALDO FUERA DE SITIO	87
5.2.1	ROLES DE CONFIANZA.....	87
5.2.2	NÚMERO DE PERSONAS REQUERIDAS POR TAREA	94
5.2.3	IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL.....	94
5.2.4	ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES.....	95
5.3.1	REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN.....	96
5.3.2	PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES	97
5.3.3	REQUERIMIENTOS DE CAPACITACIÓN.....	97
5.3.4	REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN	98
5.3.5	FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES..	98
5.3.6	SANCIONES PARA ACCIONES NO AUTORIZADAS	98
5.3.7	REQUISITOS DE CONTRATACIÓN A TERCEROS.....	99
5.3.8	DOCUMENTACIÓN SUMINISTRADA AL PERSONAL	100
5.4.1	TIPOS DE EVENTOS REGISTRADOS	101
5.4.2	FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)	103
5.4.3	PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA	103
5.4.4	PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA	104
5.4.5	PROCEDIMIENTOS DE RESPALDO (BACKUP) DE REGISTRO (LOGS) DE AUDITORÍA	104
5.4.6	SISTEMA DE RECOLECCIÓN DE INFORMACIÓN DE AUDITORÍA (INTERNO VS EXTERNO).....	104
5.4.7	NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO	105
5.4.8	EVALUACIÓN DE VULNERABILIDADES	105
5.5.1	TIPOS DE REGISTROS ARCHIVADOS	105
5.5.2	PERIODOS DE RETENCIÓN PARA ARCHIVOS	106
5.5.3	PROTECCIÓN DE ARCHIVOS	106
5.5.4	PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVOS.....	107

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

5.5.5	REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS	107
5.5.6	SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO)	107
5.5.7	PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA.....	107
5.6.	CAMBIO DE CLAVE.....	109
5.7.	RECUPERACION DE DESASTRES Y COMPROMISO.....	110
5.7.1	PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO	110
5.7.2	CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES.....	111
5.7.3	PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD	112
5.7.4	CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE.....	113
6.	CONTROLES TÉCNICOS DE SEGURIDAD	116
6.1.1	GENERACIÓN DEL PAR DE CLAVES.....	116
6.1.2	ENTREGA DE LA CLAVE PRIVADA AL TITULAR.....	117
6.1.3	ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO ...	117
6.1.4	ENTREGA DE LA CLAVE PÚBLICA DEL PCSC A LA PARTE USUARIA.	117
6.1.5	TAMAÑO DE LA CLAVE	118
6.1.6	GENERACIÓN DE PARÁMETROS DE CLAVES ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD	118
6.1.7	PROPÓSITOS DE USOS DE CLAVE (CONFORME AL CAMPO KEY USAGE X509 V3).....	118
6.2.1	ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO	119
6.2.2	CONTROL MULTI-PERSONA DE CLAVE PRIVADA.....	119
6.2.3	CUSTODIA (ESCROW) DE LA CLAVE PRIVADA.....	120
6.2.4	RESPALDO/COPIA DE LA CLAVE PRIVADA	120
6.2.5	ARCHIVADO DE LA CLAVE PRIVADA.....	121
6.2.6	TRANSFERENCIA DE CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRYPTOGRÁFICO.....	121

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

6.2.7	ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO.....	121
6.2.8	MÉTODO DE ACTIVACIÓN DE CLAVE PRIVADA.....	121
6.2.9	MÉTODOS DE DESACTIVACIÓN DE LA CLAVE PRIVADA	122
6.2.10	MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA.	122
6.3.1	ARCHIVO DE LA CLAVE PÚBLICA	124
6.3.2	PERÍODO OPERACIONAL DEL CERTIFICADO Y PERÍODO DE USO DEL PAR DE CLAVES	124
6.4.1	GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN	125
6.4.2	PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN	125
6.4.3	OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN.....	126
6.5.1	REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS	126
6.5.2	CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR.....	128
6.5.3	CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO	128
6.6.1	CONTROLES PARA EL DESARROLLO DEL SISTEMA	130
6.6.2	CONTROLES DE GESTIÓN DE SEGURIDAD	130
6.6.3	CONTROLES DE SEGURIDAD DEL CICLO DE VIDA	130
6.6.4	CONTROLES EN LA GENERACIÓN DE LCR	130
6.7.1	DIRECTRICES GENERALES.....	131
6.7.2	FIREWALL.....	132
6.7.3	SISTEMA DE DETECCIÓN DE INTRUSO (IDS).....	132
6.7.4	REGISTRO DE ACCESO NO AUTORIZADO A LA RED.....	133
7.	PERFILES DE CERTIFICADOS, LCR Y OCSP.....	134
7.1.1	NÚMERO DE VERSIÓN	134
7.1.2	EXTENSIONES DEL CERTIFICADO.....	134
7.1.3	IDENTIFICADORES DE OBJETO DE ALGORITMOS.....	136
7.1.4	FORMAS DEL NOMBRE.....	136

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

7.1.5	RESTRICCIONES DEL NOMBRE.....	137
7.1.6	IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO	138
7.1.7	USO DE LA EXTENSIÓN RESTRICCIONES DE POLÍTICA (POLICY CONSTRAINTS)	138
7.1.8	SEMÁNTICA Y SINTAXIS DE LOS CALIFICADORES DE POLÍTICA (POLICY QUALIFIERS).....	138
8.	AUDITORÍA DE CUMPLIMIENTO Y OTRASEVALUACIONES	141
9.	OTROS ASUNTOS LEGALES Y COMERCIALES	145
9.6.1.1.	AUTORIZACIÓN PARA CERTIFICADO	151
9.6.1.2.	PRECISIÓN DE LA INFORMACIÓN	151
9.6.1.3.	IDENTIFICACIÓN DEL SOLICITANTE DEL CERTIFICADO	151
9.6.1.4.	CONSENTIMIENTO DE LOS TITULARES DE CERTIFICADO	152
9.6.1.5.	SERVICIO.....	152
9.6.1.6.	REVOCACIÓN	152
9.6.1.7.	EXISTENCIA LEGAL	152
10.	DOCUMENTOS DE REFERENCIA	158

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

CONTROL DOCUMENTAL

DOCUMENTO	
TÍTULO: DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FISICA del PCSC de la POLICIA NACIONAL - DEPARTAMENTO DE IDENTIFICACIONES	NOMBRE DEL ARCHIVO: DPC F2 PNDI v1.2
CÓDIGO: DPC-PNDI-V1.2	SOPORTE LÓGICO: https://www.identificaciones.gov.py/firma_digital/DPC/DPC%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
1.1	07/02/2023	Versión inicial
1.2.	11/07/23	Ítem 5.6 Cambio de Clave Ítem 9.7 Extensión de Garantía

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

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

CONTROL DEL DOCUMENTO		
PREPARADO POR:	REVISADO POR:	ACEPTADO POR:
CONSORCIO CDE	CONSORCIO CDE	Ministerio del Interior

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

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.

Esta Declaración de Prácticas de Certificación (DPC) describe los procedimientos que utiliza el PCSC de la PNDI para ofrecer sus servicios de manera correcta. La estructura de la DPC se basa en lo establecido en la Resolución MIC N° 811/2022 "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-ICCP-03 , Versión 1.0." y en el RFC 364.

Cualquier referencia a los formularios en este DPC también se entenderá como una referencia a cualquier otro formulario que el PCSC de la PNDI o entidades vinculadas a él puedan adoptar. Además, el PCSC de la PNDI se encarga de mantener actualizada toda la información de su DPC.

Los certificados emitidos por el PCSC de la PNDI contienen la clave pública correspondiente a sus claves privadas y están relacionados con el servicio de expedición de certificados electrónicos calificados de firma electrónica. Es importante mencionar que la firma electrónica calificada basada en certificados calificados, conforme a la legislación vigente, tiene un efecto

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

jurídico equivalente a una firma manuscrita.

Es importante señalar que los certificados cualificados de firma electrónica sólo pueden emitirse a personas físicas y que el PCSC de la PNDI emitirá únicamente certificados del tipo F2.

1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Nombre	Declaración de Prácticas de Certificación 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

1.3. PARTICIPANTES DE LA ICPP

1.3.1. AUTORIDADES CERTIFICADORAS (AC)

Esta DPC se refiere exclusivamente al PCSC de la PNDI.

El PCSC de la PNDI es una entidad habilitada por la AA, encargada de operar una AC en el marco de la ICPP, cuenta con un certificado emitido por la AC-Raiz-Py y solo podrá emitir certificados a personas físicas que sean usuarios finales. El PCSC de la PNDI se considera un Prestador Cualificado de Servicios de Confianza que presta servicios de creación, verificación y validación de certificados cualificados.

Las claves privadas de los firmantes almacenadas en dispositivos estandarizados conforme a lo establecido en el documento DOC-ICPP-04 [1],

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

y los certificados de firmas electrónicas cualificadas realizadas con la clave privada del firmante son válidas de conformidad a la Ley N° 6822/2021.

1.3.2. AUTORIDAD DE REGISTRO (AR)

Los datos referentes a las AR habilitadas por el PCSC de la PNDI para los procesos de recepción, validación y direccionamiento de solicitudes de emisión o de revocación de los certificados electrónicos, y de identificación de sus solicitantes, 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 de la PNDI, indicando la fecha de la inhabilitación.

La AR puede ser propia del PCSC de la PNDI o delegada a un tercero cuyo funcionamiento deberá ser autorizado por la AC Raíz-Py con la habilitación correspondiente.

Las AR delegadas son autoridades de registro vinculadas al PCSC de la PNDI mediante un acuerdo operacional.

1.3.3. AUTORIDADES DE VALIDACIÓN (AV)

Los datos referentes a las AV habilitadas por el PCSC de la PNDI, para suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una AR y certificados por el PCSC se encuentran en la

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

dirección de página web(URL) <https://www.identificaciones.gov.py/autoridad-de-validacion-av/>

El PCSC de la PNDI publica 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.

La AV puede ser propia del PCSC de la PNDI o delegada a un tercero cuyo funcionamiento deberá ser autorizado por la AC Raíz-Py con la habilitación correspondiente.

Las AVs delegadas son autoridades de validación vinculadas al PCSC de la PNDI mediante un acuerdo operacional.

1.3.4. TITULARES DEL CERTIFICADO

Toda persona física podrá ser titular de los certificados emitidos por PCSC de la PNDI. Es obligación de todo titular el conocimiento de la presente DPC, así como de la normativa vigente.

1.3.5. PARTE USUARIA

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

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

AR vinculada para desempeñar actividades descritas en esta DPC o en una PC y se clasifican en tres categorías, conforme al tipo de servicio prestado:

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

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

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

El PCSC deberá igualmente publicar información referente a:

- Lista de todos los PSSs habilitados
- Lista de los PSSs que se han inhabilitado por el PCSC, indicando la fecha de la inhabilitación.

1.4. USO DEL CERTIFICADO

1.4.1. USOS APROPIADOS DEL CERTIFICADO

El PCSC de la PNDI implementa las siguientes políticas de Certificación:

- PC F2 PNDI v1.2

<https://www.identificaciones.gov.py/firmadigital/PC/PC%20F2%20PNDI%20v1.1.pdf>

El PCSC de la PNDI, implementa lo correspondiente a cada tipo de certificado que emita en su política de certificación en adelante PC, las que determinan los usos apropiados que debe darse a cada certificado.

A continuación, se describen los usos apropiados del Certificado de la AC Raíz-

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

Py ydel PCSC de la PNDI.

TIPO	DESCRIPCIÓN DE USO APROPIADO
Certificado de AC Raíz-Py	Firma de Certificado a PCSC. Firma de LCR del PCSC. - Firma de Certificado (Certificate Signing). - Firma LCR sin conexión (Off line CRL Signing)
Certificado del PCSC	Firma de Certificado a sus suscriptores. Firma de LCR desus suscriptores. - Firma de Certificado (Certificate Signing) - Firma LCR sin conexión (Off line CRL Signing) - Firma de LCR (CRL Signing).

- Firma de Certificado (Certificate Signing): se usa en caso de que la clave pública del suscriptor es utilizada para verificar una firma en certificados. Esta extensión solo se puede utilizar en los certificados de AC. Si el Certificate Signing se activa, en la extensión del perfil restricciones básicas deberá aparecer la restricción tipo de sujeto (subject type) = AC.
- Firma LCR (LCR Signin Lg) y Firma del LCR sin conexión (Off line LCR Signing): se activa cuando la clave pública del suscriptor se utiliza para la verificación de firmas en la lista de revocación de certificados.

1.4.2. USOS PROHIBIDOS DEL CERTIFICADO

Cada PC implementada por el PCSC de la PNDI determina las limitaciones y restricciones en el uso de los certificados que emite. No es objetivo de esta

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

DPC ladeterminación de dichas limitaciones y restricciones.

1.5. ADMINISTRACIÓN DE LA POLÍTICA

1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre del PCSC: 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

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

1.5.3. PERSONA QUE DETERMINA LA ADECUACIÓN DE LA DPC A LA PC

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

1.5.4. PROCEDIMIENTOS DE APROBACIÓN DE LA DPC

El personal autorizado del PCSC de la PNDI, conforme con la reglamentación vigente, validará el contenido de la Declaración de Prácticas de Certificación (DPC) y sus posteriores enmiendas o modificaciones, y luego será puesta a

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

consideración de la Dirección General de Comercio Electrónico en su carácter de AC Raíz-Py de la ICPP 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.

Autenticación: proceso técnico que permite determinar la identidad de la persona física.

Autenticación electrónica: un proceso electrónico que posibilita la identificación electrónica de una persona física o del origen y la integridad de datos en formato electrónico.

Autoridad de Aplicación: Ministerio de Industria y Comercio a través de la Dirección General de Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.

Autoridad de Certificación: entidad que presta servicios de emisión, gestión, revocación u otros servicios de confianza basados en certificados cualificados. En el marco de la ICPP, son Autoridades de Certificación, la AC Raíz-Py y el PCSC.

Autoridad de Certificación Raíz del Paraguay: órgano técnico, cuya función principal es coordinar el funcionamiento de la ICPP. La AC Raíz-Py tiene los certificados de más alto nivel, posee un certificado autofirmado

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

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. 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.

Cadena de certificación: lista ordenada de certificados que contiene un certificado del firmante y certificados de la AC, que termina en un certificado raíz. El emisor del certificado del firmante 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, 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.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

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

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

Contrato de prestación de servicio de confianza: Acuerdo entre la AC Raíz-Pyy 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 le 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.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

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

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.

Dossier del titular del certificado: conjunto formado por la verificación de los documentos de identificación utilizados para la emisión, suspensión o revocación del certificado, solicitud de certificado, contrato de prestación de servicios, y por la solicitud de revocación, cuando sea el caso. Este dossier

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

deberá estar en formato de archivo digital, en el cual se escanean los documentos en formato papel, si los hubiere y se firma la solicitud de certificado y contrato de prestación de servicios con la clave privada del titular, después de la autorización del AGR por medio de la firma de dichos documentos, siempre y cuando sea informado y aceptado su contenido por parte de su solicitante y firmada electrónicamente con un certificado cualificado después de la generación de las claves y anterior a la instalación del certificado correspondiente.

Emisor del certificado: persona física 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, 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

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

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 Solicitante de certificado: comprende la etapa de la confirmación de la identidad de una persona física, 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 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

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

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-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. **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

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

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.

Prestador Cualificado de Servicios de Confianza: prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la habilitación.

Política de Seguridad: es un conjunto de directrices destinadas a definir la protección del personal, seguridad física, lógica y de red, clasificación de la información, salvaguarda de activos de la información, 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

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY				
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES				
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2		

cuales 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 el 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.

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, suscrito por el solicitante en nombre propio en el caso de certificados cualificados de firma electrónica para persona física.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

Solicitud de revocación: documento que se instrumenta mediante un formato autorizado de solicitud para la revocación de un certificado.

Verificación y validación de firma: determinación y validación de que la firma 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 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.

1.6.2. ACRÓNIMOS

ACRÓNIMOS	DESCRIPCIÓN
AA	Autoridad de Aplicación
AGD	Autoridad de Gestión de Datos
AGR	Agente de Registro
P	País (C por su sigla en inglés, Country)

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

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)
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.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

HSM	Módulo de seguridad criptográfico basado en Hardware (HSM por su sigla en inglés Hardware Security module)
ISO	Organización Internacional para la Estandarización (por sus siglas en inglés International Organization for Standardization)
MIC	Ministerio de Industria y Comercio
O	Organización (del inglés Organization)
OCSP	Servicio de Validación de certificado en línea (OCSP por sus siglas en inglés Online Certificate Status Protocol)
OID	Identificador de Objeto (OID por sus siglas en inglés Object Identifier)
OU	Unidad Organizacional (OU, por sus siglas en inglés Organization Unit)
PAS	Pasaporte
PCN	Plan de Continuidad del Negocio
PKI	Infraestructura de Clave Pública (PKI por su sigla en inglés Public Key Infrastructure)
ICPP	Infraestructura de Clave Pública del Paraguay
OEC	Organismo de Evaluación de la Conformidad

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

PCSC	Prestador cualificado de servicios de confianza
PS	Política de Seguridad
PSS	Prestador de Servicio 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
UPS	Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés, uninterruptible power supply)
URL	Localizador uniforme de recursos (URL por sus siglas en inglés, Uniform Resource Locator).
AV	Autoridad de validación (VA por sus siglas en inglés, Validation Authority)

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

2.1 REPOSITORIOS

El PCSC de la PNDI mantiene un repositorio disponible de conformidad con lassiguientes obligaciones:

- Poner a disposición, inmediatamente después de su emisión, loscertificados emitidos por PCSC de la PNDI y su LCR / OCSP.
- Estar disponible para consultas durante 24 (veinticuatro) horas al día, 7(siete) días a la semana.
- Implementar los recursos necesarios para la seguridad de los datosalmacenados allí.
- Proporcionar 2 (dos) repositorios, en infraestructuras de red segregada,para la distribución del LCR/OCSP.
- Garantizar que en su sitio web exista un enlace a la lista de confianza pertinente al utilizar la etiqueta de confianza «PY» para los servicios deconfianza cualificados.

El PCSC de la PNDI cumple con los siguientes requisitos:

- Localización física y lógica: el repositorio se aloja en un centro de datos seguro y protegido. Los datos se almacenan en servidores seguros que solopodrán ser accedidos por personal autorizado y disponibles es la dirección web:
<https://www.identificaciones.gov.py/>

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

- Disponibilidad: El repositorio del PCSC de la PNDI está disponible para consultas durante el 99.5% (noventa y nueve, punto cinco por ciento) del mes, 24 (veinticuatro) horas al día, 7 (siete) días a la semana. Si se produce una interrupción, se notificará al personal encargado de inmediato para solucionar el problema lo antes posible. Además el PCSC de la PNDI proporciona 02 (dos) repositorios, en infraestructuras de red segregadas, para la distribución de LCR / OCSP.
- Protocolos de acceso: solo los usuarios autorizados tienen acceso al repositorio. La autenticación y la autorización se lleva a cabo mediante el uso de credenciales de usuario únicas y contraseñas robustas. Los usuarios deberán cambiar sus contraseñas en forma periódica.
- Requisitos de seguridad: El repositorio se protege mediante medidas de seguridad física y lógica. Los datos se cifran en tránsito y en reposo. Se llevan a cabo copias de seguridad periódicas y se almacenarán fuera del sitio principal. Se implementan medidas de seguridad para proteger el repositorio contra amenazas informáticas y se actualizan periódicamente para abordar las vulnerabilidades conocidas.

2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

El PCSC de la PNDI pone a disposición pública la información mencionada a continuación, en un servicio de directorio y / o en su sitio web de conformidad con las normas y criterios establecidos en esta DPC, en la siguiente URL:

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

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

La disponibilidad de información publicada por el PCSC de la PNDI en el servicio dedirectorio y/o página web es del 99.5% (noventa y nueve, punto cinco por ciento) del mes, 24 (veinticuatro) horas al día, 7 (siete) días a la semana.

