



MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 1
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

**DIRECTIVAS OBLIGATORIAS
PARA LA FORMULACIÓN Y ELABORACIÓN DE
LA POLÍTICA DE CERTIFICACIÓN DE LOS
PRESTADORES DE SERVICIOS DE
CERTIFICACIÓN DE LA PKI-Paraguay**

DOC-PKI-04


Versión 2.0

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 2
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

CONTROL DOCUMENTAL

Documento	
Título: DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA POLÍTICA DE CERTIFICACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC)	Nombre Archivo: DOC-PKI-04-V2.0
Código: DOC-PKI-04	Soporte Lógico: https://www.acraiz.gov.py/
Fecha: 30/09/2020	Ubicación Física: DGFDyCE
Versión: 2.0	


Registro de cambios		
Versión	Fecha	Motivo de cambio
1.0	03/11/2016	Versión inicial
1.1	28/11/2019	2.5.4.5 Perfiles del Certificado
		7.3 Perfil del OCSP
2.0	30/09/2020	1. Introducción
		3. Identificación y autenticación
		4. Requerimientos operacionales del ciclo de vida del certificado
		5. Controles de seguridad física, de gestión y de operaciones
		6. Controles técnicos de seguridad

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 3
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

		7. Perfiles de certificados, CRL y OCSP
		9. Otros asuntos legales y comerciales
		10. Documentos de referencia


Distribución del documento	
Nombre	Área
Ministerio de Industria y Comercio (MIC)	Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE)
Autoridad Certificadora (CA)	Prestadores de Servicios de Certificación (PSC)
Documento Público	https://www.acraiz.gov.py/

Control del documento		
Elaborado por:	Verificado por:	Aprobado por:
JENNY RUIZ DÍAZ	LUJAN OJEDA	LUCAS SOTOMAYOR


MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 4
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

Contenido


1. INTRODUCCIÓN	14
1.1. DESCRIPCIÓN GENERAL	14
1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO	15
1.3. PARTICIPANTES DE LA PKI.....	16
1.3.1. AUTORIDADES CERTIFICADORAS (CA)	16
1.3.2. AUTORIDADES DE REGISTRO (RA)	16
1.3.3. SUSCRIPTORES	17
1.3.4. PARTE QUE CONFÍA	17
1.3.5. OTROS PARTICIPANTES	17
1.4. USO DEL CERTIFICADO	18
1.4.1. USOS APROPIADOS DEL CERTIFICADO	18
1.4.2. USOS PROHIBIDOS DEL CERTIFICADO	19
1.5. ADMINISTRACIÓN DE LA POLÍTICA	19
1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO	19
1.5.2. PERSONA DE CONTACTO.....	19
1.5.3. PERSONA QUE DETERMINA LA ADECUACIÓN DE LA CPS A LA CP	20
1.5.4. PROCEDIMIENTOS DE APROBACIÓN DE LA CP	20
1.6. DEFINICIONES, SIGLAS Y ACRÓNIMOS	20
1.6.1. DEFINICIONES.....	20
1.6.2. SIGLAS Y ACRÓNIMOS.....	27
2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO	31
2.1 REPOSITORIOS	31
2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN	31
2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN	31
2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS	31
3. IDENTIFICACIÓN Y AUTENTICACIÓN	31
3.1 NOMBRES	31
3.1.1 TIPOS DE NOMBRES	31
3.1.2 NECESIDAD DE NOMBRES SIGNIFICATIVOS	31
3.1.3 ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES	31

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 5
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020


3.1.4	REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES	31
3.1.5	UNICIDAD DE NOMBRES	32
3.1.6	PROCEDIMIENTO PARA RESOLVER DISPUTA DE NOMBRE	32
3.1.7	RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS	32
3.2	VALIDACIÓN INICIAL DE IDENTIDAD	32
3.2.1	MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA	32
3.2.2	AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA	32
3.2.3	AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA	32
3.2.4	AUTENTICACIÓN DE IDENTIDAD DE UNA MÁQUINA O APLICACIÓN	32
3.2.5	INFORMACIÓN DEL SUSCRIPTOR NO VERIFICADA	33
3.2.6	VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)	33
3.2.7	CRITERIOS PARA INTEROPERABILIDAD	33
3.3	IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE NUEVAS CLAVES ..	33
3.3.1	IDENTIFICACIÓN Y AUTENTICACIÓN PARA EMISIÓN DE NUEVAS CLAVES ANTES DE SU EXPIRACIÓN	33
3.3.2	IDENTIFICACIÓN Y AUTENTICACIÓN PARA EMISIÓN DE NUEVAS CLAVES DESPUÉS DE LA REVOCACIÓN O EXPIRACIÓN DEL CERTIFICADO	33
3.4	IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN	33
4.	REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO	33
4.1	SOLICITUD DEL CERTIFICADO	33
4.1.1	QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO	33
4.1.2	PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES	33
4.2.	PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO	34
4.2.1	EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN	34
4.2.2	APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO	34
4.2.3.	TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO	34
4.3	EMISIÓN DEL CERTIFICADO	34
4.3.1	ACCIONES DEL PSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS	34
4.3.2	NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DEL CERTIFICADO DIGITAL	34
4.4.	ACEPTACIÓN DEL CERTIFICADO	34

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 6
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020


4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO	34
4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PSC	34
4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR EL PSC A OTRAS ENTIDADES	34
4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO	34
4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL SUScriptor	34
4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LA PARTE QUE CONFÍA	34
4.6 RENOVACIÓN DEL CERTIFICADO	34
4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO	34
4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN	34
4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO	35
4.6.4 NOTIFICACIÓN AL SUScriptor SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO	35
4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO	35
4.6.6 PUBLICACIÓN POR EL PSC DEL CERTIFICADO RENOVADO	35
4.6.7 NOTIFICACIÓN POR EL PSC DE LA EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES	35
4.7 RE-EMISIÓN DE CLAVES DE CERTIFICADO (RE-KEY)	35
4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO	35
4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA	35
4.7.3 PROCESAMIENTO DE SOLICITUDES DE RE-EMISIÓN DE CLAVES DE CERTIFICADO	35
4.7.4 NOTIFICACIÓN AL SUScriptor SOBRE LA RE-EMISIÓN DE UN NUEVO CERTIFICADO	35
4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE-EMITIDO	35
4.7.6 PUBLICACIÓN POR EL PSC DE LOS CERTIFICADOS RE-EMITIDOS	35
4.7.7 NOTIFICACIÓN POR EL PSC DE LA RE-EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES	35
4.8 MODIFICACIÓN DE CERTIFICADOS	35
4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO	35
4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO	36

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 7</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>


4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO .	36
4.8.4 NOTIFICACIÓN AL SUScriptor DE LA EMISIÓN DE UN NUEVO CERTIFICADO	36
4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO	36
4.8.6 PUBLICACIÓN POR EL PSC DE LOS CERTIFICADOS MODIFICADOS	36
4.8.7 NOTIFICACIÓN POR EL PSC DE UNA EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES	36
4.9 REVOCACIÓN Y SUSPENSIÓN	36
4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN	36
4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN	36
4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN	36
4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN	36
4.9.5 TIEMPO DENTRO DEL CUAL EL PSC DEBE PROCESAR LA SOLICITUD DE REVOCACIÓN	36
4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LAS PARTES QUE CONFÍAN.....	36
4.9.7 FRECUENCIA DE EMISIÓN DEL CRL	36
4.9.8 LATENCIA MÁXIMA PARA CRL.....	37
4.9.9 DISPONIBILIDAD PARA REVOCACIÓN/VERIFICACIÓN DE ESTADO EN LÍNEA	37
4.9.10 REQUISITOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA.....	37
4.9.11 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES	37
4.9.12 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA ..	37
4.9.13 CIRCUNSTANCIAS PARA SUSPENSIÓN.....	37
4.9.14 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN	37
4.9.15 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN.....	37
4.9.16 LÍMITES DEL PERÍODO DE SUSPENSIÓN	37
4.10 SERVICIOS DE ESTADO DE CERTIFICADO	37
4.10.1 CARACTERÍSTICAS OPERACIONALES.....	37
4.10.2 DISPONIBILIDAD DEL SERVICIO	37
4.10.3 CARACTERÍSTICAS OPCIONALES	37
4.11 FIN DE ACTIVIDADES.....	37

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 8</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>


