




CONFIRMA

**POLÍTICA DE CERTIFICACIÓN
DEL PRESTADOR CUALIFICADO
DE SERVICIOS DE CONFIANZA
DE LA ICPP
CONFIRMA S.A.**

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	


CONTROL DOCUMENTAL

NOMBRE DEL ARCHIVO:	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	
CÓDIGO: DOC-PC -CF	VERSIÓN: 1.0
UBICACIÓN FÍSICA: CONFIRMA S.A.	FECHA: 14/04/2023
CLASIFICACION DE SEGURIDAD: Público	

CONTROL DE VERSIONES			
FECHA	VERSION	RESPONSABLES	MOTIVO DE CAMBIO
14/04/2023	1.0	CONFIRMA S.A.	Primera Edición del Documento

DISTRIBUCIÓN DEL DOCUMENTO	
ÁREA	NOMBRES
Personal con Rol de Confianza establecidos en la CPS del PSC de CONFIRMA S.A.	PSC de CONFIRMA S.A.
Documento Público	https://www.confirma.com.py/wp-content/uploads/2023/01/PC_Politica_de_Certificacion_Confirma_SA.pdf


PREPARADO POR:	REVISADO POR:	APROBADO POR:
UANATACA S.A.	CONFIRMA S.A.	CONFIRMA S.A.

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

INDICE


1. INTRODUCCIÓN	10
1.1. DESCRIPCIÓN GENERAL	10
1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO	11
1.3. PARTICIPANTES DE LA PKI	12
1.3.1. AUTORIDADES CERTIFICADORAS (AC)	12
1.3.2. AUTORIDADES DE REGISTRO (AR)	13
1.3.3. AUTORIDADES DE VALIDACIÓN (VA)	14
1.3.4. TITULARES DEL CERTIFICADO	14
1.3.5. PARTE USUARIA	15
1.3.6. OTROS PARTICIPANTES	15
1.4. USO DEL CERTIFICADO	16
1.4.1. USOS APROPIADOS DEL CERTIFICADO	16
1.4.2. USOS PROHIBIDOS DEL CERTIFICADO	16
1.5. ADMINISTRACIÓN DE LA POLÍTICA	16
1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO	16
1.5.2. PERSONA DE CONTACTO	17
1.5.3. PERSONA QUE DETERMINA LA ADECUACION DE LA DPC A LA PC	17
1.5.4. PROCEDIMIENTOS DE APROBACIÓN DE LA PC	17
1.6. DEFINICIONES, SIGLAS Y ACRÓNIMOS	18
1.6.1. DEFINICIONES	18
1.6.2. SIGLAS Y ACRÓNIMOS	26
2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO	29
2.1. REPOSITORIOS	29
2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN	29
2.3. TIEMPO O FRECUENCIA DE PUBLICACIÓN	29
2.4. CONTROLES DE ACCESO A LOS REPOSITORIOS	29
3. IDENTIFICACIÓN Y AUTENTICACIÓN	29
3.1 NOMBRES	29
3.1.1. TIPOS DE NOMBRES	29
3.1.1. NECESIDAD DE NOMBRES SIGNIFICATIVOS	29
3.1.3 ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES	29
3.1.4 REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES	29
3.1.5 UNICIDAD DE NOMBRES	30
3.1.6 PROCEDIMIENTO PARA RESOLVER DISPUTA DE NOMBRE	30
3.1.7 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS ...	30

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY

DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	


3.2 VALIDACIÓN INICIAL DE IDENTIDAD	31
3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA	31
3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA	31
3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA.....	31
3.2.4 INFORMACIÓN NO VERIFICADA DEL TITULAR DEL CERTIFICADO.....	31
3.2.5 VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO).....	31
3.2.6 CRITERIOS PARA INTEROPERABILIDAD	31
3.2.7. PROCEDIMIENTOS COMPLEMENTARIOS.....	31
3.2.8. PROCEDIMIENTOS ESPECIFICOS	31
3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE NUEVAS CLAVES	31
3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN	31
4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO	32
4.1 SOLICITUD DEL CERTIFICADO	32
4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO.....	32
4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES	32
4.2. PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO	32
4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN	32
4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO	32
4.2.3. TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO	32
4.3 EMISIÓN DEL CERTIFICADO	32
4.3.1 ACCIONES DEL PCSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS	32
4.3.2 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO POR PARTE DEL PCSC SOBRE LA EMISION DEL CERTIFICADO	32
4.4. ACEPTACIÓN DEL CERTIFICADO	33
4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO	33
4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PCSC	33
4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR EL PCSC A OTRAS ENTIDADES	33
4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO	33
4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LA PARTE USUARIA	33
4.6 RENOVACIÓN DEL CERTIFICADO	33
4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN	33
4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO	33
4.6.4 NOTIFICACIÓN AL TITULAR SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO ...	33
4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO	33
4.6.6 PUBLICACIÓN POR EL PCSC DEL CERTIFICADO RENOVADO.....	33
4.6.7 NOTIFICACIÓN POR EL PCSC DE LA EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES	34
4.7 RE-EMISIÓN DE CLAVES DE CERTIFICADO (RE-KEY)	34
4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO.....	34
4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA	34

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY

DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA


4.7.3 PROCESAMIENTO DE SOLICITUDES DE RE-EMISIÓN DE CLAVES DE CERTIFICADO	34
4.7.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO SOBRE LA RE-EMISIÓN DE UN NUEVO CERTIFICADO	34
4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE- EMITIDO	34
4.7.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS RE-EMITIDOS	34
4.7.7 NOTIFICACIÓN POR EL PSC DE LA RE-EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES	34
4.8 MODIFICACIÓN DE CERTIFICADOS	34
4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO	34
4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO	34
4.8.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO DE LA EMISIÓN DE UN NUEVO CERTIFICADO	35
4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO	35
4.8.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS MODIFICADOS	35
4.8.7 NOTIFICACIÓN POR EL PCSC DE UNA EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES	35
4.9 REVOCACIÓN Y SUSPENSIÓN	35
4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN	35
4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN	35
4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN	35
4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN	35
4.9.5 TIEMPO DENTRO DEL CUAL EL PCSC DEBE PROCESAR LA SOLICITUD DE REVOCACIÓN	35
4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LA PARTE USUARIA	35
4.9.7 FRECUENCIA DE EMISIÓN DEL LCR	35
4.9.8 LATENCIA MÁXIMA PARA LCR	35
4.9.9 DISPONIBILIDAD PARA REVOCACIÓN/VERIFICACIÓN DE ESTADO EN LÍNEA	35
4.9.10 REQUISITOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA	35
4.9.11 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES	36
4.9.12 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA	36
4.9.13 CIRCUNSTANCIAS PARA SUSPENSIÓN	36
4.9.15 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN	36
4.9.16 LÍMITES DEL PERÍODO DE SUSPENSIÓN	36
4.10 SERVICIOS DE ESTADO DE CERTIFICADO	36
4.10.2 DISPONIBILIDAD DEL SERVICIO	36
4.10.3 CARACTERÍSTICAS OPCIONALES	36
4.11 FIN DE ACTIVIDADES	36
4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES	36
4.12.2 POLÍTICAS Y PRÁCTICAS DE RECUPERACIÓN Y ENCAPSULACIÓN DE CLAVES DE SESIÓN	36
5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES	37
5.1 CONTROLES FÍSICOS	37
5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO	37