En caso de interrupción por causa de fuerza mayor, el servicio se restablecerá en un plazo no mayor a veinticuatro horas, garantizando la disponibilidad del servicio con un mínimo de 99,5% anual, un tiempo programado de inactividad máximo de 0,5% anual.

El PCSC de la PNDI mantiene publicada, entre otros aspectos la versión actualizada de:

Política de Certificado - PC F2 PNDI v1.2	https://www.identificaciones.gov.py/firma digital/PC/PC%20F2%20PNDI%20v1.1.pdf
Declaración de Prácticas de Certificación - DPC F2 v1.2	https://www.identificaciones.gov.py/firma digital/DPC/DPC%20F2%20PNDI%20v1.1.pdf
Certificado de Autoridad de Certificación Raíz - MIC	https://www.identificaciones.gov.py/
Certificado del PCSC	https://www.identificaciones.gov.py/
Lista de Certificado Revocado - LCR	https://www.identificaciones.gov.py/firma digital/crl/SignatureCRL.crl
Certificados Emitidos	https://www.identificaciones.gov.py/firma digital/ConsultaEmitidos/
Contrato de Prestación de Servicios de Confianza PCSC de la PNDI v1.2	https://www.identificaciones.gov.py/firma digital/AcuerdoDeSuscriptor/Contrato-de-prestacio%CC%81n-de-servicios-de-confianza-PSC-de-la-PNDI-v1.1.pdf

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

RESOLUCIÓN DE HABILITACIÓN DEL PCSC	https://www.identificaciones.gov.py/firma digital/resoluciones/
Legales ICPP - Leyes y Decretos	https://www.identificaciones.gov.py/firma digital/leyes-y-decretos/
Legales ICPP - Resoluciones y Reglamentos	https://www.identificaciones.gov.py/firma digital/resolucionespki/
Identificación, Domicilio y Contacto telefónico.	https://www.identificaciones.gov.py/cont acto/
Autoridad de Registro - AR	https://www.identificaciones.gov.py/firma digital/ras/
Acuerdos Operacionales entre la AR y el PCSC	NO APLICA
Autoridad de Registro revocada - Fecha de revocación	NO APLICA
Autoridad de Validación - AV	https://www.identificaciones.gov.py/autoridad-de-validacion-av/

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

Acuerdos Operacionales entre el AV y el PCSC	NO APLICA
Autoridades de Validación revocadas - Fecha de revocación	NO APLICA
Prestador de servicio de soporte - PSS	https://www.identificaciones.gov.py/firma digital/pss/

2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN

Cuando se produzca una actualización de los documentos relacionados con el marco legal u operativo del PCSC de la PNDI, la nueva versión de los documentos mencionados en el punto 2.2, se publicará de acuerdo con lo establecido en el punto 9.12 de esta DPC.

La información de los estados de los certificados es publicada de acuerdo a lo dispuesto en el punto 4.9.7 de esta DPC.

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

2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

El acceso para la consulta de las informaciones establecidas en el punto 2.2 es abierto.

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

Sólo el personal debidamente asignado por la PNDI está autorizado a modificar, sustituir o eliminar información de su repositorio y sitio web. Los controles de acceso establecen identificación personal para el acceso a los equipamientos, utilizando contraseñas y protocolos seguros de comunicación de datos.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

3. IDENTIFICACION Y AUTENTICACION

3.1 NOMBRES

3.1.1. TIPOS DE NOMBRES

El tipo de nombre admitido para los titulares de los certificados emitidos conforme a la presente DPC son el Nombre Distintivo (Distinguished Name) según lo establecido en la ITU X.500, direcciones de correos electrónicos o direcciones de página web (URL).

3.1.2. NECESIDAD DE NOMBRES SIGNIFICATIVOS

El nombre significativo, corresponde al especificado en el documento de identificación presentado por el solicitante en el momento de registro.

3.1.3. ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES

No se admite el anonimato en los certificados emitidos por el PCSC de la PNDI. Asimismo, el seudónimo no se considera un nombre significativo del solicitante y no se utilizará como parte del certificado.

3.1.4. REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES

El uso del campo número de serie (serial number OID 2.5.4.5) se establece como un campo del nombre distintivo del sujeto. En concordancia a lo definido en la familia de estándares X.500

Certificado del PCSC de la PNDI

La Cédula Tributaria – RUC es expedida por la Subsecretaría de Estado de Tributación y debe cumplir el siguiente formato:

 TETÄ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

TIPO DE DOCUMENTO	PREFIJO	FORMATO
Cédula Tributaria	RUC	RUC99999999-9

Certificado Cualificado de Firma Electrónica de Persona Física

La Cédula de identidad es expedida por el Departamento de Identificaciones de la Policía Nacional, y deben cumplir el siguiente formato:

TIPO DE DOCUMENTO	PREFIJO	FORMATO	DESCRIPCIÓN
Cédula de identidad CI	CI	CI999999X	Siglas CI seguido del número de cédula de identidad civil, el cual puede ser alfanumérico.

Está prohibido el uso de nombres en certificados que violen los derechos de propiedad intelectual de terceros.

3.1.5. UNICIDAD DE LOS NOMBRES

El "Distinguished Name" (DN) del suscriptor, deberá ser único para cada titular del certificado, en el ámbito del PCSC de la PNDI. Números y letras adicionales podrán ser incluidos al nombre de cada entidad para asegurar la unicidad del campo.

Al respecto, del PCSC de la PNDI se reserva el derecho de tomar todas las decisiones referidas a posibles conflictos sobre la utilización y titularidad de cualquier nombre en los certificados de sus suscriptores.

3.1.6. PROCEDIMIENTO PARA RESOLVER DISPUTA DE NOMBRE

El PCSC de la PNDI se reserva el derecho de tomar todas las decisiones en el caso de que haya conflicto derivado de los nombres iguales entre varios

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

solicitantes de certificados. Durante el proceso de confirmación de identidad, corresponderá al solicitante del certificado demostrar su derecho a usar un nombre específico.

3.1.7. RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

Los procesos de tratamiento, reconocimiento, autenticación y rol de marcas registradas serán ejecutados de acuerdo con la legislación vigente sobre la materia.

3.2 VALIDACIÓN INICIAL DE IDENTIDAD

El proceso de comprobación de identidad de la persona física cuyos datos se incluyen en un certificado electrónico cualificado tiene como objetivo garantizar que el suscriptor sea la persona identificada en la solicitud del certificado, y que la información que se incluya en el certificado sea exacta. En principio, la exactitud y veracidad de la información proporcionada por el suscriptor es atribuida al mismo, sin perjuicio de la respectiva comprobación por parte del PCSC de la PNDI comprendiendo los siguientes procesos:

a) **Identificación y registro del titular del certificado:** identificación de la persona física, titular del certificado, con base en los documentos de identificación mencionado en el ítems 3.2.3, observando lo siguiente:

- i. para certificados cualificados de firma electrónica cualificada: prueba de que la persona física que se presenta como titular del certificado, es realmente aquel cuyos datos aparecen en la documentación presentada. Queda prohibido cualquier tipo de poder para tal fin.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

b) **Emisión del certificado:** luego de cotejar los datos de la solicitud del certificado con los contenidos en los documentos presentados, en la etapa de identificación, se procede a la emisión del certificado en el sistema del PCSC. Se considera que la extensión **Nombre Alternativo del Sujeto (Subject Alternative Name)** está fuertemente relacionada con la clave pública contenida en el certificado, por lo que todas las partes de esta extensión deben verificarse y el solicitante del certificado debe demostrar que tiene los derechos sobre esta información ante la autoridad competente.

3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA

La AR vinculada al PCSC de la PNDI, verifica que el solicitante del certificado tenga la clave privada correspondiente a la clave pública para la cual se solicita el certificado. El RFC 4210 y RFC 6712 se utilizan como referencia para este propósito. En el caso de que se requieran procedimientos específicos para las PC implementadas, se describen en esas PC, en el ítem correspondiente.

3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

No Aplica

3.2.2.1. DISPOSICIONES GENERALES

No Aplica.

3.2.2.2 DOCUMENTOS REQUERIDOS PARA IDENTIFICAR UNA PERSONA JURIDICA

No Aplica.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

3.2.2.3. INFORMACIÓN CONTENIDA EN UN CERTIFICADO CUALIFICADO DE SELLO ELECTRÓNICO.

No Aplica.

3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA

En este ítem, se definen los procedimientos utilizados por las ARs vinculadas al PCSC de la PNDPI para la identificación y el registro de una persona física en la ICPP.

La confirmación de la identidad de la persona física responsable del certificado es verificada por el PCSC de la PNDPI a través de sus RAs en los siguientes términos:

- a) en presencia de la persona física; o
- b) por medio de un certificado de una firma electrónica cualificada expedida de conformidad con la letra a).

3.2.3.1. PROCEDIMIENTO PARA LA IDENTIFICACIÓN DE UNA PERSONA FÍSICA

La identificación de la persona física solicitante del certificado es realizada de la siguiente manera:

- a) presentación de la siguiente documentación, en su versión oficial original, física o electrónica:
 - i) cédula de Identidad civil, si es paraguayo; o
 - ii) cédula de Identidad de extranjero, si es extranjero domiciliado en Paraguay.

Se considera documento de identidad al documento oficial, físico o electrónico,

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

según la legislación específica, emitido por el Ministerio del Interior a través de la Policía Nacional.

Los documentos electrónicos son verificados a través de fuentes oficiales de organismos competentes. Dicha verificación forma parte del dossier del titular del certificado. En caso de una identificación positiva, se omite el requerimiento de verificación descritos en el siguiente párrafo:

Los documentos en papel, para los cuales no existan formas de verificación a través de fuentes oficiales competentes, son verificados:

- a) por un agente de registro del PCSC de la PNDPI distinto del que realizó el paso de identificación;
- b) por la AR del PCSC de la PNDPI; y
- c) antes del inicio de la validez del certificado, y es revocado inmediatamente en el caso que la verificación no se haya realizado antes del inicio de su validez.

La emisión de certificados a favor de los absolutamente incapaces y de los relativamente incapaces se realizan conforme a las disposiciones de la ley vigente y las normas emitidas por la ICPP.

3.2.3.2. INFORMACIÓN CONTENIDA EN UN CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA

La información obligatoria contenida en los campos del certificado cualificado de firma electrónica expedido a una persona física debe coincidir exactamente

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

con la información contenida en los siguientes documentos:

- a) nombre completo de la persona física titular del certificado según el documento de identidad; y
- b) número de cédula de identidad civil de la persona física, según documento de identidad.

Cada PC puede definir como obligatorio llenar otros campos. Además, el titular del certificado, a su criterio y mediante una declaración expresa en el documento contrato de prestación de servicios de confianza, puede solicitar llenar el campo con la siguiente información:

- a) el correo del titular del certificado, siendo suficiente la declaración expresa en la correspondiente solicitud.

3.2.3.3. INFORMACIÓN CONTENIDA EN UN CERTIFICADO CUALIFICADO TRIBUTARIO

No Aplica

3.2.4 INFORMACIÓN NO VERIFICADA DEL TITULAR DEL CERTIFICADO

No aplica.

3.2.5 VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)

La AR vinculada al PCSC de la PNDI determina si el solicitante se encuentra apto para solicitar un tipo de certificado específico. Además, valida que el solicitante no posea impedimentos legales.

Para los Certificados Cualificados de Firma Electrónica de Persona Física, válida:

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

- Nombre y documento de identidad;y
- Mayoría de edad.

3.2.6 CRITERIOS PARA INTEROPERABILIDAD

Los servicios de confianza prestados por los prestadores de servicios de confianza establecidos fuera del país serán reconocidos como legalmente equivalentes a los servicios de confianza cualificados prestados por los PCSC establecidos en la República del Paraguay si los servicios de confianza son reconocidos en virtud de acuerdos de reconocimiento mutuo celebrado entre autoridades oficiales de cada país o con organizaciones internacionales de conformidad a la reglamentación correspondiente.

Los acuerdos a que se refiere el párrafo anterior deben garantizar, en particular, que:

- Los prestadores de servicios de confianza establecidos fuera del país u organizaciones internacionales y los servicios de confianza que prestan, cumplen los requisitos aplicables a los PCSC establecidos en el Paraguay y a los servicios de confianza cualificados que prestan.
- Los servicios de confianza cualificados prestados por PCSC establecidos en Paraguay son reconocidos como legalmente equivalentes a los servicios de confianza prestados por prestadores de servicios establecidos fuera del país u organizaciones internacionales con los que se celebran acuerdos.

3.2.7 PROCEDIMIENTOS COMPLEMENTARIOS

El PCSC de la PNDI comprueba la identidad y/o atributos de las personas físicas

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

antes de incluir estos atributos en un certificado en el marco de la ICPP. Se prohíbea las personas físicas utilizar en sus certificados nombres que violen los derechos de propiedad intelectual de terceros. El PCSC de la PNDI se reserva el derecho, sin responsabilidad ante ningún solicitante, de rechazar solicitudes.

El PCSC de la PNDI mantiene actualizadas sus políticas y procedimientos internos y son revisados periódicamente para cumplir con los requisitos establecidos por la AC Raíz-Py,

Además el PCSC de la PNDI mantiene un archivo con copias de todos los documentos utilizados para confirmar la identidad de una persona física. Tales copias son conservadas en papel o en formato electrónico, sujetas a las condiciones definidas en el documento DOC-ICPP-05 [4].

3.2.8 PROCEDIMIENTOS ESPECÍFICOS

En el caso de certificado emitido a Empleados del Servicio Exterior Paraguayo, en misión permanente en el exterior, si existen impedimentos para identificación conforme previsto en el ítem 3.2, es posible enviar la documentación por vía diplomática y realizar la identificación por otros medios seguros, a ser definidos y aprobados por la AC Raíz-Py.

3.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE NUEVAS CLAVES.

En este ítem se establecen los procesos de identificación y confirmación del registro del solicitante, utilizados por el PCSC de la PNDI para generar un nuevo par de claves y su correspondiente nuevo certificado.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

El proceso puede realizarse de acuerdo con una de las siguientes posibilidades:

- a) adopción del mismo requisito y procedimiento requeridos en el punto 3.2.3;
o
- b) solicitud, por medio electrónico, firmada electrónicamente utilizando un certificado cualificado de la ICPP válido del solicitante, que sea del mismo nivel de seguridad o superior, admitiéndose esta hipótesis únicamente para los certificados cualificados de firma electrónica;
- c) solicitud, por medio electrónico, utilizando un medio de identificación electrónica expedido en virtud de un sistema de identificación electrónica de nivel alto.

Si se requieren procedimientos específicos para las PCs implementadas por el PCSC de la PND, estos estarán descritos en esas PCs, en el ítem correspondiente.

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

El solicitante de la revocación de un certificado cualificado emitido por el PCSC de la PND en el marco de la ICPP debe estar identificado. Únicamente los agentes descritos en el ítem 4.9.2 podrán solicitar la revocación de dicho certificado.

El procedimiento para solicitar la revocación de un certificado cualificado por parte del PCSC de la PND se describe en el ítem 4.9.3.

Las solicitudes de revocación de certificados deben registrarse.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1 SOLICITUD DEL CERTIFICADO

Este ítem describe todos los requisitos y procedimientos operacionales establecidos por el PCSC de la PNDI y las AR, a ella vinculadas, para la solicitud de emisión de certificados. Estos requisitos y procedimientos comprenden todas las acciones necesarias tanto del solicitante individual como del PCSC de la PNDI y sus AR en el proceso de solicitud del certificado e incluyen:

- La comprobación de los atributos de identificación que constan en el certificado conforme al punto 3.2;
- El uso de un certificado cualificado de firma electrónica del AGR responsable de gestionar las solicitudes de emisión y revocación de certificados; y
- Un Contrato de prestación de servicios de confianza firmado con firma electrónica cualificada por el titular del certificado.

En caso de imposibilidad técnica de firmar electrónicamente el contrato de prestación de servicio de confianza será aceptada la firma manuscrita del contrato por parte del titular. En este caso se verificará la firma contra el documento de identificación y se adjuntará al dossier de titular del certificado, el documento manuscrito digitalizado y firmado con firma electrónica cualificada por el AGR, conforme al DOC- ICPP-05 [4].

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

El formato del documento contrato de prestación de servicio de confianza, según será el tipo de certificado a ser emitido, se encuentra establecido por la AC Raíz-Py.

4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

La presentación de la solicitud será siempre a través de una AR vinculada al PCSC de la PNDI.

Puede presentar la solicitud de certificado cualificado de firma electrónica para persona física toda persona mayor de edad, sin distinción, con un documento de identidad válido, que será el sujeto a cuyo nombre se emita el certificado.

4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

En los siguientes ítems se describen las obligaciones generales de las entidades involucradas. Si existen obligaciones específicas para las PCs implementadas por el PCSC de la PNDI, se describirán en dichas PCs, en el ítem correspondiente.

4.1.2.1. RESPONSABILIDADES Y OBLIGACIONES DEL PCSC DE LA PNDI

Responsabilidades:

- El PCSC de la PNDI será responsable de los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que les impone la normativa vigente;
- El PCSC de la PNDI asumirá toda la responsabilidad frente a terceros por la actuación de las personas u otros prestadores en los que deleguen la

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

ejecución de alguna/s de las funciones necesarias para prestación de servicios de confianza, incluyendo las actuaciones de comprobación de identidad previas a la expedición de un certificado cualificado.

Obligaciones

Las obligaciones del PCSC de la PNDI responsable de esta DPC, comprende al menos lo siguiente:

- a) publicar información veraz y acorde con las reglamentaciones vigentes, en su sitio principal de Internet:
 - i) su DPC, y las PC aprobadas que implementa;
 - ii) las informaciones definidas en el ítem 2.2. de este documento y
 - iii) las informaciones sobre la desvinculación de una AR.
- b) no almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma de la persona física a las que hayan emitido certificados, salvo en caso de su gestión en nombre del firmante o del creador del sello. En este caso, el PCSC de la PNDI tendrá la obligación de:
 - I. utilizar sistemas y productos fiables, incluidos los canales de comunicación electrónica seguros;
 - II. aplicar procedimientos y mecanismos técnicos y organizativos adecuados, para garantizar que el entorno sea fiable y se utilice bajo el control exclusivo del titular del certificado;
 - III. custodiar y proteger los datos de creación de firma, de sello frente

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

a cualquier alteración, destrucción o acceso no autorizado; y

IV. garantizar su continua disponibilidad.

c) disponer de un servicio de consulta sobre el estado de validez y

revocación de los certificados emitidos accesible al público;

d) conservar la información relativa a los servicios prestados por el término de diez años;

e) en el caso de cese de sus operaciones, comunicar a los que preste sus servicios y al organismo de supervisión con una antelación mínima de dos meses el cese efectivo de la actividad.

El plan de cese del PCSC de la PNDPI podrá incluir la transferencia de clientes a otro prestador cualificado, una vez acreditada la ausencia de oposición de los mismos;

f) comunicar al organismo de supervisión cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, debe comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra él;

g) asegurarse de que el titular del certificado puede controlar el acceso y uso de los datos de creación de firma correspondientes a los de verificación que consten en el certificado, antes de la expedición de un certificado cualificado;

h) enviar el informe de evaluación de la conformidad a la AC Raíz-Py en el plazo de tres días hábiles tras su recepción. El incumplimiento de esta obligación conlleva la suspensión de la cualificación al prestador y al servicio que éste presta, y su

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

eliminación de la lista de confianza;

- i) notificar, en un plazo de veinticuatro horas tras tener conocimiento de ellas, a la AC Raíz-Py de las violaciones de seguridad que sufran, entendiéndose como violación de seguridad a un evento que afecta de manera crítica la confidencialidad, integridad y/o disponibilidad de los activos de información y tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes;
- j) gestionar los incidentes de seguridad que les afecten, debiendo prever los mecanismos adecuados para su prevención, detección, análisis y resolución;
- k) ampliar tras la resolución del incidente, la información suministrada en la notificación inicial con arreglo a las directrices que pueda establecer AC Raíz- Py;
- l) facilitar a la AC Raíz-Py toda la información y colaboración precisas para el ejercicio de sus funciones. En particular, deben permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate conforme al servicio que se preste. En sus inspecciones podrán ir acompañados de expertos o peritos en las materias sobre las que versen aquéllas;
- m) adoptar las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan. Habida cuenta de los últimos avances tecnológicos, dichas medidas garantizan un nivel de seguridad proporcional al grado de riesgo. En particular, se adoptarán

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

medidas para evitar y reducir al mínimo el impacto de los incidentes de seguridad e informar a los interesados de los efectos negativos de cualquiera de tales incidentes.