4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES	37
4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES	37
4.12.2 POLÍTICAS Y PRÁCTICAS DE RECUPERACIÓN Y ENCAPSULACIÓN DE CLAVES DE SESIÓN.....	37
5 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES	38
5.1 CONTROLES FÍSICOS.....	38
5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO.....	38
5.1.2 ACCESO FÍSICO	38
5.1.3 ENERGÍA Y AIRE ACONDICIONADO	38
5.1.4 EXPOSICIÓN AL AGUA	38
5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO.....	38
5.1.6 ALMACENAMIENTO DE MEDIOS	38
5.1.7 ELIMINACIÓN DE RESIDUOS	38
5.1.8 RESPALDO FUERA DE SITIO	38
5.2 CONTROLES PROCEDIMENTALES	39
5.2.1 ROLES DE CONFIANZA	39
5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA	39
5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL	39
5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES.....	39
5.3. CONTROLES DE PERSONAL	39
5.3.1. REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN.	39
5.3.2. PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES	39
5.3.3. REQUERIMIENTOS DE CAPACITACIÓN.....	39
5.3.4. REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN	39
5.3.5. FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES.....	39
5.3.6. SANCIONES PARA ACCIONES NO AUTORIZADAS	39
5.3.7. REQUISITOS DE CONTRATACIÓN A TERCEROS.....	39
5.3.8. DOCUMENTACIÓN SUMINISTRADA AL PERSONAL.....	39
5.4. PROCEDIMIENTO DE REGISTRO DE AUDITORÍA	39
5.4.1 TIPOS DE EVENTOS REGISTRADOS	39
5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS).....	39

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 9</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>


5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA	39
5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA	39
5.4.5. PROCEDIMIENTOS DE RESPALDO (BACKUP) DE REGISTRO (LOGS) DE AUDITORÍA	40
5.4.6. SISTEMA DE RECOLECCIÓN DE INFORMACIÓN DE AUDITORÍA (INTERNO VS EXTERNO)	40
5.4.7. NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO	40
5.4.8. EVALUACIÓN DE VULNERABILIDADES	40
5.5. ARCHIVOS DE REGISTROS	40
5.5.1. TIPOS DE REGISTROS ARCHIVADOS	40
5.5.2. PERIODOS DE RETENCIÓN PARA ARCHIVOS	40
5.5.3 PROTECCIÓN DE ARCHIVOS.....	40
5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO	40
5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS.....	40
5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO).....	40
5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA.....	40
5.6 CAMBIO DE CLAVE	40
5.7. RECUPERACIÓN DE DESASTRES Y COMPROMISO	40
5.7.1. PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO	40
5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES	40
5.7.3. PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD .	41
5.7.4. CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE	41
5.8. EXTINCIÓN DE UN PSC O ENTIDADES VINCULADAS	41
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.....	42
6.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO	42
6.1.4. ENTREGA DE LA CLAVE PÚBLICA DE LA CA A LAS PARTES QUE CONFÍAN.	42
6.1.5. TAMAÑO DE LA CLAVE	42

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 10
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020


6.1.6. GENERACIÓN DE PARÁMETROS DE CLAVE ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD	43
6.1.7. PROPÓSITOS DE USOS DE CLAVE (CAMPO KEY USAGE X.509 V3)	43
6.2. CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO Y PROTECCIÓN DE LA CLAVE PRIVADA	43
6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO	43
6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA	43
6.2.3 CUSTODIA (ESCROW) DE LA CLAVE PRIVADA	44
6.2.4. RESPALDO/COPIA DE LA CLAVE PRIVADA	44
6.2.5. ARCHIVADO DE LA CLAVE PRIVADA	44
6.2.6. TRANSFERENCIA DE CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRIPTOGRÁFICO.....	45
6.2.7. ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO	45
6.2.8. MÉTODO DE ACTIVACIÓN DE CLAVE PRIVADA.....	46
6.2.9. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA	47
6.2.10. MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA	47
6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES	47
6.3.1. ARCHIVO DE LA CLAVE PÚBLICA	47
6.3.2. PERÍODO OPERACIONAL DEL CERTIFICADO Y PERÍODO DE USO DEL PAR DE CLAVES	47
6.4 DATOS DE ACTIVACIÓN	48
6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN	48
6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN.....	48
6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN	49
6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR	49
6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS	49
6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR.....	49
6.5.3. CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO.....	49
6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA.....	49
6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA	49
6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD	50

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 11
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020


6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA	50
6.6.4. CONTROLES EN LA GENERACIÓN DE CRL	50
6.7 CONTROLES DE SEGURIDAD DE RED	50
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	51
7.1.1. NÚMERO DE VERSIÓN	51
7.1.2. EXTENSIONES DEL CERTIFICADO	51
7.1.3. IDENTIFICADORES DE OBJETO DE ALGORITMOS.....	56
7.1.4. FORMAS DEL NOMBRE	56
7.1.5. RESTRICCIONES DEL NOMBRE	58
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 CRL	60
7.2.1 NÚMERO (S) DE VERSIÓN	60
7.2.2 CRL Y EXTENSIONES DE ENTRADAS DE CRL	61
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	61
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

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 12</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

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	62
9.1. TARIFAS	62
9.1.1. TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS	62
9.1.2. TARIFAS DE ACCESO A CERTIFICADOS.....	62
9.1.3. TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN.....	62
9.1.4. TARIFAS POR OTROS SERVICIOS.....	62
9.1.5. POLÍTICAS DE REEMBOLSO	62
9.2. RESPONSABILIDAD FINANCIERA	63
9.2.1. COBERTURA DE SEGURO	63
9.2.2. OTROS ACTIVOS.....	63
9.2.3. COBERTURA DE SEGURO O GARANTÍA PARA USUARIOS FINALES.....	63
9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL	63
9.3.1. ALCANCE DE LA INFORMACIÓN CONFIDENCIAL	63
9.3.2. INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL.....	63
9.3.3. RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL.....	63
9.4. PRIVACIDAD DE INFORMACIÓN PERSONAL	63
9.4.1. PLAN DE PRIVACIDAD	63
9.4.2. INFORMACIÓN TRATADA COMO PRIVADA.....	63
9.4.3. INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA.....	63
9.4.4. RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA.....	63
9.4.5. NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA..	63
9.4.6. DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO	63
9.4.7. OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN	63
9.4.8. INFORMACIÓN A TERCEROS	63
9.5. DERECHO DE PROPIEDAD INTELECTUAL.....	64
9.6. REPRESENTACIONES Y GARANTÍAS.....	64
9.6.1. REPRESENTACIONES Y GARANTÍAS DE LA PSC	64

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 13</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

9.6.2. REPRESENTACIONES Y GARANTÍAS DE LA RA	64
9.6.3. REPRESENTACIONES Y GARANTÍAS DEL SUScriptor	64
9.6.4. REPRESENTACIONES Y GARANTÍAS DE LAS PARTES QUE CONFÍAN	64
9.6.5. REPRESENTACIONES Y GARANTÍAS DEL REPOSITORIO.....	64
9.6.6. REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES	64
9.7. EXENCIÓN DE GARANTÍA	64
9.8. LIMITACIONES DE RESPONSABILIDAD LEGAL	64
9.9. INDEMNIZACIONES	64
9.10. PLAZO Y FINALIZACIÓN	64
9.10.1 PLAZO.....	64
9.10.2. FINALIZACIÓN.....	64
9.10.3. EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA	64
9.11. NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES	65
9.12. ENMIENDAS	65
9.12.1. PROCEDIMIENTOS PARA ENMIENDAS	65
9.12.2. PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN	65
9.12.3. CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS	65
9.13. DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS	65
9.14. NORMATIVA APLICABLE	65
9.15. ADECUACIÓN A LA LEY APLICABLE	65
9.16. DISPOSICIONES VARIAS.....	65
9.16.1 ACUERDO COMPLETO	65
9.16.2. ASIGNACIÓN	66
9.16.3. DIVISIBILIDAD	66
9.16.4. APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DE DERECHOS) 66	
9.16.5. FUERZA MAYOR.....	66
9.17. OTRAS DISPOSICIONES.....	66
10. DOCUMENTOS DE REFERENCIA	67
10.1 REFERENCIAS EXTERNAS	67
10.2 REFERENCIAS A DOCUMENTOS QUE COMPONEN LA PKI-Paraguay	68

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 14</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

1. INTRODUCCIÓN

1.1. DESCRIPCIÓN GENERAL

Este documento establece los requisitos mínimos que obligatoriamente deberán ser observados por los Prestadores de Servicio de Certificación (PSC) en su carácter de Autoridad de Certificación Intermedia (CAI) y como integrantes de la Infraestructura de Clave Pública del Paraguay (PKI-Paraguay), para la formulación y la elaboración de su política de certificación (CP)

Toda Política de Certificación elaborada en el ámbito de la Infraestructura de Clave Pública del Paraguay (PKI-Paraguay) debe obligatoriamente adoptar la misma estructura empleada en este documento.

Son 6 (seis) los tipos de certificados digitales, inicialmente previstos, para los usuarios de la PKI-Paraguay, siendo 3 (tres) relacionados con firma digital y 3 (tres) con cifrado conforme lo descrito a continuación:

Tipos de certificados de firma digital:


- i. F1
- ii. F2
- iii. F3

Tipos de certificados de cifrado

- i. C1
- ii. C2
- iii. C3

Los tipos de certificados indicados anteriormente definen escalas de requisitos 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: tamaño de la clave criptográfica, medios de almacenamiento de clave, proceso

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 15
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

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

El par de claves criptográficas relacionadas a los tipos de certificado F1 y C1 deberán obligatoriamente ser y almacenados en un:

- i. dispositivo Smart Card sin capacidad de generación de claves y protegidos por contraseña y/o identificación biométrica; o
- ii. token sin capacidad de generación de claves y protegidos por contraseña y/o identificación biométrica; o
- iii. un repositorio protegido por contraseña y/o identificación biométrica cifrado por software.

