DIGITO
FIRMA DIGITAL

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Versión: 4.0

Año 2022

documenta sociedad anonima

CONTROL DOCUMENTAL

DOCUMENTO	
Título:	Declaración de Practicas de Certificación del PCSC de Documenta S.A.
Fecha:	04/08/2022
Versión:	4.0.0
Código:	PCSC-DOC-DPCV4.0.0
Ubicación física:	Documenta S.A.
Soporte lógico:	https://www.digito.com.py

REGISTRO DE CAMBIOS		
Versión	**Fecha**	**Motivo del cambio**
2.0.0	02/01/2.017	Modificación de la Normativa Vigente
3.0.0	28/03/2.022	Modificación de la Normativa Vigente
4.0.0	04/08/2.022	Modificación de la Normativa Vigente

DISTRIBUCION DEL DOCUMENTO	
Nombre	**Área**
PCSC Documenta S. A	Todas las Áreas
AR vinculadas a PCSC Documenta S.A.	Todas las Áreas
AV vinculadas a PCSC Documenta S.A.	Operadores
Ministerio de Industria y Comercio	Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE)
DOCUMENTO PÚBLICO Y GRATUITO https://www.documenta.com.py	

Preparado	**Verificado**	**Aceptado**
JAVIER DÁVALOS Jefe Operaciones y Productos Documenta S.A.	**ROBERTO FRETES** Supervisor Operaciones Dígito Documenta S.A.	**JOSE ORICCHIO URRUTIA** Presidente Documenta S.A.

Contenido

CONTROL DOCUMENTAL 2
1. INTRODUCCIÓN 12
1.1. DESCRIPCIÓN GENERAL 12
1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO 12
1.3. PARTICIPANTES DE LA ICP 12
1.3.1. AUTORIDADES CERTIFICADORAS (CA) 12
1.3.2. AUTORIDADES DE REGISTRO (AR) 14
1.3.3. AUTORIDADES DE VALIDACIÓN (AV) 14
1.3.4. TITULARES DEL CERTIFICADO 14
1.3.5. PARTE USUARIA 14
1.3.6. OTROS PARTICIPANTES 15
1.3.6.1 PRESTADORES DE SERVICIOS DE SOPORTE (PSS) 15
1.4. USO DEL CERTIFICADO 15
1.4.1. USOS APROPIADOS DEL CERTIFICADO 15
1.4.2. USOS PROHIBIDOS DEL CERTIFICADO 16
1.5 ADMINISTRACIÓN DE LA POLÍTICA 16
1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO 16
1.5.2. PERSONA DE CONTACTO 16
1.5.3. PERSONA QUE DETERMINA LA ADECUACIÓN DE LA DPC A LA PC 16
1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA DPC 16
1.6 DEFINICIONES, SIGLAS Y ACRÓNIMOS 16
1.6.1 DEFINICIONES 16
1.6.2 SIGLAS Y ACRÓNIMOS 22
2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO 24
2.1 REPOSITORIOS 24
2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN 24
2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN 25
2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS 25
3. IDENTIFICACIÓN Y AUTENTICACIÓN 25
3.1 NOMBRES 26
3.1.1. TIPOS DE NOMBRES 26
3.1.2. NECESIDAD DE NOMBRES SIGNIFICATIVOS 26

3.1.3. ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES 26
3.1.4. REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES 26
3.1.5. UNICIDAD DE NOMBRES 27
3.1.6. PROCEDIMIENTO PARA RESOLVER DISPUTA DE NOMBRE 27
3.1.7. RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS 27
3.2 VALIDACIÓN INICIAL DE IDENTIDAD 28
3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA 28
3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA 29
3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA 31
3.2.4 INFORMACIÓN NO VERIFICADA DEL TITULAR DEL CERTIFICADO 33
3.2.5 VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO) 33
3.2.6 CRITERIOS PARA INTEROPERABILIDAD 33
3.2.7 PROCEDIMIENTOS COMPLEMENTARIOS 34
3.2.8 PROCEDIMIENTOS ESPECÍFICOS 34
3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DENUEVAS CLAVES 34
3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN 35
4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO 35
4.1 SOLICITUD DEL CERTIFICADO 35
4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO 36
4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES 36
4.2 PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO 41
4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN 41
4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO 41
4.2.3 TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO 41
4.3 EMISIÓN DEL CERTIFICADO 42
4.3.1 ACCIONES DEL PCSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS 42
4.3.2 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO SOBRE LA EMISIÓN DEL CERTIFICADO ELECTRÓNICO 42
4.4 ACEPTACIÓN DEL CERTIFICADO 42
4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO 42
4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PCSC 42
4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR EL PCSC A OTRAS ENTIDADES 42
4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO 43
4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR O RESPONSABLE 43
4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LA PARTE USUARIA 43

4.6 RENOVACIÓN DEL CERTIFICADO 44
4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO 44
4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN 44
4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO 44
4.6.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO 44
4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO 44
4.6.6 PUBLICACIÓN POR EL PCSC DEL CERTIFICADO RENOVADO 44
4.6.7 NOTIFICACIÓN POR EL PCSC DE LA EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES 44
4.7 RE-EMISIÓN DE CLAVES DE CERTIFICADO (RE-KEY) 44
4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO 44
4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA 44
4.7.3 PROCESAMIENTO DE SOLICITUDES DE RE-EMISIÓN DE CLAVES DE CERTIFICADO 45
4.7.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO SOBRE LA RE-EMISIÓN DE UN NUEVO CERTIFICADO 45
4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE- EMITIDO 45
4.7.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS RE-EMITIDOS 45
4.7.7 NOTIFICACIÓN POR EL PCSC DE LA RE-EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES 45
4.8 MODIFICACIÓN DE CERTIFICADOS 45
4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO 45
4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO 45
4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO 45
4.8.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO DE LA EMISIÓN DE UN NUEVO CERTIFICADO 45
4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO 45
4.8.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS MODIFICADOS 46
4.8.7 NOTIFICACIÓN POR EL PCSC DE UNA EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES 46
4.9 REVOCACIÓN Y SUSPENSIÓN 46
4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN 46
4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN 47
4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN 48
4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN 48
4.9.5 TIEMPO DENTRO DEL CUAL EL PCSC DEBE PROCESAR LA SOLICITUD DE REVOCACIÓN 48
4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LA PARTE USUARIA 48

4.9.7 FRECUENCIA DE EMISIÓN DEL LCR 49
4.9.8 LATENCIA MÁXIMA PARA LCR 49
4.9.9 DISPONIBILIDAD PARA REVOCACIÓN/VERIFICACIÓN DE ESTADO EN LÍNEA 49
4.9.10 REQUISITOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA 50
4.9.11 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES 50
4.9.12 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA 50
4.9.13 CIRCUNSTANCIAS PARA SUSPENSIÓN 50
4.9.14 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN 51
4.9.15 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN 51
4.9.16 LÍMITES DEL PERÍODO DE SUSPENSIÓN 52
4.10 SERVICIOS DE ESTADO DEL CERTIFICADO 52
4.10.1 CARACTERÍSTICAS OPERACIONALES 52
4.10.2 DISPONIBILIDAD DEL SERVICIO 52
4.10.3 CARACTERÍSTICAS OPCIONALES 52
4.11 FIN DE ACTIVIDADES 52
4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES 52
4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES 52
4.12.2 POLÍTICAS Y PRÁCTICAS DE RECUPERACIÓN Y ENCAPSULACIÓN DE CLAVES DE SESIÓN 53
5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES 53
5.1 CONTROLES FÍSICOS 53
5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO 53
5.1.2 ACCESO FÍSICO 53
5.1.3 ENERGÍA Y AIRE ACONDICIONADO 56
5.1.4 EXPOSICIÓN AL AGUA 57
5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO 57
5.1.6 ALMACENAMIENTO DE MEDIOS 57
5.1.7 ELIMINACIÓN DE RESIDUOS 57
5.1.8 RESPALDO FUERA DE SITIO 58
5.2 CONTROLES PROCEDIMENTALES 58
5.2.1 ROLES DE CONFIANZA 58
5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA 60
5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL 60
5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES 60
5.3 CONTROLES DE PERSONAL 61

5.3.1..... REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN 61
5.3.2 PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES 61
5.3.3 REQUERIMIENTOS DE CAPACITACIÓN 61
5.3.4 REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN 62
5.3.5 FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES 62
5.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS 62
5.3.7 REQUISITOS DE CONTRATACIÓN A TERCEROS 63
5.3.8 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL 63
5.4 PROCEDIMIENTO DE REGISTRO DE AUDITORÍA 63
5.4.1 TIPOS DE EVENTOS REGISTRADOS 63
5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS) 65
5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA 65
5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA 65
5.4.5 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE REGISTRO (LOGS) DE AUDITORÍA 65
5.4.6 SISTEMA DE RECOLECCIÓN DE INFORMACIÓN DE AUDITORÍA (INTERNO VS EXTERNO) .. 65
5.4.7 NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO 65
5.4.8 EVALUACIÓN DE VULNERABILIDADES 65
5.5 ARCHIVOS DE REGISTROS 65
5.5.1 TIPOS DE REGISTROS ARCHIVADOS 66
5.5.2 PERÍODOS DE RETENCIÓN PARA ARCHIVOS 66
5.5.3 PROTECCIÓN DE ARCHIVOS 66
5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO 66
5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS 66
5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO) 66
5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA 67
5.6 CAMBIO DE CLAVE 67
5.7 RECUPERACIÓN DE DESASTRES Y COMPROMISO 68
5.7.1 PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO 68
5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES 69
5.7.3 PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD 69
5.7.4 CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE 69
5.8 EXTINCIÓN DE UN PCSC O ENTIDADES VINCULADAS 70
6. CONTROLES TÉCNICOS DE SEGURIDAD 70
6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES 70