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY

DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA


5.1.2 ACCESO FÍSICO	37
5.1.3 ENERGÍA Y AIRE ACONDICIONADO	37
5.1.4 EXPOSICIÓN AL AGUA	37
5.1.6 ALMACENAMIENTO DE MEDIOS.....	37
5.1.8 RESPALDO FUERA DE SITIO	37
5.2 CONTROLES PROCEDIMENTALES	37
5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA	37
5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL	38
5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES	38
5.3. CONTROLES DE PERSONAL.....	38
5.3.1. REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN	38
5.3.2. PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES	38
5.3.3. REQUERIMIENTOS DE CAPACITACIÓN	38
5.3.4. REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN.....	38
5.3.5. FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES	38
5.3.6. SANCIONES PARA ACCIONES NO AUTORIZADAS	38
5.3.7. REQUISITOS DE CONTRATACIÓN A TERCEROS	38
5.3.8. DOCUMENTACIÓN SUMINISTRADA AL PERSONAL	38
5.4. PROCEDIMIENTO DE REGISTRO DE AUDITORÍA	38
5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)	38
5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA	38
5.4.5. PROCEDIMIENTOS DE RESPALDO (BACKUP) DE REGISTRO (LOGS) DE AUDITORÍA	38
5.4.6. SISTEMA DE RECOLECCIÓN DE INFORMACIÓN DE AUDITORÍA (INTERNO VS EXTERNO)	38
5.4.7. NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO	39
5.4.8. EVALUACIÓN DE VULNERABILIDADES.....	39
5.5.2. PERIODOS DE RETENCIÓN PARA ARCHIVOS.....	39
5.5.3 PROTECCIÓN DE ARCHIVOS.....	39
5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO	39
5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS	39
5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO)	39
5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA	39
5.6 CAMBIO DE CLAVE	39
5.7. RECUPERACIÓN DE DESASTRES Y COMPROMISO.....	39
5.7.1. PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO	39
5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES	39
5.7.3. PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD	39
5.7.4. CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE	40
5.8. EXTINCIÓN DE UN PCSC O ENTIDADES VINCULADAS.....	40
6. CONTROLES TÉCNICOS DE SEGURIDAD.....	41
6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES	41
6.1.1. GENERACIÓN DEL PAR DE CLAVES	41
6.1.2. ENTREGA DE LA CLAVE PRIVADA AL SUScriptor	43

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY

DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA


6.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO	43
6.1.4. ENTREGA DE LA CLAVE PÚBLICA DEL PCSC A LA PARTE USUARIA	43
6.1.5. TAMAÑO DE LA CLAVE	44
6.1.6. GENERACIÓN DE PARÁMETROS DE CLAVE ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD	44
6.1.7. PROPÓSITOS DE USOS DE CLAVE (CAMPO KEY USAGE EN X.509 V3)	45
6.2. CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO Y PROTECCIÓN DE LA CLAVE PRIVADA	45
6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO	45
6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA	45
6.2.3 CUSTODIA (ESCROW) DE LA CLAVE PRIVADA	45
6.2.4. RESPALDO/COPIA DE LA CLAVE PRIVADA	46
6.2.5. ARCHIVADO DE LA CLAVE PRIVADA	47
6.2.6. TRANSFERENCIA DE CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRIPTOGRÁFICO	47
6.2.7. ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO	47
6.2.8. MÉTODO DE ACTIVACIÓN DE CLAVE PRIVADA	47
6.2.9. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA	47
6.2.10. MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA	48
6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES	48
6.3.1. ARCHIVO DE LA CLAVE PÚBLICA	48
6.3.2. PERÍODO OPERACIONAL DEL CERTIFICADO Y PERÍODO DE USO DEL PAR DE CLAVES	48
6.4 DATOS DE ACTIVACIÓN	49
6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN	49
6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN	50
6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN	50
6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR	50
6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS	50
6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR	50
6.5.3. CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO	50
6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA	50
6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA	50
6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD	51
6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA	51
6.6.4. CONTROLES EN LA GENERACIÓN DE LCR	51
6.7 CONTROLES DE SEGURIDAD DE RED	51
6.7.1. DIRECTRICES GENERALES	51
6.7.2. FIREWALL	51
6.7.3. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)	51
6.7.4. REGISTRO DE ACCESO NO AUTORIZADO A LA RED	51
6.8. FUENTES DE TIEMPO	51
7. PERFILES DE CERTIFICADOS, CRL Y OCSP	51
7.1. PERFIL DEL CERTIFICADO	52
7.1.1. NÚMERO DE VERSIÓN	52

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY


DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

7.1.2. EXTENSIONES DEL CERTIFICADO	52
7.1.3. IDENTIFICADORES DE OBJETO DE ALGORITMOS	56
7.1.4. FORMAS DEL NOMBRE	56
7.1.5. RESTRICCIONES DEL NOMBRE	57
7.1.6. IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO	59
7.1.7. USO DE LA EXTENSIÓN RESTRICCIONES DE POLÍTICA (POLICY CONSTRAINTS)	59
7.1.8. SEMÁNTICA Y SINTAXIS DE LOS CALIFICADORES DE POLÍTICA (POLICY QUALIFIERS)	60
7.1.9. SEMÁNTICA DE PROCESAMIENTO PARA LA EXTENSIÓN DE POLÍTICAS DE CERTIFICADO (CERTIFICATE POLICIES)	60
7.2. PERFIL DE LA LCR.....	60
7.2.1 NÚMERO (S) DE VERSIÓN	60
7.2.2 CRL Y EXTENSIONES DE ENTRADAS DE CRL.....	60
7.3. PERFIL DE OCSP.....	61
7.3.1. NÚMERO (S) DE VERSIÓN	61
7.3.2. EXTENSIONES DE OCSP.....	61
8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES	62
8.1. FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN.....	62
8.2. IDENTIFICACIÓN/CALIFICACIÓN DEL EVALUADOR.....	62
8.3. RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA	62
8.4. ASPECTOS CUBIERTOS POR LA EVALUACIÓN.....	62
8.5. ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA	62
8.6. COMUNICACIÓN DE RESULTADOS	62
9. OTROS ASUNTOS LEGALES Y COMERCIALES.....	63
9.1. TARIFAS	63
9.1.1. TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS	63
9.1.1.1. TARIFAS DE ACCESO A CERTIFICADOS	63
9.1.1.2. TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN	63
9.1.1.3. TARIFAS POR OTROS SERVICIOS.....	63
9.1.1.4. POLÍTICAS DE REEMBOLSO.....	63
9.1.2. RESPONSABILIDAD FINANCIERA	64
9.2.1. COBERTURA DE SEGURO	64
9.2.1.1. OTROS ACTIVOS.....	64
9.2.1.2. COBERTURA DE SEGURO O GARANTÍA PARA USUARIOS FINALES	64
9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL.....	64
9.3.1. ALCANCE DE LA INFORMACIÓN CONFIDENCIAL	64
9.3.2. INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL	64
9.3.3. RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL.....	64

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY

DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

9.4. PRIVACIDAD DE INFORMACIÓN PERSONAL	64
9.4.3. INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA	64
9.4.4. RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA	65
9.4.5. NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA	65
9.4.6. DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO	65
9.4.7. OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN	65
9.4.8. INFORMACIÓN A TERCEROS	65
9.4. DERECHO DE PROPIEDAD INTELECTUAL	65
9.6.1.1. AUTORIZACION PARA CERTIFICADO	66
9.6.1.2. PRECISIÓN DE LA INFORMACION	66
9.6.1.3. IDENTIFICACION DEL SOLICITANTE	66
9.6.1.4. CONSENTIMIENTO DE LOS TITULARES DEL CERTIFICADO	66
9.6.1.5. SERVICIO	66
9.6.1.6. REVOCACION	66
9.6.5. REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES	66
9.7. EXENCIÓN DE GARANTÍA	66
9.10. PLAZO Y FINALIZACIÓN.....	66
9.10.1 PLAZO	66
9.10.2. FINALIZACIÓN	67
9.10.3. EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA	67
9.11. NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES	67
9.12. ENMIENDAS.....	67
9.12.2. PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN	67
9.12.3. CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS.....	67
9.13. DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS	68
9.15. ADECUACIÓN A LA LEY APLICABLE	68
9.16. DISPOSICIONES VARIAS	68
9.16.1 ACUERDO COMPLETO	68
9.16.2. ASIGNACIÓN	68
9.16.3. DIVISIBILIDAD	68
9.16.4. APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DE DERECHOS) ...	68
9.16.5. FUERZA MAYOR.....	68
10.1 REFERENCIAS EXTERNAS.....	69
10.2. REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP.....	69
10.3. INDICE DE TABLAS	70