- n) notificar al organismo de supervisión y al centro de respuestas a incidentes Cibernéticos del Ministerio de Tecnologías de la Información y Comunicación (MITIC), sin demoras indebidas, pero en cualquier caso en un plazo de veinticuatro horas tras tener conocimiento sobre cualquier violación de la seguridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes. Cuando la violación de seguridad pueda atentar contra una persona física o jurídica a la que se ha prestado el servicio de confianza, se deberá notificar también a la persona física o jurídica, sin demora indebida, la violación de seguridad. El organismo de supervisión notificado informará al público o exigirá al prestador de servicios de confianza que lo haga, en caso de considerar que la divulgación de la violación de seguridad reviste interés público.
- o) informar al organismo de supervisión de cualquier cambio en la prestación de servicios de confianza cualificados, y de su intención de cesar tales actividades.
- p) contar con personal y, si procede, con subcontratistas, que posean los conocimientos especializados, la fiabilidad, la experiencia y las cualificaciones necesarios y hayan recibido la formación adecuada en materia de seguridad y normas de protección de datos personales y que apliquen procedimientos

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

administrativos y de gestión que correspondan a normas internacionales.

- q) con respecto al riesgo de la responsabilidad por daños, mantener recursos financieros suficientes u obtener pólizas de seguros de responsabilidad adecuadas.
- r) antes de entrar en una relación contractual, informar, de manera clara y comprensible, a cualquier persona que desee utilizar un servicio de confianza cualificado acerca de las condiciones precisas relativas a la utilización de dicho servicio, incluidas las limitaciones de su utilización.
- s) utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad y la fiabilidad técnicas de los procesos que sustentan.
- t) utilizar sistemas fiables para almacenar los datos que se les faciliten de forma verificable, de modo que:
 - i) estén a disposición del público para su recuperación sólo cuando se haya obtenido el consentimiento de la persona a la que corresponden los datos.
 - ii) solo personas autorizadas puedan hacer anotaciones y modificaciones en los datos almacenados.
 - iii) pueda comprobarse la autenticidad de los datos.
- u) tomar medidas adecuadas contra la falsificación y el robo de datos.
- v) registrar y mantener accesible durante un período de tiempo definido por la AC Raíz-Py, incluso cuando hayan cesado las

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

actividades del PCSC de la PNDI, toda la información pertinente referente a los datos expedidos y recibidos por el PCSC de la PNDI, en particular al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio. Esta actividad de registro podrá realizarse por medios electrónicos.

- w) Contar con un plan de cese actualizado para garantizar la continuidad del servicio,
- x) garantizar un tratamiento lícito de los datos personales.
- y) mantener actualizada una base de datos de certificados.
- z) cuando el PCSC de la PNDI revoca un certificado, deberán registrar su revocación en su base de datos de certificados y publicar el estado de revocación del certificado oportunamente y, en todo caso, en un plazo de veinticuatro horas después de la recepción de la solicitud.

aa) recolectar los datos personales directamente de la persona a quien esos datos se refieran. La recolección y procesamiento en general de los datos personales se realizarán solo en la medida en que los mismos sean necesarios para la prestación del servicio de confianza. Los datos personales no pueden ser procesados para otro fin distinto al acordado, sin el consentimiento expreso del titular de los datos.

bb) constatar la verdadera identidad del firmante o titular del certificado y conservar la documentación que la acredite en caso de expedir certificados que consignen seudónimos.

cc) revelar la verdadera identidad del firmante o titular del certificado en caso de expedir certificados que consignen seudónimos, cuando lo soliciten los

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

órganos judiciales y otras autoridades públicas para el ejercicio de las funciones.

dd) proporcionar a cualquier parte usuaria información sobre el estado de validez o revocación de los certificados cualificados expedidos por ellos. Esta información debe estar disponible al menos por cada certificado en cualquier momento y con posterioridad al período de validez del certificado en una forma automatizada que sea fiable, gratuita y eficiente.

ee) operar de acuerdo a su DPC y PC que implementan;

ff) generar y gestionar sus pares de claves criptográficas;

gg) asegurar la protección de sus claves privadas;

hh) distribuir su propio certificado;

ii) emitir, expedir y distribuir los certificados de los usuarios finales;

jj) informar la emisión del certificado al respectivo solicitante;

kk) revocar o suspender los certificados por él emitidos, de acuerdo con lo establecido en la PC correspondiente y en la DPC;

ll) emitir, gestionar y publicar sus LCRs y disponibilizar la consulta online del estado de los certificados emitidos (OCSP-On-line Certificate Status Protocol);

mm) utilizar un protocolo de comunicación seguro cuando se preste servicios a través de la web a los solicitantes o usuarios de certificados electrónicos;

nn) identificar y registrar todas las acciones ejecutadas, conformes a las normas, prácticas y reglas establecidas por AC Raíz-Py;

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY				
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES				
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2		

oo) adoptar las medidas de seguridad y de control previstas en la DPC, PC y PS que se implementan, con sujeción a las normas, criterios, prácticas y procedimientos establecidos por la AC Raíz-Py.

pp) mantener el cumplimiento de sus procesos, procedimientos y actividades con las normas, prácticas y reglas establecidos por AC Raíz-Py, y la normativa vigente;

qq) mantener y garantizar la integridad, confidencialidad y seguridad de la información por él tratado;

rr) mantener y anualmente realizar prueba de su PCN;

ss) informar a la AC Raíz-Py, mensualmente, la cantidad de certificados electrónicos emitidos y revocados;

tt) no emitir el certificado con una fecha de caducidad que se extienda más allá de la fecha de vencimiento de su propio certificado.

uu) someterse a una auditoría al menos una vez cada veinte y cuatro meses, corriendo con los gastos que ello genere, por un OEC debidamente acreditado, y remitir el informe de evaluación de la conformidad correspondiente al organismo de supervisión en el plazo de tres días hábiles tras su recepción;

vv) someterse a auditoría o evaluación de conformidad, corriendo con los gastos que ello genere, en cualquier momento, solicitada por el organismo de supervisión;

ww) asegurarse de que todas las aprobaciones de solicitudes de certificados sean realizadas por un AGR y en una estación de trabajo declarada; y

xx) cumplir con las demás disposiciones reglamentadas por la AC Raíz-Py para asegurar que el PCSC de la PNDPI se ajusta a la normativa vigente.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

4.1.2.2. RESPONSABILIDADES Y OBLIGACIONES DE LA ARDEL PCSC DE LA PNDI

Responsabilidades

La AR vinculada al PCSC de la PNDI será responsable por los daños y perjuicios que ocasione.

Obligaciones

En este apartado de la DPC, están incluidas las obligaciones de las ARs vinculadas al PCSC de la PNDI responsable de la DPC, las mismas son:

- a) recibir las solicitudes de emisión, suspensión revocación de certificados;
- b) confirmar la identidad del solicitante y validar la solicitud;
- c) remitir la solicitud de emisión o revocación del certificado al PCSC de la PNDI por medio de acceso remoto al ambiente de la AR alojado en sus instalaciones, utilizando un protocolo de comunicación seguro, conforme al patrón definido en el documento DOC-ICPP-05 [4];
- d) informar a los respectivos titulares la emisión o revocación de sus certificados;
- e) mantener el cumplimiento de sus procesos, procedimientos y actividades con las normas, criterios, prácticas y reglas establecidas por el PCSC vinculado, la AC Raíz-Py y en especial con lo contenido en el documento DOC-ICPP-05 [4];
- f) mantener y anualmente realizar prueba de su PCN;
- g) proceder a la comprobación de las firmas y de la validez de los

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

documentos presentados en la forma del ítem 3.2.3.; y

h) divulgar sus prácticas, relacionadas con la cadena del PCSC de la PNDI, de acuerdo a los principios y criterios establecidos por la AC Raiz-Py para las ARs.

4.2 PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

La AR vinculada al PCSC de la PNDI realiza las funciones de identificación y autenticación conforme al ítem 3 de esta DPC.

4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

El PCSC de la PNDI y sus AR vinculadas, con la debida justificación formal, aceptarano rechazarán las solicitudes de certificados de los solicitantes de acuerdo con los procedimientos descritos en esta DPC y la normativa vigente.

4.2.3 TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO

El PCSC de la PNDI cumple con los procedimientos determinados por la AC Raíz-Py. No habrá tiempo máximo para procesar solicitudes en el marco de la ICPP.

4.3 EMISIÓN DEL CERTIFICADO

4.3.1 ACCIONES DEL PCSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS

Una vez ejecutadas las labores de identificación y autenticación de los solicitantes de parte de una AR vinculada al PCSC de la PNDI y verificada que

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

el solicitante cumpla con los requisitos establecidos en esta DPC, en su correspondiente PC, con las normas técnicas y la legislación vigente que rige la materia, el PCSC de la PNDI procederá a la emisión del correspondiente certificado. La emisión del certificado implica la autorización definitiva de la solicitud por parte del PCSC de la PNDI.

Una vez emitido el certificado, el PCSC de la PNDI activa los mecanismos informáticos necesarios para que el certificado quede inscrito en el repositorio correspondiente. El PCSC de la PNDI firma con su clave privada las claves públicas de los certificados que emite.

Todos los certificados iniciarán su vigencia en el momento de su emisión. El periodo de vigencia estará sujeto a una posible extinción anticipada, cuando se den las causas que motivan la revocación del certificado según consta en el apartado 4.9.

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

El certificado electrónico cualificado y las claves se encuentran en posesión del titular desde su generación y emisión, por lo que no se requiere de notificación alguna.

4.4 ACEPTACIÓN DEL CERTIFICADO

4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

La aceptación de todo certificado emitido por el PCSC de la PNDI será declarada por el respectivo titular en el Contrato de prestación de servicios de confianza PCSC de la PNDI mediante la firma de éste.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

El titular asume la totalidad de las obligaciones y responsabilidades, así como el reconocimiento de que está de acuerdo con los términos y condiciones contenidos en el Contrato de prestación de servicios de confianza PCSC de la PNDI, que rige los derechos y obligaciones entre el PCSC de la PNDI y el titular, y de que éste conoce la existencia de la presente DPC y la PC vinculada al certificado emitido, que recogen técnica y operativamente los servicios de certificación electrónica prestados en el marco de la ICPP.

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PCSC

El PCSC de la PNDI publicará información de los certificados que emite a través de un mecanismo de consulta que estará disponible en su sitio principal de internet.

Además, el PCSC de la PNDI publica en su repositorio público su certificado digital y el de la AC Raíz.

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

No se definen entidades externas que necesiten o requieran ser notificados acerca de los certificados emitidos por el PCSC de la PNDI.

4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

El titular de un certificado debe usar el par de claves y el certificado correspondiente de acuerdo a esta DPC y la correspondiente PC que implementa el PCSC de la PNDI.

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

El PCSC de la PNDI utiliza su clave privada y garantiza su protección según lo

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

previsto en esta DPC.

Obligaciones del Titular del Certificado

Este ítem se describen las obligaciones de los titulares decertificados emitidos porel PCSC de la PNDI, contenidas del contrato de prestación de servicio de confianzareferidos en el ítem 4.1, y que se enumeran a continuación:

- a) proporcionar al PCSC de la PNDI información veraz, completa y exacta para la prestación del servicio de confianza, en particular, sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción de su vigencia;
- b) comunicar sin demora al PCSC de la PNDI de cualquier modificación de las circunstancias que incidan en la prestación del servicio de confianza, en particular, aquellas reflejadas en el certificado electrónico;
- c) conservar adecuadamente sus datos de creación de firma, asegurar su confidencialidad y proteger de todo acceso o revelación de éstos o, en su caso, de los medios que den acceso a ellos;
- d) solicitar la revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación defirma o, en su caso, de los medios que den acceso a ellos.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

e) no utilizar los datos de creación de firma cuando haya expirado el período de validez del certificado electrónico o el PCSC de la PNDI le notifique la extinción o suspensión de su vigencia.

f) utilizar sus certificados y claves privadas de forma adecuada, según lo previsto en la PC del PCSC de la PNDI correspondiente;

g) conocer sus derechos y obligaciones, contemplados en la DPC y la PC correspondiente la certificado emitido por el de la PNDI y demás documentos aplicables de la ICPP; y

h) informar al PCSC de la PNDI de cualquier compromiso de su clave privada y solicitar la revocación inmediata del certificado correspondiente.

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

Conforme a lo estipulado en el ítem 9.6.4 de esta DPC.

4.6 RENOVACIÓN DEL CERTIFICADO

Conforme a lo estipulado en el ítem 3.3 de esta DPC..

4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADOS

Conforme a lo estipulado en el ítem 3.3 de esta DPC.

4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN

Conforme a lo estipulado en el ítem 4.1.1 de esta DPC.

4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO

Conforme a lo estipulado en el ítem 4.2 de esta DPC.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

4.6.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO

Conforme a lo estipulado en el ítem 4.2 de esta DPC.

4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO

Conforme a lo estipulado en el ítem 4.4.1 de esta DPC

4.6.6 PUBLICACIÓN POR EL PCSC DEL CERTIFICADO RENOVADO

Conforme a lo estipulado en el ítem 4.4.2 de esta DPC.

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

Conforme a lo estipulado en el ítem 4.4.3 de esta DPC

4.7 RE-EMISIÓN DE CLAVES DE CERTIFICADO

La reemisión del certificado no está permitida por esta DPC, cuando un certificado requiera ser reemitido debe solicitarse un nuevo certificado, de acuerdo con la sección 4.1 de esta DPC.

4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO

No aplica.

4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA

No aplica.

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

No aplica.

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

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

No aplica.

4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE-EMITIDO

No aplica.

4.7.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS RE-EMITIDOS

No aplica.

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

No aplica.

4.8 MODIFICACIÓN DE CERTIFICADOS

No aplica.

4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO

No aplica.

4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

No aplica.

4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

No aplica.

4.8.4 NOTIFICACIÓN AL SUSCRIPTOR DE LA EMISIÓN DE UN NUEVO CERTIFICADO

No aplica.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

No aplica.

4.8.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS MODIFICADOS

No aplica.

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

No aplica.

4.9 REVOCACIÓN Y SUSPENSIÓN

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

Un certificado emitido por el PCSC de la PNDI deberá obligatoriamente ser revocado en las siguientes circunstancias:

- a) solicitud formulada por la persona física titular del certificado.
- b) violación o puesta en peligro del secreto de los datos de creación de firma del titular del certificado, o del PCSC, o utilización indebida de dichos datos por un tercero.
- c) resolución judicial o administrativa competente que lo ordene.
- d) fallecimiento del firmante; incapacidad sobrevenida, total o parcial, del firmante y extinción de la personalidad jurídica o disolución del creador del sello,
- e) cese en la actividad del PCSC del PNDI salvo que la gestión de los certificados electrónicos expedidos por aquél sea transferida a

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

otro prestador de servicios de confianza.

f) descubrimiento de la falsedad o inexactitud de los datos aportados para la expedición del certificado y que consten en él, o alteración posterior de las circunstancias verificadas para la expedición del certificado.

El PCSC de la PNDI podrá establecer cualquier otra causa lícita de revocación.

En su caso, y de manera previa o simultánea a la indicación de revocación de un certificado electrónico cualificado en el servicio de consulta sobre el estado de validez o revocación de los certificados por él expedidos, el PCSC de la PNDI informará al firmante acerca de esta circunstancia, especificando los motivos, la fecha y la hora en que el certificado quedará sin efecto.

El PCSC de la PNDI revocará, dentro del plazo definido en el ítem 4.9.3, el certificado del titular del certificado que incumpla con las políticas, estándares y reglas establecidas en el marco de la ICPP.

La AC Raíz-Py también podrá determinar la revocación del certificado del PCSC que incumpla con la legislación vigente o las políticas, estándares, prácticas y reglas establecidas en el marco de la ICPP.

4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN

La revocación de certificados sólo podrá realizarse:

- a) por solicitud formulada por la persona física titular del certificado;
- b) resolución judicial o administrativa competente que lo ordene;
- c) por el PCSC de la PNDI; y

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

d) por una AR vinculada al PCSC de la PNDI;

4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

Quienes están autorizados a solicitar la revocación, conforme al punto 4.9.2, pueden, fácilmente y en cualquier tiempo, solicitar la revocación de sus respectivos certificados.

Como directrices generales se establece que:

- El solicitante de revocación de un certificado será identificado;
- Las solicitudes de revocación, así como las acciones resultantes de ellas serán registradas y almacenadas;
- Se documentarán las razones de la revocación de un certificado;
- La revocación de un certificado terminará con la generación y publicación de una LCR que contenga los datos del certificado revocado y, en el caso de la utilización de consulta OCSP, con la actualización del estado del certificado en la base de datos del PCSC de la PNDI.

El PCSC de la PNDI al revocar un certificado electrónico cualificado, registran su revocación en su base de datos de certificados y publican el estado del certificado oportunamente y, en todo caso, en un plazo de veinticuatro (24) horas después de la recepción de la solicitud. La revocación será efectiva inmediatamente después de su publicación.

El PCSC de la PNDI responde plenamente por todos los daños causados por el uso de un certificado en el período comprendido entre la solicitud de su

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

revocación y la emisión de la LCR correspondiente.

En caso de que sean requeridos procedimientos de revocación específicos para las PC implementadas por el PCSC de la PNDI, los mismos serán descritos en esas PC, en el ítem correspondiente.

4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

La solicitud de revocación deberá ser inmediata cuando se configuren las circunstancias definidas en el ítem 4.9.1 y el plazo para la aceptación del certificado por parte del titular será de 10 días, dentro del cual la renovación de dicho certificado podrá ser solicitada sin que se aplique alguna tarifa por el PCSC de la PNDI.

Si se requieren plazos específicos para las PC implementadas por el PCSC de la PNDI, estos deberán estar descritos en dichas PC, en el ítem correspondiente.

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

En el caso de una solicitud formalmente constituida, de acuerdo con las reglas de la ICPP, el PCSC de la PNDI procederá a la revocación del certificado, inmediatamente después de analizar la solicitud

4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LA PARTE USUARIA

Las partes que confían deben evaluar el estado del certificado y el estado de todos los certificados de la AC en la cadena a la que pertenece el certificado, antes de confiar en él.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

Para ello, las partes que confían pueden verificar el estado del certificado mediante el servicio de: OCSP o LCR más reciente, provista por el PCSC de la PNDI.

Antes de confiar en un certificado, las partes usuarias deben confirmar la validez de cada certificado en la cadena de certificación de acuerdo con los estándares IETF PKIX, incluida la verificación de la validez del certificado, encadenando el nombre del emisor y el titular del certificado, restricciones de uso de claves y políticas de certificación y estado de revocación por medio de la LCR o respuestas OCSP identificadas en cada certificado en la cadena de certificación.

4.9.7 FRECUENCIA DE EMISIÓN DE LA LCR

La LCR debe actualizarse y publicarse inmediatamente cuando surja una revocación o suspensión o con una frecuencia máxima para certificados de los usuarios finales de doce (12) horas.

La LCR mantiene publicado obligatoriamente el certificado revocado hasta que expire.