6.1.1 ..... GENERACIÓN DEL PAR DE CLAVES 70
6.1.2 ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR 71
6.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO 71
6.1.4 ENTREGA DE LA CLAVE PÚBLICA DE LA AC A LAS PARTES QUE CONFÍAN 71
6.1.5 TAMAÑO DE LA CLAVE 71
6.1.6 GENERACIÓN DE PARÁMETROS DE CLAVE ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD 71
6.1.7 PROPÓSITOS DE USOS DE CLAVE (CAMPO KEY USAGE X.509 V3) 72
6.2 CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO Y PROTECCIÓN DE LA CLAVE PRIVADA 72
6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO 72
6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA 72
6.2.3 CUSTODIA (ESCROW) DE LA CLAVE PRIVADA 72
6.2.4 RESPALDO/COPIA DE LA CLAVE PRIVADA 72
6.2.5 ARCHIVADO DE LA CLAVE PRIVADA 73
6.2.6 TRANSFERENCIA DE CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRIPTOGRÁFICO 73
6.2.7 ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO 73
6.2.8 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA 73
6.2.9 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA 73
6.2.10 MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA 74
6.3 OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES 74
6.3.1 ARCHIVO DE LA CLAVE PÚBLICA 74
6.3.2 PERÍODO OPERACIONAL DEL CERTIFICADO Y PERÍODO DE USO DEL PAR DE CLAVES 74
6.4 DATOS DE ACTIVACIÓN 74
6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN 74
6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN 75
6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN 75
6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR 75
6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS 75
6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR 76
6.5.3 CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO 76
6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA 76
6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA 76
6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD 76
6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA 77

6.6.4 ..... CONTROLES EN LA GENERACIÓN DE LCR 77
6.7 CONTROLES DE SEGURIDAD DE RED 77
6.7.1 DIRECTRICES GENERALES 77
6.7.2 FIREWALL 77
6.7.3 SISTEMA DE DETECCIÓN DE INTRUSOS (IDS) 78
6.7.4 REGISTRO DE ACCESO NO AUTORIZADO A LA RED 78
6.8 FUENTES DE TIEMPO 78
7. PERFILES DE CERTIFICADOS, LCR Y OCSP 78
7.1 PERFIL DEL CERTIFICADO 78
7.1.1 NÚMERO DE VERSIÓN 80
7.1.2 EXTENSIONES DEL CERTIFICADO 80
7.1.3 IDENTIFICADORES DE OBJETO DE ALGORÍTMOS 80
7.1.4 FORMAS DEL NOMBRE 80
7.1.5 RESTRICCIONES DEL NOMBRE 81
7.1.6 IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO 81
7.1.7 USO DE LA EXTENSIÓN RESTRICCIONES DE POLÍTICA (POLICY CONSTRAINTS) 81
7.1.8 SEMÁNTICA Y SINTAXIS DE LOS CALIFICADORES DE POLÍTICA (POLICY QUALIFIERS) 81
7.1.9 SEMÁNTICA DE PROCESAMIENTO PARA LA EXTENSIÓN DE POLÍTICAS DE CERTIFICADO (CERTIFICATE POLICIES) 81
7.2 PERFIL DE LA LCR 81
7.2.1 NÚMERO (S) DE VERSIÓN 82
7.2.2 LCR Y EXTENSIONES DE ENTRADAS DE LCR 82
7.3 PERFIL DE OCSP 82
7.3.1 NÚMERO (S) DE VERSIÓN 82
7.3.2 EXTENSIONES DE OCSP 82
8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES 83
8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN 83
8.2 IDENTIDAD/CALIDAD DEL EVALUADOR 83
8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA 83
8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN 83
8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA 84
8.6 COMUNICACIÓN DE RESULTADOS 84
9. OTROS ASUNTOS LEGALES Y COMERCIALES 84
9.1 TARIFAS 84
9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS 84

9.1.2 TARIFAS DE ACCESO A CERTIFICADOS 85
9.1.3 TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN 85
9.1.4 TARIFAS POR OTROS SERVICIOS 85
9.1.5 POLÍTICAS DE REEMBOLSO 85
9.2 RESPONSABILIDAD FINANCIERA 85
9.2.1 COBERTURA DE SEGURO 85
9.2.2 OTROS ACTIVOS 85
9.2.3 COBERTURA DE SEGURO O GARANTÍA PARA USUARIOS FINALES 85
9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL 85
9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL 85
9.3.2 INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL 86
9.3.3 RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL 86
9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL 86
9.4.1 PLAN DE PRIVACIDAD 86
9.4.2 INFORMACIÓN TRATADA COMO PRIVADA 86
9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA 87
9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA 87
9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA 87
9.4.6 DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO 87
9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN 87
9.4.8 INFORMACIÓN A TERCEROS 87
9.5 DERECHO DE PROPIEDAD INTELECTUAL 87
9.6 REPRESENTACIONES Y GARANTÍAS 88
9.6.1 REPRESENTACIONES Y GARANTÍAS DEL PCSC 88
9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA RA 89
9.6.3 REPRESENTACIONES Y GARANTÍAS DEL SUSCRIPTOR 89
9.6.4 REPRESENTACIONES Y GARANTÍAS DE LAS PARTES QUE CONFÍAN 89
9.6.5 REPRESENTACIONES Y GARANTÍAS DEL REPOSITORIO 89
9.6.6 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES 89
9.7 EXENCIÓN DE GARANTÍA 90
9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL 90
9.9 INDEMNIZACIONES 90
9.10 PLAZO Y FINALIZACIÓN 90
9.10.1 PLAZO 90

9.10.2 FINALIZACIÓN 90
9.10.3 EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA 90
9.11 NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES 90
9.12 ENMIENDAS 91
9.12.1 PROCEDIMIENTOS PARA ENMIENDAS 91
9.12.2 PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN 91
9.12.3 CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS 91
9.13 DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS 91
9.14 NORMATIVA APLICABLE 91
9.15 ADECUACIÓN A LA LEY APLICABLE 91
9.16 DISPOSICIONES VARIAS 91
9.16.1 ACUERDO COMPLETO 91
9.16.2 ASIGNACIÓN 92
9.16.3 DIVISIBILIDAD 92
9.16.4 APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DEDERECHOS) 92
9.16.5 FUERZA MAYOR 92
9.17 OTRAS DISPOSICIONES 92
10. DOCUMENTOS DE REFERENCIA 92
10.1 REFERENCIAS 92
10.2 REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP 93

1. INTRODUCCIÓN

1.1. DESCRIPCIÓN GENERAL

Este documento establece los requisitos mínimos que debe ser obligatoriamente cumplido por el Prestador Cualificado de Servicios de Confianza (PCSC) DOCUMENTA S.A., en su carácter de autoridad certificación intermedia (ACI) y como integrante de la Infraestructura de Clave Pública del Paraguay (ICPC). La Declaración de Prácticas de Certificación (DPC) es un documento que describe los procedimientos empleados por una Autoridad de Certificación (AC) para la correcta ejecución de sus servicios.

La presente DPC se ha elaborado en el ámbito de la ICPP y adopta la estructura definida en el documento DOC-ICPP-03 la cual se basa en el RFC 3647. La presente DPC se ha estructurado teniendo en cuenta las recomendaciones de la RFC 3647.

Este documento compone el conjunto normativo de la ICPP y en él se referencian otras reglamentaciones previstas en las demás normas del ICPP.

La firma electrónica cualificada basada en certificados cualificados conforme a la legislación vigente tiene un efecto jurídico equivalente a una firma manuscrita.

Un sello electrónico cualificado garantiza y da certeza de la integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado.

Los certificados cualificados de firma electrónica y los certificados cualificados tributarios solo podrán emitirse a personas físicas, los certificados de sello electrónico están reservados para personas jurídicas.

1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Nombre del documento	Declaración de Prácticas de Certificación de Documenta S.A.
Versión del documento	4.1
Fecha de aprobación	04/08/2022
Localización	https://www.digito.com.py
OID (Object Identifier)	1.3.6.1.4.1.48615.1.1.2.4.1

1.3. PARTICIPANTES DE LA ICP

1.3.1. AUTORIDADES CERTIFICADORAS (CA)

Son las personas, políticas, procedimientos y sistemas informáticos encargados de la emisión de certificados electrónicos y de la asignación a sus titulares. Así mismo, efectúan la revocación de los mencionados certificados y la generación de claves públicas y privadas, cuando así lo establecen sus prácticas y políticas. A las entidades autorizadas a emitir certificados de clave pública dentro de la ICPP se denominan:

- Autoridad Certificadora Raíz del Paraguay (AC Raíz): emite certificados a los PCSC bajo la jerarquía del Certificado Raíz. El certificado raíz es un certificado auto-firmado, en el que se inicia la cadena de confianza. Subordinados al Certificado Raíz, se encuentran los certificados emitidos al PCSC. En el Paraguay, la cadena de certificación tiene como máximo dos niveles, en el primer nivel se encuentra la AC Raíz, en el segundo nivel, uno o varios PCSC, éstos solo podrán emitir certificados electrónicos a usuarios finales. Se constituye como AC Raíz del Paraguay el MIC.
- Autoridad Certificadora Intermedia (CAI): Es la persona jurídica que emite certificados electrónicos a usuarios finales. En el ámbito de la ICPP un PCSC es considerada una CAI.

El PCSC DOCUMENTA S.A. es una entidad habilitada por la AA, encargada de operar una AC en el marco de la ICPP, cuenta con un certificado electrónico emitido por la AC Raíz-Py y solo podrá emitir certificados a usuarios finales.

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

Un PCSC presta servicios de creación, verificación y validación de firmas electrónicas cualificadas y/o sello electrónico cualificado y certi0ficados relativos a estos servicios.

El PCSC DOCUMENTA S.A. además podrá ser habilitado para prestar servicios de generación o gestión de datos de creación de firma electrónica y/o datos de creación de sello electrónico en nombre del firmante o creador del sello en los términos establecidos en el documento DOC-ICPP-04 [1] y DOC-ICPP-07 [2].

El PCSC DOCUMENTA S.A., una vez habilitado para brindar servicios de generación o gestión de datos de creación de firma electrónica y/o datos de creación de sello electrónico en nombre del firmante o creador del sello, deberá utilizar sistemas y productos fiables, incluidos canales de comunicación electrónicos seguros, aplicar procedimientos y mecanismos técnicos y organizativos adecuados para garantizar que el entorno sea confiable y que los datos de creación se utilicen bajo el control exclusivo del titular del certificado. Además, deberá custodiar y proteger los datos de creación de firma frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

Las claves privadas de los firmantes y/o de los creadores de sellos almacenadas en dispositivos estandarizados conforme lo establecido en el documento DOC-ICPP-04 [1], y las firmas electrónicas cualificadas o los sellos electrónicos cualificados realizadas con la clave privada del firmante y/o creador del sello son válidas de conformidad a la Ley N° 6822/2021.

1.3.2. AUTORIDADES DE REGISTRO (AR)

Son las personas, políticas, procedimientos y sistemas informáticos encargados de los procesos de recepción, identificación y remisión de solicitudes de emisión o revocación de certificados electrónicos y de identificación de sus solicitantes.