El par de claves criptográficas relacionadas a los tipos de certificado F2 y C2 deberán obligatoriamente ser generados y almacenados en módulos criptográficos tipo Hardware en un:

- i. dispositivo Smart Card con capacidad de generación de claves; o
- ii. token criptográfico u otro dispositivo equivalente, con capacidad de generación de claves.


El par de claves criptográficas relacionadas a los tipos de certificado F3 y C3 deberán obligatoriamente ser generados y almacenados en módulos criptográficos tipo Hardware en un:

- i. módulo de seguridad hardware (HSM).

Los certificados de firma o de cifrado pueden, conforme a la necesidad, ser emitidos por los PSC, para personas físicas, personas jurídicas, máquinas o aplicaciones.

1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

En este ítem debe ser identificada la CP, indicando como mínimo el nombre, versión, fecha de aprobación, localización y el OID (Object Identifier) del documento.

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 16</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

También se debe identificar el documento de Declaración de Prácticas de Certificación (CPS) del PSC, donde estarán descritas sus prácticas y procedimientos de certificación.

1.3. PARTICIPANTES DE LA PKI

1.3.1. AUTORIDADES CERTIFICADORAS (CA)

En este ítem deben ser identificadas las CAs integrantes de la PKI-Paraguay a la que se refiere la CPS. Estas pueden ser:

- i. CA Raíz-Py; y
- ii. CAI.


Un PSC es una entidad habilitada por la AA, encargada de operar una CA en el marco de la PKI-Paraguay, debe contar con un certificado digital emitido por la CA Raíz-Py y solo podrá emitir certificados a usuarios finales. En el ámbito de la PKI-Paraguay un PSC es considerada una CAI.

1.3.2. AUTORIDADES DE REGISTRO (RA)

En este ítem debe identificarse la dirección de la página web (URL), donde se publican los datos referentes a las autoridades de registro (RA) habilitadas por el PSC para el proceso de recepcionar y encaminar solicitudes de emisión o de revocación de certificados digitales y de identificar presencialmente a los solicitantes. Las informaciones a ser publicadas en el sitio son:

- a) la lista de todas las RA habilitadas;
- b) para cada RA, las direcciones de todas las instalaciones técnicas, autorizadas por la CA Raíz-Py para funcionar;
- c) acuerdos operacionales celebrados entre un PSC y una RA delegada; y
- d) la lista de todas las RA cuya habilitación fue revocada, con la indicación de la fecha de revocación.

El PSC deberá mantener las informaciones siempre actualizadas.

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 17</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

La RA puede ser propia del PSC o delegada a un tercero cuyo funcionamiento deberá ser autorizado por la CA Raíz-Py con la habilitación correspondiente.

Las RA delegadas son autoridades de registro vinculadas a un PSC mediante un acuerdo operacional.

1.3.3. SUSCRIPTORES

En este ítem se especifican las personas físicas o jurídicas que podrán ser titulares de los certificados emitidos según esta CP.

1.3.4. PARTE QUE CONFÍA

Se entenderá por parte que confía, toda persona física o jurídica, diferente al titular del certificado que decide aceptar y confiar en un certificado digital emitido dentro de la PKI-Paraguay.

Una parte que confía puede o no, ser un suscriptor.

1.3.5. OTROS PARTICIPANTES


1.3.5.1. PRESTADORES DE SERVICIOS DE SOPORTE (PSS)

En este ítem se identifica la dirección de página web (URL), donde deberán estar publicados los datos referentes a los Prestadores de Servicio de Soporte (PSS) vinculados al PSC, sea directamente o sea por intermedio de sus RA.

PSS son entidades externas a las que recurre la CA o la RA para desempeñar actividades descritas en esta CPS o en una CP 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.

El PSC deberá mantener las informaciones arriba citadas siempre actualizadas.

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 18</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

El funcionamiento de un PSS vinculado a un PSC mediante un acuerdo operacional deberá ser autorizado por la CA Raíz-Py con la habilitación correspondiente.

1.3.5.2. AUTORIDADES DE VALIDACIÓN (VA)

En este ítem se identifica la dirección de página web (URL), donde deberán estar publicados los datos referentes a las Autoridades de Validación (VA) vinculadas al PSC.

La VA puede ser una entidad propia o externa a un PSC responsable de suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una RA y certificados por la autoridad de certificación.

El funcionamiento de una VA vinculada a un PSC mediante un acuerdo operacional deberá ser autorizado por la CA Raíz-Py con la habilitación correspondiente.

1.3.5.3. PRESTADORES DE SERVICIO DE ALMACENAMIENTO (PSA)

En este ítem se identifica la dirección de página web (URL), donde deberán estar publicados los datos referentes a los Prestadores de Servicios de Almacenamiento vinculados al PSC.


El PSA es una entidad vinculada indefectiblemente a un PSC mediante un acuerdo operacional que deberá ser autorizada por la CA Raíz-Py con la habilitación correspondiente para prestar servicios de almacenamiento de claves privadas para usuarios finales o servicios de firma digital y de verificación de firmas digitales en documentos y transacciones electrónicas o ambos.

Un PSC habilitado, conforme a las disposiciones de la normativa vigente, tiene prohibido almacenar y copiar claves privadas de sus suscriptores, por lo cual no puede constituirse en un PSA.

1.4. USO DEL CERTIFICADO

1.4.1. USOS APROPIADOS DEL CERTIFICADO

En este ítem deben ser relacionadas las aplicaciones para las cuales los certificados definidos por la CP son los adecuados.

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 19
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

Las aplicaciones y otros programas que soporten el uso de un certificado digital de cierto tipo contemplado por la PKI-Paraguay deben aceptar cualquier certificado del mismo tipo, o superior, emitido por cualquier PSC habilitado por la CA Raíz.

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

Certificados de los tipos F1, F2, F3 serán utilizados en aplicaciones como confirmación de identidad y firma de documentos electrónicos con verificación de integridad de sus informaciones.

Certificados de los tipos C1, C2, C3 serán utilizados en aplicaciones como cifrado de documentos, base de datos, mensajes y otras informaciones electrónicas con la finalidad de garantizar su confidencialidad.

1.4.2. USOS PROHIBIDOS DEL CERTIFICADO

En este ítem deben ser relacionadas, cuando corresponda, las aplicaciones para las que existen restricciones o prohibiciones en el uso de estos certificados.

1.5. ADMINISTRACIÓN DE LA POLÍTICA

En este ítem deben ser incluidos el nombre, la dirección y otras informaciones del PSC responsable de la CP. También se debe proporcionar el nombre, los números de teléfono y la dirección de correo electrónico de una persona de contacto.

1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre del PSC:


1.5.2. PERSONA DE CONTACTO

Nombre:

Teléfono:

Fax:

Página web:

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 20</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

E-mail:

Otros:

1.5.3. PERSONA QUE DETERMINA LA ADECUACIÓN DE LA CPS A LA CP

Nombre:

Teléfono:

E-mail:

Otros:


1.5.4. PROCEDIMIENTOS DE APROBACIÓN DE LA CP

Los procedimientos para la aprobación de CP del PSC son establecidos a criterio de CA Raíz-Py de la PKI-Paraguay.


1.6. DEFINICIONES, SIGLAS Y ACRÓNIMOS

1.6.1. DEFINICIONES


- 1) **Acuerdo de Suscriptores:** es un acuerdo entre la CA Raíz-Py y el PSC, y entre el PSC y el usuario final, que establece los derechos, obligaciones y responsabilidades de las partes con respecto a la emisión y gestión de los certificados. Este acuerdo, requiere la aceptación explícita de las partes intervinientes.
 - 2) **Agente de registro:** persona responsable de la realización de las actividades inherentes a la RA. Es la persona que realiza la identificación de los solicitantes en la solicitud de emisión/revocación de certificado.
 - 3) **Armario ignífugo:** armario equipado con sistemas de protección contra el fuego para aislar los productos almacenados en su interior.
 - 4) **Autenticación:** proceso técnico que permite determinar la identidad de la persona que firma electrónicamente, en función del mensaje firmado por ésta, y al cual se le vincula. Este proceso no otorga certificación notarial ni fe pública.
-

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 21</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>


- 5) **Autoridad de Aplicación:** Ministerio de Industria y Comercio a través de la Dirección General de Firma Digital y Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.
- 6) **Autoridad de Certificación:** entidad que presta servicios de emisión, gestión, revocación u otros servicios inherentes a la certificación digital. En el marco de la PKI-Paraguay, son Autoridades de Certificación, la CA Raíz-Py y el PSC.
- 7) **Autoridad de Certificación Raíz del Paraguay:** órgano técnico, cuya función principal es coordinar el funcionamiento de la PKI-Paraguay. La CA 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 CA Raíz-Py son ejercidas por la AA.
- 8) **Autoridad de Certificación Intermedia:** entidad cuyo certificado de clave pública ha sido firmado digitalmente por la CA Raíz-Py; es responsable de la emisión de certificados a usuarios finales. Un Prestador de Servicios de Certificación es considerado una Autoridad de Certificación Intermedia.
- 9) **Autoridad de Registro:** entidad responsable de la interfaz entre el usuario y el Prestador de Servicios de Certificación (PSC). Siempre está vinculado a un PSC y su función es recibir solicitudes de emisión o revocación de certificados digitales del solicitante, identificar de forma presencial al mismo y remitir la solicitud al PSC. La RA puede ser propia del PSC o delegada a un tercero.
- 10) **Autoridad de Validación:** entidad responsable de suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una autoridad de registro y certificados por la autoridad de certificación. La VA puede ser propia del PSC o delegada a un tercero.
- 11) **Cadena de certificación:** lista ordenada de certificados que contiene un certificado de usuario final y certificados de las CA, que termina en un certificado raíz. El emisor del certificado del usuario final es el titular del certificado del PSC y a su vez, el emisor del certificado del PSC es el titular del certificado de CA Raíz-Py. El usuario final o la parte que confía debe verificar la validez de los certificados en la cadena de certificación.