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

1. INTRODUCCIÓN

1.1. DESCRIPCIÓN GENERAL

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


Toda Política de Certificación elaborada en el ámbito de la Infraestructura de Clave Pública del Paraguay (ICPP) debe obligatoriamente adoptar la misma estructura empleada en el documento DOC -ICPP-04 VERSION 1.0

La estructura de esta PC se basa en lo estipulado en la Resolución MIC No 811/2022 DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA POLÍTICA DE CERTIFICACIÓN DE LOS PCSC DE LA ICPP, DOC-ICPP-04, Versión 1.0.

Esta PC es aplicable a los siguientes certificados:

- Certificado Cualificado de Firma Electronica:
 - F2
 - F3

Los tipos de certificados “F” o “S” definen escalas de seguridad (1, 2 y 3), asociados con requisitos menos o más estrictos atendiendo al tipo de certificado. El nivel de seguridad estará caracterizado por los requisitos mínimos definidos para aspectos como: algoritmo y tamaño de la clave

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

criptográfica, medios de almacenamiento de clave, proceso de generación del par de claves, procedimiento de identificación del titular del certificado, frecuencia de emisión de la lista de certificados revocados (LCR) y el plazo de validez del certificado.

El par de claves criptográficas relacionadas al tipo de certificado F2 y S2 deberá obligatoriamente ser generados y almacenados en módulos criptográficos tipo hardware en un:

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


El par de claves criptográficas relacionadas a los tipos de certificado F3 y S3 deberá obligatoriamente ser generado y almacenado en módulos criptográficos tipo hardware gestionado y custodiado por un PCSC en un:

- o módulo de seguridad hardware (HSM).

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

1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Nombre del Documento	Política de certificación del Prestador Cualificado de Servicios de Confianza
Versión del Documento	V1.0

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

Fecha de Aprobación	14/04/23
OID (Object Identifier):	1.3.6.1.4.1.58404.1.1.1.1
Ubicación de la PC	https://www.confirma.com.py/wp-content/uploads/2023/01/PC_Politica_de_Certificacion_Confirma_SA.pdf
Ubicación de la DPC relacionada	https://www.confirma.com.py/wp-content/uploads/2023/01/Declaracion_de_practicass_de_certificacion_Confirma_SA.pdf


1.3. PARTICIPANTES DE LA ICPP

1.3.1. AUTORIDADES CERTIFICADORAS (AC)

Esta PC se refiere exclusivamente al PCSC CONFIRMA S.A. El PCSC CONFIRMA S.A. 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-Raíz-Py y solo podrá emitir certificados a usuarios finales. El PCSC CONFIRMA S.A. es considerada una ACI.

CONFIRMA S.A. presta servicios de CREACIÓN, VERIFICACIÓN Y VALIDACIÓN DE FIRMAS ELECTRÓNICAS CUALIFICADAS y CERTIFICADOS RELATIVOS A ESTOS SERVICIOS.

Además, CONFIRMA S.A. se encuentra habilitado para prestar servicios de GENERACIÓN O GESTIÓN DE DATOS DE CREACIÓN DE FIRMA ELECTRÓNICA EN NOMBRE DEL FIRMANTE en los términos establecidos en el documento DOC-ICPP-07 [2].

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

CONFIRMA S.A., habilitado para brindar servicios de GENERACIÓN O GESTIÓN DE DATOS DE CREACIÓN DE FIRMA ELECTRÓNICA EN NOMBRE DEL FIRMANTE, utiliza sistemas y productos fiables, incluidos canales de comunicación electrónicos seguros, aplicar procedimientos y mecanismos técnicos y organizativos adecuados para garantizar que el entorno sea confiable y que los datos de creación de firma se utilicen bajo el control exclusivo del titular del certificado. Además, custodia y protege los datos de creación de firma frente a cualquier alteración, destrucción o acceso no autorizado, así como garantiza su continua disponibilidad.


Las claves privadas de los firmantes almacenadas en dispositivos estandarizados conforme lo establecido en el documento DOC-ICPP-06 [3], y las firmas electrónicas cualificadas hechas por la clave privada del firmante en otros sistemas son válidas de conformidad a la Ley N.º 6822/2021.

1.3.2. AUTORIDADES DE REGISTRO (AR)

La AR puede ser propia del PCSC 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 a un PCSC mediante un acuerdo operacional.

Los datos referentes a las AR habilitadas por COMFIRMA S.A. 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)

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

<https://www.confirma.com.py/autoridades-de-registro/>

El PCSC de CONFIRMA S.A. mantiene publicada en el sitio principal de internet las siguientes informaciones actualizadas.

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

1.3.3. AUTORIDADES DE VALIDACIÓN (AV)

La AV puede ser una entidad propia o externa al PCSC de CONFIRMA S.A. responsable de suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una AR y certificados por el PCSC.

Las informaciones actualizadas sobre:


- Lista de todas las Avs Habilitadas
- Lista de las AVs que se han inhabilitado por el PCSC de Confirma S.A. indicando su fecha de inhabilitación.

Se encuentran en la dirección de página web (URL):

<https://www.confirma.com.py/autoridades-de-validacion/>

1.3.4. TITULARES DEL CERTIFICADO

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

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

1.3.5. PARTE USUARIA

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

1.3.6. OTROS PARTICIPANTES

1.3.6.1. PRESTADORES DE SERVICIOS DE SOPORTE (PSS)


Las PSS son entidades externas a las que recurre la AC o la AR de CONFIRMA S.A. para desempeñar actividades descritas en esta PC o en una DPC y se clasifican en tres categorías, conforme al tipo de actividades prestadas.

- a) disponibilización de infraestructura física y lógica;
- b) disponibilización de recursos humanos especializados; y
- c) disponibilización de infraestructura física y lógica y de recursos humanos especializados.

Las informaciones actualizadas de las PSS a la que recurre el PCSC de CONFIRMA S.A. se encuentran en la dirección de página web (URL): <https://www.confirma.com.py/prestadores-de-servicios-de-soporte/>

El funcionamiento de un PSS vinculado al PCSC de CONFIRMA S.A. se realiza mediante un acuerdo operacional, el cual es autorizado por la AC Raíz-Py con la habilitación correspondiente.

El PCSC de CONFIRMA S.A. también publica en su sitio web información referente a:

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

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

1.4. USO DEL CERTIFICADO

1.4.1. USOS APROPIADOS DEL CERTIFICADO

Las aplicaciones y otros programas que soporten el uso de un certificado electrónico de cierto tipo contemplado por la ICPP aceptan cualquier certificado del mismo tipo, o superior, emitido por el PCSC de CONFIRMA S.A.

El PCSC CONFIRMA S.A. tiene en cuenta el nivel de seguridad proporcionado para el certificado definido por esta PC en la definición de aplicaciones para el certificado, conforme a lo estipulado en el ítem 1.1.

Certificados de los tipos F2, F3 serán utilizados en aplicaciones como confirmación de identidad y firma de documentos electrónicos con verificación de integridad de sus informaciones.