DOCUMENTA S.A. cumple funciones de AR. Además, podrá mediante un acuerdo operacional establecer Autoridades de Registros Delegadas siempre y cuando las mismas estén autorizadas por la AC Raíz con la habilitación correspondiente.

Los datos referentes a las AR habilitadas por DOCUMENTA S.A. se encuentran en la dirección de página web (URL) https://www.digito.com.py/autoridades-de-registro

El PCSC DOCUMENTA S.A. mantiene publicada en el sitio las siguientes informaciones actualizadas:

- Lista de todas las AR habilitadas;
- para cada RA, las direcciones de todas las instalaciones técnicas, autorizadas por la AC Raíz-Py para funcionar;
- acuerdos operacionales celebrados entre el PCSC DOCUMENTA S.A. y una AR delegada; y
- la lista de todas las AR cuya habilitación fue revocada, con la indicación de la fecha de revocación.

1.3.3. AUTORIDADES DE VALIDACIÓN (AV)

Son entidades propias o externas a las que recurre la AC mediante un acuerdo operacional autorizado por la AC Raíz-Py con la habilitación correspondiente para suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una AR y certificados por la AC.

Las informaciones actualizadas de las VA habilitadas por el PCSC DOCUMENTA S.A. se encuentran en la dirección de página web (URL) https://www.digito.com.py/autoridades-de-validacion en donde se publica:

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

1.3.4. TITULARES DEL CERTIFICADO

Se definen como aquellas personas físicas o jurídicas que podrán ser titulares de los certificados emitidos por el PCSC según corresponda a un certificado cualificado de firma electrónica, tributario o de sello electrónico cualificado respectivamente conforme a esta DPC.

1.3.5. PARTE USUARIA

Se entenderá por parte usuaria, toda persona física o jurídica, diferente al titular del certificado que

decide aceptar y confiar en un certificado electrónico emitido dentro de la ICPP.

Una parte usuaria puede o no, ser un titular de certificado.

1.3.6. OTROS PARTICIPANTES

1.3.6.1 PRESTADORES DE SERVICIOS DE SOPORTE (PSS)

PSS son entidades externas a las que recurre la AC o la AR mediante un acuerdo operacional autorizado por la AC Raíz-Py con la habilitación correspondiente para desempeñar actividades descritas en esta DPC o en una PC y se clasifican en tres categorías, conforme al tipo de actividades prestadas;

A) disponibilización de infraestructura física y lógica;

B) disponibilización de recursos humanos especializados; y

C) disponibilización de infraestructura física y lógica y de recursos humanos especializados.

Las informaciones actualizadas de las PSS habilitadas por el PCSC DOCUMENTA S.A. se encuentran en la dirección de página web (URL) https://www.digito.com.py/prestadores-de-servicios

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

1.4. USO DEL CERTIFICADO

1.4.1. USOS APROPIADOS DEL CERTIFICADO

Las Políticas de Certificación del PCSC DOCUMENTA S.A. correspondientes a cada tipo de certificado que emita son las que determinan los usos apropiados que debe darse a cada certificado.

A continuación, las PC implementadas por el PCSC DOCUMENTA S.A.

Política	OID
Política de Certificación Sello Electrónico S1 V.1	1.3.6.1.4.1.48315.1.1.1.7.1
Política de Certificación Sello Electrónico S2 V.1	1.3.6.1.4.1.48315.1.1.1.8.1
Política de Certificación Sello Electrónico S3 V.1	1.3.6.1.4.1.48315.1.1.1.9.1
Política de Certificación de Firma Electrónica Tipo F2 V.1	1.3.6.1.4.1.48315.1.1.1.10.1
Política de Certificación de Firma Electrónica Tipo F3 V.1	1.3.6.1.4.1.48315.1.1.1.11.1
Política de Certificación de Firma Electrónica Tipo F3 V.1	1.3.6.1.4.1.48315.1.1.1.11.1
Política de Certificación de Certificado Cualificado Tributario F1 V.1	1.3.6.1.4.1.48315.1.1.1.12.1
Política de Certificación de Certificado Cualificado Tributario F2 V.1	1.3.6.1.4.1.48315.1.1.1.13.1
Política de Certificación de Certificado Cualificado Tributario F3 V.1	1.3.6.1.4.1.48315.1.1.1.14.1

1.4.2. USOS PROHIBIDOS DEL CERTIFICADO

Los certificados deben emplearse de acuerdo con las funciones y finalidades definidas en su correspondiente PC, sin que puedan utilizarse para otras tareas y otros fines no contemplados en aquella.

Las PC implementadas por el PCSC DOCUMENTA S.A. son las identificadas en el ítem anterior.

1.5 ADMINISTRACIÓN DE LA POLÍTICA

1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre del PCSC: DOCUMENTA S.A.

1.5.2. PERSONA DE CONTACTO

Nombre: JEFE OPERACIONES Y PRODUCTOS DIGITO DE DOCUMENTA S.A.

Teléfono: 021 7290002

Página web: https://www.digito.com.py

E-mail: firmadigital@documenta.com.py

Dirección: Avda. Rca. Argentina 893 c/ Alberto de Souza, Asunción - Paraguay

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

Nombre: JEFE DE OPERACIONES Y PRODUCTOS

Teléfono: 021 7290002

E-mail: firmadigital@documenta.com.py

Dirección: Avda. Rca. Argentina 893 c/ Alberto de Souza, Asunción – Paraguay

La entidad competente para determinar la adecuación de esta DPC es el personal del PCSC DOCUMENTA S.A. con autorización del Directorio, conforme con los estatutos de la empresa. Además, según lo establecido en la normativa vigente, la AA será la encargada de determinar la adecuación de la DPC de los PCSC que formen parte de la ICPP.

1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA DPC

El Directorio y el personal autorizado del PCSC DOCUMENTA S.A., conforme con los estatutos de la empresa, aprobaran el contenido de la DPC y sus posteriores enmiendas. Luego será puesta a consideración de la AA para su aprobación.

1.6 DEFINICIONES, SIGLAS Y ACRÓNIMOS

1.6.1 DEFINICIONES

1) **Agente de registro**: persona responsable de la realización de las actividades inherentes a

la AR. Es la persona que realiza la identificación de los solicitantes en la solicitud de emisión/revocación de certificados de firma electrónica cualificada o sello electrónico cualificado.

2) **Autenticación**: proceso técnico que permite determinar la identidad de una persona física o jurídica.
3) **Autenticación electrónica**: proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico.
4) **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.
5) **Autoridad de Certificación**: entidad que presta servicios de emisión, gestión, revocación u otros servicios inherentes a la certificación digital. En el marco de la ICPP, son Autoridades de Certificación la AC Raíz-Py y el PCSC.
6) **Autoridad de Certificación Raíz del Paraguay**: órgano técnico, cuya función principal es coordinar el funcionamiento de la ICPP. La AC Raíz-Py tiene los certificados de más alto nivel, posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza. Las funciones de la AC Raíz-Py son ejercidas por la AA.
7) **Autoridad de Certificación Intermedia**: entidad cuyo certificado de clave pública ha sido emitido por la AC Raíz-Py; es responsable de la emisión de certificados cualificados a personas físicas y jurídicas. Un Prestador Cualificados de Servicios de Confianza es considerado una Autoridad de Certificación Intermedia.
8) **Autoridad de Registro:** entidad responsable de la interfaz entre el usuario y el Prestador de Servicios de Certificación (PCSC). Siempre está vinculado a un PCSC y su función es recibir solicitudes de emisión o revocación de certificados electrónicos del solicitante, identificar de forma presencial al mismo y remitir la solicitud al PCSC. La AR puede ser propia del PCSC o delegada a un tercero. entidad responsable de tramitar las distintas solicitudes inherentes a certificados cualificados, identificar al solicitante y remitir las solicitudes al PCSC. La AR puede ser propia del PCSC o delegada a un tercero.
9) **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 AV puede ser propia del PCSC o delegada a un tercero.
10) **Gestión de datos de creación de firma o sello electrónico:** El PCSC podrá, en nombre del firmante o creador de sello gestionar los datos de creación de firma o sello electrónico a los que hayan prestado sus servicios, este servicio deberá ser provisto por un PCSC siempre y cuando cuente con la debida habilitación.
11) **Cadena de certificación:** lista ordenada de certificados que contiene un certificado de usuario final y certificados de las AC, que termina en un certificado raíz. El emisor del

certificado del usuario final es el titular del certificado del PCSC y a su vez, el emisor del certificado del PCSC es el titular del certificado de AC Raíz-Py. El usuario final o la parte usuaria debe verificar la validez de los certificados en la cadena de certificación.

12) **Certificado cualificado de firma electrónica:** un certificado de firma electrónica que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 43 de la ley Nº 6822/2021.
13) **Certificado cualificado de sello electrónico:** un certificado de sello electrónico que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 53 de la ley Nº 6822/2021.
14) **Certificado cualificado tributario:** certificado expedido por un Prestador Cualificado de Servicios de Confianza, el cual podrá ser utilizado para todos los fines convencionales ante el Sistema Marangatu, Sistema Integrado de Facturación Electrónica Nacional, otros Sistemas de Información administrados por la Subsecretaría de Estado de Tributación (SET) así como otros usos afines autorizados por la Autoridad de Aplicación.
15) **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.
16) **Cifrado asimétrico**: tipo de cifrado que utiliza un par de claves criptográficas diferentes (ejemplo: privado y público) y matemáticamente relacionadas.
17) **Contrato de prestación de servicio de confianza:** Acuerdo entre la AC Raíz-Py y el PCSC, o entre el PCSC y el titular o responsable del certificado que contiene información relativa al solicitante del certificado y además establece los derechos, obligaciones y responsabilidades de las partes con respecto a la prestación del servicio. Este contrato, requiere la aceptación explícita de las partes intervinientes.
18) **Claves criptográficas**: valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.
19) **Clave pública y privada**: la criptografía en la que se basa la ICPP, 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 electrónico, mientras que a la otra se le denomina privada y está bajo exclusivo control del titular del certificado.
20) **Compromiso**: violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.
21) **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 AC, constituye un recinto seguro que alberga, entre otras cosas, los módulos criptográficos de hardware, protege la infraestructura tecnológica y es el lugar donde se ejecutan servicios del ciclo de vida del certificado. La importancia del data center radica en la protección que brinda a la clave

privada y asegura la confianza en los certificados electrónicos emitidos por la AC.