En caso que sean utilizadas frecuencias de emisión específicas de LCR para las PCs implementadas por el PCDC de la PNDI, serán descriptos en esas PCs, en el ítem correspondiente.

4.9.8 LATENCIA MÁXIMA PARA LCR

El tiempo máximo entre la generación de una LCR y su correspondiente publicación en el repositorio es de 1 hora.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

4.9.9 DISPONIBILIDAD PARA REVOCACIÓN / VERIFICACIÓN DE ESTADO EN LÍNEA

Los recursos disponibles para la revocación/verificación en línea son:

Verificación:

a) Consultando la LCR o Delta-LCR más reciente emitida por el PCSC de PNDI. que está disponible en su repositorio público.

b) Mediante la consulta de certificados en línea, disponible en la siguiente URL:

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

Revocación:

a) Todas las revocaciones de los certificados del PCSC de la PNDI se realizan de forma presencial.

Todo certificado debe tener su validez verificada, en la respectiva LCR o consultado certificados en línea, antes de ser utilizado.

Además, debe confirmarse la autenticidad de la LCR mediante la verificación de la firma del PCSC de la PNDI y del período de validez de la LCR.

4.9.10 REQUISITOS DE VERIFICACIÓN DE LA LCR

EL PCSC de la PNDI mantendrá disponible un repositorio con información del estado de los certificados emitidos y la LCR, el cual puede ser accedido vía web.

Adicionalmente, el PCSC de la PNDI implementa el servicio de validación en línea OCSP.

Todo certificado deberá tener su validez verificada, en la respectiva LCR, antes

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

de utilizarlo.

La autenticidad de la LCR deberá también ser confirmada, por medio de la verificación de la firma del PCSC de la PNDI emisor en el periodo de validez de la LCR.

4.9.11 OTRAS FORMAS DE ADVERTENCIA DE REVOCACIÓN DISPONIBLES

El PCSC de la PNDI dispone de un Sistema de Consulta de Certificados emitidos en su repositorio público.

El PCSC de la PNDI notificará en un plazo de 24 (veinticuatro) horas como máximo a la DGCE respecto a circunstancias que produzcan el compromiso de sus claves o su imposibilidad de uso. En caso de que la clave privada del PCSC de la PNDI se vea comprometida, se revocarán de inmediato los certificados emitidos de acuerdo a la legislación vigente, comunicando dicha acción a todos los suscriptores y terceros que confían.

4.9.12 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE LA CLAVE PRIVADA

En caso de compromiso de claves del PCSC de la PNDI, será notificado, en la medida posible a todos los participantes de la ICPP, en especial a:

- a) Todos los titulares de certificados emitidos;
- c) La DGCE; y
- b) Terceros que confían, los que se tenga conocimiento.

En caso de compromiso de claves del Titular de Certificado emitido por el

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

PCSC de la PNDI, el titular deberá notificar al PCSC de la PNDI, de forma inmediata.

Los métodos para comunicación de compromiso o sospecha de compromiso de claves son:

- a) Mediante el correo electrónico consignado en la solicitud de certificado;
- b) Mediante un teléfono consignado en la solicitud de certificado: o
- c) Mediante presencia física del titular a una AR vinculada al PCSC de la PNDI.

4.9.13 CIRCUNSTANCIAS PARA SUSPENSIÓN

No aplica.

4.9.14 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

No aplica.

4.9.15 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

No aplica.

4.9.16 LÍMITES DEL PERÍODO DE SUSPENSIÓN

No aplica.

4.10 SERVICIOS DE ESTADO DEL CERTIFICADO

4.10.1 CARACTERÍSTICAS OPERACIONALES

El PCSC de la PNDI proporciona un servicio de estado de certificado en forma de un punto de distribución de LCR en los certificados y OCSP, conforme al ítem

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

4.9.9

4.10.2 DISPONIBILIDAD DEL SERVICIO

Los sistemas de distribución de LCRs y de consulta en línea del estado de los certificados están disponibles de forma ininterrumpida durante las veinticuatro horas, los siete días de la semana (24/7), tanto para la parte usuaria como para los firmantes u otras partes que lo requieran. En caso de interrupción por causa de fuerza mayor, el servicio será restablecido en un plazo no mayor a veinticuatro (24) horas, garantizando la disponibilidad del servicio con un mínimo de 99,5% anual, un tiempo programado de inactividad máximo de 0.5% anual.

4.10.3 CARACTERÍSTICAS OPCIONALES

El servicio OCSP, que permite consultar el estado de los certificados es una característica opcional para la AC Raíz-Py, sin embargo, para el PCSC de la PNDI constituye una característica obligatoria.

Para hacer uso del servicio de validación en línea es responsabilidad de las partes usuarias disponer de un cliente OCSP que cumpla el RFC 6960.

4.11 FIN DE ACTIVIDADES

Los requisitos y procedimientos en caso de extinción o cese de los servicios del PCSC de la PNDI se encuentran definidos en el ítem 5.8 de esta DPC.

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

El PCSC de la PNDI **NO almacena ni copia**, por sí o a través de un tercero, los datos de creación de firma de la persona física a la que ha

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

prestado su servicio..

4.12.2POLÍTICAS Y PRÁCTICAS DE RECUPERACIÓN Y ENCAPSULACIÓN DE CLAVES

No aplica.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

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

En los ítems siguientes, son descritos los controles de seguridad implementados por el PCSC de la PNDI y por sus ARs a ella vinculadas, para ejecutar de modo seguro sus funciones de generación de claves, identificación, certificación, auditoría y archivo de los registros.

5.1 CONTROLES FÍSICOS

En las secciones siguientes, se describen los controles físicos referentes a las instalaciones que albergan los sistemas del PCSC de la PNDI y de las ARs vinculadas.

5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

La localización del edificio donde se residen los sistemas de certificación no se encuentra públicamente identificada. No son admitidos ambientes compartidos que permitan la visibilidad de las operaciones de emisión y revocación de certificados. Las operaciones mencionadas son segregadas en compartimientos cerrados y físicamente protegidos.

Los sistemas están físicamente separados de otros existentes en el lugar, de forma que solo el personal autorizado del PCSC de la PNDI pueda acceder a ellos, garantizando así la independencia de estos equipos y sistemas de terceros alojados en el lugar.

Las instalaciones del PCSC de la PNDI cuentan al menos con las siguientes medidas de protección:

- Muros Perimetrales reforzados.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

- Sistemas de UPS Redundantes.
- Generación de Energía Redundante.
- Doble Acometida Eléctrica.
- Sistemas de enfriamiento de precisión redundante.
- Sistemas de detección, extinción y supresión automática de fuego.
- Sistema de Monitoreo de la Infraestructura.
- Sistemas de puesta a tierra y protección contra rayos.
- Sistemas de Aire Acondicionado HVAC.
- Suministro de energía eléctrica regulada y con protección.
- Sistemas de CCTV con grabación de movimiento.
- Sistemas de iluminación de emergencia.
- Ambiente alejado de sótanos para prevenir posibles inundaciones.

Las instalaciones donde se emiten los certificados del PCSC de la PNDI se protegen con su propio y único perímetro físico.

5.1.2 ACCESO FÍSICO

El PCSC de la PNDI implementa un sistema de control de acceso físico que garantiza la seguridad de sus instalaciones, conforme al punto "control de accesos" de la norma ISO 27002:2022 y los siguientes puntos:

5.1.2.1 NIVELES DE ACCESO FÍSICO

Los centros de datos donde se aloja la infraestructura tecnológica de PCSC de la PNDI cuentan con seis niveles de seguridad física:

- **PRIMER NIVEL:** Primera barrera de acceso a las instalaciones del PCSC de la PNDI. Para acceder en el área del nivel 1, cada persona debe ser identificada y registrada por el personal de seguridad, a

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

partir de ese nivel personas extrañas a la operativa del PCSC de la PNDI deberán transitar debidamente identificadas y acompañadas. Ningún tipo de proceso operacional o administrativo del PCSC de la PNDI es ejecutado en ese nivel. Excepto en los casos previstos por la ley, la posesión de armas no será admitida en las instalaciones del PCSC de la PNDI, desde el nivel 1. A partir de ese nivel, equipos de grabación, fotografía, vídeo, sonido o similares, así como los ordenadores portátiles, será controlado su ingreso y sólo pueden ser utilizados mediante la autorización formal y supervisada. Además, no se permitirá el ingreso con kepis, gorros, cascos, lentes o gafas, u otros accesorios que permitan la correcta visualización del rostro de la persona. El mismo tiene un factor de autenticación biométrica.

SEGUNDO NIVEL: Área interna al perímetro anterior, de acceso más estricto y restringido que el primero. Requiere una identificación individual de las personas que en él accedan. Ese es el nivel mínimo de seguridad requerido para la ejecución de cualquier proceso operacional o administrativo del PCSC de la PNDI. El paso del primer al segundo perímetro exige por lo menos un factor de autenticación electrónica (cuenta con autenticación biométrica y pines de acceso) y tarjeta de identificación visible.

- **TERCER NIVEL:** Área interna al perímetro anterior, de acceso más estricto y restringido que el segundo. Es el primer nivel en albergar material y actividades sensibles de la operativa del PCSC de la PNDI. Cualquier actividad relativa al ciclo de vida de los certificados electrónicos estará localizada a partir de este nivel. Personas que

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

no están involucradas con esas actividades no tienen permiso para acceder a este nivel. Las personas que no cuenten con permiso de acceso no pueden permanecer en ese nivel salvo que estuviesen acompañadas por alguien que tenga permiso de acceso. En este nivel son controladas tanto las entradas como las salidas de cada persona autorizada. Los mecanismos de control requeridos para acceder a ese nivel son dos: algún tipo de identificación individual, como una tarjeta electrónica, y la identificación biométrica. Teléfonos móviles y otros equipos de comunicación portátil, con excepción de los necesarios para el funcionamiento del PCSC de la PNDI, no son aceptadas desde el nivel 3.

CUARTO NIVEL: acceso al área de operaciones críticas del PCSC de la PNDI. Área interna al nivel anterior, de acceso más estricto y restringido que el tercero. En el cuarto nivel se desplegarán actividades especialmente sensibles a la operación del PCSC de la PNDI, tales como la emisión y revocación de los certificados y la emisión de la CRL. Todos los sistemas y equipamientos necesarios a estas actividades están localizados a partir de este nivel. El nivel 4 posee 2 (dos) factores de autenticación como mínimo (uno de ellos biométrico) y tarjeta de identificación visible y, adicionalmente, se exige, en cada acceso a su ambiente, la identificación de, como mínimo, 2 (dos) personas autorizadas. En este nivel, la permanencia de esas personas es exigida mientras el ambiente estuviera ocupado. En el cuarto nivel, todas las barreras físicas (paredes y barrotes) deben ser sólidas, extendiéndose desde el piso real al techo real. Las paredes, piso y techo fueron

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

realizadas de modo a prevenir las amenazas de acceso no autorizado, agua, vapor, gas y fuego. Las tuberías de refrigeración, de energía o de comunicación no permiten la penetración física en las áreas de cuarto nivel. Adicionalmente, se tiene una protección contra las interferencias electromagnéticas externas. Este ambiente fue construido según las normas internacionales aplicables.

- **QUINTO NIVEL:** Interno al ambiente del nivel 4. Consiste en una Jaula dematerial resistente y con cerradura antirrobo, donde están almacenados: materiales criptográficos, tales como, claves, datos de activación, sus copias y equipamientos criptográficos.
- **SEXTO NIVEL:** Interno al ambiente del nivel 5. Gabinete reforzado ubicado en el interior de una jaula con cerradura antirrobo y acceso biométrico. Los datos de activación de la clave privada del PCSC de la PNDI son almacenados en ese ambiente.

5.1.2.2 SISTEMAS FÍSICOS DE DETECCIÓN:

La transición entre los diferentes perímetros de acceso, así como la sala de operaciones del nivel 4, son monitoreadas por cámaras de video ligadas a un sistema de grabación 24x7. El posicionamiento y la capacidad de esas cámaras no permiten recuperar las contraseñas digitadas en los controles de acceso.

Los vídeos resultantes de grabación 24x7 serán almacenados, como mínimo, 4 (cuatro) años. Las grabaciones serán testeadas aleatoriamente por lo menos cada 3 (tres) meses. Esos medios son almacenados en el ambiente del nivel 4.

Todas las puertas de transición entre los ambientes de niveles 3 y 4 son monitoreadas por un sistema de notificación de alarmas.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

En todos los ambientes del cuarto nivel, se cuenta con una alarma de detección demovimientos.

Los sistemas de notificación de alarmas utilizan por los menos 2 (dos) medios de notificación: sonoro y visual.

El sistema de monitoreo de las cámaras de video, así como el sistema de notificación de alarmas, están permanentemente monitoreados por el personal autorizado en el ambiente de nivel 3. Las instalaciones del sistema de monitoreo, a su vez, están monitoreados por cámaras de video cuyo posicionamiento permite el seguimiento de las acciones del personal autorizado.

5.1.2.3 SISTEMA DE CONTROL DE ACCESO:

El almacenamiento del sistema de control de acceso está en el ambiente de nivel 4.

5.1.2.4 MECANISMOS DE EMERGENCIA:

Mecanismos específicos son implementados por el PCSC de la PNDI para garantizarla seguridad de su personal y de sus equipamientos en situaciones de emergencia.

Estos mecanismos permiten el desbloqueo de las puertas por medio de accionamiento mecánico, para la salida de emergencia de todos los ambientes con control de acceso. La salida efectuada por medio de estos mecanismos acciona inmediatamente las alarmas de apertura de puertas.

El PCSC de la PNDI puede especificar e implementar otros mecanismos de emergencia específicos, necesarios para cada tipo de instalación. Todos los

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

procedimientos referentes a esos mecanismos de emergencia son documentados. Los mecanismos y procedimientos de emergencia son verificados semestralmente, por medio de simulación de situaciones de emergencia.

5.1.3 ENERGÍA Y AIRE ACONDICIONADO

Las áreas donde se ubican los equipos de la infraestructura tecnológica del PCSC de la PNDI cuentan con suministros de electricidad y aire acondicionados adecuados a los requisitos de los equipos en ellas instalados. La infraestructura se encuentra protegida contra caídas de tensión o cualquier otra anomalía en el suministro eléctrico.

EL PCSC de la PNDI dispone de:

- Sistemas de alimentación ininterrumpida (UPS, por sus siglas en inglés Uninterruptible Power Supply)
- Grupo electrógeno con potencia suficiente para soportar la carga del Centro de Datos, incluido los equipos informáticos y equipos de refrigeración.
- Sistema de puesta a tierra implantado.
- Cables eléctricos protegidos por tuberías y conductos apropiados.
- Conductos separados para los cables de energía, de telefonía y de datos.
- Tuberías, conductos, canaletas, paneles y cajas (de paso, distribución y terminación) diseñadas y construidas de forma a facilitar la inspección y detección de intentos de manipulación.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

Todos los cables son catalogados, identificados e inspeccionados periódicamente, al menos cada (6) meses, en busca de evidencias de violación y anomalías.

Son mantenidos y actualizados los registros sobre la topología de red de cables, de acuerdo a los requisitos de confidencialidad establecidos en el ítem “seguridad en las telecomunicaciones” de la norma ISO 27002/2023. Cualquier modificación en esared es previamente documentada.

No son admitidas instalaciones provisionales, cableados expuestos o directamente conectados a tomas sin utilización de conectores adecuados.

El sistema de climatización cumple con los requisitos de temperatura y humedad exigidos por los equipamientos utilizados en el ambiente y deben disponer de filtros de polvos. En los ambientes del nivel 4, el sistema de climatización es independiente y tolerante a fallas.

La temperatura de los ambientes atendidos por los sistemas de climatización es permanentemente monitoreada por el sistema de notificación de alarmas.

Los sistemas de aire acondicionado de los ambientes de nivel 4 son internos, con cambio de aire realizados apenas por la abertura de la puerta.

La capacidad de redundancia de toda la estructura de energía acondicionada está garantizada, por medio de:

- Generadores de una capacidad de carga compatible;
- Generadores de reserva;
- Sistemas de UPS redundantes; y
- Sistemas redundantes de aire acondicionado.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

5.1.4 EXPOSICIONES AL AGUA

La estructura interna al ambiente del nivel 4, provee protección física contra exposición al agua, filtraciones e inundaciones proveniente de cualquier fuente externa.

Además, la infraestructura del PCSC de la PNDI cuenta con:

- Sistemas de control de humedad y temperatura, monitorizado en tiempo real.
- Sistema de drenaje y piso elevado.

5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

El área donde se encuentra la infraestructura tecnológica del PCSC de la PNDI dispone de sistemas inteligentes de detección y extinción de incendios para la protección de su contenido. Los mismos posibilitan activar las alarmas preventivas antes que el humo sea visible, activados solamente con la presencia de partículas que caracterizan el sobrecalentamiento de materiales eléctricos y otros materiales combustibles presentes en las instalaciones

El cableado se sitúa en un suelo falso o techo falso y dispone de los medios adecuados (detectores en suelo y techo) para la protección del mismo contra incendios.

En las instalaciones del PCSC de la PNDI no está permitido fumar o portar objetos que produzcan fuego o chispa.

El nivel 4 posee un sistema para la detección precoz de humo y un sistema de extinción de incendios por gas.

En caso de incendio de las instalaciones del PCSC de la PNDI, o el aumento

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

de la temperatura interna del ambiente del nivel 4, no deberá exceder 50 grados Celsius, y el ambiente soportará esta condición, al menos, 1 (una) hora.

5.1.6 ALMACENAMIENTO DE MEDIOS

El PCSC de la PNDI asegura el adecuado manejo y protección de los medios de almacenamiento de información, que contengan datos críticos o sensibles del sistema, contra daños accidentales (agua, fuego, electromagnetismo) de tal forma que la información se dispone en medios de forma segura, según la clasificación de la información en ellas contenidas. Además cuenta con mecanismos que permiten impedir, detectar y prevenir su uso no autorizado, acceso o su divulgación.

La información relacionada a la infraestructura del PCSC de la PNDI se almacena de forma segura en armarios ignífugos y cofres de seguridad, según la clasificación de la información en ellos contenida. Los cofres de seguridad son de acero o material de resistencia equivalente, y ofrecen resistencia:

- Al fuego por al menos 60 minutos.
- Aberturas forzadas.
- Asimismo, posee tranca con llave manual o electrónica. Además, es suficientemente pesado, de forma a dificultar su retiro.

5.1.7 ELIMINACIÓN DE RESIDUOS

Todos los documentos en papel que contengan información clasificada como sensible serán triturados antes de ir como residuos.

Todos los dispositivos electrónicos que ya no son utilizables y que se han utilizado previamente para el almacenamiento de información sensible, serán destruidos físicamente.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

5.1.8 RESPALDO FUERA DE SITIO

El PCSC de la PNDI cuenta con una instalación de respaldo con niveles de protección física y ambiental similar al sitio principal y con separación física adecuada.

En caso de siniestro que torne inoperante la instalación principal del PCSC de la PNDI, la instalación de respaldo tomará totalmente las operaciones en condiciones idénticas en un máximo de 48 (cuarenta y ocho) horas.

5.2 CONTROLES PROCEDIMENTALES

En los siguientes ítems de la DPC se describen los requisitos para la caracterización y el reconocimiento de los Roles de Confianza en el PCSC de la PNDI y las ARs vinculadas a ella, junto con las responsabilidades definidas para cada perfil. Para cada tarea asociada a los perfiles definidos, también se establecerán el número de personas necesarias para su ejecución

5.2.1 ROLES DE CONFIANZA

El PCSC de la PNDI garantizará la segregación de tareas para las funciones críticas, con el fin de evitar que un empleado o funcionario que asume un rol de confianza utilice incorrectamente su sistema de certificación sin ser detectado. Las acciones de cada uno de los empleados o funcionarios se limitarán de acuerdo a su perfil.