1.4.2. USOS PROHIBIDOS DEL CERTIFICADO

Los certificados emitidos por el PCSC de CONFIRMA S.A. deben ser utilizados dentro del marco de la normativa vigente que rige la materia. Cualquier otro uso de los certificados no especificado en esta PC y en la normativa vigente, está fuera del alcance y responsabilidad de esta PC.

1.5. ADMINISTRACIÓN DE LA POLÍTICA

1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre del PSC: CONFIRMA S.A.

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

Dirección: Ruiz Díaz de Melgarejo Nro. 985 c/ Antonio Taboada

Teléfono: (+595 21) 218 0 218

Página web: <https://www.confirma.com.py/>

E-mail: info@confirma.com.py

1.5.2.PERSONA DE CONTACTO

Nombre: GERENTE DE CONFIRMA S.A.

Teléfono: (+595 21) 218 0 218

Página web: <https://www.confirma.com.py/>

E-mail: info@confirma.com.py

Dirección: Ruiz Díaz de Melgarejo Nro. 985 c/ Antonio Taboada

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

Nombre: GERENTE DE CONFIRMA S.A.

Teléfono: (+595 21) 218 0 218


Página web: <https://www.confirma.com.py/>

E-mail: info@confirma.com.py

Dirección: Ruiz Díaz de Melgarejo Nro. 985 c/ Antonio Taboada

1.5.4.PROCEDIMIENTOS DE APROBACIÓN DE LA CP

Los procedimientos para la aprobación de CP del PCSC DE CONFIRMA S.A. son establecidos a criterio de AC Raíz-Py de la ICPP.


INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

1.6. DEFINICIONES, SIGLAS Y ACRÓNIMOS

1.6.1. DEFINICIONES

- **Agente de registro:** persona responsable de la realización de las actividades inherentes a la AR. Realiza la identificación de los solicitantes en la solicitud de emisión/revocación de certificados de firma electrónica cualificada o sello electrónico cualificado.
- **Autenticación:** proceso técnico que permite determinar la identidad de la persona física o jurídica.
- **Autoridad de Aplicación:** Ministerio de Industria y Comercio a través de la Dirección General de Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.
- **Autoridad de Certificación:** entidad que presta servicios de emisión, gestión, revocación u otros servicios de confianza basados en certificados cualificados. En el marco de la ICPP, son Autoridades de Certificación, la AC Raíz-Py y el PCSC.
- **Autoridad de Certificación Raíz del Paraguay:** órgano técnico, cuya función principal es coordinar el funcionamiento de la ICPP. La AC Raíz-Py tiene los certificados de más alto nivel, posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza. Las funciones de la AC Raíz-Py son ejercidas por la AA.
- **Autoridad de Certificación Intermedia:** entidad cuyo certificado ha sido emitido por la AC Raíz-Py, es responsable de la emisión de certificados cualificados a personas físicas y jurídicas. Un Prestador cualificado de Servicios de Confianza es considerado una Autoridad de Certificación Intermedia.
- **Autoridad de Registro:** entidad responsable de tramitar las distintas solicitudes inherentes a certificados cualificados, identificar al


INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY

DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

solicitante y remitir las solicitudes al PCSC. La AR puede ser propia del PCSC o delegada a un tercero.


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

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY


DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

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

- **Cifrado:** es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido de manera que sólo pueda leerlo la persona que disponga de la clave del cifrado adecuada para decodificarla.
- **Contrato de prestación de servicio de confianza:** Acuerdo entre la AC Raíz-Py y el PCSC, o entre el PCSC y el titular o responsable del certificado que contiene información relativa al solicitante del certificado y además establece los derechos, obligaciones y responsabilidades de las partes con respecto a la prestación del servicio. Este contrato, requiere la aceptación explícita de las partes intervinientes.
- **Claves criptográficas:** valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.
- **Clave pública y privada:** la criptografía en la que se basa la ICPP, es la criptografía asimétrica. En ella, se emplean un par de claves: lo que se cifra con una de ellas, sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y está incorporada en el certificado electrónico, mientras que a la otra se le denomina privada y está bajo exclusivo control del titular o responsable del certificado.
- **Compromiso:** violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.
- **Datos de activación:** valores de los datos, distintos al par de claves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos.


INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

- **Declaración de Prácticas de Certificación:** documento en el cual se determina la declaración de las prácticas que emplea una AC al emitir certificados y que define la infraestructura, políticas y procedimientos que utiliza la AC para satisfacer los requisitos especificados en la PC vigente.
- **Documento de identidad:** documento válido y vigente que permite acreditar la identidad de la persona, a los efectos del proceso de emisión, suspensión o revocación del certificado cualificado electrónico será considerada la cédula de identidad civil o el pasaporte del solicitante.
- **Emisor del certificado:** persona física o jurídica cuyo nombre aparece en el campo emisor de un certificado.
- **Emisión de certificado:** es la autorización de la emisión del certificado en el sistema del PCSC previa comprobación de la concordancia de los datos de solicitud del certificado con los contenidos en los documentos presentados.
- **Firma electrónica cualificada:** una firma electrónica que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica, la cual deberá estar vinculada al firmante de manera única, permitir la identificación del firmante, haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo y estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.
- **Firmante:** una persona física que crea una firma electrónica.
- **Generador:** máquina encargada de generar electricidad a partir de un motor de gasolina o diésel. La instalación de este equipo

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	


deberá ser de tal forma que, al interrumpirse el suministro de energía eléctrica del proveedor externo, el mismo debe arrancar automáticamente tomando la carga de las instalaciones del data center de la AC, incluyendo los circuitos de iluminación, de los equipos informáticos, equipos de refrigeración, circuitos de monitoreo, prevención de incendios; en fin de todos los circuitos eléctricos críticos para el funcionamiento de las instalaciones tecnológicas.

- **Habilitación:** autorización que otorga el MIC, una vez cumplidos los requisitos y condiciones establecidos en la norma.
- **Identificador de Objeto:** sistema de identificación para entidades físicas o virtuales basado en una estructura arbórea de componentes de identificación. El árbol de OID se define plenamente en las Recomendaciones UIT-T y las normas internacionales ISO.
- **Identificación del Titular de certificado:** comprende la etapa de la confirmación de la identidad de una persona física o jurídica, realizada a través de la presencia física del interesado o mediante otros medios que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, conforme a los supuestos establecidos en la Ley y en base a los documentos de identificación previstos en la presente DPC.
- **Infraestructura de Claves Públicas del Paraguay:** conjunto de personas, normas, leyes, políticas, procedimientos y sistemas informáticos necesarios para proporcionar una plataforma criptográfica de confianza que garantiza la presunción de validez legal para actos electrónicos firmados o cifrados con certificados electrónicos cualificados y claves criptográficas emitidas por esta infraestructura.


INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

- **Integridad:** característica que indica que un mensaje de datos o un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.
- **Lista de Certificados Revocados:** lista emitida por una AC, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.
- **Lista de Confianza:** Lista publicada en el sitio web oficial de la AC Raíz - Py y que contiene información relativa a los Prestadores cualificados de servicios de confianza y a los servicios cualificados que éstos prestan conforme a la Ley No 6822/21.
- **Módulo criptográfico:** software o hardware criptográfico que genera y almacena claves criptográficas.
- **Módulo de Seguridad de Hardware:** dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.
- **Normas Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la prestación de los servicios mencionados en la presente DPC.
- **Organismo de Evaluación de Conformidad:** organismo que desempeña actividades de evaluación de la conformidad a un prestador de servicios de confianza y de los servicios de confianza que este presta conforme a la Ley No 6822/2021.
- **Organismo de Supervisión:** organismo que concede y retira la cualificación a los prestadores de servicios de confianza y a los servicios de confianza que prestan además de las funciones establecidas en el artículo 17 de la Ley No 6822/2021.
- **Parte usuaria:** persona física o jurídica que confía en el servicio de confianza.


INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY

DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

- **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 cual es suficiente para permitir la reconstrucción, revisión e inspección de la secuencia de los ambientes y de las actividades que rodean o que conducen a cada acontecimiento en la ruta de una transacción desde su inicio hasta la salida de los resultados finales.
- **Repositorio:** sitio principal de Internet confiable y accesible, mantenido por la AC con el fin de difundir su información pública.

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

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


INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

- **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. SIGLAS Y ACRÓNIMOS


Sigla/Acrónimo	Descripción
AA	Autoridad de Aplicación
AGR	Agente de Registro
P	País (C por su sigla en inglés, Country)
AC	Autoridad de Certificación (CA por sus siglas en inglés, Certificate Authority)
ACI	Autoridad de Certificación Intermedia (CAI por sus siglas en inglés, Certificate Authority Intermediate)
AC Raíz-Py	Autoridad Certificadora Raíz del Paraguay
CI	Cédula de identidad civil
NC	Nombre Común (CN por sus siglas en inglés, Common Name)
PC	Políticas de Certificación (CP por sus siglas en inglés, Certificate Policy)
DPC	Declaración de Prácticas de Certificación (DPC por sus siglas en inglés, Certification Practice Statement)
LCR	Lista de certificados revocados (CRL por sus siglas en inglés, Certificate Revocation List)

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY


DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

CSR	Solicitud de firma de Certificado (CSR por sus siglas en inglés, certificate Signing Request)
DGCE	Dirección General de Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.
HSM	Módulo de Seguridad Criptográfico basado en Hardware (HSM por sus siglas en inglés, Hardware Security Module)
ISO	Organización Internacional para la Estandarización (ISO por sus siglas en inglés, International Organization for Standardization).
MIC	Ministerio de Industria y Comercio
O	Organización (por su sigla en inglés, Organization)
OCSP	Servicio de validación de certificados en línea (OCSP por sus siglas en inglés, Online Certificate Status Protocol)
OID	Identificador de Objeto (OID por sus siglas en inglés, Object Identifier)
OU	Unidad Organizacional (OU por sus siglas en inglés, Organization Unit)
PAS	Pasaporte
ICPP	Infraestructura de Clave Pública del Paraguay
PCSC	Prestador cualificado de servicios de confianza
PSS	Prestador de Servicios de Soporte
Py	Paraguay
AR	Autoridad de Registro (RA por sus siglas en inglés, Registration Authority).
RFC	Petición de Comentarios (RFC por sus siglas en inglés, Request For Comments)

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY

DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

RUC	Registro único del contribuyente
URL	Localizador uniforme de recursos (URL por sus siglas en inglés, Uniform Resource Locator)
AV	Autoridad de validación (AV por sus siglas en inglés, Validation Authority)

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

En los apartados siguientes son referidos a los ítems correspondientes de la DPC del PCSC CONFIRMA S.A. o son detallados los aspectos específicos para la PC, si los hubiere.

2.1. REPOSITORIOS

2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

2.3. TIEMPO O FRECUENCIA DE PUBLICACIÓN

2.4. CONTROLES DE ACCESO A LOS REPOSITORIOS

3. IDENTIFICACIÓN Y AUTENTICACIÓN


3.1 NOMBRES

3.1.1. TIPOS DE NOMBRES

3.1.2. NECESIDAD DE NOMBRES SIGNIFICATIVOS

3.1.3. ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES


3.1.4. REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

3.1.5. UNICIDAD DE NOMBRES

3.1.6 PROCEDIMIENTO PARA RESOLVER DISPUTA DE NOMBRE

3.1.7 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

3.2 VALIDACIÓN INICIAL DE IDENTIDAD

3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA

3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA

3.2.4 INFORMACIÓN NO VERIFICADA DEL TITULAR DEL CERTIFICADO

3.2.5 VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)

3.2.6 CRITERIOS PARA INTEROPERABILIDAD

3.2.7. PROCEDIMIENTOS COMPLEMENTARIOS


3.2.8. PROCEDIMIENTOS ESPECIFICOS

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA

SOLICITUDES DE NUEVAS CLAVES

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA

SOLICITUDES DE REVOCACIÓN

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

En los apartados siguientes son referidos a los ítems correspondientes de la DPC del PCSC de CONFIRMA S.A. o son detallados los aspectos específicos para la CP, si los hubiere.

4.1 SOLICITUD DEL CERTIFICADO

4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

4.2. PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN


4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

4.2.3. TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO

4.3 EMISIÓN DEL CERTIFICADO

4.3.1 ACCIONES DEL PCSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS

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

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PCSC

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

4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

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

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

4.6 RENOVACIÓN DEL CERTIFICADO

4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO


4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN

4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO

4.6.4 NOTIFICACIÓN AL TITULAR SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO

4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO

4.6.6 PUBLICACIÓN POR EL PCSC DEL CERTIFICADO RENOVADO

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

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

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

4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO

4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA

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

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

4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE- EMITIDO

4.7.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS RE-EMITIDOS


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

4.8 MODIFICACIÓN DE CERTIFICADOS

4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO

4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

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

4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

4.8.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS MODIFICADOS

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

4.9 REVOCACIÓN Y SUSPENSIÓN

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN

4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

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


4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LA PARTE USUARIA

4.9.7 FRECUENCIA DE EMISIÓN DEL LCR

4.9.8 LATENCIA MÁXIMA PARA LCR

4.9.9 DISPONIBILIDAD PARA REVOCACIÓN/VERIFICACIÓN DE ESTADO EN LÍNEA

4.9.10 REQUISITOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

4.9.11 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES

4.9.12 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA

4.9.13 CIRCUNSTANCIAS PARA SUSPENSIÓN

4.9.14 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

4.9.15 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

4.9.16 LÍMITES DEL PERÍODO DE SUSPENSIÓN

4.10 SERVICIOS DE ESTADO DE CERTIFICADO

4.10.1 CARACTERÍSTICAS OPERACIONALES

4.10.2 DISPONIBILIDAD DEL SERVICIO


4.10.3 CARACTERÍSTICAS OPCIONALES

4.11 FIN DE ACTIVIDADES

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

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

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

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

En los apartados siguientes son referidos a los ítems correspondientes de la DPC del PCSC responsable o ser detallados los aspectos específicos para la PC, si los hubiere

5.1 CONTROLES FÍSICOS

5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

5.1.2 ACCESO FÍSICO

5.1.2.1 NIVELES DE ACCESO FÍSICO

5.1.2.2 SISTEMAS FÍSICOS DE DETECCIÓN

5.1.2.3 SISTEMAS DE CONTROL DE ACCESO

5.1.2.4 MECANISMOS DE EMERGENCIA

5.1.3 ENERGÍA Y AIRE ACONDICIONADO

5.1.4 EXPOSICIÓN AL AGUA

5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

5.1.6 ALMACENAMIENTO DE MEDIOS


5.1.7 ELIMINACIÓN DE RESIDUOS

5.1.8 RESPALDO FUERA DE SITIO

5.2 CONTROLES PROCEDIMENTALES

5.2.1 ROLES DE CONFIANZA

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES

5.3. CONTROLES DE PERSONAL

5.3.1. REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

5.3.2. PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

5.3.3. REQUERIMIENTOS DE CAPACITACIÓN

5.3.4. REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

5.3.5. FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

5.3.6. SANCIONES PARA ACCIONES NO AUTORIZADAS

5.3.7. REQUISITOS DE CONTRATACIÓN A TERCEROS

5.3.8. DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

5.4. PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

5.4.1 TIPOS DE EVENTOS REGISTRADOS


5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)