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 22</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

- 12) **Certificado Digital:** es un documento electrónico, generado y firmado por una CA legalmente habilitada para el efecto, el cual vincula un par de claves con una persona física o jurídica confirmando su identidad.
- 13) **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.
- 14) **Cifrado asimétrico:** tipo de cifrado que utiliza un par de claves criptográficas diferentes (ejemplo: privado y público) y matemáticamente relacionadas.
- 15) **Claves criptográficas:** valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.
- 16) **Clave pública y privada:** la criptografía en la que se basa la PKI-Paraguay, es la criptografía asimétrica. En ella se emplea un par de claves: lo que se cifra con una de ellas, sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y está incorporada en el certificado digital, mientras que a la otra se la denomina privada y está bajo exclusivo control del titular del certificado.
- 17) **Compromiso:** violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.
- 18) **Data Center (Centro de Datos):** infraestructura compuesta por el espacio físico para la instalación de equipos informáticos y de comunicación con adecuados sistemas de energía, aire acondicionado y seguridad. Es parte de una CA, constituye un recinto seguro que alberga, entre otras cosas, los módulos criptográficos de hardware, protege la infraestructura tecnológica y es el lugar donde se ejecutan servicios del ciclo de vida del certificado. La importancia del data center radica en la protección que brinda a la clave privada y asegura la confianza en los certificados digitales emitidos por la CA.
- 19) **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.
-


<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 23</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

- 20) **Declaración de Prácticas de Certificación:** declaración de las prácticas que emplea una CA al emitir certificados y que define la infraestructura, políticas y procedimientos que utiliza la CA para satisfacer los requisitos especificados en la CP vigente.
- 21) **Documento de identidad:** documento válido y vigente que permite acreditar la identidad de la persona, a los efectos del proceso de emisión/revocación del certificado digital será considerada la cédula de identidad o el pasaporte del solicitante.
- 22) **Dossier de titular del certificado:** Conjunto formado por la verificación de los documentos de identificación utilizados para la emisión del certificado y solicitud de certificado y acuerdo de suscriptores, y por la solicitud de revocación, cuando sea el caso. Este dossier deberá estar en formato de archivo digital, en el cual se escanean los documentos en formato papel, si los hubiere y se firma la solicitud de certificado y acuerdo de suscriptores con la clave privada del titular, después de la autorización del AGR por medio de la firma de dichos documentos, siempre y cuando sea informado y aceptado su contenido por parte de su solicitante y firmada digitalmente después de la generación de las claves y anterior a la instalación del certificado correspondiente.
- 23) **Emisor del certificado:** persona jurídica cuyo nombre aparece en el campo emisor de un certificado.
- 24) **Emisión de certificado:** es la autorización de la emisión del certificado en el sistema del PSC previa comprobación de la concordancia de los datos de solicitud del certificado con los contenidos en los documentos presentados.
- 25) **Firma Digital:** es una firma electrónica certificada por un prestador habilitado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincula únicamente al mismo y a los datos a lo que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.
- 26) **Generador:** máquina encargada de generar electricidad a partir de un motor de gasolina o diésel. La instalación de este equipo deberá ser de tal forma que, al interrumpirse el suministro de energía eléctrica del proveedor externo, el mismo debe arrancar automáticamente tomando la carga de las instalaciones del data center de la CA,


<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 24</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

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.


- 27) **Habilitación:** autorización que otorga el MIC, una vez cumplidos los requisitos y condiciones establecidos en la norma.
 - 28) **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.
 - 29) **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, con base en los documentos de identificación, y la etapa de emisión del certificado, conforme a la presente CPS.
 - 30) **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 digitales y claves criptográficas emitidas por esta infraestructura.
 - 31) **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.
 - 32) **Lista de certificados revocados:** lista emitida por una CA, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.
 - 33) **Módulo criptográfico:** software o hardware criptográfico que genera y almacena claves criptográficas.
 - 34) **Módulo de Seguridad de Hardware:** dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.
-

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 25</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

- 35) **Normas Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la prestación de los servicios mencionados en la presente CPS.
- 36) **Parte que confía (relying parties):** es toda persona física o jurídica diferente del titular, que decide aceptar y confiar en un certificado emitido en el marco de la PKI-Paraguay.
- 37) **Perfil del certificado:** especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).
- 38) **Política de Certificación:** documento en el cual la CA define el conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad particular y/o una clase de aplicaciones con requisitos comunes de seguridad.
- 39) **Prestador de Servicios de Almacenamiento:** es una entidad vinculada indefectiblemente a un PSC mediante un acuerdo operacional que deberá ser autorizada por la CA Raíz-Py con la habilitación correspondiente para prestar servicios de almacenamiento de claves privadas para usuarios finales o servicios de firma digital y de verificación de firmas digitales en documentos y transacciones electrónicas o ambos.
- 40) **Prestador de Servicios de Certificación:** entidad habilitada por la AA, encargada de operar una CA en el marco de la PKI-Paraguay. El PSC debe contar con un certificado digital emitido por la CA Raíz-Py y solo podrá emitir certificados a usuarios finales.
- 41) **Prestador de Servicios de Soporte:** entidad externa vinculada a un PSC mediante un acuerdo operacional a la que recurre la CA o la RA y autorizada la CA Raíz-Py para desempeñar actividades descritas en la CPS o en una CP.
- 42) **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.
- 43) **Repositorio:** sitio principal de Internet confiable y accesible, mantenido por la CA con el fin de difundir su información pública.
-

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 26</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>


- 44) **Rol de confianza:** función crítica que desempeña personal de la CA, que si se realiza insatisfactoriamente puede tener un impacto adverso sobre el grado de confianza proporcionado por la CA.
- 45) **Servicio OCSP:** permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la CA sobre el estado de un certificado.
- 46) **Solicitante de Certificado:** persona física o jurídica que solicita la emisión de un certificado a una CA.
- 47) **Solicitud de certificado:** documento que se instrumenta mediante un formato autorizado de solicitud de certificado suscripto por el solicitante en nombre propio en el caso de certificados para persona física, o bien en nombre del titular en el caso de certificados de persona jurídica, con anterioridad a la emisión y entrega de un certificado, ya sea en un documento específico de la solicitud o como parte del Acuerdo de Suscriptores.
- 48) **Solicitud de Firma de Certificado:** petición de certificado digital que se envía a la CA. Mediante la información contenida en el CSR, la CA, puede emitir el certificado digital una vez realizadas las comprobaciones que correspondan.
- 49) **Suscriptor:** persona física o jurídica titular de un certificado digital emitido por una CA. Un suscriptor puede ser un PSC o un usuario final.
- 50) **Usuario final:** persona física o jurídica titular de un certificado digital emitido por un PSC.
- 51) **Verificación de firma:** determinación y validación de que la firma digital fue creada durante el periodo operacional de un certificado válido por la clave privada correspondiente a la clave pública que se encuentra en el certificado y que el mensaje no ha sido alterado desde que su firma digital fue creada.
- 52) **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.
- 53) **X.509:** estándar desarrollado por la ITU, que define el formato electrónico básico para certificados electrónicos.
-

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 27
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020


1.6.2. SIGLAS Y ACRÓNIMOS

Tabla N° 1 –Siglas y Acrónimos

Sigla/Acrónimo	Descripción
AA	Autoridad de Aplicación
C	País (C por su sigla en inglés, Country)
CA	Autoridad de Certificación (CA por sus siglas en inglés, Certificate Authority)
CAI	Autoridad de Certificación Intermedia (CAI por sus siglas en inglés, Certificate Authority Intermediate)
CA Raíz-Py	Autoridad Certificadora Raíz del Paraguay
CI	Cédula de Identidad
CN	Nombre común (CN por sus siglas en inglés, Common Name)
CP	Políticas de Certificación (CP por sus siglas en inglés, Certificate Policy)
CPS	Declaración de Prácticas de Certificación (CPS por sus siglas en inglés, Certification Practice Statement)
CRL	Lista de certificados revocados (CRL por sus siglas en inglés, Certificate Revocation List).