22) **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.
23) **Declaración de Prácticas de Certificación**: declaración de las prácticas que emplea una AC al emitir certificados y que define la infraestructura, políticas y procedimientos que utiliza la AC para satisfacer los requisitos especificados en la PC vigente.
24) **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 electrónico será considerada la cédula de identidad o el pasaporte del solicitante.
25) **Dossier de titular del certificado**: Conjunto formado por la verificación de los documentos de identificación utilizados para la emisión del certificado, solicitud de certificado y Contrato de Prestación de Servicios de Confianza, 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 Contrato de Prestación de Servicios de Confianza 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.
26) **Emisor del certificado**: persona jurídica cuyo nombre aparece en el campo emisor de un certificado.
27) **Emisión de certificado**: es la autorización de la emisión del certificado en el sistema del PCSC previa comprobación de la concordancia de los datos de solicitud del certificado con los contenidos en los documentos presentados.
28) **Firma electrónica cualificada:** una firma electrónica que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica, la cual deberá estar vinculada al firmante de manera única, permitir la identificación del firmante, haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo y estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.
29) **Firmante:** una persona física que crea una firma electrónica.
30) **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, 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.

31) **Habilitación**: autorización que otorga el MIC, una vez cumplidos los requisitos y condiciones establecidos en la norma.
32) **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.
33) **Identificación del Solicitante 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 en la presente DPC.
34) **Infraestructura de Claves Públicas del Paraguay**: conjunto de personas, normas, leyes, políticas, procedimientos y sistemas informáticos necesarios para proporcionar una plataforma criptográfica de confianza que garantiza la presunción de validez legal para actos electrónicos firmados o cifrados con certificados electrónicos y claves criptográficas emitidas por esta infraestructura.
35) **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.
36) **Lista de Certificados Revocados:** lista emitida por una AC, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.
37) **Lista de Confianza:** Lista publicada en el sitio web oficial de la AC Raíz - Py y que contiene información relativa a los Prestadores cualificados de servicios de confianza y a los servicios cualificados que éstos prestan conforme a la Ley Nº 6822/21.
38) **Módulo criptográfico:** software o hardware criptográfico que genera y almacenas claves criptográficas.
39) **Módulo de Seguridad de Hardware:** dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.
40) **Normas Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la prestación de los servicios mencionados en la presente DPC.
41) **Organismo de Evaluación de Conformidad:** organismo que desempeña actividades de evaluación de la conformidad a un prestador de servicios de confianza y de los servicios de confianza que este presta conforme a la Ley Nº 6822/2021.
42) **Organismo de Supervisión:** organismo que concede y retira la cualificación a los prestadores de servicios de confianza y a los servicios de confianza que prestan además de las funciones establecidas en el artículo 17 de la Ley Nº 6822/2021.
43) **Parte usuaria:** es toda persona física o jurídica diferente del titular, que decide aceptar y confiar en un certificado emitido en el marco de la ICPP.
44) **Perfil del certificado:** especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).

45) **Política de Certificación:** documento en el cual la AC define el conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad particular y/o una clase de aplicaciones con requisitos comunes de seguridad.
46) **Prestador Cualificado de Servicios de Confianza:** prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la habilitación.
47) **Política de Seguridad:** es un conjunto de directrices destinadas a definir la protección del personal, seguridad física, lógica y de red, clasificación de la información, salvaguarda de activos de la información, gerenciamiento de riesgos, plan de continuidad de negocio y análisis de registros de eventos de una AC.
48) **Prestador de Servicios de Soporte:** entidad externa vinculada a un PCSC mediante un acuerdo operacional a la que recurre la AC o la AR y autorizada la AC Raíz-Py para desempeñar actividades descritas en la DPC o en una PC.
49) **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.
50) **Repositorio**: sitio principal de Internet confiable y accesible, mantenido por la AC con el fin de difundir su información pública.
51) **Rol de confianza:** función crítica que desempeña personal de la AC, que si se realiza insatisfactoriamente puede tener un impacto adverso sobre el grado de confianza proporcionado por la AC.
52) **Servicio OCSP:** permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la AC sobre el estado de un certificado.
53) **Solicitante de Certificado**: persona física o jurídica que solicita la emisión de un certificado a una AC.
54) **Solicitud de Firma de Certificado**: petición de certificado electrónico que se envía a la AC. mediante la información contenida en el CSR, la AC, puede emitir el certificado electrónico una vez realizadas las comprobaciones que correspondan.
55) **Solicitud de certificado**: documento que se instrumenta mediante un formato autorizado de solicitud de certificado o como parte del documento específico denominado Contrato de Prestación de Servicios de Confianza, suscripto por el solicitante en nombre propio en el caso de certificados cualificados de firma electrónica para persona física, o bien en nombre del titular en el caso de certificados cualificados para persona jurídica.
56) **Solicitud de revocación**: documento que se instrumenta mediante un formato autorizado de solicitud para la revocación de un certificado.
57) **Verificación y validación de firma o sello:** determinación y validación de que la firma o sello electrónico fue creado durante el periodo operacional de un certificado válido, por la clave privada correspondiente a la clave pública que se encuentra en el certificado y

que el mensaje no ha sido alterado desde que su creación.

58) **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.

59) **X.509**: estándar desarrollado por la ITU, que define el formato electrónico básico para certificados electrónicos.

1.6.2 SIGLAS Y ACRÓNIMOS

Tabla Nº 1 - Siglas y Acrónimos

Sigla/Acrónimo	Descripción
AA	Autoridad de Aplicación
AC	Autoridad de Certificación
AGD	Autoridad de Gestión de Datos
AGR	Agente de Registro
C	Country (C por su sigla en inglés, Country)
CAI	Autoridad de Certificación Intermedia
AC Raíz-Py	Autoridad Certificadora Raíz del Paraguay
CI	Cédula de identidad
CN	Nombre común (CN por sus siglas en inglés, Common Name)
PC	Políticas de Certificación
DPC	Declaración de Prácticas de Certificación
LCR	Lista de certificados revocados
CRL	Lista de certificados revocados (CRL por sus siglas en inglés, Certificate Revocation List)
CSR	Solicitud de firma de Certificado (CSR por sus siglas en inglés, certificate Signing Request)
DGCE	Dirección General de Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.

DN	Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de un directorio X.500.
HSM	Módulo de Seguridad Criptográfico basado en Hardware (HSM por sus siglas en inglés, Hardware Security Module)
ISO	Organización Internacional para la Estandarización (ISO por sus siglas en inglés, International Organization for Standardization).
MIC	Ministerio de Industria y Comercio
O	Organización (por su sigla en inglés, Organization)
OCSP	Servicio de validación de certificados en línea (OCSP por sus siglas en inglés, Online Certificate Status Protocol)
OID	Identificador de Objeto (OID por sus siglas en inglés, Object Identifier)
OU	Unidad Organizacional (OU por sus siglas en inglés, Organization Unit)
PAS	Pasaporte
PCN	Plan de Continuidad del Negocio
PKI	Infraestructura de Clave Pública (PKI por sus siglas en inglés, Public Key Infrastructure).
ICPP	Infraestructura de Claves Públicas del Paraguay
OEC	Organismo de Evaluación de la Conformidad
PCSC	Prestador Cualificado de Servicios de Certificación
PS	Política de Seguridad
PSS	Prestador de Servicios de Soporte
Py	Paraguay
AR	Autoridad de Registro
RFC	Petición de Comentarios (RFC por sus siglas en inglés, Request For Comments)
RUC	Registro único del Contribuyente
SN	Número de Serie (por sus siglas en inglés, Serial Number)

UPS	Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés, uninterruptible power supply)
URL	Localizador uniforme de recursos (URL por sus siglas en inglés, Uniform Resource Locator).
AV	Autoridad de validación

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

2.1 REPOSITORIOS

El repositorio de PCSC DOCUMENTA S.A. cumple con las siguientes obligaciones:

a) poner a disposición, inmediatamente después de su emisión, los certificadosemitidos por el PCSC y su CRL/OCSP;
b) estar disponible para consultas las 24 (veinticuatro) horas del día, los 7 (siete)días de la semana;
c) implementar los recursos necesarios para la seguridad de los datos allí almacenados; y
d) proporcionar 02 (dos) repositorios, en infraestructuras de red segregada, para la distribución del LCR/OCSP.

El repositorio del PCSC DOCUMENTA S.A. consiste en un servicio Web de acceso libre que no contiene ninguna información de naturaleza confidencial. Las informaciones del repositorio son publicadas en la página web https://www.digito.com.py El acceso se realiza vía HTTPS.

2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

El repositorio del PCSC DOCUMENTA S.A. está disponible durante 24 horas al día, 7 días a la semana. Consiste en un servicio Web de acceso libre. Dicho repositorio no contiene ninguna información de naturaleza confidencial. En caso de interrupción por causa de fuerza mayor, el servicio se deberá restablecer en un plazo no mayor a veinticuatro horas, garantizando la disponibilidad del servicio con un mínimo de 99,5% anual, un tiempo programado de inactividad máximo de 0,5% anual. El PCSC DOCUMENTA S.A. mantiene un repositorio en su sitio principal de internet que permite a las partes que confían verificar en línea la revocación de un Certificado y cualquier otra información necesaria para validar el estado del mismo.

El PCSC DOCUMENTA S.A. mantiene publicada, entre otros aspectos la versión actualizada de:

a) PC y DPC que implementan;
b) el certificado de la AC Raíz-Py;
c) su propio certificado;
d) la lista de certificados revocados;
e) certificados emitidos;
f) proforma del Contrato de Prestación de Servicios de Confianza;

g) la información relevante del resultado de la última auditoría que hubiere sidoobjeto;
h) leyes, decretos, reglamentos y resoluciones que rigen la actividad de la ICP-Paraguay;
i) Identificación, domicilio y medios de contacto;
j) una lista, actualizada periódicamente, que contiene las AR propias y delegadas con las respectivas direcciones de las instalaciones técnicas de operación, autorizadas por la CA Raíz-Py para funcionar;
k) acuerdos operacionales celebrados entre un PCSC y una AR delegada;
l) una lista actualizada de todas las ARs cuya habilitación fue revocada, con indicación de la fecha de revocación;
m) la lista de todas las AVs habilitadas;
n) para cada AV, las direcciones de todas las instalaciones técnicas, autorizadas por la AC Raíz-Py para funcionar;
o) acuerdos operacionales celebrados entre un PCSC y una AV delegada;
p) la lista de todas las AVs cuya habilitación fue revocada, con la indicación de la fecha de revocación; y
q) una lista, actualizada periódicamente de los PSS vinculados a un PCSC.