5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

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

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

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

5.4.7. NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

5.4.8. EVALUACIÓN DE VULNERABILIDADES

5.5. ARCHIVOS DE REGISTROS

5.5.1. TIPOS DE REGISTROS ARCHIVADOS

5.5.2. PERIODOS DE RETENCIÓN PARA ARCHIVOS

5.5.3 PROTECCIÓN DE ARCHIVOS

5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO

5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO)

5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA


5.6 CAMBIO DE CLAVE

5.7. RECUPERACIÓN DE DESASTRES Y COMPROMISO

5.7.1. PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO

5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES

5.7.3. PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD


INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

5.7.3.1 CERTIFICADO DE ENTIDAD ES REVOCADO

5.7.3.2 CLAVE DE ENTIDAD ESTÁ COMPROMETIDA

5.7.4. CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

5.8. EXTINCIÓN DE UN PCSC O ENTIDADES VINCULADAS

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

6. CONTROLES TÉCNICOS DE SEGURIDAD

En los siguientes ítems, la PC define las medidas de seguridad necesarias para proteger las claves criptográficas de los titulares de certificados emitidos según la CP. También son definidos otros controles técnicos de seguridad utilizados por el PCSC de CONFIRMA S.A.y por las ARs a ella vinculadas para la ejecución de sus funciones operativas.

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES


6.1.1. GENERACIÓN DEL PAR DE CLAVES

Cuando el titular del certificado sea:

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

El algoritmo para utilizar las claves criptográficas de titulares de certificados, está definido conforme al documento DOC-ICPP-06(1)

Cuando es generada, la clave privada del titular del certificado deberá ser cifrada mediante un algoritmo simétrico conforme al documento DOC-ICPP-06 [1], en un medio de almacenamiento definido para cada tipo de certificado previsto en la ICPP conforme a lo estipulado en la Tabla N° 2 de este ítem.

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

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


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

- a) la confidencialidad de las claves privadas utilizadas para la creación de firmas electrónicas, esté garantizada razonablemente .
- b) las claves privadas utilizadas para la creación de firma electrónica sólo puedan aparecer una vez en la practica.
- c) exista la seguridad razonable de que claves privadas utilizadas para la creación de firma electrónica no pueden ser hallados por deducción y de que la firma está protegido con seguridad contra la falsificación mediante las tecnologías disponibles en el momento.
- d) las claves privadas utilizadas para la creación de firma electrónica electrónico puedan ser protegidas por el firmante legítimo de forma fiable frente a su utilización por otros.

Estos medios de almacenamiento de claves privadas no alteraran los datos que deben firmarse o sellarse ni impedirán que dichos datos se muestren al firmante o creador del antes de firmar o sellar.

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

Tabla N° 2 – Medio de almacenamiento de claves criptográficas.

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

TIPO DE CERTIFICADO	MEDIO DE ALMACENAMIENTO
F2	<ul style="list-style-type: none"> Hardware criptográfico certificado por el MIC (Tarjeta inteligente o token con capacidad de generación de claves).
F3	<ul style="list-style-type: none"> Hardware criptográfico certificado por el MIC (HSM)


6.1.2. ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR

Para el caso de claves privadas asociadas a certificados de los tipos F2 la clave es generada en el dispositivo criptográfico al momento de la emisión y el titular es responsable de este. Del mismo modo, las claves privadas asociadas a los certificados de los tipos F3 son generadas en un dispositivo de creación de firma bajo el control exclusivo del titular o responsable del certificado, en el cual quedarán custodiadas por el PCSC CONFIRMA S.A. para su gestión, por tanto, no existe entrega alguna de la clave privada al titular o responsable del certificado.

6.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

La clave pública generada bajo control del usuario final es entregada al PCSC CONFIRMA S.A mediante el envío de una solicitud de firma de certificado (CSR) que concuerda con la especificación del

PKCS#10, firmado con la clave privada correspondiente a la clave pública que se solicita certificar.

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

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

La clave pública del PCSC de CONFIRMA S.A. está a disposición de la parte usuaria (ver apartado 2.1)

Las formas para la entrega de un certificado emitido por el PCSC de CONFIRMA S.A. podrá comprender, entre otras:


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

6.1.5. TAMAÑO DE LA CLAVE

Los algoritmos y tamaños de clave a ser utilizados por el PCSC de CONFIRMA S.A. en los diferentes tipos de certificados emitidos en el marco de la ICPP , se definen en el documento DOC-ICPP-06 [3].

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

Los parámetros de generación y verificación de calidad de claves asimétricas de las personas físicas titulares de certificados, adoptarán el estándar definido en el documento DOC-ICPP-06 [3].

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

6.1.7. PROPÓSITOS DE USOS DE CLAVE (CAMPO KEY USAGE EN X.509 V3)

Conforme a lo establecido en la DPC de Confirma S.A

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

En los apartados siguientes, la PC del PCSC debe define los requisitos para la protección de las claves privadas de los titulares de certificados emitidos según su PC.

6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO

Los estándares requeridos para los módulos de generación de las claves criptográficas, son de conformidad con las normas establecidas en el documento DOC-ICPP-06 [3].


Los requisitos aplicables al módulo criptográfico utilizado para almacenar la clave privada del titular o responsable del certificado. Pueden indicarse estándares de referencia, observando los estándares definidos en el documento DOC- ICPP-06 [3].

6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA

Ítem no aplicable.

6.2.3 CUSTODIA (ESCROW) DE LA CLAVE PRIVADA

Las claves privadas correspondientes a los certificados de los tipos F3 expedidos a usuarios finales, deberán estar custodiadas en módulos

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

criptográficos administrados por el PCSC de CONFIRMA S.A. conforme a lo establecido en el documento DOC-ICPP-07 [2], de forma que únicamente el firmante pueda acceder a su clave privada. El acceso deberá quedar garantizado mediante el uso de 2 (dos) factores de autenticación

6.2.4. RESPALDO/COPIA DE LA CLAVE PRIVADA


Cualquier titular de un certificado, a su criterio, puede mantener una copia de su propia clave privada.

El PCSC de CONFIRMA S.A. no puede conservar una copia de seguridad de la clave privada asociada a los certificados de tipo F2.

Sin perjuicio del inciso d) del ítem 6.1.1, los PCSC de CONFIRMA S.A. podrá duplicar las claves privadas asociadas a los certificados de los tipos F3 conforme a lo establecido en el documento DOC-ICPP-07 [2], únicamente con el objeto de efectuar una copia de seguridad de las citadas claves siempre que se cumplan los siguientes requisitos:

- a)** la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales.
- b)** el número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio.

En cualquier caso, la copia de seguridad debe almacenarse cifrada mediante un algoritmo simétrico aprobado por el documento DOC-ICPP-06 [1] y protegida con un nivel de seguridad no inferior al definido para la clave original.

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

Además de las observaciones anteriores, esta PC describe todos los requisitos y procedimientos aplicables al proceso de generar una copia de respaldo.

6.2.5. ARCHIVADO DE LA CLAVE PRIVADA

Las claves privadas asociadas a certificados de los tipos, F2, del PCSC de CONFIRMA S.A. nunca son 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

Como establezca la DPC de CONFIRMA S.A.

6.2.7. ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO


Conforme al ítem 6.1

6.2.8. MÉTODO DE ACTIVACIÓN DE CLAVE PRIVADA

La activación de la clave privada la podrá efectuar el titular de la misma mediante el uso de al menos un factor de seguridad pudiendo ser contraseñas, tokens, biometría, etc.).