Los roles de confianza asignados al empleado del PCSC de la PNDI contemplan las siguientes responsabilidades que a continuación serán descritos:

- **RESPONSABLE/S DE SEGURIDAD:** Deberán llevar a cabo la actualización e implementación de las políticas y procedimientos de seguridad que han sido aprobados por el

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

PCSC, controlar la formalización de los convenios entre el personal y el PCSC, comunicar las medidas disciplinarias acordadas, supervisando su cumplimiento. Asimismo, deberá cumplir y hacer cumplir las políticas de seguridad del PCSC y deberá encargarse de cualquier aspecto relativo a la seguridad de la ICPP, desde la seguridad física hasta la seguridad de las aplicaciones, pasando por la seguridad de la red. Será el encargado de gestionar los sistemas de gestión perimetral y en concreto de verificar la correcta gestión de las reglas de los firewalls. Deberá comprobar la correcta instalación, configuración y gestión de los sistemas de detección de intrusos y de las herramientas asociadas a éstos, asimismo deberá resolver o hacer que resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, etc. y es el encargado de la gestión y control de seguridad física, y de los movimientos de material fuera de las instalaciones del PCSC;

- **RESPONSABLE/S DE COORDINACIÓN DE ÁREA:** Bajo su control y supervisión, se encuentra el personal adscrito a la misma y sus funciones son:
 - Recibir y dar curso a las denuncias que podrían afectar a su personal, proponiendo las medidas disciplinarias correspondientes.
 - Efectuar un control permanente de la adecuación de los recursos materiales y humanos que cuenta el área a su cargo, con el fin de atender las necesidades de

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

servicio que tiene encomendadas.

- Controla la formalización de los convenios entre el personal dela PNDI en su carácter de PCSC.

RESPONSABLE/S DE SISTEMAS: Los responsables de este rol no deberán estar implicados en tareas de auditoría interna. Serán encargados de la instalación y configuración de sistemas operativos, del mantenimiento y actualización de los programas instalados; con capacidad para configurar, mantener los sistemas, pero sin acceso a los datos. Asimismo, deberán establecer y documentar los procedimientos de monitoreo de los sistemas y de los servicios que prestan. Serán responsables de mantener el inventario de servidores y resto de componentes de los sistemas de certificación del PCSC y asumirán la gestión de los servicios de ruteamiento y gestión de reglasde firewall, gestión y mantenimiento de los sistemas de detección de intrusos, etc. Serán encargados de la instalación de hardware criptográfico del PCSC y de la eliminación del hardware criptográfico del PCSC de producción. Serán responsables del mantenimiento o reparación de equipos en general así como de dispositivos criptográficos del PCSC (incluida la instalación de nuevo hardware, firmware o software), Igualment e serán responsables de los desmontajes y la eliminación permanente por el uso;

- **RESPONSABLE/S DE LA OPERACIÓN DIARIA DEL PCSC:** Será encargada de realizar las tareas de ejecución y

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

revisión de las copias de seguridad del sistema. Asimismo, debe velar, para que se lleven a cabo las copias de seguridad local y del traslado de las mismas de acuerdo con lo establecido en la política de seguridad. Serán responsables de mantener la información suficiente como para poder restaurar cualquiera de los sistemas en el menor tiempo posible. Serán encargados de la gestión y mantenimiento de los sistemas de energía, aire acondicionado y prevención de incendios;

RESPONSABLE DE AUDITORÍA: Serán los responsables de las tareas de ejecución y revisión de auditoría de los sistemas que conforman la infraestructura tecnológica del PCSC. Esta auditoría deberá realizarse de acuerdo con las normas y criterios de auditoría establecidos en la presente DPC. Además, deberá tener acceso a todos los registros del sistema mencionados;

- **RESPONSABLE DE DESARROLLO DE SISTEMAS DEL PCSC:** Serán los encargados del diseño de las arquitecturas de programación, de control y supervisión de los desarrollos encomendados y de la correcta documentación de las aplicaciones; y
- **RESPONSABLE DE RECURSOS HUMANOS:** Es el responsable de analizar antecedentes laborales, facilitar condiciones para la evaluación de la idoneidad técnica, implementar controles de seguridad personal, entregar los materiales correspondientes al rol a desempeñar,

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

confeccionar legajos de antecedentes laborales, calificaciones personales, etc.

- **RESPONSABLE LEGAL:** Es el responsable de mantener actualizados los requisitos legales exigidos por el ente regulador (MIC), elaborar y administrar los contratos, participar en la capacitación del personal en materia legal, asistir a los conflictos legales derivados de la operatoria del PCSC.
- **RESPONSABLES DEL CICLO DE VIDA DE CLAVES CRIPTOGRÁFICAS:** Son los responsables de la gestión del ciclo de vida de las claves criptográficas (ejemplo: oficial criptográfico, oficial de activación, etc.);
 - **Administrador de implementación:** es el encargado de gestionar el HSM incluyendo:
 - Inicialización del HSM. Resguarda la contraseña; Administrador de acceso al equipo;
 - Define o modifica políticas de seguridad globales al HSM;
 - Puede crear particiones en el HSM;
 - Tiene acceso a la configuración de HA; y
 - Tiene privilegios para instalar el módulo PED.
 - **Oficial de Seguridad:** Es responsable de:
 - EL Oficial de Seguridad custodia la inicialización o cambio de PIN de Seguridad en las llaves (Token) de

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

autorización de acceso; y

- Cada inicialización de llave o cambio de PIN requiere la aprobación del oficial de seguridad.
- **Oficial de Criptografía:** Es el propietario de las particiones del HSM. Cualquier modificación a realizarse dentro de las llaves custodiadas en la partición requiere el PIN de seguridad del Oficial de Criptografía. Custodia el acceso (challenge de acceso) a las particiones desde las aplicaciones conectadas al HSM. En otras palabras, para establecer conexión desde una aplicación de servidor hacia la partición del HSM se requiere - Challenge de acceso.
- **Oficial de Dominio:** representa la primera capa de seguridad de acceso al HSM. Todas las particiones están creadas bajo el mismo dominio por tanto cualquier acceso al HSM para realizar cambios en las particiones requiere el PIN de seguridad de Dominio.
- **Auditor:** Tiene Privilegios de acceso a archivos de logs de seguridad que permanecen en el equipo HSM. Toda actividad que suponga acceder a registros de funcionalidad del HSM requiere la contraseña de acceso con rol de Auditor
- **Oficial AC:** Se encarga de generar y configurar el

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY				
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES				
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2		

certificado SubCA. El oficial AC accediendo al servidor AC y utilizando la aplicación KMS genera las llaves criptográficas del certificado SubCA y posteriormente la Solicitud de firma de Certificado (CSR). Este CSR es entregado al custodio correspondiente de la entidad MIC. Una vez firmado el certificado SubCA el oficial se encarga de configurar el certificado Root CA y SubCA en el servidor AC de la PKI.

- **Oficial AR:** Se encarga de la administración de la interfaz de Autoridad de Registro y asegurar la publicación de la CRL y la DELTA CRL.
- **Administrador de la AR:** En sus funciones está gestionar la firma del certificado (CSR) de autenticación de la CRL, configurarlo en el servicio OCSP, inicializar los servicios OCSP.

Agentes de registros:

Son los responsables de la realización de las actividades inherentes a una AR, realizan la identificación de los solicitantes en la solicitud de emisión/revocación de un certificado y autorizan en el sistema la emisión o revocación del mismo.

Todos los operadores del sistema de certificación del PCSC deberán recibir entrenamiento específico antes de obtener cualquier tipo de acceso. El tipo o nivel de acceso serán determinados, en un documento formal, con base en las necesidades de cada perfil.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

Cuando un empleado o funcionario se desvincula del PCSC, sus permisos de acceso deberán ser revocados inmediatamente. Cuando hay un cambio en la posición o función que el empleado o funcionario ocupa dentro del PCSC, deberán ser revisados y actualizados en su caso, sus permisos de acceso. Deberá existir una lista de revocación, con todos los recursos, antes disponibilizados, que el empleado o funcionario deberá devolver al PCSC en el momento de su desvinculación.

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Se requiere un mínimo de 2 (dos) empleados con rol de confianza para realizar las tareas ejecutadas en el ambiente donde está localizado el equipamiento de certificación del PCSC de la PNDI. Las demás tareas del PCSC de la PNDI pueden ser ejecutadas por un único empleado.

El PCSC mantiene y ejecuta procedimientos de control rigurosos para asegurar la segregación de funciones.

Esta DPC establece el requisito de control multiusuarios para la generación y la utilización de la clave privada del PCSC de la PNDI en el punto 6.2.2.

5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Todo empleado que asume un rol de confianza en el PCSC de la PNDI es identificado y su perfil es verificado antes de que:

- Sea incluido en la lista de acceso a las instalaciones del PCSC de la PNDI.
- Sea incluido en la lista para acceso físico al sistema de certificación del PCSC de la PNDI.
- Reciba un medio de autenticación electrónica para ejecutar sus

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

actividades operacionales en el PCSC de la PNDI.

- Reciba una cuenta de usuario del sistema de certificación del PCSC de la PNDI.

Los certificados, cuentas y contraseñas utilizados para la identificación y autenticación de los empleados:

- Son directamente asignados a un único empleado.
- No son compartidos.
- Se restringe a las acciones asociadas con el perfil para el que fueron creados.

5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES.

Entre los roles se establecen las siguientes incompatibilidades, de forma que un usuario no pueda tener dos roles marcados como “incompatibles”:

- Los responsables del ciclo de vida de claves criptográficas no podrán cumplir funciones de los responsables de auditoría interna.
- Los responsables de sistemas no podrán cumplir funciones de los Responsables de seguridad ni de los responsables de auditoría interna.
- Los responsables de seguridad no podrán cumplir funciones de los responsables de sistemas, de los responsables del ciclo de vida de claves criptográficas ni de los responsables de auditoría interna.
- Los responsables de auditoría interna no podrán cumplir otra función.

Los roles que requieren separación de los deberes incluyen (pero no está limitado) a los responsables de ejecutar las siguientes responsabilidades:

- a) la puesta en operación del PCSC en producción;

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

b) la emisión o destrucción de los certificados del PCSC; y

c) la validación de información en los sistemas de certificación del PCSC y de solicitudes de emisión / revocación / suspensión o información del titular o responsable del certificado.

5.3 CONTROLES DE PERSONAL

En los siguientes ítems de la esta DPC serán descriptos los requisitos y procedimientos, implementados por el PCSC de la PNDI., por las ARs y PSSs vinculadas a todo su personal, refiriéndose a aspectos como: verificación de antecedentes e idoneidad, capacitación, rotación de puestos, sanciones por acciones no autorizadas, controles para contratación y documentación a ser proporcionada.

Todos los empleados o funcionarios del PCSC de la PNDI., de las ARs y de los PSSs vinculados, a cargo de las tareas operativas, se hayan registrado en un contrato o término de responsabilidad:

Los términos y condiciones del perfil que ocuparán;

El compromiso de observar las reglas, políticas y normas aplicables a la ICPP; y el compromiso de no divulgar información confidencial a la que tenga acceso.

5.3.1 REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

El personal que ejecuta tareas de confianza en el PCSC de la PNDI, y en sus AR vinculadas, poseen cualificación y experiencia en entornos de servicios de certificación e infraestructura de clave pública, conforme a lo establecido en el Ítem7 “Seguridad ligada a los recursos humanos” de la norma ISO 27002/2022

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

y además debieron:

- Haber demostrado capacidad para ejecutar sus deberes.
- Haber suscripto un acuerdo de confidencialidad y disponibilidad.
- No poseer otros deberes que puedan interferir o causar conflicto con los del PCSC.
- No tener antecedentes de negligencia o incumplimiento de labores.
- No tener antecedentes judiciales ni policiales.

5.3.2 PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Con propósito de resguardar la seguridad y credibilidad de las entidades, todo personal del PCSC de la PNDI y de sus AR vinculadas involucradas en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados es sometido a:

- a) confirmación de empleos anteriores;
- b) verificación de referencias profesionales;
- c) título académico obtenido; y
- d) verificación de antecedentes judiciales y policiales.

5.3.3 REQUERIMIENTOS DE CAPACITACIÓN

Todo el personal del PCSC de la PNDI y de sus ARs vinculadas, involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados reciben entrenamientos que están documentados suficientemente para el dominio de los siguientes temas:

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

- a) principios y mecanismos de seguridad del PCSC y de las ARs vinculadas;
- b) sistema de certificación en uso del PCSC;
- c) procedimientos de recuperación de desastres y continuidad del negocio;
- d) reconocimiento de firmas y validación de documentos presentados en los ítems 3.2.2., 3.2.3. y 3.2.4.;
- e) normativa vigente que rige la materia; y
- f) otros asuntos relacionados con las actividades bajo su responsabilidad.

5.3.4 REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

Todo el personal del PCSC de la PNDI y de sus AR vinculadas, involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados son mantenidos y actualizados sobre eventuales cambios o modificaciones tecnológicas de los sistemas del PCSC de la PNDI o de sus AR.

El PCSC de la PNDI y sus AR vinculadas proveen programas de entrenamiento y de actualización a su personal para asegurar que el personal mantenga el nivel requerido de eficiencia para ejecutar sus labores satisfactoriamente.

5.3.5 FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

Esta DPC establece como política a ser adoptada por el PCSC de la PNDI y sus ARs vinculadas, la rotación de sus roles de confianza establecidos en el punto 5.2.1 con una frecuencia, como mínimo, una vez cada 5 años.

5.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS

Las prácticas que debe cumplir el personal del PCSC de la PNDI y de sus AR vinculadas, y el procedimiento sancionador que incumplan las mismas, son recogidas en el Reglamento Interno del PCSC de la PNDI y de acuerdo a lo

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

estipulado en el documento suscripto para los roles de confianza.

Ante la eventual acción no autorizada, real o sospechada, realizada por una persona responsable del proceso operacional del PCSC de la PNDI o de una de sus AR vinculadas, el PCSC de la PNDI suspenderá de inmediato el acceso de esa persona a su sistema de certificación e iniciará un sumario administrativo para determinar los hechos y, si es necesario, tomará las medidas legales pertinentes.

El sumario administrativo contendrá, como mínimo, los siguientes puntos:

- Relato de lo ocurrido con el modo de operación;
- Identificación de los involucrados;
- Eventuales perjuicios causados;
- Las sanciones aplicadas, si fuere el caso; y
- Conclusiones.

Concluido el sumario administrativo, el PCSC de la PNDI encargado comunicará sus conclusiones a la AC Raíz-Py

Las sanciones que podrían aplicarse como resultado de un sumario administrativo son:

- a) advertencia;
- b) suspensión por un plazo determinado; o
- c) cese de sus funciones

5.3.7 REQUISITOS DE CONTRATACIÓN A TERCEROS

El PCSC de la PNDI y sus AR vinculadas, pueden contratar personal externo, consultores o terceros, conforme a lo establecido en los Ítems: 7 "Seguridad

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

ligada a los recursos humanos” y 15 “Relaciones con suministradores” norma ISO 27002:2022 bajo las siguientes condiciones mínimas:

- Que exista un contrato con cláusulas propias de los roles de confianza y que estipula sanciones para las actuaciones no autorizadas.
- Que el PCSC de la PNDI o los AR vinculados no posean personal disponible para los roles de confianza.
- Que el personal al contratar cumpla con los mismos requisitos del ítem 5.3.1.
- Que una vez finalizados los servicios contratados, se revoken los accesos.

5.3.8 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

El PCSC de la PNDI y sus AR vinculadas proporcionan a sus personales toda la documentación y buenas prácticas de seguridad de la información necesarias para el correcto desempeño de sus tareas. Entre las documentaciones se encuentran:

- a) su DPC;
- b) las PCs que implementan;
- c) la política de seguridad que implementa el PCSC;
- d) documentación operacional relativa a sus actividades; y
- e) contratos, normas y políticas relevantes para sus actividades.

Toda documentación entregada o puesta a disposición del personal estará clasificada y es mantenida actualizada.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

5.4 PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

En los siguientes ítems de la presente DPC se describen los aspectos de los sistemas de auditoría y registro de eventos implementados por el PCSC de la PNDI con el fin de mantener un entorno o ambiente seguro.

5.4.1 TIPOS DE EVENTOS REGISTRADOS

El PCSC de la PNDI registra en archivos de auditoría todos los eventos relacionados a la seguridad del sistema de certificación. Entre otros, los siguientes eventos están incluidos obligatoriamente en los archivos de auditoría:

- a) iniciación y terminación del sistema de certificación;
- b) los intentos de crear, eliminar, establecer contraseñas o cambiar los privilegios del sistema de los operadores del PCSC;
- c) los cambios en la configuración del PCSC o en sus claves;
- d) los cambios en las políticas de creación de certificados;
- e) los intentos de acceso (login) y de salida del sistema (logout);
- f) los intentos no autorizados de acceso a los archivos del sistema;
- g) la generación de claves propias del PCSC o de claves de sus usuarios finales;
- h) la emisión y revocación de certificados;
- i) la generación de la LCR;
- j) los intentos de iniciar, remover, habilitar y deshabilitar a los usuarios desistemas y actualizar y recuperar sus claves;
- k) las operaciones fallidas de escritura o lectura en el repositorio de los certificados y de la LCR, en su caso; y

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

l) las operaciones de escritura en ese repositorio, en su caso.

El PCSC de la PNDI registra, electrónica o manualmente, informaciones de seguridad no generadas directamente por el sistema de certificación, tales como:

- Registros de accesos físicos;
- El mantenimiento y los cambios en la configuración de sus sistemas;
- Los cambios de personal y los cambios de su rol de confianza;
- Los informes de discrepancia y de compromiso; y
- El registro de destrucción de los medios de almacenamiento que contienen las claves criptográficas, de datos de activación de certificados, o de la información personal de los usuarios.

Todos los registros de auditoría, electrónicos o manuales, contienen la fecha y hora del evento registrado y la identidad del agente que lo causó.

Para facilitar los procesos de auditoría, toda documentación relacionada a los servicios del PCSC de la PNDI es almacenada, electrónicamente y/o manualmente, en un local único, conforme a lo establecido en el ítem 12 “seguridad en la operativa” de la norma ISO 27002/2022.

La AR vinculada al PCSC de la PNDI, registra electrónicamente y/o manualmente archivos de auditorías de todos los eventos relacionados a la validación y aprobación de la solicitud, así como la revocación de los certificados. Los siguientes eventos están obligatoriamente incluidos en los archivos de auditoría:

- Los agentes de registros que realizan las operaciones;
- Fecha y hora de las operaciones;

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

- La asociación entre los agentes que realizan la validación, aprobación y el certificado generado;
- La firma electrónica cualificada del ejecutante.

El PCSC de la PNDI a la que está vinculada la AR establece en un documento que está disponible en las auditorías de cumplimiento, el local de archivo de las copias de los documentos utilizados para la identificación del titular del certificado, presentados en el momento de la solicitud y revocación de certificados. Además, el formulario de solicitud y el contrato de Prestación de Servicios de Confianza . Los mismos podrán ser archivos físicos o electrónicos.

5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)

El personal del PCSC de la PNDI con el rol de auditor realiza al menos una vez al mes revisiones de los registros de auditoría, sin necesidad de previo aviso. Todos los eventos significativos serán explicados en un informe de auditoría de registros. Tal análisis involucra una inspección breve de todos los registros, con la verificación de que no fueron alterados, seguida de una investigación más detallada de cualquier alerta o irregularidades en esos registros. Todas las medidas adoptadas como resultado de este análisis son debidamente documentadas.

5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

La información generada en los registros de auditoría se conservará localmente por dos meses y, consecuentemente, se almacenarán de la manera descrita en el ítem 5.5.2.

Además de las revisiones oficiales, los registros de auditoría son revisados en

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

respuesta a una alerta, por irregularidades o incidentes dentro de los sistemas de la AC.

5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

El PCSC de la PNDI establece mecanismos obligatorios incluidos en su sistema de registro de eventos para proteger sus registros de auditoría contra lectura no autorizada, modificación y eliminación.