2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN

Las enmiendas o modificaciones de la DPC se publicarán de acuerdo con lo establecido en el punto 9.12 de este documento. Las actualizaciones del Contrato de Prestación de Servicios de Confianza serán publicadas cuando sufran modificaciones. La información de estados de certificado, es publicada de acuerdo con a lo dispuesto en el punto 4.9.7 de este documento. Las demás informaciones mencionadas en el punto anterior, serán actualizadas lo más pronto posible y con un máximo de un día hábil desde que se dispongan o surjan modificaciones.

2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

El acceso para la consulta de las informaciones establecidas en el Ítem 2.2 es abierto. Sólo el personal asignado de DOCUMENTA S.A. está autorizada a modificar, sustituir o eliminar información de su repositorio y sitio web. Los controles de acceso establecen identificación personal para el acceso a los equipamientos, utilizando contraseñas y protocolos seguro de comunicación de datos.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

El PCSC DOCUMENTA S.A. comprobará la identidad y/o atributos de las personas físicas y jurídicas antes de incluir estos atributos en un certificado electrónico en el marco de la ICPP. Se prohíbe a las personas físicas y jurídicas utilizar en sus certificados nombres que violen los derechos de propiedad

intelectual de terceros. El PCSC DOCUMENTA S.A. se reserva el derecho, sin responsabilidad ante ningún solicitante, de rechazar solicitudes.

El PCSC DOCUMENTA S.A. mantendrá políticas y procedimientos internos que deben ser revisados periódicamente para cumplir con los requisitos establecidos por la AC Raíz-Py,

Todo el proceso de identificación del titular del certificado debe ser registrado y firmado digitalmente por los ejecutantes. Dichos registros deben realizarse de tal manera que permitan la completa reconstrucción de los procesos realizados, para fines de auditoría.

Se debe mantener un archivo con copias de todos los documentos utilizados para confirmar la identidad de una persona física o jurídica y anexar al dossier del Titular del Certificado. Dichas copias podrán conservarse en papel o en formato digital, sujeto a las condiciones definidas en el documento DOC-ICPP-05.

3.1 NOMBRES

3.1.1. TIPOS DE NOMBRES

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

3.1.2. NECESIDAD DE NOMBRES SIGNIFICATIVOS

En todos los casos los nombres distintivos de los titulares de los certificados son significativos, ajustándose a las normas impuestas en el apartado anterior.

3.1.3. ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES

Se admitirá el uso de seudónimos en los certificados cualificados firma electrónica emitidos por el PCSC DOCUMENTA S.A. En este caso, se deberá constatar la verdadera identidad del titular del certificado y conservar la documentación que la acredite, en el dossier de titular del certificado.

El PCSC DOCUMENTA S.A. estará obligado a revelar la identidad cuando lo soliciten los órganos judiciales y otras autoridades públicas para el ejercicio de las funciones.

3.1.4. REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES

3.1.4.1 CERTIFICADO CUALIFICADO DE SELLO ELECTRÓNICO

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

Tabla Nº 2 - RUC Certificado Cualificado de Sello Electrónico

Tipo de Documento	Prefijo	Formato	Descripción
Cédula Tributaria – RUC	RUC	RUC99999999-9	Siglas RUC seguido del número de RUC.

3.1.4.2 CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA O CERTIFICADO CUALIFICADO TRIBUTARIO

La Cédula de Identidad civil es expedida por el Departamento de Identificaciones de la Policía Nacional, y debe cumplir el siguiente formato:

Tabla Nº 3 - CI Certificado Cualificado de Firma Electrónica o Certificado Cualificado Tributario

Tipo de Documento	Prefijo	Formato	Descripción
Cédula de identidad	CI	CI999999	Siglas CI seguido del número de cédula de identidad, el cual puede ser alfanumérico.

El Pasaporte es expedido por un órgano nacional competente y en el caso de extranjeros por un órgano de su país de origen, y debe cumplir el siguiente formato:

Tabla Nº 4 - PAS Certificado Cualificado de Firma Electrónica o Certificado Cualificado Tributario

Tipo de Documento	Prefijo	Formato	Descripción
Pasaporte	PAS	PASQ999999	Siglas PAS seguido del número de Pasaporte, el cual puede ser alfanumérico.

3.1.5. UNICIDAD DE NOMBRES

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

3.1.6. PROCEDIMIENTO PARA RESOLVER DISPUTA DE NOMBRE

El PCSC DOCUMENTA S.A. se reserva el derecho de tomar todas las decisiones en el caso de que haya conflicto derivado de los nombres iguales entre varios solicitantes de certificados. Durante el proceso de confirmación de identidad corresponderá al solicitante del certificado demostrar su derecho a usar un nombre específico.

3.1.7. RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

El PCSC DOCUMENTA S.A. no arbitrará, mediará o resolverá ninguna disputa concerniente a la

propiedad de nombres, nombre de dominio, nombres de empresas o instituciones y marcas registradas.

Se prohíbe a los solicitantes de certificados que incluyan nombres en las solicitudes que puedan suponer infracción de derechos de terceros.

El PCSC DOCUMENTA S.A. no determina si un solicitante de certificado tiene derecho sobre las marcas que puedan aparecer en una solicitud de certificado.

El PCSC DOCUMENTA S.A. se reserva el derecho de rechazar una solicitud a causa de conflicto de nombre.

3.2 VALIDACIÓN INICIAL DE IDENTIDAD

Los requisitos y procedimientos de identificación del titular del certificado y emisión del certificado utilizados por las AR vinculadas al PCSC DOCUMENTA S.A. son:

a) Identificación y registro del titular del certificado: identificación de la persona física o jurídica, titular del certificado, con base en los documentos de identificación mencionados en los ítems 3.2.2 y 3.2.3, observando lo siguiente:

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

   II. Para certificados de sello electrónico: prueba de que los documentos presentados refieren efectivamente a la persona jurídica que es el titular del certificado, y que la persona física que se presenta como un representante de la persona jurídica realmente posea tal atribución conforme a los estatutos o normas correspondientes a su funcionamiento que se encuentren vigentes al momento de la solicitud.

   III. Para certificados tributarios: conforme a lo establecido en el ítem I. En el caso de que el titular del certificado corresponda a una empresa unipersonal y conforme al ítem II. si corresponde a una persona jurídica.

b) Emisión del certificado: luego de cotejar los datos de solicitud de certificado con los contenidos en los documentos presentados, en la etapa de identificación, se procede a la emisión del certificado en el sistema del PCSC. Se considera que la extensión del Subject Alternative Name está fuertemente relacionada con la clave pública contenida en el certificado, por lo que todas las partes de esa extensión deben ser verificadas, y el solicitante del certificado debe demostrar que tiene los derechos sobre esta información ante los organismos competentes, o que está autorizado por el titular de la información para utilizarlos.

3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA

En caso de que el par de claves sea generado por el solicitante del certificado, la posesión de la clave privada, correspondiente a la clave pública para la que solicita que se genere el certificado, quedará probada mediante el envío de la petición de certificado (CSR) en formato PKCS#10 u otras demostraciones

criptográficas equivalentes, aprobadas por la Autoridad de Aplicación, en la cual se incluirá la clave pública firmada mediante la clave privada asociada. Este procedimiento podrá ser modificado por el que establezca en cada caso la Política de Certificación aplicable.

3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

3.2.2.1 DISPOSICIONES GENERALES

Será designado como responsable del certificado el representante de la persona jurídica conforme al ítem 3.2, numeral 'a', inciso (ii), quien tendrá el control de la clave privada.

La confirmación de la identidad de la persona jurídica y de la persona física responsable del certificado será verificada por el PCSC bien directamente o bien por medio de un tercero en los siguientes términos:

a) presentación de la lista de documentos enumerados en el punto 3.2.2.2;

b) presentación de la lista de documentos del responsable del certificado, enumerados en el ítem 3.2.3.1;

c) firma electrónica cualificada del contrato de prestación de servicio de confianza mencionado en el ítem 4.1 por el responsable del certificado. En caso de no ser factible, la AR solicitará que el contrato sea firmado manuscritamente por el responsable del certificado para su comparación con el documento de identidad. En este caso, se adjuntará al dossier de titular de certificado, el documento manuscrito digitalizado y firmado con firma electrónica cualificada por el AGR, debiendo mantenerse el original en papel para fines de auditoría.

Se prescinde lo dispuesto en el ítem “b” si el responsable del certificado posee un certificado cualificado de firma electrónica de la ICPP vigente, o cuando utilice un medio de identificación electrónica expedido en virtud de un sistema de identificación electrónica de nivel alto. En estos casos la verificación de los documentos enumerados en el punto 3.2.2.2 se puede realizar electrónicamente, siempre que se realice a través de fuentes oficiales de organismos competentes.

3.2.2.2 DOCUMENTOS REQUERIDOS PARA IDENTIFICAR UNA PERSONA JURÍDICA.

La confirmación de la identidad de una persona jurídica se hará mediante la presentación, de por lo menos los siguientes documentos:

a) si la entidad es pública:
   i. copia simple de la Ley o Carta Orgánica que crea o autoriza su creación;
   ii. documento (original o copia autenticada) que acredite la representación;y
   iii. cédula tributaria.

b) si la entidad es privada:
   i. copia autenticada del estatuto o documento de creación;
   ii. copia autenticada del acta de la última asamblea ordinaria y extraordinaria o del

documento equivalente que acredite la representación;

iii. prueba de la inscripción en el registro oficial correspondiente; y

iv. cédula tributaria.

Las comprobaciones de los documentos citados precedentemente podrán realizarse por vía electrónica, siempre que se trate de fuentes oficiales de organismos competentes. Estas validaciones deberán incluirse obligatoriamente en el dossier del titular del certificado.

Los documentos, que no puedan comprobarse conforme a las condiciones del párrafo anterior deberán verificarse:

a) por un AGR que no sea el que realizó el paso de identificación; y
b) antes del inicio de la validez del certificado, debiendo ser revocadoinmediatamente en el caso que la verificación no se haya realizado antes del inicio de su validez.

3.2.2.3 INFORMACIÓN CONTENIDA EN UN CERTIFICADO EMITIDO PARA UNA PERSONA JURÍDICA

La información obligatoria contenida en los campos del certificado expedido a una persona jurídica debe coincidir exactamente con la información contenida en los siguientes documentos:

a) nombre de la razón social según documento constitutivo y sin abreviaturas;
b) número de registro único del contribuyente (RUC) según la cédula tributaria;
c) nombre completo de la persona física responsable del certificado según documento de identidad; y
d) nombre completo de la persona física responsable del certificado según documento de identidad; y
e) número de cédula de identidad policial o número de pasaporte de la persona física responsable del certificado según documento de identidad.