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 28
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020


CSR	Solicitud de firma de Certificado (CSR por sus siglas en inglés, certificate Signing Request)
DGFDyCE	Dirección General de Firma Digital y Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.
DNS	Servicio de nombre de dominio (DNS por sus siglas en inglés, Domain Name Server)
FIPS	Estándares Federales de Procesamiento de la Información (FIPS por sus siglas en inglés, Federal Information Processing Standards)
HSM	Módulo de seguridad criptográfico basado en Hardware (HSM por 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)
PIN	Número de Identificación Personal, (por sus siglas en inglés, Personal Identification Number)

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 29
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

PKI	Infraestructura de Clave Pública (PKI por sus siglas en inglés, Public Key Infrastructure).
PKI-Paraguay	Infraestructura de Claves Públicas del Paraguay
PSA	Prestador de Servicios de Almacenamiento
PSC	Prestador de Servicios de Certificación
PSS	Prestador de Servicios de Soporte
PY	Paraguay
RA	Autoridad de Registro (RA por sus siglas en inglés, Registration Authority).
RFC	Petición de Comentarios (RFC por sus siglas en inglés, Request For Comments)
RSA	Sistema criptográfico de clave pública desarrollado por Rivest, Shamir y Adleman.
RUC	Registro único del contribuyente
SN	Número de Serie (por sus siglas en inglés, Serial Number)
TLS	Capa de conexión segura (TLS por sus siglas en inglés, Transport Layer Security).

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 30
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

URL	Localizador uniforme de recursos (URL por sus siglas en inglés, Uniform Resource Locator).
VA	Autoridad de validación (VA por sus siglas en inglés, Validation Authority)

<p>MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 31</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

En los apartados siguientes deben ser referidos a los ítems correspondientes de la CPS del PSC responsable o ser detallados los aspectos específicos para la CP, 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

En los apartados siguientes deben ser referidos a los ítems correspondientes de la CPS del PSC responsable o ser detallados los aspectos específicos para la CP, si los hubiere.

3.1 NOMBRES

3.1.1 TIPOS DE NOMBRES

3.1.2 NECESIDAD DE NOMBRES SIGNIFICATIVOS


3.1.3 ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES

3.1.4 REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES

3.1.4.1 CERTIFICADO DE PERSONA JURÍDICA

3.1.4.2 CERTIFICADO DE PERSONA FÍSICA

3.1.4.3 CERTIFICADO DE MÁQUINA O APLICACIÓN

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 32</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

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

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

3.2.2.1 DOCUMENTOS REQUERIDOS PARA IDENTIFICAR UNA PERSONA JURÍDICA.

3.2.2.2 INFORMACIÓN CONTENIDA EN UN CERTIFICADO EMITIDO PARA UNA PERSONA JURÍDICA

3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA


3.2.3.1 DOCUMENTOS REQUERIDOS PARA IDENTIFICAR UNA PERSONA FÍSICA.

3.2.3.2 INFORMACIÓN CONTENIDA EN UN CERTIFICADO EMITIDO PARA UNA PERSONA FÍSICA

3.2.4 AUTENTICACIÓN DE IDENTIDAD DE UNA MÁQUINA O APLICACIÓN

3.2.4.1 DOCUMENTOS REQUERIDOS PARA LA IDENTIFICACIÓN DE UNA MÁQUINA O APLICACIÓN

3.2.4.2 INFORMACIÓN CONTENIDA EN UN CERTIFICADO EMITIDO PARA UNA MÁQUINA O APLICACIÓN

<p>MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 33</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

3.2.5 INFORMACIÓN DEL SUSCRIPTOR NO VERIFICADA

3.2.6 VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)

3.2.7 CRITERIOS PARA INTEROPERABILIDAD

3.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE NUEVAS CLAVES

3.3.1 IDENTIFICACIÓN Y AUTENTICACIÓN PARA EMISIÓN DE NUEVAS CLAVES ANTES DE SU EXPIRACIÓN

3.3.2 IDENTIFICACIÓN Y AUTENTICACIÓN PARA EMISIÓN DE NUEVAS CLAVES DESPUÉS DE LA REVOCACIÓN O EXPIRACIÓN DEL CERTIFICADO

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

En los apartados siguientes deben ser referidos a los ítems correspondientes de la CPS del PSC responsable o ser 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

4.1.2.1 RESPONSABILIDADES Y OBLIGACIONES DEL PSC

4.1.2.2 RESPONSABILIDADES Y OBLIGACIONES DE LA RA

<p>MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 34</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

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 PSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS

4.3.2 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DEL CERTIFICADO DIGITAL

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PSC

4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR EL PSC 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 SUSCRIPTOR

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

4.6 RENOVACIÓN DEL CERTIFICADO

4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO

4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 35
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO

4.6.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO

4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO

4.6.6 PUBLICACIÓN POR EL PSC DEL CERTIFICADO RENOVADO

4.6.7 NOTIFICACIÓN POR EL PSC 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 SUSCRIPTOR 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 PSC 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

<p>MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 36</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

Este ítem no aplica.

4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

4.8.4 NOTIFICACIÓN AL SUSCRIPTOR DE LA EMISIÓN DE UN NUEVO CERTIFICADO

4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

4.8.6 PUBLICACIÓN POR EL PSC DE LOS CERTIFICADOS MODIFICADOS

4.8.7 NOTIFICACIÓN POR EL PSC 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 PSC DEBE PROCESAR LA SOLICITUD DE REVOCACIÓN

4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LAS PARTES QUE CONFÍAN

4.9.7 FRECUENCIA DE EMISIÓN DEL CRL

<p>MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 37</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

4.9.8 LATENCIA MÁXIMA PARA CRL

4.9.9 DISPONIBILIDAD PARA REVOCACIÓN/VERIFICACIÓN DE ESTADO EN LÍNEA

4.9.10 REQUISITOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA

4.9.11 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES

4.9.12 REQUERIMIENTOS ESPECIALES POR 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

<p>MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 38</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

5 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

En los apartados siguientes deben ser referidos a los ítems correspondientes de la CPS del PSC responsable o ser detallados los aspectos específicos para la CP, 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

<p>MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 39</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

5.2 CONTROLES PROCEDIMENTALES

5.2.1 ROLES DE CONFIANZA

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES

5.3. CONTROLES DE PERSONAL

5.3.1. REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

5.3.2. PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

5.3.3. REQUERIMIENTOS DE CAPACITACIÓN

5.3.4. REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

5.3.5. FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

5.3.6. SANCIONES PARA ACCIONES NO AUTORIZADAS

5.3.7. REQUISITOS DE CONTRATACIÓN A TERCEROS

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

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 40</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

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

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

5.4.7. NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

5.4.8. EVALUACIÓN DE VULNERABILIDADES

5.5. ARCHIVOS DE REGISTROS

5.5.1. TIPOS DE REGISTROS ARCHIVADOS

5.5.2. PERIODOS DE RETENCIÓN PARA ARCHIVOS

5.5.3 PROTECCIÓN DE ARCHIVOS

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

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 41
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

5.7.3. PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD

5.7.3.1 CERTIFICADO DE ENTIDAD ES REVOCADO

5.7.3.2 CLAVE DE ENTIDAD ESTÁ COMPROMETIDA

5.7.4. CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

5.8. EXTINCIÓN DE UN PSC O ENTIDADES VINCULADAS

6. CONTROLES TÉCNICOS DE SEGURIDAD

La CP debe definir las medidas de seguridad, necesarias para proteger las claves criptográficas de los titulares de certificados emitidos según la CP. También deben ser definidos otros controles técnicos de seguridad utilizados por el PSC y por las RAs a ella vinculadas para la ejecución de sus funciones operacionales.

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES


6.1.1. GENERACIÓN DEL PAR DE CLAVES

Cuando el titular del certificado sea una persona física, éste será el responsable de generar el par de claves criptográficas. Cuando el titular del certificado sea una persona jurídica, la persona física autorizada y con la atribución de representante conforme a los estatutos o normas correspondientes a su funcionamiento, será la persona responsable de la generación del par de claves criptográficas, del uso del certificado y poseedor de la clave privada.

En este ítem, la CP debe describir todos los requisitos y procedimientos referentes al proceso de generación de claves aplicables al certificado que define.

El algoritmo a ser utilizado para las claves criptográficas de titulares de certificados está definido en el documento DOC-PKI-06 [1].

Cuando es generada, la clave privada de la persona física o jurídica, titular del certificado deberá ser grabada cifrada mediante un algoritmo simétrico aprobado en el documento DOC-

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 42</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

PKI-06 [1], en un medio de almacenamiento definido para cada tipo de certificado previsto en la PKI-Paraguay conforme a lo estipulado en la Tabla N° 2 del ítem 6.2.7.

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.

6.1.2. ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR

Ítem no aplicable.

6.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

La CP debe detallar los procedimientos utilizados para la entrega de la clave pública del titular del certificado al PSC responsable. En los casos en los que se genere una solicitud de certificado (CSR) por el titular, deberá adoptarse el formato definido en el documento DOC-PKI-06 [1].