También el PCSC de la PNDI establece mecanismos obligatorios de protección de información manual de auditoría contra la lectura no autorizada, modificación y eliminación.

Los mecanismos de protección establecidos por el PCSC de la PNDI obedecen a lo dispuesto al Ítem 12 "seguridad en la operativa" de la norma ISO 27002/2022.

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

El PCSC de la PNDI ejecuta procedimientos de respaldo, de todo el sistema de certificación (sistemas operacionales, aplicación y base de datos) de dos formas:

- a) Diariamente: copia de seguridad; y
- b) Mensualmente: copia almacenada para procesos de auditoría

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

Los archivos de registro de auditoría son almacenados en los repositorios internos, mediante una combinación de procesos ejecutados manualmente y por las aplicaciones del PCSC de la PNDI.

Lista de riesgos contemplados:

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

- Inserción o alteración fraudulenta de un registro de sesión.
- Supresión fraudulenta de sesiones intermedias.
- Inserción, alteración o supresión fraudulenta de un registro histórico.
- Inserción, alteración o supresión fraudulenta del registro de una tabla de consultas.

5.4.7 NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

En el caso de que un evento fuera registrado por el conjunto de sistemas de auditoría del PCSC de la PNDI, no se requiere notificar al causante de dicho evento, a excepción de que el evento sea de índole accidental y resulta probable que pueda volver a ocurrir.

5.4.8 EVALUACIÓN DE VULNERABILIDADES

Los eventos que indiquen posibles vulnerabilidades, detectados en el análisis periódico de los registros de auditoría del PCSC de la PNDI, serán analizadas detalladamente y, dependiendo de su gravedad, son registradas por separado. Las acciones correctivas que surjan son implementadas y registradas con fines de auditoría.

5.5 ARCHIVOS DE REGISTROS

En los ítems siguientes de esta DPC es descrita la política general de archivo de registros de la DPC, implementada por el PCSC de la PNDI. y por las AR a ella vinculada.

5.5.1 TIPOS DE REGISTROS ARCHIVADOS

Los tipos de registros archivados comprenden entre

otros:

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

- a- solicitudes de certificados;
- b- solicitudes de revocación de certificados;
- c- notificaciones de compromiso de claves privadas;
- d- emisiones y revocaciones de certificados;
- e- emisiones de LCR;
- f- cambio de claves criptográficas del PCSC responsable;
- g- Información de auditoría prevista en el ítem 5.4.1.

5.5.2 PERIODOS DE RETENCIÓN PARA ARCHIVOS

La LCR y los certificados emitidos de firma digital serán conservados permanentemente para fines de consulta histórica.

Las copias de los documentos para identificación del titular del certificado, presentados en el momento de la solicitud y de la revocación de certificados, el formulario de solicitud y contrato de prestación de servicios de confianza serán conservados, como mínimo, por 10 años, a contar desde la fecha de expiración o revocación del certificado.

Las demás informaciones, inclusive los archivos de auditoría deberán ser almacenadas, como mínimo, 10 años.

5.5.3 PROTECCIÓN DE ARCHIVOS

Todos los registros archivados son clasificados y almacenados con los requisitos de seguridad compatibles con esta clasificación, de acuerdo a lo establecido en el ítem 12 "seguridad en la operativa" de la norma ISO 27002/2022.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVOS

El PCSC de la PNDI:

- Mantiene procedimientos adecuados de respaldo de archivos (físicos y electrónicos), tanto en el sitio principal como en el alterno, que aseguren la disponibilidad de los mismos, de acuerdo a un análisis de riesgos determinado por los factores de operación del PCSC de la PNDI.
- Realiza una segunda copia de todo el material archivado en un local externo al PCSC de la PNDI, recibiendo el mismo tipo de protección utilizada para el archivo principal.
- Establece seguir los mismos periodos de retención definidos para los registros de las cuales son copias.
- Verifica la integridad de esas copias de seguridad, como mínimo, cada 6 (seis) meses.

5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

No aplica.

5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO)

Los archivos del PCSC de la PNDI son de manejo interno de cada una, y se requiere que por lo menos se mantengan dos copias de seguridad, una de las cuales debe ser almacenada fuera del sitio principal de operaciones.

5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA

La información archivada está protegida, de forma que nadie salvo las propias

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

aplicaciones de visualización y gestión de eventos pueda acceder a ellos. Sólo el personal autorizado tiene acceso a los archivos físicos de soportes y archivos informáticos, para llevar a cabo verificaciones de integridad u otras.

Esta verificación debe ser llevada a cabo por el Auditor, que debe tener acceso a las herramientas de verificación y control de integridad de la información archivada.

5.6 CAMBIO DE CLAVE

El PCSC de la PNDI cambia sus claves de acuerdo con el tiempo de uso y tiempo operacional de los certificados emitidos dentro de la ICPP, este cambio técnicamente implica la emisión de un nuevo certificado.

El tiempo operacional de un certificado coincide con el descrito en los campos de "Válido desde" y "Válido hasta" del mismo. El tiempo de uso refiere al establecido para los certificados emitidos por la jerarquía de la ICPP para determinados usos, como se aprecia a continuación:

TIPO DE CERTIFICADO	TIEMPO DE USO EN AÑOS	TIEMPO OPERACIONAL EN AÑOS	DESCRIPCIÓN
Certificado cualificado de firma electrónica F2(módulo hardware)	4	4	El certificado emitido al titular o responsable del certificado es otorgado por un tiempo máximo de 4 (cuatro) años, al finalizar ese período pierde su validez.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

Certificado de la PCSC de la PNDI	6	10	El Certificado emitido al PCSC tendrá un tiempo operacional de 10 (diez) años, que resulta de la suma del tiempo de uso de su certificado [6 (seis) años] más el tiempo de validez máximo del certificado emitido al usuario final [4 (cuatro) años]. Solamente durante el tiempo de uso de su certificado, el PCSC podrá emitir certificados a usuarios finales. En los años restantes del tiempo operacional, sólo podrá firmar o sellar la LCR de usuarios finales
Certificado AC Raíz	10	20	El Certificado emitido a la AC Raíz-Pytendrá: Un tiempo operacional de 20 años, que resulta de la suma del tiempo de uso de su certificado (10 años) más el tiempo de validez máximo del certificado de su suscriptor (10 años). Solamente durante el tiempo de uso de su certificado, la AC Raíz-Py podrá emitir certificados a un PCSC. En los años restantes del tiempo operacional sólo podrá firmar la LCR de PCSC.

Del cuadro anterior, se deduce que en determinado momento puede haber dos certificados del mismo nivel y tipo activos, donde el tiempo de vigencia simultánea de los certificados debe ser de al menos el tiempo operacional del certificado de unsuscriptor.

Por lo tanto, el certificado anterior podrá ser utilizado únicamente para firmar la LCR correspondiente y validar la cadena de confianza de la ICPP, el nuevo

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

certificado emitido, será utilizado para emitir nuevos certificados y firmar la nueva lista de LCR.

El PCSC de la PNDI garantiza que el tiempo máximo de uso en años de los certificados de niveles inferiores emitidas por ella, se ajusta con el tiempo operacional de todos los niveles superiores.

5.7 RECUPERACIÓN DE DESASTRES Y COMPROMISO

Los requisitos relacionados a los procedimientos de notificación y de recuperación de desastres, previstos en el plan de continuidad del negocio del PCSC de la PNDI., se establecen conforme a lo establecido en el ítem 17 “aspectos de seguridad de la información en la gestión de la continuidad del negocio” de la norma ISO 27002/2022, para garantizar la continuidad de sus servicios críticos.

5.7.1 PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO

El PCSC de la PNDI cuenta con un PCN, con acceso restringido, probado al menos una vez al año, para garantizar la continuidad de sus servicios críticos. También debe contar con un Plan de Respuesta a Incidentes y un Plan de Recuperación ante Desastres.

En este ítem la DPC describe los procedimientos previstos en el PCN de las ARs vinculadas para la recuperación total o parcial de las actividades de las ARs, conteniendo al menos la siguiente información:

- a) identificación de eventos que pueden causar interrupciones en los procesos del negocio, por ejemplo, fallas de equipos, inundaciones e

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

incendios, si fuera el caso;

b) identificación y concordancia de todas las responsabilidades y procedimientos de emergencia;

c) implementación de procedimientos de emergencia que permitan la recuperación y restauración dentro de los plazos necesarios;

d) documentación de procesos y procedimientos conforme a lo establecido;

e) capacitación adecuada del personal en procedimientos y procesos de emergencia definidos, incluida la gestión de crisis; y

f) prueba y actualización de planes.

5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES

Si los recursos hardware, software, y/o datos se alteran o se sospecha que han sido alterados se detendrá el funcionamiento de la ICPP hasta que se restablezca la seguridad del entorno con la incorporación de nuevos componentes cuya adecuación pueda acreditarse. De forma simultánea se realizará una auditoría para identificar la causa de la alteración y asegurar que no vuelva a producirse.

En el caso de verse afectados certificados emitidos, se notificará del hecho a los usuarios de los mismos y se procederá a una nueva certificación. Los procedimientos de recuperación utilizados en caso de que la revocación del certificado del PCSC de la PNDI se describe en el punto 5.7.3.

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

5.7.3 PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD

5.7.3.1. CERTIFICADO DE ENTIDAD ES REVOCADO

a) En caso de revocación del certificado del PCSC de la PNDI:

Informar a todos sus suscriptores.

Indicar que los certificados y la información del estado de revocación que han sido entregados usando la clave de la AC del PCSC de la PNDI. ya no son válidos.

b) En caso de revocación del certificado del Titular de Firma electrónica cualificada:

El PCSC de la PNDI informará al titular cuyo certificado fue revocado acerca de los motivos y procedimientos realizados.

5.7.3.2. CLAVE DE ENTIDAD ESTÁ COMPROMETIDA

a) En caso de compromiso de la clave privada del PCSC de la PNDI.:

- Informar inmediatamente al MIC la situación y solicitar la revocación de su certificado.
- Informar a todos sus suscriptores.
- Indicar que los certificados y la información del estado de revocación que han sido entregados usando la clave del PCSC de la PNDI ya no son válidos.

b) En caso de compromiso de la clave privada del Titular de Firma electrónica cualificada

El titular del Certificado debe informar al PCSC de la PNDI. en el menor tiempo posible y solicitar la revocación del certificado afectado.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

5.7.4 CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

El PCSC de la PNDI cuenta con un:

- Plan de Continuidad del Negocio, que incluye un proceso para probar, implementar y mantener el mismo.
- Plan de recuperación frente a desastres destinado a mitigar los efectos de cualquier desastre natural o producido por el hombre, que incluye un proceso para probar, implementar y mantener el mismo. Dicho plan se enfoca en la restauración de los servicios de sistemas de información y de las funciones esenciales del negocio. Dicho plan está redactado conforme a lo establecido en el ítem 17 “aspectos de seguridad de la información en la gestión de la continuidad del negocio” de la norma ISO 27002:2022
- Un Sitio Alternativo de Contingencia cuenta con protecciones de seguridad física equivalentes al sitio principal. El sitio alternativo tiene la capacidad de restaurar o recuperar operaciones esenciales dentro de las veinticuatro horas siguientes al desastre, mínimamente con soporte para las siguientes funciones: revocación de certificados y publicación de información de revocación.

5.8 EXTINCIÓN DE UN PCSC

En caso que el PCSC de la PNDI, deje de operar deberá cumplir, como mínimo, con lo siguiente:

- a) solicitar a la AA, con al menos un mes de anticipación la cancelación de sus suscripción en el registro público de PCSCs, comunicándole el

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

destino que dará a los datos de los certificados, especificando, en su caso, los que va a transferir y a quién, cuando proceda;

b) notificar a sus titulares o responsables de certificados por él emitidos, con al menos un mes de anticipación antes de la suspensión efectiva o cese de sus operaciones;

c) publicar en su sitio principal de Internet la fecha de suspensión de los servicios con al menos un mes de anticipación;

d) publicar la fecha de suspensión de sus servicios por el plazo de 3 días consecutivos en un diario de gran circulación, 10 días hábiles antes de la suspensión efectiva o cese de las operaciones;

e) preservar toda la información en concordancia con esta DPC y la normativa aplicable; y

f) proceder a la eliminación y destrucción de la clave privada mediante un mecanismo que impida su reconstrucción.

En caso de que el PCSC de la PNDI, deje de operar, no emitirá bajo ningún sentido ningún certificado, pero continuará dando soporte a las operaciones de revocación de certificados y publicación de LCR. Recién una vez vencidos o revocados todos los certificados emitidos, y cuya revocación esté publicada, cesará la responsabilidad del PCSC.

El titular del certificado, podrá seguir utilizando el certificado emitido hasta que se extinga el plazo de vigencia o hasta que fuera revocado. En caso de que el certificado llegue a su fecha de expiración no se podrá confiar en dicho

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

certificado.

El MIC custodiará toda la información referida al cese de operación del PCSC de la PNDI, además publicará el cese de actividades o finalización del servicio del PCSC de la PNDI en su sitio principal de internet.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

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 del PNDI y por sus AR vinculadas en la ejecución de sus funciones operacionales.

Los detalles relativos a las claves de los titulares de los certificados se podrán consultar en la Política de Certificación.

6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1 GENERACIÓN DEL PAR DE CLAVES

El par de claves criptográficas del PCSC de la PNDI fue generado por el propio personal, de acuerdo al procedimiento establecido en el documento Ceremonia de generación de claves, posterior a la habilitación otorgada por el MIC vía resolución ministerial. El par de claves criptográficas se generan y almacenan en módulos de hardware criptográficos con certificación FIPS 140-2 Nivel 3. Se garantiza que la clave privada de firma nunca permanecerá fuera del módulo donde fue generada, a menos que se almacene en un mecanismo de recuperación de claves.

El par de claves es generado solamente por el titular del certificado correspondiente. Los procedimientos específicos son descritos en su PC implementada.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

6.1.2 ENTREGA DE LA CLAVE PRIVADA AL TITULAR

Este punto no es aplicable porque la generación y guarda de una clave privada será responsabilidad exclusiva del titular del certificado correspondiente.

6.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

La clave pública es tratada desde su generación mediante mecanismos seguros que aseguran su autenticidad e integridad, impidiendo que sea alterada en su tránsito.

La clave pública generada bajo el control PCSC de la PNDI es entregada a la AC RAÍZ-PY 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 la generación del CSR mencionado, se adopta el formato definido en el documento DOC-ICPP-06 [5]

La clave pública generada bajo control del usuario final se entrega a través de un intercambio en línea utilizando funciones automáticas del software de certificación del PCSC de la PNDI.

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

La clave pública del PCSC de la PNDI se encuentra incluida en el certificado del mismo. El certificado del PCSC de la PNDI no se encuentra incluido en los certificados personales generados por el usuario final. El certificado del PCSC de la PNDI es obtenido del repositorio que está a disposición de los titulares de certificados y terceros aceptantes para realizar cualquier tipo de

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

comprobación.

La clave pública del PCSC de la PNDI es entregada a las partes que confían utilizando el formato del estándar PKCS#7, definido en el documento DOC-ICPP-06 [5]

El certificado del PCSC de la PNDI se encuentra disponible para su descarga en su repositorio público, en el siguiente enlace:

<https://www.identificaciones.gov.py/firmadigital/que-es-el-certificado-de-firma-electronica/>

6.1.5 TAMAÑO DE LA CLAVE

El tamaño de las claves criptográficas del PCSC de la PNDI es de 4096 bits.

El tamaño de las claves para cada tipo de certificado emitido por la PNDI viene definido por la política de certificación correspondiente.

6.1.6 GENERACIÓN DE PARÁMETROS DE CLAVES ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD

Los parámetros de generación de claves asimétricas para el PCSC de la PNDI cumplen con el estándar definido en el documento DOC-ICPP-06 [5].

Los parámetros de verificación de calidad son verificados de acuerdo con las normas establecidas en el documento DOC-ICPP-06 [5].

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

La Clave privada del PCSC de la PNDI podrá ser utilizado con el único propósito de:

- Firmar los certificados emitidos por el PCSC de la PNDI;

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

- Firmar la LCR correspondiente; y

Los usos admitidos de la clave para cada tipo de certificado emitido por el PCSC de la PNDI vienen definidos por la política de certificación correspondiente.

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

Los requisitos aplicables para el módulo criptográfico utilizado para el almacenamiento de la clave privada de los Titulares de Certificados del PCSC de la PNDI, se basan en lo definido en el documento DOC-ICPP-06 [5], los cuáles son los siguientes:

- Requisito obligatorio: Certificado por el MIC
- Estándares: FIPS 140-2 nivel 3 (para certificados tipo F2).

Cada PC implementada por el PCSC de la PNDI especifica los requisitos específicos aplicables.

6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO

Los módulos criptográficos de generación de claves asimétricas del PCSC de la PNDI adoptan los patrones definidos en el documento DOC-ICPP-06 [5].

6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA

La forma de control múltiple aplicado por el PCSC de la PNDI es del tipo "N" personas de un grupo "M", requerido para la utilización de las claves privadas. Donde serán requeridos N= 3 (tres) de M= 5 (cinco) titulares de activación de clave, formalmente designadas.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

6.2.3 CUSTODIA (ESCROW) DE LA CLAVE PRIVADA

El PCSC de la PNDI solo custodia su propia clave privada con niveles de seguridad adecuados a lo establecido en esta DPC.

El PCSC de la PNDI no almacena ni copia las claves privadas de los titulares de certificados de firma digital.

Los certificados tipo F2 están bajo la custodia del titular del mismo, y éste será el responsable de mantenerla bajo su exclusivo control.

6.2.4 RESPALDO/COPIA DE LA CLAVE PRIVADA

El PCSC de la PNDI indica que cualquier persona física, titular del certificado, podrá, a su criterio, mantener una copia de su propia clave privada.

El PCSC de la PNDI mantiene una copia de seguridad de su propia clave privada bajo la protección de dispositivos seguros y a los que sólo las personas con roles de confianza autorizadas por la PNDI tienen acceso. La copia de clave privada del PCSC de la PNDI son únicamente para propósitos de recuperación en caso de una contingencia o desastre.

EL PCSC de la PNDI no mantiene copia de seguridad de la clave privada del titular del certificado de firma electrónica cualificada por ella emitida.

La copia de seguridad descrita es almacenada cifrada por un algoritmo simétrico en los estándares que pueden ser 3DES – 112 bits o AES – 128 o 256 bits en modo de operación CBC o GCM y protegida con un nivel de seguridad de estándar FIPS 140-2 nivel 3.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

6.2.5 ARCHIVADO DE LA CLAVE PRIVADA

Las claves privadas de los certificados de firma electrónica cualificada nunca serán archivadas.

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

6.2.6 TRANSFERENCIA DE CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRIPTOGRÁFICO

La clave privada del PCSC de la PNDI puede ser transferida de un módulo criptográfico a otro del mismo o mayor nivel de seguridad usando la RFC 4210 o 6712.

Cada PC implementada por el PCSC de la PNDI define, cuando sea aplicable, los requisitos de transferencia de la clave privada de los titulares del certificado de un módulo criptográfico a otro.

6.2.7 ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

Esta sección se encuentra conforme a lo establecido en el ítem 6.1 de esta DPC.

6.2.8 MÉTODO DE ACTIVACIÓN DE CLAVE PRIVADA

La clave privada del PCSC de la PNDI sólo puede ser activada por agentes de registro designados por el PCSC. a través del sistema de certificación.

La confirmación de identidad de los agentes de registro autorizados se realiza también haciendo uso de autenticación a través de biometría o contraseña.

La activación de la clave privada para usuarios finales la podrá efectuar el

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

titular dela misma mediante el uso de al menos un factor de seguridad (contraseñas).

Cada PC implementada por el PCSC de la PNDI describe los requisitos y los procedimientos necesarios para la activación de la clave privada del titular de certificado.