Cada PC puede definir como obligatorio llenar otros campos. Además, el responsable del certificado, a su criterio y mediante una declaración expresa en el documento de solicitud de certificado y Contrato de Prestación de Servicios de Confianza, puede solicitar llenar los campos con las siguientes informaciones:

a) el correo del responsable del certificado;
b) nombre de la unidad de la organización en el que presta servicio el responsable del certificado;
c) posición o función asignada al responsable del certificado en la organización en el que presta servicio; y
d) el título académico del responsable del certificado.

Para ello, en el caso del correo electrónico se considerará suficiente la declaración expresa en la correspondiente solicitud. Dado el caso de incorporar otra información, la misma debe contar con respaldo documental en formato original o copia autenticada. Las copias de los mismos deben ser incluidas al dossier del titular del certificado.

Respecto a la responsabilidad derivada del uso del certificado de una persona jurídica, los actos realizados con el certificado electrónico de una persona jurídica están sujetos a las obligaciones establecidas en la normativa y a las facultades de representación conferidas al responsable de uso indicado en el certificado.

3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA

En esta sección se deben definir los procedimientos empleados por las AR vinculadas al PCSC DOCUMENTA S.A. para confirmar la identidad de la persona física.

La confirmación de la identidad de la persona física deberá realizarse en los siguientes términos:

a) presencia física del titular del certificado; o,

b) a distancia, utilizando un medio de identificación electrónica expedido en virtud de un sistema de identificación de nivel alto, para los cuales se haya garantizado la presencia de la persona física previamente a la expedición del certificado cualificado; o,

c) por medio de un certificado de una firma electrónica cualificada expedido de conformidad con la letra a) o b), o

d) mediante videoconferencia, de acuerdo con los procedimientos y requisitos técnicos definidos en la normativa de AC Raíz-Py, DOC-ICPP-17 [3], que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, garantizando la validación de la misma identificación, mediante el uso de tecnologías electrónicas seguras de comunicación, interacción y documentación. La seguridad equivalente será confirmada por un OEC.

3.2.3.1 DOCUMENTOS REQUERIDOS PARA IDENTIFICAR UNA PERSONA FÍSICA.

La identificación de la persona física solicitante del certificado debe realizarse de la siguiente manera:

Presentación de la siguiente documentación, en su versión oficial original, física o electrónica:

i) cédula de Identidad civil o pasaporte, si es paraguayo;

ii) cédula de Identidad de extranjero, si es extranjero domiciliado en Paraguay; o

iii) pasaporte, si es extranjero no domiciliado en Paraguay.

Se considera documento de identidad al documento oficial, físico o electrónico, según la legislación específica, emitido por el Ministerio del Interior a través de la Policía Nacional.

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

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

a) por un agente de registro distinto del que realizó el paso de identificación;

b) por la AR vinculada o AR propia del PCSC; y

c) antes del inicio de la validez del certificado, debiendo ser revocado inmediatamente en el caso que la verificación no se haya realizado antes del inicio de su validez.

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

3.2.3.2 INFORMACIÓN CONTENIDA EN UN CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA

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

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

Cada PC puede definir como obligatorio llenar otros campos. Además, el titular del certificado, a su criterio y mediante una declaración expresa en el documento de solicitud de certificado y Contrato de Prestación de Servicios de Confianza, puede solicitar llenar los campos con las siguientes informaciones:

a) el correo del titular del certificado;
b) el nombre de la organización en el que presta servicio el titular del certificado;
c) el nombre de la unidad de la organización en el que presta servicio el titular del certificado;
d) el número de RUC de la organización en el que presta servicio el titular del certificado
e) el número de RUC del titular del certificado si no se registran los datos de la organización en la que presta servicio;
f) posición o función designada al titular del certificado en la organización en el que presta servicio; y
g) el título académico del titular del certificado.

Para ello, en el caso del correo electrónico se considerará suficiente la declaración expresa en la correspondiente solicitud. Dado el caso de incorporar otra información, la misma debe contar con respaldo documental en formato original o copia autenticada. Las copias de los mismos deben ser incluidas al dossier del titular del certificado.

3.2.3.3 INFORMACIÓN CONTENIDA EN UN CERTIFICADO CUALIFICADO TRIBUTARIO

La información obligatoria contenida en los campos del certificado cualificado tributario expedido a una persona física debe coincidir exactamente con la información contenida en los siguientes documentos:

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

c) nombre de la organización en el que presta servicio el titular del certificado o razón social del titular del certificado en caso de tratarse de una organización unipersonal, según cédula tributaria; y

d) 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 en caso de tratarse de una organización unipersonal, según cédula tributaria.

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

a) el correo del titular del certificado;

b) el nombre de la unidad de la organización en el que presta servicio el titular del certificado;

c) posición o función asignada al titular del certificado en la organización en el que presta servicio; y

d) el título académico del titular del certificado.

Para ello, en el caso del correo electrónico se considerará suficiente la declaración expresa en la correspondiente solicitud. Dado el caso de incorporar otra información, la misma debe contar con respaldo documental en formato original o copia autenticada. Las copias de los mismos deben ser incluidas en el dossier de titular del certificado.

3.2.4 INFORMACIÓN NO VERIFICADA DEL TITULAR DEL CERTIFICADO

No aplica.

3.2.5 VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)

La AR vinculada al PCSC DOCUMENTA S.A, debe validar la capacidad del solicitante de un certificado y que no posea impedimentos legales. En el caso de certificados cualificados para firma electrónica, debe validar que el solicitante sea mayor de edad y en el caso de certificados cualificados para sello electrónico debe además validar la autoridad invocada por el representante con facultades suficientes para solicitar el certificado.

3.2.6 CRITERIOS PARA INTEROPERABILIDAD

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

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

a) Los prestadores de servicios de confianza establecidos fuera del país u organizaciones internacionales y los servicios de confianza que prestan, cumplen los requisitos aplicables a los PCSC

establecidos en el Paraguay y a los servicios de confianza cualificados que prestan.

b) Los servicios de confianza cualificados prestados por PCSC establecidos en Paraguay son reconocidos como legalmente equivalentes a los servicios de confianza prestados por prestadores de servicios establecidos fuera del país u organizaciones internacionales con los que se celebran acuerdos.

3.2.7 PROCEDIMIENTOS COMPLEMENTARIOS

El PCSC DOCUMENTA SA comprobará la identidad y/o atributos de las personas físicas y jurídicas antes de incluir estos atributos en un certificado en el marco de la ICPP. Se prohíbe a las personas físicas y jurídicas utilizar en sus certificados nombres que violen los derechos de propiedad intelectual de terceros. El PCSC se reserva el derecho, sin responsabilidad ante ningún solicitante, de rechazar solicitudes.

El PCSC mantendrá políticas y procedimientos internos que deben ser revisados periódicamente para cumplir con los requisitos establecidos por la AC Raíz-Py,

Se debe mantener un archivo con copias de todos los documentos utilizados para confirmar la identidad de una persona física o jurídica. Tales copias podrán ser conservadas en papel o en formato electrónico, sujetas a las condiciones definidas en el documento DOC-ICPP-05 [4].

3.2.8 PROCEDIMIENTOS ESPECÍFICOS

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

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DENUEVAS CLAVES

El PCSC DOCUMENTA S.A. podrá generar un nuevo par de claves y su correspondiente nuevo certificado a un titular de certificado, de acuerdo con una de las siguientes posibilidades:

a) adopción de los mismos requisitos y procedimientos requeridos en los puntos 3.2.2 o 3.2.3;
b) solicitud, por medio electrónico, firmada electrónicamente utilizando un certificado cualificado de la ICPP válido del solicitante, que sea del mismo nivel de seguridad o superior, admitiéndose esta hipótesis únicamente para los certificados cualificados de firma electrónica y a los certificados cualificados tributarios;
c) solicitud, por medio electrónico, sellada electrónicamente utilizando un certificado cualificado de sello electrónico de la ICPP válido de una persona jurídica, que sea del mismo nivel de seguridad o superior, siempre que, mantenido en esta condición, presente un documento electrónico comprobable mediante fuente oficial de organismos competentes, que acredite el poder de representación legal en relación con la organización, siendo admitida esta hipótesis únicamente para los certificados cualificados

de sello electrónico;

d) solicitud, por medio electrónico, utilizando un medio de identificación electrónica expedido en virtud de un sistema de identificación electrónica de nivel alto.

e) mediante videoconferencia, de acuerdo con el procedimiento y requisitos técnicos definidos en la normativa de AC Raíz-Py, DOC-ICPP-17 [3], que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, garantizando la validación de la misma identificación, mediante el uso de tecnologías electrónicas seguras de comunicación, interacción y documentación. La seguridad equivalente será confirmada por un OEC.

Si se requieren procedimientos específicos para las PCs implementadas, estos deben estar descritos en estas PCs, en el ítem correspondiente.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

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

El solicitante de la revocación de un certificado cualificado de la ICPP debe estar identificado. Únicamente los agentes descriptos en el ítem 4.9.2 pueden solicitar la revocación de dicho certificado.

Las solicitudes de revocación de certificados serán siempre registradas.

Los procedimientos aceptados para la identificación del solicitante de la revocación de certificado incluyen algunos de los siguientes medios:

- Mediante el código de revocación que es enviado al suscriptor en el correo consignado en el momento de la emisión del certificado.
- Presencialmente, el procedimiento utilizado para confirmar la identidad de una persona física o jurídica deberá realizarse de acuerdo a los requisitos y procedimientos requeridos en los ítems 3.2.2 o 3.2.3 según sea el caso.
- Cualquier otro medio establecido por el PCSC DOCUMENTA S.A. y aprobado por la AA que permita una identificación veraz y segura.

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1 SOLICITUD DEL CERTIFICADO

Los requisitos y procedimientos mínimos para la solicitud de emisión de certificados son:

a) la comprobación de los atributos de identificación que constan en el certificado,conforme al ítem 3.2;

b) el uso de un certificado cualificado de firma electrónica del AGR responsable de gestionar las solicitudes de emisión, suspensión y revocación de certificados.

c) Un Contrato de Prestación de Servicios de Confianza firmado con una firma electrónica cualificada por el titular del certificado o por la persona responsable del certificado, en el caso de un certificado cualificado de sello electrónico.