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


En este ítem, la CP debe definir las formas para la entrega del certificado del PSC responsable y de todos los certificados de la cadena de certificación, para los usuarios de la PKI-Paraguay, la cual podrá comprender, entre otras:

- a) en el momento de entrega de un certificado a su titular, usando el formato definido en el documento DOC-PKI-06 [1];
- b) un directorio;
- c) una página WEB del PSC; y
- d) otros medios seguros aprobados por el MIC.

6.1.5. TAMAÑO DE LA CLAVE

En este ítem se debe definir el tamaño de las claves criptográficas asociadas a los certificados emitidos según la CP.

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

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 43</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

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

La CP debe prever que los parámetros de generación y verificación de calidad de claves asimétricas de las personas físicas o jurídicas titulares de certificados, adoptarán el estándar definido en el documento DOC-PKI-06 [1].

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

En este ítem, la CP debe especificar los propósitos para los cuales, podrán ser utilizadas las claves criptográficas de los titulares de los certificados, así como las posibles restricciones aplicables, de conformidad con los usos definidos para los certificados correspondientes (ítem 1.4).

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

En los apartados siguientes, la CP debe definir los requisitos para la protección de las claves privadas de los titulares según la CP.


6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO

En este ítem, en su caso, deben ser especificados los estándares requeridos para los módulos de generación de las claves criptográficas, de conformidad con las normas establecidas en el documento DOC-PKI-06 [1].

En este ítem la CP debe describir los requisitos aplicables al módulo criptográfico utilizado para almacenar la clave privada del titular del certificado. Pueden indicarse estándares de referencia, observando los estándares definidos en el documento DOC-PKI-06 [1].

6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA

Ítem no aplicable.

<p>MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 44</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

6.2.3 CUSTODIA (ESCROW) DE LA CLAVE PRIVADA

En este ítem, la CP debe identificar quién es el agente de custodia (escrow), de qué manera está la clave en custodia (por ejemplo, incluye el texto en claro, cifrado, por división de clave) y cuáles son los controles de seguridad del sistema de custodia.

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 PSC responsable de la CP no puede conservar una copia de seguridad de la clave privada del titular del certificado de firma digital emitido por este. A solicitud del respectivo titular, o de una empresa u organismo, cuando el titular del certificado sea su empleado/funcionario o cliente, el PSC podrá mantener una copia de seguridad de la clave privada correspondiente al certificado de cifrado emitido por ella.

Un PSA habilitado por el MIC podrá custodiar una copia de seguridad de la clave privada correspondiente al certificado de firma digital o cifrado emitido por un PSC al cual está vinculado conforme a lo establecido en los documentos DOC-PKI-07 [2] y DOC-PKI-08 [3].


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

Además de las observaciones anteriores, la CP debe describir todos los requisitos y procedimientos aplicables al proceso de generar una copia de respaldo.

6.2.5. ARCHIVADO DE LA CLAVE PRIVADA

En este ítem, en una CP que define certificados de cifrado, deben ser descritos, cuando sea el caso, los requisitos para el archivado de las claves privadas. Las claves privadas asociadas a certificados de firma digital no deben archivar.

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

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 45</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

6.2.6. TRANSFERENCIA DE CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRIPTOGRÁFICO

En este ítem, cuando corresponda, deben ser definidos los requisitos para la inserción de la clave privada del titular en un módulo criptográfico.

6.2.7. ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

Los medios de almacenamiento de la clave privada deberán asegurar, por medios técnicos y de procedimiento adecuados, como mínimo, que:

- a) la clave privada es única y su confidencialidad es suficientemente asegurada;
- b) la clave privada no puede, con una seguridad razonable, ser deducida y debe estar protegida contra falsificaciones realizadas a través de las tecnologías disponibles en la actualidad; y
- c) la clave privada puede ser eficazmente protegida por el legítimo titular contra su utilización por parte de terceros.


Esos medios de almacenamiento no deben modificar los datos que serán firmados, ni deben impedir que esos datos sean presentados al firmante antes del proceso de firma.

Respecto al almacenamiento de claves privadas de usuarios finales en el ámbito de la PKI-Paraguay, éste podrá ser realizado conforme a los siguientes supuestos:

- i. por una entidad debidamente habilitada como PSA, en los términos del documento DOC-PKI-07 [2] y DOC-PKI-08 [3]; o
- ii. por organizaciones que requieran el almacenamiento de claves privadas de sus empleados o funcionarios en los términos del documento DOC-PKI-09 [4];

En los supuestos mencionados en el párrafo anterior, para hacer efectivo el almacenamiento de claves privadas de usuarios finales se deberá cumplir con las siguientes condiciones:

- i. se requerirá el conocimiento y consentimiento expreso del titular del certificado en concordancia con las disposiciones establecidas en la CPS del PSC; y

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 46
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

ii. se limitará exclusivamente a los certificados del Tipo F3.


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

Tipo de certificado	Medio de almacenamiento
F1 y C1	<ul style="list-style-type: none"> • Tarjeta inteligente o token, ambos sin capacidad de generación de claves y protegidos por contraseña y/o identificación biométrica homologado por el MIC; o • Repositorio protegido por contraseña y/o identificación biométrica, cifrado por software homologado por el MIC.
F2 y C2	<ul style="list-style-type: none"> • Hardware criptográfico homologado el MIC (Tarjeta inteligente o token con capacidad de generación de claves)
F3 y C3	<ul style="list-style-type: none"> • Hardware criptográfico homologado por el MIC (HSM)

Cuando corresponda, la CP debe describir los requisitos aplicables al módulo criptográfico utilizado para almacenar la clave privada de usuario final. Pueden indicarse estándares de referencia, como los definidos en el documento DOC-PKI-06 [1].

6.2.8. MÉTODO DE ACTIVACIÓN DE CLAVE PRIVADA

En este ítem de la CP, deben ser descritos los requisitos y los procedimientos necesarios para la activación de la clave privada de la persona física o jurídica del titular del certificado. Deben ser definidos los agentes autorizados para activar esa clave, el método de confirmación de identidad de esos agentes (por ejemplo, contraseñas, tokens, biometría, etc.) y las acciones necesarias para la activación.

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 47
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

6.2.9. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

En este ítem de la CP, deben ser descritos los requisitos y los procedimientos necesarios para la desactivación de la clave privada de la persona física o jurídica titular del certificado. Deben ser definidos los agentes autorizados para desactivar esa clave, el método de confirmación de identidad de esos agentes y las acciones necesarias para la desactivación.

6.2.10. MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA

En este ítem de la CP, deben ser descritos los requisitos y los procedimientos necesarios para la destrucción de la clave privada de la persona física o jurídica titular del certificado y de sus copias de seguridad si las hubiere. Deben ser definidos los agentes autorizados, el método de confirmación de identidad de esos agentes y las acciones necesarias, tal como la destrucción física, la sobreescritura o la eliminación de los medios de almacenamiento.

6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES


6.3.1. ARCHIVO DE LA CLAVE PÚBLICA

La CP debe prever que las claves públicas de los titulares de certificados de firma digital y las CRL serán almacenadas por el PSC emisor, luego de la expiración de los certificados correspondientes, de manera permanente, para verificación de firmas generadas durante su período de vigencia.

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

En caso de que la CP se refiere a certificado de firma digital, ella debe prever que las claves privadas de sus titulares deberán ser utilizadas únicamente durante el periodo de validez correspondiente. Las correspondientes claves públicas podrán ser utilizadas durante todo el periodo de tiempo determinado por la normativa vigente, para la verificación de firmas generadas durante el plazo de validez de los respectivos certificados.

En caso de que la CP se refiere a certificado de cifrado, ella debe definir los periodos de usos de las claves correspondientes.

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 48
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

La tabla 3 define los períodos máximos de validez admitidos para cada tipo de certificado previsto por la PKI-Paraguay.

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)
F1 y C1	1	1	Emitido por un tiempo máximo de 1 (un) año, al finalizar ese período pierde su validez.
F2 y C2	2	2	Emitido por un tiempo máximo de 2 (dos) años, al finalizar ese período pierde su validez.
F3 y C3	2	2	Emitido por un tiempo máximo de 2 (dos) años, al finalizar ese período pierde su validez.

6.4 DATOS DE ACTIVACIÓN


En los siguientes ítems de la CP, deben ser 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

La CP debe garantizar que los datos de activación de la clave privada del titular del certificado, si se utiliza, serán únicos.

6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

La CP debe garantizar que los datos de activación de la clave privada del titular del certificado, si se utiliza, serán protegidos contra el uso no autorizado.

MINISTERIO DE INDUSTRIA Y COMERCIO	Dirección General de Firma Digital y Comercio Electrónico	Página 49
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

En este ítem, cuando fuera el caso, deben ser definidos otros aspectos referentes a los datos de activación. Entre esos otros aspectos, pueden ser considerados algunos de aquellos tratados, en relación a las claves, en los ítems 6.1 al 6.3.

6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

La CP debe describir 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 CPS.

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

En caso de que el PSC exija un software específico para la utilización de certificados emitidos según la CP, en los ítems siguientes deben ser descritos los controles implementados en el desarrollo y la gestión de la seguridad referentes a ese software.