6.2.9 MÉTODOS DE DESACTIVACIÓN DE LA CLAVE PRIVADA

La clave privada del PCSC de la PNDI, instalada en el entorno de producción de susistema de certificación, se ubica a nivel de seguridad 6, donde sólo se permite el acceso al ambiente en doble autenticación, debidamente autorizadas por el sistemade control de acceso de la PNDI.

Dentro de este ambiente, sólo personal con rol de confianza tienen acceso al sistemade certificación de producción, donde se ejecutan los comandos de desactivación del sistema para la desactivación de la clave del PCSC de la PNDI, después de su debida identificación y autorización hecha a través de mecanismos nativos del sistema operativo.

Estos funcionarios se identifican mediante su cédula de identidad y su legajo de personal con rol de confianza que contiene, entre otros, fotografía, nombre y rol.

Cada PC implementada por el PCSC de la PNDI describe los requisitos y los procedimientos necesarios para la desactivación de clave privada del titular de certificado.

6.2.10 MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA.

El PCSC de la PNDI elimina sus claves privadas de los módulos criptográficos

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

y el respaldo de las mismas cuando hayan expirado o hayan sido revocadas.

El PCSC de la PNDI solicitará al MIC que participe de la ceremonia de destrucción de su clave privada.

En presencia de funcionarios del MIC, y el control multipersona, los cuales serían representados por el personal con rol de Responsable de coordinación de área, rol de Responsable de seguridad y el representante legal del PCSC de la PNDI en el ambiente del nivel 6, con sus respectivos token, se realizará la destrucción de la clave privada original y sus copias de seguridad reiniciando los medios de almacenamiento de las claves privadas, no dejando información remanente sensible en estos medios.

El personal con rol de Responsable de coordinación de área y rol de Responsable de seguridad identifican mediante su cédula de identidad y su legajo de personal con rol de confianza que contiene, entre otros, fotografía, nombre, rol y su token.

El representante legal del PCSC de la PNDI se identifica a través de cédula de identidad y su correspondiente legajo de RRHH

El procedimiento de destrucción de clave privada, debe estar documentado y realizado por personal con rol de confianza con control multi persona.

La destrucción de la clave privada debe constar en los registros de auditoría.

Los procedimientos necesarios para la destrucción de la clave privada de la persona física y de sus copias de seguridad si las hubiere, es responsabilidad del titular del certificado.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

La destrucción se puede realizar de las siguientes formas:

- Destrucción física.
- Sobreescritura.
- Eliminación de los medios de almacenamiento: mediante el uso de un factor de seguridad (contraseñas).

Cada PC implementada por el PCSC de la PNDI describe los requisitos y los procedimientos necesarios para la destrucción de la clave privada de la entidad titular de certificado.

6.3 OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

6.3.1 ARCHIVO DE LA CLAVE PÚBLICA

Las claves públicas del PCSC de la PNDI y de los titulares de los certificados de firma electrónica cualificada, así como las LCR emitidas y sistemas de OCSP, son almacenados y gestionados por el PCSC de la PNDI, después de la expiración de los certificados correspondientes, por un periodo de 10 años desde su última emisión, para la verificación de las firmas generadas durante su periodo de validez.

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

La clave privada del PCSC de la PNDI y de los titulares de certificados de firma electrónica, será utilizada únicamente durante el periodo de validez estipulado en el punto 5.6 de esta DPC. La clave pública podrá ser utilizada 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.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

Cada PC implementada por el PCSC responsable debe definir el periodo máximo de validez del certificado que define, con base a los requisitos aplicables establecidos en esta DPC y en el documento DOC-ICPP-04 [1].

6.4 DATOS DE ACTIVACIÓN

Los datos de activación, distintos de las claves criptográficas, son aquellos requeridos para la operación de algunos módulos criptográficos. Cada PC implementada por el PCSC de la PNDI describe los requisitos específicos aplicables.

6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

El PCSC de la PNDI garantiza que los datos de activación del equipo de encriptación que almacena las claves privadas del PCSC de la PNDI son únicos.

El PCSC de la PNDI mantiene estrictos controles de los datos de activación para operar los módulos criptográficos conforme a lo establecido en el ítem 6.2.2.

La PC del PCSC de la PNDI garantiza que los datos de activación de la clave privada del titular del certificado serán únicos.

6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

El PCSC de la PNDI garantiza que los datos de activación de su clave privada están protegidos contra el uso no autorizado mediante el mecanismo de encriptación y control de acceso físico.

Cada PC implementada por el PCSC de la PNDI garantiza que los datos de activación de la clave privada del titular del certificado están protegidos contra

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

el uso no autorizado.

6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Entre esos otros aspectos pueden ser considerados algunos de aquellos tratados, en relación de las claves, en los ítems 6.1 al 6.3.

6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

La generación del par de claves del PCSC de la PNDI se realiza offline para impedir el acceso remoto no autorizado.

Cada computador donde operan los sistemas del PCSC de la PNDI requieren acceso remoto, poseen autenticación mutua y los sistemas operativos están configurados de acuerdo con los estándares del sistema operativo utilizado y son revisados periódicamente.

Las actualizaciones y parches de los sistemas operativos son aplicados de acuerdo a las recomendaciones de los fabricantes y la utilización de programas utilitarios del sistema es restringida al personal autorizado, y está estrictamente controlado. Se mantiene un sistema de pruebas separado del sistema de producción para comprobar el correcto funcionamiento antes del paso a producción. La AC tiene procedimientos de control del cambio para el hardware, los componentes de la red y los cambios de configuración del sistema.

Cada computador del PCSC de la PNDI, relacionado directamente con los procesos de emisión, expedición, distribución, suspensión, revocación y gestión de certificados, deberá implementar, entre otras, las siguientes

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

características:

- a) control de acceso a los servicios y perfiles del PCSC;
- b) clara segregación de tareas y atribuciones relacionadas con cada rol de confianza del PCSC;
- c) uso de criptografía para seguridad de base de datos, cuando sea requerido por la clasificación de su información;
- d) generación y almacenamiento de registros de auditoría del PCSC;
- e) mecanismos internos de seguridad para garantizar la integridad de datos y procesos críticos; y
- f) mecanismos para copias de seguridad (backup).

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

Cualquier equipo o parte del mismo, para ser sometidos a mantenimiento harán un borrado completo de la información confidencial que contenga, controlar su número de serie, las fechas de envío y recepción. Al regresar a las instalaciones del PCSC de la PNDI, el equipo que fue sometido a mantenimiento será inspeccionado. Cualquier equipo que ya no se utilice de forma permanente, serán destruidas, de manera definitiva, todas las informaciones sensibles almacenadas, relativas a la actividad del PCSC de la PNDI. Todos estos eventos serán registrados con fines de auditoría.

Cualquier equipo incorporado en el PCSC de la PNDI será preparado y configurado según lo previsto en la **política de seguridad** implementada u otro documento aplicable con el fin de mostrar el nivel de seguridad requerido

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

para su propósito.

6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

La seguridad computacional del PCSC de la PNDI sigue las recomendaciones Common Criteria.

6.5.3 CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO

Los requisitos de seguridad computacional de las estaciones de trabajo y de los computadores portátiles utilizados por la AR para los procesos de validación y aprobación de certificados, están adecuados conforme a lo descripto en el documento DOC-ICPP-05 [4], en los ítems 4.1, 4.2 y 5.

En general las estaciones de trabajo de la AR, incluidos los equipamientos portátiles, reciben, por lo menos, las siguientes configuraciones de seguridad:

- Control de acceso lógico al sistema operativo;
- La exigencia de utilizar contraseñas fuertes y seguras;
- Políticas de contraseñas y bloqueo de cuentas;
- Logs de auditoría del sistema operativo activo que registre:
 - ❖ Inicio y apagado del sistema;
 - ❖ Intentos de crear, eliminar, establecer contraseñas o cambiar los privilegios de los sistemas de operaciones de la AR;
 - ❖ Cambios en la configuración de la estación;
 - ❖ Intentos de acceso (login) y de salida del sistema (logout);
 - ❖ Intentos no autorizados de acceso a los archivos del sistema;

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

❖ Intentos de iniciar, eliminar, habilitar y deshabilitar a los usuarios y de actualizar y recuperar sus claves.

- Poseer antivirus, antispyware y anti-troyano, instalados, actualizados y habilitados;
- Firewall personal activado, con permisos de acceso mínimo necesarios para las actividades. Este requerimiento puede ser sustituido por firewall corporativo, para los equipos instalados en redes que tienen tal dispositivo;
- Protector de pantalla accionado como máximo 2 (dos) minutos de inactividad y exigiendo para su desbloqueo la contraseña del usuario;
- Sistema operativo actualizado, con la aplicación de las correcciones necesarias (patches, hotfix, etc.);
- Utilizar solamente software con licencias y solamente aquellos necesarios para llevar a cabo las actividades del usuario;
- Impedimento de acceso remoto, a través de otro equipo conectado a la red utilizado por la AR, excepto para las actividades de soporte remoto; y
- Equipo que requieran la identificación de forma segura del AGR durante la identificación del solicitante del certificado;
- Utilización de fecha y hora oficial paraguaya, sincronizando la misma con la utilización de una fuente confiable de tiempo ajustados al país.

6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

En este apartado son descritos los controles implementados por el PCSC de la PNDI y por las AR a ella vinculadas en el desarrollo de sistemas y en la gestión

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

de la seguridad.

6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA

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

6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

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

El PCSC de la PNDI utiliza una metodología formal de gestión de configuración para la instalación y el mantenimiento continuo del sistema

6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

El PCSC de la PNDI debe informar, cuando esté disponible, el nivel de madurez asignado al ciclo de vida de cada sistema, basado en criterios tales como: Trusted Software Development Methodology (TSDM) o el Capability Maturity Model do Software Engineering Institute (CMM-SEI).

6.6.4 CONTROLES EN LA GENERACIÓN DE LCR

Antes de publicarse, las LCRs generadas por el PCSC de la PNDI se revisan en

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

cuanto a la consistencia de su contenido, comparándolo con el contenido esperado en relación al número de LCR, fecha / hora de emisión y otra información relevante.

6.7 CONTROLES DE SEGURIDAD DE RED

6.7.1 DIRECTRICES GENERALES

Se describen a continuación los controles relativos a la seguridad de red del PCSC de la PNDI, incluidos firewalls y recursos similares.

En los servidores del sistema de certificación del PCSC de la PNDI, sólo los servicios estrictamente necesarios para el funcionamiento de la aplicación están habilitados.

Todos los servidores y elementos de la infraestructura y protección de redes, tales como ruteadores, hubs, switches, firewalls y sistemas de detección de intrusos (IDS), localizados en el segmento de red en que se hospeda el sistema de certificación del PCSC de la PNDI, están localizados y operan en un ambiente de nivel 4 (cuatro) o superior conforme a lo establecido en las normativas.

Las últimas versiones de los sistemas operativos y servidores de aplicaciones, así como las eventuales correcciones (parches), disponibilizadas por los respectivos fabricantes son implementadas inmediatamente después del testeado en el ambiente de homologación.

El acceso lógico a los elementos de la infraestructura y protección de la red están restringidos por medio de un sistema de autenticación y autorización de acceso. Los ruteadores conectados a redes externas implementan filtros de paquetes de datos, que solo permitan conexiones a los servicios y servidores

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

previamente definidos como objeto de acceso externo.

Los equipos del PCSC de la PNDI se encuentran dentro de los límites de la red interna, dicha red está protegida contra ataques. Los puertos y servicios que no requieran se encuentran inactivos.

Los sitios Web del PCSC están provistos de certificados SSL.

6.7.2 FIREWALL

Los Mecanismos de Firewall se implementan en equipos de uso específico, configurado exclusivamente para esa función. Un firewall promueve el aislamiento, en subredes específicas, de los equipos servidores con acceso externo - la denominada "zona desmilitarizada" (DMZ) en relación a los equipos con acceso exclusivamente interno al PCSC de la PNDI.

El Software del firewall, entre otras características, implementa registros de auditoría.

6.7.3 SISTEMA DE DETECCIÓN DE INTRUSO (IDS)

El sistema de detección de intruso del PCSC de la PNDI está configurado para reconocer ataques en tiempo real y responder automáticamente con medidas tales como: enviar traps SNMP, ejecutar programas definidos por la administración de redes, enviar e-mail a los administradores, enviar mensajes de alerta al firewall o al terminal de gerenciamiento, promoviendo la desconexión automática de conexiones sospechosas, o la reconfiguración del firewall.

El sistema de detección de intrusiones es capaz de reconocer diferentes patrones de ataques, incluso contra el propio sistema, con la posibilidad de

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

actualizar su base de reconocimiento.

El sistema de detección de intruso provee un registro de los eventos en logs, recuperables en archivos de tipo texto, e implementa una gestión de la configuración.

6.7.4 REGISTRO DE ACCESO NO AUTORIZADO A LA RED

Los intentos de acceso no autorizados en los routers, Firewalls o IDS son registrados en archivos para posterior análisis, que podrá ser automatizada. La frecuencia de los exámenes de los archivos de registro es diaria y todas las acciones tomadas como resultado de dicho examen son documentadas.

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

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

7. PERFILES DE CERTIFICADOS, LCR Y OCSP

En los siguientes puntos de la DPC, son descritos los aspectos del certificado del PCSC de la PNDI y de la LCR emitidas por el PCSC de la PNDI.

Cada PC implementada por el PCSC de la PNDI, especifica los formatos de los certificados generados y las correspondientes LCR, incluidas las informaciones sobre los patrones adoptados, sus perfiles, versiones y extensiones.

7.1 PERFIL DEL CERTIFICADO

El certificado digital del PCSC de la PNDI cumple con el formato definido por la norma ITU X.509 V.3 Information technology Open systems interconnection The Directory: Public-key and attribute certificate frameworks según el perfil establecido en la RFC 5280.

7.1.1 NÚMERO DE VERSIÓN

El Certificado del PCSC de la PNDI soporta y utiliza 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 obligatorias en el marco de la ICPD utilizadas en el certificado del PCSC de la PNDI son:

- a) **Identificador de la clave de la Autoridad Certificadora "Authority Key Identifier", no crítica:** el campo Key Identifier debe contener el hash SHA-1 de la clave pública de la AC Raíz-Py que emite el certificado;
- b) **Identificador de la clave de la persona física titular del certificado "Subject Key Identifier", no crítica:** debe contener el

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

hash SHA-1 de la clave pública del PCSC titular del certificado;

c) **Uso de Claves “Key Usage”, crítica:** solamente los bits KeyCertSign y CRLSign deben estar activados;

d) Directivas del Certificado “Certificate Policies”, no crítica:

d.1.1) el campo **policyIdentifier** debe contener los OIDs de las PCs implementadas por el PCSC titular del certificado, para la emisión de certificados de personas físicas.

d.1.2) el campo policyQualifiers

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

d.1.2.2 el campo User Notice debe decir: “Sujeta a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de [nombre del PCSC]”

e) **Restricciones Básicas “Basic Constraints”, crítica:**

e.1 el campo **Subject Type** debe contener CA=True

e.2 el campo **PathLenConstraint** debe tener valor cero;

f) Puntos de distribución de las LCR “LCR Distribution Points”, no crítica:

f.1 el campo **Distribution Point 1** debe contener la dirección web donde se obtiene la LCR correspondiente al certificado

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

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

g.1.1 en el campo **Access Method 1** debe contener el identificador de método de acceso a la información de revocación (O CSP)

g.1.2 en el campo **Access Location 1** debe contener la dirección Web del servicio del OCSP

g.2.1 en el campo **Access Method 2** debe contener el identificador de método de acceso del certificado de la AC Raiz-Py

g.2.2 en el campo **Access Location 2** debe contener la dirección web donde se encuentra alojado el certificado de la AC Raiz-Py

7.1.3 IDENTIFICADORES DE OBJETO DE ALGORITMOS

Los certificados del PCSC de la PNDI. son firmados utilizando el algoritmo definido en el documento DOC-ICPP-06 [5].

7.1.4 FORMAS DEL NOMBRE

El nombre del PCSC de la PNDI referente a la extensión subject del certificado, adopta el "Distinguished Name" (DN) del estándar ITU X.500/ISO 9594 y es la que se describe en la siguiente forma:

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

OID=2.5.4.6 C= PY;

OID=2.5.4.10 O= ICPP

**OID=2.5.4.11 OU= Prestador Cualificado de Servicios de
Confianza**

OID: 2.5.4.3 CN= Ministerio del Interior

OID: 2.5.4.5 Serial Number= 80001140-6

7.1.5 RESTRICCIONES DEL NOMBRE

Los nombres contenidos en los certificados están restringidos a distinguished nameX.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:

Caracteres	Código (hexadecimal)
Blanco	20
!	21
"	22

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

#	23
\$	24
%	25
&	26
'	27
(	28
)	29
*	2a
+	2B
,	2C
-	2D
.	2E
/	2F
:	3a
;	3B
=	3D
?	3F
@	40
\	5C

7.1.6 IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO

El OID asignado a la DPC de la PNDI 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 del PCSC de la PNDI, la extensión "Certificate Policies", contiene la URL de la DPC de la AC Raíz del Paraguay emitente del certificado.

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

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

Las extensiones críticas deben interpretarse de acuerdo con RFC 5280.

7.2 PERFIL DE LA LCR

Las Listas de Certificados Revocados LCRs son firmadas utilizando el algoritmo definido en el documento DOC-ICPP-06 [5].

7.2.1. NÚMERO (S) DE VERSIÓN

Las LCR generadas por el PCSC de la PNDI implementan la versión 2 del 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 AC Raíz-Py define las siguientes extensiones de LCR como obligatorias:

- Identificador de la clave de la Autoridad Certificadora**
“Authority Key Identifier” no crítico: debe contener el hash SHA-1 de la clave pública del PCSC que firma o sella la LCR;
- Número de LCR “CRL Number” no crítico:** 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.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

7.3 PERFIL DE OCSP

Las Respuestas OCSP deberán ser firmados utilizando el algoritmo definido en el documento DOC-ICPP-06 [5].

7.3.1. NÚMERO (S) DE VERSIÓN

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

7.3.2. EXTENSIONES DE OCSP

En conformidad con RFC 6960.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

8. AUDITORÍA DE CUMPLIMIENTO Y OTRASEVALUACIONES

8.1. FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

Se llevará a cabo una auditoría al menos cada veinticuatro (24) meses, corriendo con los gastos que ello genere, por un OEC. La finalidad de la auditoría es confirmar que tanto los PCSC, como los servicios de confianza cualificados que prestan cumplen con los requisitos establecidos en esta DPC y en la normativa vigente. Los PCSC enviarán el informe de evaluación de la conformidad correspondiente a la AC Raíz-Py en el plazo de 3 (tres) días hábiles tras su recepción.

Sin perjuicio de lo dispuesto en el párrafo anterior, la AC Raíz-Py podrá en cualquier momento auditar o solicitar a un OEC que realice una evaluación de conformidad de los PCSC, corriendo con los gastos dichos PCSC, para confirmar que tanto ellos como los servicios de confianza cualificados que prestan cumplen los requisitos de esta DPC y de la normativa vigente.

Además cada PCSC, deberá implementar un programa de auditorías internas conforme a lo estipulado en el ítem 18 “cumplimiento” de la norma ISO 27002/2022 para la verificación de su sistema de gestión.

Cuando la AC Raíz-Py requiera a un PCSC que corrija el incumplimiento de requisitos de esta DPC o de la normativa vigente, y este prestador no actúe en consecuencia, en su caso, en el plazo fijado por la AC Raíz-Py, la AC Raíz-Py, teniendo en cuenta en particular el alcance, la duración y las consecuencias de este incumplimiento, puede retirar la cualificación al prestador o al servicio que este presta y actualizar la lista de confianza. La AC Raíz-Py comunicará al PCSC la retirada de su cualificación o de la cualificación del servicio de que se

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

trate.