6.2.9. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Sin Estipulaciones.

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

6.2.10. MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA

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

6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

6.3.1. ARCHIVO DE LA CLAVE PÚBLICA

Las claves públicas de los titulares de certificados de firma digital y las CRL son almacenadas por el PCSC de CONFIRMA S.A., luego de la expiración de los certificados correspondientes, por un periodo de 10 (diez) años desde su última emisión, para la verificación de firmas generados durante su periodo de validez.


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

Las claves privadas de titulares del PCSC de CONFIRMA S.A. deberán ser utilizadas únicamente durante el periodo de validez correspondiente. Las correspondientes claves publicas podrán ser utilizadas durante todo el periodo de tiempo determinado por la normativa vigente, para la verificación de firmas generadas durante el plazo de validez de los respectivos certificados.

La tabla 3 define los periodos máximos de validez admitidos para cada tipo de certificado previsto por la ICPP.

Tabla N° 3 – Período de validez de los certificados

Tipo de certificado	Tiempo de uso en años	Tiempo operacional en años	Periodo máximo de validez del certificado (en años)

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

F2	4	4	Emitido por un tiempo máximo de 4 (cuatro) años, al finalizar ese periodo pierde su validez.
F3	4	4	Emitido por un tiempo máximo de 4 (cuatro) años, al finalizar ese período pierde su validez.


6.4 DATOS DE ACTIVACIÓN

En los siguientes ítems de la PC de PCSC de CONFRIMA S.A , son descritos los requerimientos de seguridad referentes a los datos de activación. Los datos de activación, distintos a las claves criptográficas, son aquellos requeridos para la operación de algunos módulos criptográficos.

6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Para certificados de firma electrónica cualificada tipo F2 y F3, la generación y almacenamiento del par de claves son realizados en dispositivos criptográficos hardware con capacidad de generación de claves siendo activados y protegidos por contraseñas y/o PIN.

Dicha contraseña y/o PIN es generado por el titular previamente a la solicitud del certificado y posee una longitud mínima y máxima determinada por el dispositivo.

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

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

6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Sin estipulaciones

6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

La PC del PCSC de CONFIRMA S.A. describe los requisitos de seguridad computacional del equipamiento donde será generado el par de claves criptográficas de los titulares de certificados, observando los requerimientos generales previstos en la DPC.

6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR


Ítem no aplicable.

6.5.3. CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO

Ítem no aplicable.

6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

6.6.4. CONTROLES EN LA GENERACIÓN DE LCR

6.7 CONTROLES DE SEGURIDAD DE RED

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

6.7.1. DIRECTRICES GENERALES

6.7.2. FIREWALL

6.7.3. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)


6.7.4. REGISTRO DE ACCESO NO AUTORIZADO A LA RED

6.8. FUENTES DE TIEMPO

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

7. PERFILES DE CERTIFICADOS, LCR Y OCSP

En los siguientes ítems son descritos los formatos de los certificados y de las LCR/OCSP generados según el PC.

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

Son incluidas las informaciones sobre las normas adoptadas, sus perfiles, versiones y extensiones. Los requisitos mínimos establecidos en los siguientes ítems son obligatoriamente considerados en todos los tipos de certificados admitidos en el ámbito de la ICPP.

7.1. PERFIL DEL CERTIFICADO

Todos los certificados emitidos por el PCSC de CONFIRMA S.A., según sus respectivas PCs, están conformes al formato definido por la norma ITU X.509 o ISO/IEC 9594-8.


7.1.1. NÚMERO DE VERSIÓN

Todos los certificados emitidos por el PCSC de CONFIRMA S.A., según su PC, implementan la versión 3 (tres) del certificado definido en la norma ITU X.509 de acuerdo con el perfil establecido en la RFC 5280.

7.1.2. EXTENSIONES DEL CERTIFICADO

La ICPP define las siguientes extensiones como obligatorias:

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

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

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

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

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

d.3) **para certificados de firma de respuesta OCSP:** solamente el propósito *OCSPSigning* *OID = 1.3.6.1.5.5.7.3.9* debe estar presente;

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


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

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

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

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

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

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

e.2.2) el campo **policyQualifiers**

e.2.2.1) el campo **CPS Pointer** debe contener la dirección web de la DPC del PCSC que emite el certificado.

f. Restricciones Básicas “Basic Constraints”, crítica:

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

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

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

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

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

h.1) Primer acceso

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


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

h.2) Segundo acceso

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

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

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

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

i.1) Para CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA:

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

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

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

CUALIFICADA"]

1.2) para certificado del tipo F3: ["FIRMA ELECTRÓNICA

CUALIFICADA CENTRALIZADA"]

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

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

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

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

4. **DirectoryName OID=2.5.4.12:** [posición o función designada al titular del certificado en la organización en el que presta servicio o título académico del titular del certificado];

i.2.3) 2 (dos) campos otherName, NO obligatorios, que contienen:

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


2. **DirectoryName OID= 2.5.4.12:** [posición o función designada al responsable del certificado en la organización en el que presta servicio];

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

1. **DirectoryName OID= 2.5.4.11:** [nombre de la unidad de la organización

en el que presta servicio el titular del certificado]; y

2. **DirectoryName OID=2.5.4.12:** [posición o función designada al titular

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

del certificado en la organización en el que presta servicio];

Los campos otherName definidos por la ICPP deben cumplir con las siguientes

especificaciones:

a) El conjunto de información definido en cada campo otherName debe almacenarse como una cadena de tipo **ASN.1 OCTET STRING** o **PRINTABLE STRING**; y

b) Solo se pueden utilizar los caracteres de la A a la Z, del 0 al 9, observando lo establecido en el ítem 7.1.5 del presente documento.

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

7.1.3. IDENTIFICADORES DE OBJETO DE ALGORITMOS


OID de algoritmo criptográfico podrá ser: sha256WithRSAEncryption (1.2.840.113549.1.1.11) OID de clave pública: RSAEncryption (1.2.840.113549.1.1.1)

7.1.4. FORMAS DEL NOMBRE

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

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

i) **OID=2.5.4.6 CP= PY**

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

ii) OID=2.5.4.10 O= CERTIFICADO CUALIFICADO DE FIRMA ELECTRONICA

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

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

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

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


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

7.1.5. RESTRICCIONES DEL NOMBRE

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

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

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


INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

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

Tabla 4 - Caracteres especiales permitidos en los nombres

Caracteres	Código (hexadecimal)
Blanco	20
!	21
"	22
#	23
\$	24
%	25
&	26
'	27
(28
)	29
*	2A

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY


DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

7.1.6. IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO

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

7.1.7. USO DE LA EXTENSIÓN RESTRICCIONES DE POLÍTICA (POLICY CONSTRAINTS)

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

Este Ítem no aplica.

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

En los certificados emitidos por el PCSC de CONFIRMA S.A.n según su PC, el campo **policyQualifiers** de la extensión Políticas de certificado "Certificate Policies", contiene la dirección web (URL) de la DPC del PCSC responsable.

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

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

7.2. PERFIL DE LA LCR


Los Listas de Certificados Revocados LCR es firmado selladas utilizando el algoritmo definido en el documento DOC-ICPP-06 [1].

7.2.1 NÚMERO (S) DE VERSIÓN

Las LCRs generadas por el PCSC de CONFIRMA S.A. implementa la versión 2 del LCRs definida en el estándar ITU X.509, de acuerdo con el perfil establecido en el RFC 5280.