6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA

En este ítem de la CP, deben ser abordados aspectos tales como: seguridad del ambiente y del personal de desarrollo, prácticas de ingeniería del software adoptadas, metodología de desarrollo de software, entre otros.

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 50</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

En este ítem, deben ser descritos los procedimientos y las herramientas utilizadas para garantizar que el software y su ambiente operacional, implementan los niveles de seguridad configurados.

6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA


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

6.6.4. CONTROLES EN LA GENERACIÓN DE CRL

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

6.7 CONTROLES DE SEGURIDAD DE RED

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

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 51</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

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 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, CRL Y OCSP

En los siguientes ítems deben ser descritos los formatos de los certificados y de las CRL/OCSP generado según el CP. Deben ser incluidas informaciones sobre las normas adoptadas, sus perfiles, versiones y extensiones. Los requisitos mínimos establecidos en los siguientes ítems deberán ser obligatoriamente considerados en todos los tipos de certificados admitidos en el ámbito de la PKI-Paraguay.

7.1. PERFIL DEL CERTIFICADO

Todos los certificados emitidos por el PSC responsable, según sus respectivas CP, deberán estar 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 PSC responsable, según su CP, deberán implementar 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

En este ítem, la CP debe describir todas las extensiones de certificado utilizadas y su criticidad.


La PKI-Paraguay define las siguientes extensiones como obligatorias:

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 52</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

- a) **Identificador de la clave de la Autoridad Certificadora "Authority Key Identifier", no crítico:** El campo key Identifier debe contener el hash SHA-1 de la clave pública del PSC;
- b) **Identificador de la clave del suscriptor "Subject Key Identifier", no crítico:** debe contener el hash SHA-1 de la clave pública del titular del certificado;
- c) **Uso de Claves "KeyUsage", crítico:**
 - c.1) **para certificados de Firma y/o Protección de correo electrónico:** debe contener el bit digitalSignature activado, pudiendo contener los bits *keyEncipherment* y *nonRepudiation* activados;
 - c.2) **para certificados de cifrado:** solo se pueden activar los bits *keyEncipherment* y *dataEncipherment*;
 - c.3) **para certificados de firma de respuesta OCSP:** debe contener el bit *digitalSignature* activado, pudiendo contener el bit *nonRepudiation* activado;
- d) **Uso extendido de la clave "Extended Key Usage", no crítico:**
 - d.1) **para certificados de Firma y/o Protección de correo electrónico:** al menos uno de los propósitos client authentication OID= 1.3.6.1.5.5.7.3.2 o E-mail protection OID = 1.3.6.1.5.5.7.3.4 debe estar activado y pudiendo implementar otros propósitos instituidos, siempre que sean verificables y previstos por el PSC en su CP, 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) **Políticas de Certificación "Certificate Policies", no crítica:**
 - e.1.1) el campo *policyIdentifier* debe contener el OID de la CP aplicable;
 - e.1.2) el campo *policyQualifiers* debe contener la dirección Web de la CP aplicable;
 - e.2.1) el campo *policyIdentifier* debe contener el OID de la CPS aplicable;
 - e.2.2) el campo *policyQualifiers* debe contener la dirección Web de la CPS aplicable;

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 53</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

- f) **Restricciones Básicas "Basic Constraints", crítica:** debe contener el campo SubjectType CA:No True y el campo PathLenConstraint: Ninguno;
- g) **Puntos de distribución de las CRL "CRL Distribution Points", no crítica:** debe contener 02 (dos) direcciones Web donde se obtenga la CRL correspondiente;
- h) **Acceso a la Información de la Autoridad Certificadora "Authority Information Access", no crítica:**
- h.1) La primera entrada debe contener el método de *acceso id-ad-ca/issuer* al certificado del PSC, para recuperar la cadena de certificación, utilizando uno de los siguientes protocolos de acceso, HTTP, HTTPS o LDAP;
- h.2) La segunda entrada debe contener el método de acceso *id-ad-ocsp*, con la dirección respectiva del respondedor OCSP implementado por el PSC, utilizando uno de los siguientes protocolos de acceso, HTTP, HTTPS o LDAP;
- i) **Nombre Alternativo del Sujeto "Subject Alternative Name", no crítica,** en los siguientes formatos:
- i.1) Para certificado de PERSONA FÍSICA:**
- i.1.1) 6 (seis) campos otherName, NO obligatorios, que contienen:**
1. **Rfc822Name=** [*email del titular del certificado*];
 2. **DirectoryName OID= 2.5.4.10:** [*nombre de la organización en el que presta servicio el titular del certificado*];
 3. **DirectoryName OID= 2.5.4.11:** [*nombre de la unidad de la organización en el que presta servicio el titular del certificado*];
 4. **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*];
 5. **DirectoryName OID=2.5.4.12:** [*posición o función designada al titular del certificado en la organización en el que presta servicio*];
-

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 54</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

6. **DirectoryName** **OID=2.5.4.1:** [*título académico del titular del certificado*];

i.2) Para certificado de PERSONA JURÍDICA:

i.2.1) 2 (dos) campos otherName, obligatorios, que contienen:

1. **DirectoryName** **OID=2.5.4.3:** [*nombre y apellido del responsable del certificado*];
2. **DirectoryName** **OID= 2.5.4.5:** [*siglas CI seguido del número de cédula de identidad civil o las siglas PAS seguido del número de pasaporte según sea el caso*];

i.2.2) 4 (cuatro) campos otherName, NO obligatorios, que contienen:

1. **Rfc822Name=** [*email del responsable del certificado*];
2. **DirectoryName** **OID= 2.5.4.11:** [*nombre de la unidad de la organización en el que presta servicio el responsable del certificado*];
3. **DirectoryName** **OID= 2.5.4.12:** [*posición o función designada al responsable del certificado en la organización en el que presta servicio*];
4. **DirectoryName** **OID=2.5.4.1:** [*título académico del responsable del certificado*];


i.3) Para certificado de MÁQUINA O APLICACIÓN si el titular es persona física:

i.3.1) 1 (un) campo otherName, obligatorio, que contiene:

1. **DirectoryName** **OID=2.5.4.3:** [*nombre y apellido del responsable del certificado*];

i.3.2) 6 (seis) campo otherName, NO obligatorio, que contiene:

1. **Rfc822Name=** [*email del responsable del certificado*];
2. **DirectoryName** **OID= 2.5.4.10:** [*nombre de la organización en el que presta servicio el titular del certificado*];
3. **DirectoryName** **OID= 2.5.4.11:** [*nombre de la unidad de la organización en el que presta servicio el titular del certificado*];
4. **DirectoryName** **OID=2.5.4.5:** [*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*];

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 55</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

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

6. **DirectoryName OID=2.5.4.1:** *[título académico del titular del certificado];*

i.4) Para certificado de MÁQUINA O APLICACIÓN si el titular es persona jurídica:

i.4.1) 3 (tres) campos otherName, obligatorios, que contienen:

1. **DirectoryName OID=2.5.4.10:** *[nombre de la organización titular del certificado];*

2. **DirectoryName OID=2.5.4.3:** *[nombre y apellido del responsable del certificado];*

3. **DirectoryName OID=2.5.4.5:** *[siglas CI seguido del número de cédula de identidad civil o las siglas PAS seguido del número de pasaporte según sea el caso];*

i.4.2) 4 (dos) campos otherName, NO obligatorio, que contienen:

1. **Rfc822Name=** *[email del responsable del certificado];*

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


3. **DirectoryName OID=2.5.4.12:** *[posición o función designada al responsable del certificado en la organización];*

4. **DirectoryName OID=2.5.4.1:** *[título académico del responsable del certificado].*

Los campos otherName definidos por la PKI-Paraguay 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.

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 56</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

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 CA Raíz.


7.1.3. IDENTIFICADORES DE OBJETO DE ALGORITMOS

En este ítem de la CP debe ser indicado el OID (Object Identifier) del algoritmo criptográfico utilizado para la firma de certificado de usuario final de acuerdo al algoritmo admitido en el ámbito de la PKI-Paraguay, conforme a lo estipulado en el documento DOC-PKI-06 [1].