Ante la imposibilidad técnica de firmar electrónicamente el Contrato de Prestación de Servicios de Confianza se aceptará la firma manuscrita del contrato por parte del titular o responsable en el caso de un certificado cualificado de sello electrónico. En este caso será necesaria la verificación de su firma contra el documento identidad presentado y se adjuntará al dossier de titular del certificado, el documento manuscrito y firmado con firma electrónica cualificada por el AGR, conforme al DOC-ICPP-05 [4].

El formato del documento Contrato de Prestación de Servicio de Confianza, según sea el tipo de certificado a ser emitido, será establecido por la AC Raíz-Py.

4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

La presentación de la solicitud debe ser siempre a través de una AR vinculada al PCSC DOCUMENTA S.A.

Las personas que pueden presentar una solicitud de certificado, que, en el marco de la ICPP, son:

a) para el caso de certificado cualificado de firma electrónica o tributario, toda persona, mayor de edad, sindistinción, con un documento de identidad válido y vigente, que será el sujeto a cuyo nombre se emita el certificado;
b) para el caso de certificado cualificado de sello electrónico, el representante de la persona jurídica;

4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

4.1.2.1 RESPONSABILIDADES Y OBLIGACIONES DEL PCSC

Responsabilidades:

a) el PCSC DOCUMENTA S.A. es responsable de los daños que causen a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que les impone la normativa vigente;
b) el PCSC DOCUMENTA S.A. asume toda la responsabilidad frente a terceros por la actuación de las personas u otros prestadores en los que deleguen la ejecución de alguna/s de las funciones necesarias para prestación de servicios de confianza, incluyendo las actuaciones de comprobación de identidad previas a la expedición de un certificado cualificado.

Obligaciones:

Las obligaciones del PCSC DOCUMENTA S.A. son:

a) publicar información veraz y acorde con las reglamentaciones vigentes, en su sitio principal de Internet:
    - su DPC, y las PC aprobadas que implementa;

- las informaciones definidas en el ítem 2.2 de este documento,
- las informaciones sobre la desvinculación de una AR
- disponer de un servicio de consulta sobre el estado de validez y revocación de los certificados emitidos accesible al público;

b) no almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma, de sello de la persona física o jurídica a la que hayan emitido certificados, salvo en caso de su gestión en nombre del firmante o del creador del sello. En este caso, el PCSC tiene la obligación de:

- utilizar sistemas y productos fiables, incluidos canales de comunicación electrónica seguros;
- Aplicar procedimientos y mecanismos técnicos y organizativos adecuados, para garantizar que el entorno sea fiable y se utilice bajo el control exclusivo del titular del certificado;
- Custodiar y proteger los datos de creación de firma y/o de sello frente a cualquier alteración, destrucción o acceso no autorizado; y
- Garantizar su continua disponibilidad.

c) Conservar la información relativa a los servicios prestado por el término de diez años;

d) Constituir un seguro de responsabilidad civil por el importe mínimo de quinientos salarios mínimos previstos para actividades diversas no especificadas, excepto si el prestador pertenece al sector público. Si presta más de un servicio de los previstos en la normativa, se añadirán ciento cincuenta salarios mínimos más por cada servicio. La citada garantía puede ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea cogerente con lo dispuesto en el párrafo anterior.

e) informar a la parte usuaria y los titulares de certificados sobre las garantías, cobertura, condiciones y limitaciones establecidas a la póliza de seguro de responsabilidad civil contraída en los términos indicado en el inciso e) de este ítem;

f) en el caso de cese de sus operaciones, comunicar a los que preste sus servicios y al organismo de supervisión con una antelación mínima de dos meses el cese efectivo de la actividad. El plan de cese del PCSC puede incluir la transferencia de clientes a otro prestador cualificado, una vez acreditada la ausencia de oposición de los mismo;

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

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

i) enviar el informe de evaluación de la conformidad a la AC Raíz-Py en el plazo de tres días hábiles tras su recepción. El incumplimiento de esta obligación conlleva la

suspensión de cualificación al prestador y al servicio que éste presta, y su eliminación de la lista de confianza;

j) notificar, en un plazo de veinticuatro horas tras tener conocimiento de ellas, a la AC Raíz-Py de las violaciones de seguridad que sufran, entendiéndose como violación de seguridad a un evento que afecta de manera crítica la confidencialidad, integridad y/o disponibilidad de los activos de información y tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes;

k) gestionar los incidentes de seguridad que les afecten, debiendo prever los mecanismos adecuados para su prevención, detección, análisis y resolución;

l) ampliar tras la resolución del incidente, la información suministrada en la notificación inicial con arreglo a las directrices que pueda establecer AC Raíz-Py;

m) facilitar a la AC Raíz-Py toda la información y colaboración precisas para el ejercicio de sus funciones. En particular, deben permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate conforme al servicio que se preste. En sus inspecciones podrán ir acompañados de expertos o peritos en las materias sobre las que versen aquéllas;

n) adoptar las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan. Habida cuenta de los últimos avances tecnológicos, dichas medidas garantizan un nivel de seguridad proporcional al grado de riesgo. En particular, se adoptarán medidas para evitar y reducir al mínimo el impacto de los incidentes de seguridad e informar a los interesados de los efectos negativos de cualquiera de tales incidentes.

o) notificar al organismo de supervisión y al centro de respuestas a incidentes Cibernéticos del Ministerio de Tecnologías de la Información y Comunicación (MITIC), sin demoras indebidas, pero en cualquier caso en un plazo de veinticuatro horas tras tener conocimiento sobre cualquier violación de la seguridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes. Cuando la violación de seguridad pueda atentar contra una persona física o jurídica a la que se ha prestado el servicio de confianza, se deberá notificar también a la persona física o jurídica, sin demora indebida, la violación de seguridad. El organismo de supervisión notificado informará al público o exigirá al prestador de servicios de confianza que lo haga, en caso de considerar que la divulgación de la violación de seguridad reviste interés público.

p) informar al organismo de supervisión de cualquier cambio en la prestación de servicios de confianza cualificados, y de su intención de cesar tales actividades.

q) contar con personal y, si procede, con subcontratistas, que posean los conocimientos especializados, la fiabilidad, la experiencia y las cualificaciones necesarios y hayan recibido la formación adecuada en materia de seguridad y normas de protección de datos personales y que apliquen procedimientos administrativos y de gestión que correspondan

a normas internacionales.

r) con respecto al riesgo de la responsabilidad por daños, mantener recursos financieros suficientes u obtener pólizas de seguros de responsabilidad adecuadas.

s) antes de entrar en una relación contractual, informar, de manera clara y comprensible, a cualquier persona que desee utilizar un servicio de confianza cualificado acerca de las condiciones precisas relativas a la utilización de dicho servicio, incluidas las limitaciones de su utilización.

t) utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad y la fiabilidad técnicas de los procesos que sustentan.

u) utilizar sistemas fiables para almacenar los datos que se les faciliten de forma verificable, de modo que:

- estén a disposición del público para su recuperación sólo cuando se haya obtenido el consentimiento de la persona a la que corresponden los datos.
- solo personas autorizadas puedan hacer anotaciones y modificaciones en los datos almacenados.
- pueda comprobarse la autenticidad de los datos.

v) Tomar medidas adecuadas contra la falsificación y el robo de datos.

w) Registrar y mantener accesible durante un periodo definido por la AC Raíz-Py, incluso cuando hayan cesado las actividades del PCSC, toda la información pertinente referente a los datos expedidos y recibidos por el PCSC, en particular al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio. Esta actividad de registro podrá realizarse por medios electrónicos.

x) Contar con un plan de cese actualizado para garantizar la continuidad del servicio.

y) Garantizar un tratamiento lícito de los datos personales.

z) Mantener actualizada una base de datos de certificados.

aa) Cuando los PCSC revocan un certificado, deberán registrar su revocación en su base de datos de certificados y publicar el estado de revocación del certificado oportunamente y, en todo caso, en un plazo de veinticuatro horas después de la recepción de la solicitud.

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

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

dd) Revelar la verdadera identidad del firmante o titular del certificado en caso de expedir certificados que consignen seudónimos, cuando lo soliciten los órganos judiciales y otras autoridades públicas para el ejercicio de las funciones.

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

ff) Operar de acuerdo a su DPC y PC que implementan;

gg) generar y gestionar sus pares de claves criptográficas;

hh) asegurar la protección de sus claves privadas;

ii) distribuir su propio certificado;

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

kk) informar la emisión del certificado al respectivo solicitante;

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

mm) emitir, gerenciar y publicar sus LCRs y disponibilizar la consulta online de la situación de los certificados emitidos (OCSP-On-line Certificate Status Protocol);

nn) utilizar protocolo de comunicación segura para proporcionar servicios a los solicitantes y usuarios de certificados electrónicos a través de la web;

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

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

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

rr) mantener y garantizar la integridad, confidencialidad y seguridad de la información por ella tratada;

ss) mantener y anualmente realizar prueba de su PCN;

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

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

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

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

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

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

4.1.2.2 RESPONSABILIDADES Y OBLIGACIONES DE LA RA

Responsabilidades

La AR será responsable de los daños que ocasione.

Obligaciones

Las obligaciones de las AR vinculadas al PCSC DOCUMENTA S.A. son:

a) recibir las solicitudes de emisión, suspensión y revocación de los certificados;
b) confirmar la identidad del solicitante y validar la solicitud;
c) remitir la solicitud de emisión, suspensión o revocación del certificado al PCSC DOCUMENTA S.A., por medio de acceso remoto al ambiente de la AR alojado en las instalaciones del PCSC DOCUMENTA S.A., utilizando un protocolo de comunicación seguro, conforme al patrón definido en el documento DOC-ICPP-05 [4];
d) informar a los respectivos titulares la emisión, suspensión o revocación de sus certificados;
e) mantener el cumplimiento de sus procesos, procedimientos y actividades con las normas, criterios, prácticas y reglas establecidas por el PCSC vinculado, la AC Raíz-Py y en especial con lo contenido en el documento DOC-ICPP-05 [4];
f) mantener y anualmente realizar prueba de su PCN;
g) proceder a la comprobación de las firmas y de la validez de los documentos presentados en la forma de los ítems 3.2.2 y 3.2.3; y
h) divulgar sus prácticas, relacionadas con el PCSC DOCUMENTA S.A. de acuerdo a los principios y criterios establecidos por la AC Raíz-Py para las AR.

4.2 PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

La AR vinculada al PCSC DOCUMENTA S.A. debe velar por la identificación y autenticación de acuerdo con las disposiciones establecidas en el ítem 3.