Tales supervisiones deberán ser efectuadas conforme a las disposiciones en materia de auditoría, reglamentadas por la AC Raíz-Py.

Todo PCSC está obligado al cumplimiento de las auditorías, éstas permiten establecer una confianza razonable en el marco de la ICPP.

La disposición o resolución que ordena una Auditoría o evaluación no será recurrible.

8.2. IDENTIDAD/CALIDAD DEL EVALUADOR

El equipo de Auditoría Interna del PCSC de la PNDI está conformado por personal calificado con experiencia en tecnología de la información, seguridad, tecnología de la PKI y criptografía.

En el caso de la auditoría externa, se contratará personal calificado con experiencia en tecnología de la información, seguridad, tecnología de ICPP y criptografía.

8.3. RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA

Para el caso de las auditorías externas, los auditores contratados deberán ser independientes e imparciales y deberán ejecutar las evaluaciones de acuerdo a los procedimientos establecidos por el Ministerio de Industria y Comercio.

La AC Raíz-Py, aplicará el procedimiento de acreditación de los OEC conforme al DOC-ICPP-11 [6] para la recepción del informe de evaluación de la conformidad y respecto a las disposiciones en materia de auditoría con arreglo a las cuales los OEC realizarán la evaluación de la conformidad de los PCSC se registrarán conforme al DOC-ICPP-12 [7].

Para el caso de las auditorías internas, el auditor será independiente funcionalmente del área objeto de evaluación.

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

8.4. ASPECTOS CUBIERTOS POR LA EVALUACIÓN

Las inspecciones y auditorías realizadas en el ámbito de la ICPP tienen como objetivo verificar si los procesos, procedimientos y actividades de las entidades que componen la ICPP están en cumplimiento de sus respectivos DPC, PC, PSS y demás normas y procedimientos establecidos por ICPP.

El PCSC de la PNDI debe informar que ha recibido una auditoría por parte del OEC para fines de habilitación por parte de la AC Raíz-Py y que es auditado al menos cada veinticuatro (24) meses, con el objetivo de mantener la habilitación con base en lo establecido en los Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP DOC-ICPP-12 [7]. Este documento aborda el objetivo, la frecuencia y el alcance de las auditorías, la identidad y las calificaciones del auditor y otros temas relacionados.

En PCSC de la PNDI debe informar que las entidades del ICPP directamente vinculados él (AV, AR y PSS), también recibieron una auditoría previa, por parte del OEC para fines de habilitación por parte de la AC Raíz-Py, y que es auditado que es auditado conforme a lo establecido en el párrafo anterior.

Los aspectos cubiertos por la Auditoría son:

- a) Controles de seguridad física y estándares técnicos de seguridad;
- b) Confidencialidad y calidad de los sistemas de control;
- c) Integridad y disponibilidad de los datos;

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

- d) Cumplimiento de los estándares tecnológicos;
- e) Seguridad del personal;
- f) Cumplimiento de la política y declaración de prácticas de certificación;
- g) Procesos de certificación de clave pública;
- h) Política de seguridad y privacidad;
- i) Controles administrativos del PCSC;
- j) Administración de los servicios del PCSC; y
- k) Revisión de contratos.

8.5. ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA

De acuerdo con los Criterios y procedimientos para la inspección de los miembros de las entidades de la ICPP (DOC-ICPP-17 [3]) y con los Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP (DOC-ICPP-12[7]).

8.6. COMUNICACIÓN DE RESULTADOS

De acuerdo con los Criterios y procedimientos para la inspección de los miembros de las entidades de la ICPP (DOC-ICPP-14 [8]) y con los Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP (DOC-ICPP-12[7]).

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1. TARIFA

EL PCSC de la PNDI. deberá comunicar al interesado en adquirir un certificado, todos los costos que deberá asumir para la obtención del certificado.

En todos los casos de incumplimiento de pago por parte del suscriptor, el PCSC de la PNDI., podrá atribuirse el derecho a la revocación del certificado emitido.

9.1.1. TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

Los certificados emitidos bajo la presente DPC son expedidos a favor de personas físicas, aplicándose aranceles diferenciales asociados conforme a la clase de certificado.

Las tarifas para la emisión y renovación de certificados por la AC Raíz-Py de la ICPP para los PCSC estarán definidas conforme al documento Directrices de la Política Tarifaria de la AC Raíz-Py de la ICPP.

9.1.2. TARIFAS DE ACCESO A CERTIFICADOS

No aplica.

9.1.3. TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN

No aplica

9.1.4. TARIFAS POR OTROS SERVICIOS

No se aplicará ninguna tarifa por el servicio de información sobre esta DPC, ni

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

las políticas de certificación administradas por el PCSC de la PNDI, ni por ningún otro servicio adicional del que se tenga conocimiento en el momento de la elaboración del presente documento.

9.1.5. POLÍTICAS DE REEMBOLSO

En el caso de que alguna Política de Certificación especifique alguna tarifa aplicable a la prestación de servicios de certificación o revocación por parte del PCSC de la PNDI para el tipo de certificados que defina, será obligado a determinar la política de reembolso correspondiente.

9.2. RESPONSABILIDAD FINANCIERA

En este ítem de la DPC, los recursos financieros suficientes para mantener las operaciones y cumplir con las obligaciones, así como para afrontar riesgos, se encuentran en conformidad a la normativa vigente.

9.2.1. COBERTURA DE SEGURO

EL PCSC de la PNDI pertenece al sector público y exceptuado de contar con un seguro de responsabilidad civil Art 10, numeral 3 inc b) de la Ley N° 6822/2021

9.2.2. OTROS ACTIVOS

Este ítem no aplica.

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

Sin Estipulaciones.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

9.3.1. ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

Durante el ciclo de vida del certificado, tanto el PCSC de la PNDI como la AR vinculada establecen, como principio general, que ningún documento, información o registro deberán ser divulgados.

9.3.2. INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL

El PCSC de la PNDI y sus AR vinculadas consideran información pública y por lo tanto accesible por terceros:

- a) los certificados y las LCRs/OCSPs emitidos por el PCSC;
- b) las PCs implementadas por el PCSC;
- c) la DPC del PCSC; y
- d) la conclusión de los informes de auditoría.
- e) Versión pública de la PS

Los Certificados, LCR/OCSP y la información corporativa o personal que necesariamente forme parte de ellos o de directorios públicos se consideran información no confidencial.

El PCSC también podrá divulgar, de forma consolidada o segmentada por tipo decertificado, el número de certificados emitidos en el ámbito de ICPP.

9.3.3. RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Los participantes que reciban o tengan acceso a información confidencial deberán contar con mecanismos que aseguren la protección y confidencialidad, evitando su uso o divulgación a terceros, bajo pena de

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

responsabilidad, de acuerdo con la ley.

La clave privada del PCSC de la PNDI es generada y mantenida por el propio PCSC de la PNDI, quien será responsable de su secreto. La divulgación o el uso indebido de la clave privada por parte del PCSC de la PNDI será de su exclusiva responsabilidad.

El PCSC de la PNDI informa en su DPC que los titulares de certificados de firma electrónica cualificada, tendrán la tarea de generar y mantener la confidencialidad de sus respectivas claves privadas. Además, son responsables de la divulgación o uso indebido de estas mismas claves.

Si existen responsabilidades específicas para las PCs implementadas, las mismas deben ser descritas en dichas PCs, en el ítem correspondiente.

9.4. PRIVACIDAD DE INFORMACIÓN PERSONAL

9.4.1. PLAN DE PRIVACIDAD

El PCSC de la PNDI y sus AR vinculadas implementan una política de privacidad de información de acuerdo con la normativa vigente.

El PCSC de la PNDI y sus AR vinculadas sólo podrán recolectar los datos personales directamente de la persona a quien esos datos se refieran, después de haber obtenido su consentimiento expreso y sólo en la medida en que los mismos sean necesarios para la emisión y mantenimiento del certificado. Los datos no podrán ser obtenidos o utilizados para otro fin, sin el consentimiento expreso del titular de los datos.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

9.4.2. INFORMACIÓN TRATADA COMO PRIVADA

Cualquier información acerca de los titulares de los certificados que no esté públicamente disponible a través del contenido del certificado emitido y servicios de LCR, es tratada como información privada.

9.4.3. INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

El tratamiento de la información que no es considerada como privada, está sujeta a lo que dispone la normativa vigente al efecto. Se considera pública la información contenida en el certificado.

9.4.4. RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

El PCSC de la PNDI y sus AR vinculadas aseguran mediante varios mecanismos que la información privada no pueda ser comprometida o divulgada a terceras partes.

9.4.5. NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

El PCSC de la PNDI establece que el titular del certificado podrá autorizar la divulgación de sus registros o que terceras personas accedan a la misma, previa autorización escrita.

Cualquier liberación de información por el PCSC de la PNDI o por sus AR vinculadas solamente será permitida mediante autorización formal del titular del certificado. Obtenida la autorización formal, el PCSC de la PNDI o su AR vinculadas no requieren notificar a los titulares de los certificados para usar información privada.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

9.4.6. DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO

El PCSC de la PNDI proporcionará documentos, informaciones o registros bajo su custodia, solamente si existe una orden judicial que lo solicite.

Igualmente, en los procesos sumariales administrativos previa presentación de la solicitud por escrito. Las informaciones a ser divulgadas serán las estrictamente solicitadas.

9.4.7. OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

Este ítem no aplica.

9.4.8. INFORMACIÓN A TERCEROS

El PCSC de la PNDI establece aplicar lo dispuesto en el ítem 9.4.5 de esta DPC, conforme a lo establecido en la normativa vigente.

9.5. DERECHO DE PROPIEDAD INTELECTUAL

El PCSC de la PNDI establece seguir las directivas, según legislación vigente.

9.6. REPRESENTACIONES Y GARANTÍAS

9.6.1. REPRESENTACIONES Y GARANTÍAS DEL PCSC

En el marco de prestación de servicios de creación, verificación y validación de firmas electrónicas cualificadas, el PCSC de la PNDI responderá por el incumplimiento de lo establecido en las Políticas, Declaración de Prácticas de certificación y en la normativa vigente. De igual manera asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la

 TETĀ REKUÁI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

prestación de dichos servicios.

El PCSC declara y garantiza lo siguiente:

9.6.1.1. AUTORIZACIÓN PARA CERTIFICADO

El PCSC de la PNDI implementa procedimientos para verificar la autorización de emisión de un certificado en el marco de la ICPP, contenidos en los ítems 3 y 4 de esta DPC. El PCSC de la PNDI, dentro del alcance de la autorización de emisión de un certificado, analiza, audita e inspecciona los procesos de la AR conforme a sus DPC, PCs y normas complementarias.

9.6.1.2. PRECISIÓN DE LA INFORMACIÓN

El PCSC de la PNDI implementa procedimientos para verificar la veracidad de la información en los certificados, contenidos en los ítems 3 y 4 de esta DPC. A su vez, la AC Raíz-Py, la veracidad de la información contenida en los certificados que emite, analiza, audita e inspecciona los procesos del PCSC y AR conforme a sus DPC, PCs y normas complementarias.

9.6.1.3. IDENTIFICACIÓN DEL SOLICITANTE DEL CERTIFICADO

El PCSC de la PNDI implementa procedimientos para verificar la identificación de los solicitantes de certificados, contenidos en los ítems 3 y 4 de esta DPC. El PCSC de la PNDI, en el ámbito de la identificación del solicitante contenida en los certificados que emite, analiza, audita e inspecciona los procesos de la AR conforme a sus DPC, PCs y normas complementarias.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

9.6.1.4. CONSENTIMIENTO DE LOS TITULARES DE CERTIFICADO

El PCSC de la PNDI implementa un contrato de prestación de servicio de confianza para la expresión del consentimiento del titular de certificado, de conformidad a lo establecido en los puntos 3 y 4 de esta DPC.

9.6.1.5. SERVICIO

El PCSC de la PNDI mantiene acceso las 24x7 a su repositorio con información sobre sus propios certificados, consulta de certificados emitidos y LCRs/OCSP.

9.6.1.6. REVOCACIÓN

El PCSC de la PNDI revocará los certificados de la ICPP por cualquier motivo especificado en este documento.

9.6.1.7. EXISTENCIA LEGAL

La DPC del PCSC de la PNDI se ajusta a las disposiciones de la Ley No 6822/2021 sus modificaciones y reglamentaciones.

9.6.2. REPRESENTACIONES Y GARANTÍAS DE LA AR

Aplica conforme al ítem 4 de esta DPC.

9.6.3. REPRESENTACIONES Y GARANTÍAS DEL TITULAR DEL CERTIFICADO

Toda la información necesaria para la identificación del titular del certificado debe proporcionarse de manera completa y precisa. Al aceptar un certificado emitido por el PCSC de la PNDI, el titular es responsable de toda la información proporcionada por él, contenida en ese certificado.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

El de la PNDI debe informar a la AC Raíz-Py de cualquier compromiso de su clave privada y solicitar la revocación inmediata de su certificado.

9.6.4. REPRESENTACIONES Y GARANTÍAS DE LAS PARTES QUE CONFÍAN

La parte que confía es aquella que confía en el contenido, validez y aplicabilidad del certificado electrónico. Constituyen derechos de los terceros:

- Negarse a utilizar el certificado para fines distintos de los previstos en la PC correspondiente.
- Comprobar, en cualquier momento, la validez del certificado.

Un certificado emitido por un PCSC de la PNDI integrante de la ICPP es considerado válido cuando:

- Ha sido emitido por la AC Raíz-Py;
- No aparece como revocado por la AC Raíz-Py;
- No estuviera expirado; y
- Puede ser verificado utilizando el certificado válido de la AC Raíz-Py.

9.6.5. REPRESENTACIONES Y GARANTÍAS DEL REPOSITORIO.

Este ítem no aplica.

9.7. EXENSIÓN DE GARANTÍA

El PCSC de la PNDI solo responderá en el caso de incumplimiento de las obligaciones contenidas en Ley No 6822/2021, sus modificaciones y reglamentaciones, en la presente DPC y en las Políticas de Certificación específicas.

9.8. LIMITACIONES DE RESPONSABILIDAD LEGAL

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

En este ítem de la DPC, el PCSC de la PNDI en el marco de su actividad como PCSC la limitación de su responsabilidad será conforme a las disposiciones de la Ley No 6822/2021, sus modificaciones y reglamentaciones.

9.9. INDEMNIZACIONES

El PCSC de la PNDI. se encuentra en conformidad a la norma vigente de las condiciones de aplicación y limitaciones considerando las responsabilidades del PCSC de la PNDI.

9.10. PLAZO Y FINALIZACIÓN

9.10.1. PLAZO

Esta DPC empieza a ser efectiva una vez publicada en el sitio de internet del PCSC de la PNDI, previa aprobación del MIC, y los nuevos certificados deben ser emitidos cumpliendo las políticas determinadas en la nueva versión de la DPC.

9.10.2. FINALIZACIÓN

La DPC de la PNDI estará en vigor mientras no se derogue expresamente por la emisión de una nueva versión.

9.10.3. EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

Los actos realizados durante la vigencia de esta DPC son válidos y eficaces a todos los efectos legales, produciendo efectos incluso después de su revocación o sustitución.

9.11. NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

PARTICIPANTES

Las notificaciones, citaciones, solicitudes o cualquier otra comunicación necesaria sujeta a las prácticas descritas en la presente DPC se realizarán, preferentemente, mediante sistema de información firmado o sellado electrónicamente, o, en su defecto, mediante oficio de la autoridad competente.

9.12.ENMIENDAS

9.12.1. PROCEDIMIENTOS PARA ENMIENDAS

Las modificaciones deben documentarse y mantenerse actualizadas a través de versiones.

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

Los cambios en los OIDs corresponden a nuevas políticas que contengan otros objetos con OID adicionales. Si la estructura del certificado se mantiene entonces no es necesario cambiar los OIDs.

9.13.DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

Todas las reclamaciones entre usuarios y el PCSC de la PNDI deberán ser comunicadas por la parte en disputa al PCSC de la PNDI, con el fin de intentar resolverlo entre las mismas partes.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

En el caso de que no se llegue a un acuerdo entre las partes, la resolución de cualquier conflicto que pudiera surgir se someterá a los juzgados y tribunales de la ciudad capital de la República del Paraguay.

La DPC del PCSC de la PNDI no prevalecerá sobre las normas, criterios, prácticas y procedimientos establecidos por el MIC.

9.14. NORMATIVA APLICABLE

El PCSC de la PNDI rige esta DPC bajo la Ley N° 6822/2021, reglamentaciones y la legislación que la sustituya o modifique, así como las demás leyes y normas vigentes en el Paraguay.

9.15. ADECUACIÓN A LA LEY APLICABLE

Esta DPC se adecua a la legislación aplicable y el PCSC de la PNDI se compromete a cumplir y observar las disposiciones previstas en ella.

9.16. DISPOSICIONES VARIAS

9.16.1. ACUERDO COMPLETO

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

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

En caso de conflicto entre esta DPC y otras resoluciones de la AC Raíz-Py, prevalecerá siempre la última editada.

9.16.2. ASIGNACIÓN

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY		
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES		
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	

Los derechos y obligaciones previstos en esta DPC son públicos e indisponibles, y no pueden ser cedidos ni transferidos a terceros.

9.16.3. DIVISIBILIDAD

La invalidez, nulidad o ineficacia de cualquiera de las disposiciones de esta DPC no perjudicará las demás disposiciones, que seguirán siendo plenamente válidas y efectivas. En este caso, la disposición inválida, nula o ineficaz se tendrá por no escrita, por lo que la presente DPC se interpretará como si no la contuviera y, en la medida de lo posible, manteniendo la intención original de las restantes disposiciones.

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

De acuerdo con la legislación vigente.

9.16.5. FUERZA MAYOR

En el contrato de prestación de servicio del PCSC de la PNDI y en ésta DPC se incluyen cláusulas de fuerza mayor para proteger al PCSC conforme a la normativa vigente.

9.17. OTRAS DISPOSICIONES

Este ítem no aplica.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

10. DOCUMENTOS DE REFERENCIA

10.1.REFERENCIA EXTERNA

Los siguientes documentos referenciados son aplicados para la confección de la Declaración de Prácticas de certificación:

- Ley No 6822/2021 “De los servicios de confianza para las transacciones electrónicas, de los documentos electrónicos y los documentos transmisibles electrónicos.”
- RFC 3647: “Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework”.
- RFC 4210: “Internet X.509 Public Key Infrastructure. Certificate Management Protocol (CMP)”.
- RFC 5280: “Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile”.
- RFC 6712: “Internet X.509 Public Key Infrastructure. HTTP Transfer for the Certificate Management Protocol (CMP)”.
- RFC 6960: “X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP”.

 TETĀ REKUĀI MOTENONDEHA MINISTERIO DEL INTERIOR	INFRAESTRUCTURA DE CLAVE PÚBLICA PARAGUAY			
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE TIPO F2 PARA PERSONA FÍSICA del PCSC de la POLICÍA NACIONAL del DEPARTAMENTO DE IDENTIFICACIONES			
	CÓDIGO: DPC-PNDI-V1.2	FECHA: 11/07/2023	versión: 1.2	

- ISO 27002:2022:” - Information technology - Security techniques - Code of practice for information security management”.
- ITU X.500/ISO 9594: “Information technology -
OpenSystemsInterconnection - 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 certificateframeworks”.

10.2.REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	Directivas obligatorias para la formulación y elaboración de la política de certificación de los Prestadores Cualificados de Servicios de Confianza de la ICPP	DOC-ICPP-04
[3]	Procedimiento de identificación del solicitante de certificados por videoconferencia en la ICPP	DOC-ICPP-17
[4]	Características mínimas de seguridad para las autoridades de registro de la ICPP.	DOC-ICPP-05
[5]	Normas de algoritmos criptográficos de la ICPP.	DOC-ICPP-06
[6]	Guía para la acreditación de los organismos de evaluación de la conformidad	DOC-ICPP-11