7.1.4. FORMAS DEL NOMBRE

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

- a) **Certificado de persona física:**
- i. **OID=2.5.4.6 C= PY;**
 - ii. **OID=2.5.4.10 O=PERSONA FISICA;**
 - iii. **OID=2.5.4.11 OU= [podrá ser: FIRMA F1, FIRMA F2, FIRMA F3, CIFRADO C1, CIFRADO C2 o CIFRADO C3, 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-PKI-03 [5]];**
 - vi. **OID: 2.5.4.4 SN= [nombre/s del titular del certificado en mayúsculas y sin tilde, conforme documento de identidad presentado];** y
 - vii. **OID:2.5.4.42 GN= [apellido/s del titular del certificado en mayúsculas y sin tilde, conforme documento de identidad presentado];**
- b) **Certificado de persona jurídica:**
- i. **OID=2.5.4.6 C= PY;**
 - ii. **OID=2.5.4.10 O=PERSONA JURIDICA;**

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 57
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

- iii. **OID=2.5.4.11 OU=** *[podrá ser: FIRMA F1, FIRMA F2, FIRMA F3, CIFRADO C1, CIFRADO C2 o CIFRADO C3, conforme lo estipulado en el punto 1.1 y 1.4.1];*
 - iv. **OID: 2.5.4.3 CN=** *[nombre del titular del certificado en mayúsculas y sin tildes, conforme documento de identificación presentado]; y*
 - v. **OID: 2.5.4.5 Serial Number=** *[conforme al formato descrito en el ítem 3.1.4.1 del documento DOC-PKI-03 [5]].*
- c) Certificado de MÁQUINA O APLICACIÓN si el titular es persona física:**
- i. **OID=2.5.4.6 C= PY;**
 - ii. **OID=2.5.4.10 O=** *[podrá ser: MAQUINA o APLICACION, conforme corresponda a una máquina o aplicación];*
 - iii. **OID=2.5.4.11 OU=** *[podrá ser FIRMA F1, FIRMA F2, FIRMA F3, CIFRADO C1, CIFRADO C2 o CIFRADO C3 conforme lo estipulado en el punto 1.1 y 1.4.1];*
 - iv. **OID: 2.5.4.3 CN=** *[podrá contener contener: la URL correspondiente, conforme documento de identificación presentado; o el nombre de la aplicación, conforme documento de identificación presentado]; y*
 - v. **OID: 2.5.4.5 Serial Number[** *conforme al formato descrito en el ítem 3.1.4.3 del documento DOC-PKI-03 [5]].*
- d) Certificado de MÁQUINA O APLICACIÓN si el titular es persona jurídica:**
- i. **OID=2.5.4.6 C= PY;**
 - ii. **OID=2.5.4.10 O=** *[podrá ser MÁQUINA o APLICACIÓN, conforme corresponda a una máquina o aplicación];*
 - iii. **OID=2.5.4.11 OU=** *[podrá ser FIRMA F1, FIRMA F2, FIRMA F3, CIFRADO C1, CIFRADO C2 o CIFRADO C3 conforme lo estipulado en el punto 1.1 y 1.4.1];*
 - iv. **OID: 2.5.4.3 CN=** *[podrá contener contener: la URL correspondiente, conforme documento de identificación; o el nombre de la aplicación, conforme documento de identificación]; y*
 - v. **OID: 2.5.4.5 Serial Number=** *[conforme al formato descrito en el ítem 3.1.4.3 del documento DOC-PKI-03 [5]].*

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 58
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

7.1.5. RESTRICCIONES DEL NOMBRE

Los certificados digitales 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 PKI-Paraguay establece las siguientes restricciones de nombres, aplicables a todos los certificados:

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

Tabla 4 - Caracteres especiales permitidos en los nombres

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

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 59
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020


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

7.1.6. IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO

En este ítem se debe informar el OID asignado a la CP y el OID asignado a la CPS, aplicables. Todo certificado emitido bajo esta CP debe contener, en la extensión "Políticas de Certificado" estas informaciones.

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

Este ítem no aplica.

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 60</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

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

En este ítem se debe informar la dirección Web (URL) de la CP y la dirección Web (URL) de la CPS, aplicables. Todo certificado emitido bajo estos documentos deben contener, en el campo policyQualifiers de la extensión Políticas de certificado "Certificate Policies" estas informaciones.

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


Extensiones críticas deben ser interpretadas conforme a la RFC 5280.

7.2. PERFIL DE LA CRL

Los Listas de Certificados Revocados CRL deberán ser firmados utilizando el algoritmo definido en el documento DOC-PKI-06 [1]

7.2.1 NÚMERO (S) DE VERSIÓN

Las CRL generadas por el PSC responsable según la CP deberán implementar la versión 2 del CRL definida en el estándar ITU X.509, de acuerdo con el perfil establecido en el RFC 5280.

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 61</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

7.2.2 CRL Y EXTENSIONES DE ENTRADAS DE CRL

En este ítem, la CPS debe describir todas las extensiones de CRL utilizadas por el PSC responsable y su criticidad.

La CA Raíz-Py define las siguientes extensiones de CRL como obligatorias:

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

7.3. PERFIL DE OCSP

Las Respuestas OCSP deberán ser firmados utilizando el algoritmo definido en el documento DOC-PKI-06 [1].

7.3.1. NÚMERO (S) DE VERSIÓN


Los servicios de respuesta de OCSP deberán implementar 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.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

En los apartados siguientes se deben referir a los ítems correspondientes de la CPS del PSC responsable o deben ser detallados los aspectos específicos para la CP si los hubiere.

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 62</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

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

9. OTROS ASUNTOS LEGALES Y COMERCIALES

En los apartados siguientes se deben referir a los ítems correspondientes de la CPS del PSC responsable o deben ser detallados los aspectos específicos para la CP si los hubiere.

9.1. TARIFAS


9.1.1. TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

9.1.2. TARIFAS DE ACCESO A CERTIFICADOS

9.1.3. TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN

9.1.4. TARIFAS POR OTROS SERVICIOS

9.1.5. POLÍTICAS DE REEMBOLSO

<p>MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 63</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

9.2. RESPONSABILIDAD FINANCIERA

9.2.1. COBERTURA DE SEGURO

9.2.2. OTROS ACTIVOS

9.2.3. COBERTURA DE SEGURO O GARANTÍA PARA USUARIOS FINALES

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

9.3.1. ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

9.3.2. INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL

9.3.3. 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


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

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 64</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

9.5. DERECHO DE PROPIEDAD INTELECTUAL

9.6. REPRESENTACIONES Y GARANTÍAS

9.6.1. REPRESENTACIONES Y GARANTÍAS DE LA PSC

9.6.2. REPRESENTACIONES Y GARANTÍAS DE LA RA

9.6.3. REPRESENTACIONES Y GARANTÍAS DEL SUSCRIPTOR

9.6.4. REPRESENTACIONES Y GARANTÍAS DE LAS PARTES QUE CONFÍAN

9.6.5. REPRESENTACIONES Y GARANTÍAS DEL REPOSITORIO

9.6.6. 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


En este ítem, se debe establecer que la CP entra en vigencia a partir de la fecha establecida en el instrumento que la aprueba y expedido por la AA

9.10.2. FINALIZACIÓN

Esta CP permanecerá en vigencia indefinidamente, siendo válida y efectiva hasta que sea revocada.

9.10.3. EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

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

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 65</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

9.11. NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

9.12. ENMIENDAS

9.12.1. PROCEDIMIENTOS PARA ENMIENDAS

En este ítem de la CP se debe indicar el procedimiento para enmiendas y que propuestas de modificación de la CP deben ser revisadas y aprobadas por la AA antes de ser implementadas. Las modificaciones deben documentarse y mantenerse actualizadas a través de versiones.

9.12.2. PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

En este ítem, deben ser descriptos los procedimientos utilizados para publicar y notificar las enmiendas o modificaciones realizadas a la CP. Toda enmienda o modificación de la CP, deberá ser publicada en el repositorio del PSC

9.12.3. CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

9.13. DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

9.14. NORMATIVA APLICABLE

9.15. ADECUACIÓN A LA LEY APLICABLE


9.16. DISPOSICIONES VARIAS

9.16.1 ACUERDO COMPLETO

En este ítem debe indicarse que los titulares y partes que confían en los certificados asumen en su totalidad el contenido de la presente CPS y CP.

Esta CP representa las obligaciones y deberes aplicables al PSC y autoridades vinculadas.

En caso de conflicto entre esta CP y otras resoluciones del MIC, prevalecerá siempre la última editada.

MINISTERIO DE INDUSTRIA Y COMERCIO	Dirección General de Firma Digital y Comercio Electrónico	Página 66
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020


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

<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 67</p>
	<p>Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay</p>	<p>Anexo II de la Resolución N° 577/2020</p>

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 N° 4017/2010 "De validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico".
 - Ley N° 4610/2012 "Que modifica y amplía la Ley N° 4017/10 "de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico".
 - Decreto N° 7369/2011 "Por el cual se aprueba el reglamento general de la Ley N° 4017/2010 "de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico".
-

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 68
	Directivas Obligatorias para la Formulación y Elaboración de la Política de Certificación de Los Prestadores de Servicios de Certificación de La PKI-Paraguay	Anexo II de la Resolución N° 577/2020

10.2 REFERENCIAS A DOCUMENTOS QUE COMPONEN LA PKI-Paraguay

Tabla N° 5 – Documentos Referenciados

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	Normas de algoritmos criptográficos de la PKI-Paraguay.	DOC-PKI-06
[2]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación de los prestadores de servicio de almacenamiento de la PKI-Paraguay.	DOC-PKI-07
[3]	Procedimientos operacionales mínimos para los prestadores de servicios de almacenamiento de la PKI-Paraguay.	DOC-PKI-08
[4]	Procedimientos operacionales mínimos para organizaciones que requieran el almacenamiento de claves privadas de la PKI-Paraguay.	DOC-PKI-09
[5]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación de los Prestadores de Servicios de Certificación	DOC-PKI-03