7.2.2 LCR Y EXTENSIONES DE ENTRADAS DE CRL

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

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

- a) Identificador de la clave de la Autoridad Certificadora “Authority Key Identifier” no crítica:** debe contener el hash SHA-1 de la clave pública del PCSC que firma o sella la LCR;
- b) Número de LCR “CRL Number” no crítica:** debe contener un número secuencial para cada LCR emitida por el PCSC; y
- c) Puntos de Distribución del Emisor “Issuing Distribution Point” crítico:** debe contener la dirección Web donde se obtiene la LCR correspondiente al certificado.

7.3. PERFIL DE OCSP


Las Respuestas OCSP son firmados utilizando el algoritmo definido en el en el documento DOC-ICPP-06 [1].

7.3.1. NÚMERO (S) DE VERSIÓN

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

7.3.2. EXTENSIONES DE OCSP


Si se implementa, debe cumplir con RFC 6960.

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

En los apartados siguientes se refieren a los ítems correspondientes de la DPC del PCSC de CONFIRMA S.A o deben ser detallados los aspectos específicos para la PC si los hubiere.

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

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

9. OTROS ASUNTOS LEGALES Y COMERCIALES

En los apartados siguientes se refieren a los ítems correspondientes de la DPC del PCSC de CONFIRMA S.A o deben ser detallados los aspectos específicos para la PC si los hubiere.

9.1. TARIFAS

9.1.1. TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

9.1.1.1. TARIFAS DE ACCESO A CERTIFICADOS

9.1.1.2. TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN


9.1.1.3. TARIFAS POR OTROS SERVICIOS

9.1.1.4. POLÍTICAS DE REEMBOLSO

El PCSC CONFIRMA SA posee una Política de Reembolso en el cual establece lo siguiente:

El PCSC CONFIRMA S.A. podrá reembolsar al solicitante de certificados la totalidad del importe abonado, cuando:

- (a) se vea afectada la seguridad de la información Indicios de falsedad o falsificación de documentos en la solicitud del certificado cualificado de firma electrónica y se decida no autorizar la emisión de este.
- (b) el producto o servicio no cumpla con los requerimientos técnicos exigidos por la AC Raíz del Paraguay, lo cuales se encuentran descriptos en la Política de Certificación y en la Declaración de Prácticas de Certificación del PCSC de CONFIRMA SA.

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

(c) cuando el producto solicitado por el Titular del certificado no corresponde al producto solicitado. Para la validación de este caso, el cliente deberá notificar el PCSC de CONFIRMA SA por medio de una nota, solicitando la devolución del dinero, indicando su inconformidad y aclarando cual fue el producto solicitado.

9.2. RESPONSABILIDAD FINANCIERA

9.2.1. COBERTURA DE SEGURO

9.2.1. OTROS ACTIVOS

9.2.3. COBERTURA DE SEGURO O GARANTÍA PARA USUARIOS FINALES

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

9.3.1. INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL


9.3.2. RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

9.4. PRIVACIDAD DE INFORMACIÓN PERSONAL

9.4.1. PLAN DE PRIVACIDAD

9.4.2. INFORMACIÓN TRATADA COMO PRIVADA

9.4.3. INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

9.4.4. RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

9.4.5. NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

9.4.6. DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO


9.4.7. OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

9.4.8. INFORMACIÓN A TERCEROS

9.4. DERECHO DE PROPIEDAD INTELECTUAL

9.6. REPRESENTACIONES Y GARANTÍAS

9.6.1. REPRESENTACIONES Y GARANTÍAS DE LA PCSC

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

9.6.1.1. AUTORIZACION PARA CERTIFICADO

9.6.1.2. PRECISIÓN DE LA INFORMACION

9.6.1.3. IDENTIFICACION DEL SOLICITANTE

9.6.1.4. CONSENTIMIENTO DE LOS TITULARES DEL CERTIFICADO

9.6.1.5. SERVICIO

9.6.1.6. REVOCACION

9.6.1.7. EXISTENCIA LEGAL

9.6.2. REPRESENTACIONES Y GARANTÍAS DE LA AR

9.6.3. REPRESENTACIONES Y GARANTÍAS DEL TITULAR DEL CERTIFICADO

9.6.4. REPRESENTACIONES Y GARANTÍAS DE LAS PARTES USUARIAS

9.6.5. REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES

9.7. EXENCIÓN DE GARANTÍA


9.8. LIMITACIONES DE RESPONSABILIDAD LEGAL

9.9. INDEMNIZACIONES

9.10. PLAZO Y FINALIZACIÓN

9.10.1 PLAZO

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

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

9.10.2. FINALIZACIÓN

La presente PC permanecerá en vigencia indefinidamente, siendo válida y efectiva hasta que sea revocada.

9.10.3. EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

Los actos realizados durante la vigencia de esta PC 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 PARTICIPANTES

9.12. ENMIENDAS


9.12.1. PROCEDIMIENTOS PARA ENMIENDAS

El procedimiento para enmiendas y que propuestas de modificación de la PC del PCSC de CONFIRMA S.A son revisadas y aprobadas por la AC Raíz-Py antes de ser implementadas. 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 PC, deberá ser publicada en el repositorio del PCSC de CONFIRMA S.A.

9.12.3. CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

9.13. DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

9.14. NORMATIVA APLICABLE

9.15. ADECUACIÓN A LA LEY APLICABLE

9.16. DISPOSICIONES VARIAS

9.16.1 ACUERDO COMPLETO

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

Esta PC representa las obligaciones y deberes aplicables al PCSC de CONFIRMA S.A. y autoridades vinculadas.

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


9.16.2. ASIGNACIÓN

9.16.3. DIVISIBILIDAD

9.16.4. APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DE DERECHOS)

9.16.5. FUERZA MAYOR

9.17. OTRAS DISPOSICIONES

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY			
DOCUMENTO	CODIGO	VERSION	 CONFIRMA
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	

10. DOCUMENTOS DE REFERENCIA

10.1 REFERENCIAS EXTERNAS

- RFC 5280: "Internet X.509 Public Key Infrastructure.Certificate and Certificate Revocation List (CRL) Profile".
- RFC 6960: "X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP".
- TU X.500/ISO 9594: "Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services".
- ITU X.509/ISO/IEC9594-8:"-Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks".
- Principles and Criteria for Certification Authorities.
- WebTrustSM/TM Principles and Criteria for Registration Authorities.
- Ley 6822/2021 "de los servicios de confianza para las transacciones electrónicas, el documento electrónico y los documentos trasmisibles electrónicos


10.2. REFERENCIAS A DOCUMENTOS QUE COMPONEN LA

ICPP

Tabla No 5 – Documentos Referenciados

REF.	NOMBRE DOCUMENTO	DEL	CODIGO
[1]	Normas de algoritmos criptográficos de la ICPP.		DOC-ICPP-06
[2]	Procedimientos operacionales		DOC-ICPP-07

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY


DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

	mínimos para el servicio de generación o gestión de datos de creación de firma electrónica y/o sello electrónico. DOC-ICPP-07	
[3]	Directivas obligatorias para la formulación y elaboración de la declaración de practicas de certificación de los prestadores cualificados de servicios de confianza de la ICPP.	DOC-ICPP-03
[4]	DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA POLÍTICA DE CERTIFICACIÓN DE LOS PCSC DE LA ICPP	DOC-ICPP-04

10.3. INDICE DE TABLAS

REF.	NOMBRE DEL DOCUMENTO
1	Siglas y Acrónimos
2	Medio de almacenamiento de claves criptográficas.
3	Periodo de validez de los certificados

INFRAESTRUCTURA DE LA CLAVE PÚBLICA DEL PARAGUAY

DOCUMENTO	CODIGO	VERSION	
POLÍTICA DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA CONFIRMA SA	DOC – PC – CF	1.0	 CONFIRMA

4	Caracteres especiales permitidos en los nombres
5	Documentos Referenciados