4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

El PCSC DOCUMENTA S.A y las AR vinculadas podrán, con la debida justificación formal, aceptar o rechazar solicitudes de certificados de los solicitantes de acuerdo con los procedimientos descriptos en esta DPC y la normativa vigente.

4.2.3 TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO

El PCSC DOCUMENTA S.A. debe cumplir con los procedimientos determinados por la AC Raíz-

Py. No habrá tiempo máximo para procesar solicitudes en el marco de la ICPP.

4.3 EMISIÓN DEL CERTIFICADO

4.3.1 ACCIONES DEL PCSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS

La emisión del certificado implica la autorización definitiva de la solicitud por parte de la RA. Cuando el PCSCDOCUMENTA S.A. emita un certificado de acuerdo con una solicitud de certificado, efectuará las notificaciones que se establecen en el ítem 4.3.2.

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

Todo lo especificado en este apartado queda supeditado a lo estipulado por las distintas PC para la emisión de certificados acogidos a las mismas.

4.3.2 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO SOBRE LA EMISIÓN DEL CERTIFICADO ELECTRÓNICO

El envío de la notificación al solicitante se realizará por medio del correo electrónico, provisto por éste durante la inscripción de sus datos previa a la emisión del certificado. Cada PC DE DOCUMENTA S.A. podrá establecer otro mecanismo de notificación mediante el que se informará al solicitante de la emisión de su certificado.

4.4 ACEPTACIÓN DEL CERTIFICADO

4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

La aceptación del certificado es la acción mediante la cual su titular da inicio a sus obligaciones respecto a la ICP Paraguay.

La aceptación de todo certificado emitido deberá ser declarada expresamente por el respectivo titular en la Solicitud y Contrato de Prestación de Servicios de Confianza. En caso de los certificados cualificados de sello electrónico, la declaración expresa deberá ser de la persona física responsable de ese certificado.

La no aceptación de un certificado por su titular implica la revocación del mismo.

En la PC correspondiente se podrán detallar o ampliar la forma en que se acepta el certificado.

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PCSC

El certificado del PCSC DOCUMENTA S.A. y los certificados emitidos a usuarios finales, deberán ser publicados de acuerdo con el punto 2.2 de esta DPC.

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

No se definen entidades externas que necesiten o requieran ser notificados respecto a los certificados emitidos por el PCSC.

4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

El titular o responsable de un certificado debe usar el par de claves y el certificado correspondiente de acuerdo a la DPC y las PC que implementa el PCSC DOCUMENTA S.A., establecidas de acuerdo con este documento y con el documento DOC-ICPP-04 [1].

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

El PCSC DOCUMENTA S.A. utiliza su clave privada y garantiza la protección de esta clave según lo previsto en esta DPC.

Obligaciones del Titular o Responsable del Certificado

Las obligaciones de los titulares de certificados emitidos por el PCSC DOCUMENTA S.A., contenidas en el contrato de prestación de servicio de confianza referidos en el ítem 4.1, se enumeran a continuación:

a) Proporcionar al PCSC o a la RA vinculada información completa, veraz y exacta para la prestación del servicio de confianza, en particular, sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia;
b) Comunicar sin demora al PCSC o a la RA vinculada de cualquier modificación de las circunstancias que incidan en la prestación del servicio de confianza, en particular, aquellas reflejadas en el certificado electrónico;
c) Conservar adecuadamente sus datos de creación de firma o sello, asegurar su confidencialidad y proteger de todo acceso o revelación de éstos o, en su caso, de los medios que den acceso a ellos;
d) Solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma o sello o, en su caso, de los medios que den acceso a ellos.
e) No utilizar los datos de creación de firma o sello cuando haya expirado el periodo de validez del certificado electrónico o el PCSC le notifique la extinción o suspensión de su vigencia.
f) utilizar sus certificados y claves privadas de forma adecuada, según lo previsto en la PC correspondiente;
g) conocer sus derechos y obligaciones, contemplados en la DPC y la PC correspondiente y demás documentos aplicables de la ICPP; e

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

USUARIA

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

4.6 RENOVACIÓN DEL CERTIFICADO

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

4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO

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

4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN

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

4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO

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

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

Conforme a lo estipulado en el ítem 4.3.2 de esta DPC.

4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO

Conforme a lo estipulado en el ítem 4.4.1 de esta DPC.

4.6.6 PUBLICACIÓN POR EL PCSC DEL CERTIFICADO RENOVADO

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

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

Conforme a lo estipulado en el ítem 4.4.3 de esta DPC.

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

Este ítem no aplica.

4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO

Este ítem no aplica.

4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA

Este ítem no aplica.

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

Este ítem no aplica.

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

Este ítem no aplica.

4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE-EMITIDO

Este ítem no aplica.

4.7.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS RE-EMITIDOS

Este ítem no aplica.

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

Este Ítem no aplica.

4.8 MODIFICACIÓN DE CERTIFICADOS

Este ítem no aplica.

4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO

Este ítem no aplica.

4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

Este ítem no aplica.

4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

Este ítem no aplica.

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

Este ítem no aplica.

4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

Este ítem no aplica.

4.8.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS MODIFICADOS

Este ítem no aplica.

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

Este ítem no aplica.

4.9 REVOCACIÓN Y SUSPENSIÓN

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

Un certificado deberá obligatoriamente ser revocado en las siguientes circunstancias:

a) que afecten la información contenida en el certificado:

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

b) que afectan la seguridad de la clave o del certificado:

   i. compromiso de la clave privada o de la infraestructura o sistemas del PCSC DOCUMENTA S.A., siempre que afecte a la fiabilidad de los certificados emitidos a partir de este incidente;

   ii. infracción, por el PCSC DOCUMENTA S.A., de los requisitos previstos en los procedimientos de gestión de los certificados, establecidos en su propia PC y DPC;

   iii. violación o puesta en peligro de la confidencialidad de los datos de creación de la firma o de sello, o del PCSC, o utilización indebida de dichos datos por un tercero.

   iv. acceso o utilización no autorizada, por un tercero, de la clave privada del titular; y

   v. el uso irregular por el titular, o falta de diligencia en la custodia de la clave privada;

   vi. cese de actividad del PCSC DOCUMENTA S.A. salvo que la gestión de los certificados electrónicos expedidos sea transferida a otro prestador de servicios de confianza.

c) circunstancias que afectan la seguridad del dispositivo criptográfico, en caso de que aplique:

   - compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico;
   - pérdida o inutilización por daños del dispositivo criptográfico; y
   - acceso no autorizado, por un tercero, a los datos de activación de la clave privada

del titular del certificado;

d) circunstancias que afectan al titular o responsable del certificado:
   i. infracción del titular o responsable del certificado en sus obligaciones, responsabilidady garantías, establecidas en la PC y DPC del PCSC que emitió el certificado;
   ii. fallecimiento del firmante; incapacidad sobrevenida, total o parcial, del firmante; y/o la extinción de la persona jurídica o disolución del creador del sello;
   iii. solicitud formulada por el firmante, la persona física titular o jurídica representada por un tercero autorizado, el creador del sello de acuerdo con lo establecido en la PC y en la DPC.
   iv. Resolución judicial o administrativa competente que ordene la revocación o suspensión de un certificado.
e) otras causales especificadas en la normativa y reglamentación vigente.

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

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

La AC Raíz-Py podrá determinar la revocación del certificado del PCSC DOCUMENTA S.A. si incumple con la legislación vigente o las políticas, estándares, prácticasy reglas establecidas en el marco de la ICPP.

4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN

La revocación de un certificado sólo podrá realizarse:

a) por solicitud formulada del firmante, la persona física o jurídica representada por éste, un tercero autorizado o el creador del sello;

b) por resolución judicial o administrativa competente que lo ordene.

c) por solicitud de la empresa u organización, cuando en el certificado se detalla el cargo o función que ocupa en la organización y es proporcionado por la misma al titular, por ser éste, su empleado o funcionario;

d) por DOCUMENTA S.A. en su condición de PCSC emitente;

e) por una AR vinculada al PCSC DOCUMENTA S.A.;

f) por determinación de la AC Raíz-Py; y

g) por una autoridad judicial competente.

4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

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

Como directrices generales, se establece que:

a) el solicitante de revocación de un certificado será identificado;

b) las solicitudes de revocación, así como las acciones resultantes de ellas serán registradas y almacenadas;

c) se documentarán las razones de la revocación de un certificado; y

d) la revocación de un certificado terminará con la generación y publicación de una LCR que contenga los datos del certificado revocado y, en el caso de la utilización de consulta OCSP, con la actualización del estado del certificado en la base de datos del PCSC.

El PCSC DOCUMENTA S.A., registrará la revocación de los certificados electrónicos cualificados en su base de datos de certificados y publicará el estado del certificado oportunamente y, en todo caso, en un plazo de veinticuatro (24) horas después de la recepción de la solicitud. La revocación será efectiva inmediatamente después de su publicación.

Se garantiza que el PCSC DOCUMENTA S.A. responde plenamente por todos los daños causados por el uso de un certificado en el período comprendido entre la solicitud de su revocación y la emisión de la LCR correspondiente.

En caso de que sean requeridos procedimientos de revocación específicos para las PC implementadas, los mismos deben ser descriptos en esas PC, en el ítem correspondiente.

4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

La revocación será inmediata cuando se configuren las circunstancias definidas en el ítem 4.9.1, por tanto, no existe ningún periodo de gracia asociado a este procedimiento durante el que se pueda anular la solicitud de emisión, o para la aceptación del certificado por su titular, dentro del cual la revocación de dicho certificado podrá ser solicitada sin que se aplique alguna tarifa por el PCSC.

Si se requieren plazos específicos para las DPC implementadas, estos deberán estar descriptos en dichas DPC, en el ítem correspondiente.

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

En el caso de una solicitud formalmente constituida, de acuerdo con las reglas de la ICP-Paraguay, el PCSC DOCUMENTA S.A. procesará la revocación inmediatamente después de analizar la solicitud.

4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LA PARTE USUARIA

La evaluación del estado de certificado, y de todos los certificados de la AC en la cadena a la que pertenece el mismo, es obligatoria para cada uso de los certificados por la parte usuaria antes de confiar en él. Para ello, las partes usuarias pueden verificar el estado del certificado mediante el servicio de: OCSP o LCR más reciente, proveída por el PCSC.

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

Las partes que confían deberán comprobar la validez de la LCR previamente a cada uno de sus usos y descargar la nueva LCR del repositorio del PCSC DOCUMENTA S.A. al finalizar el periodo de validez de la que posea. Las listas de revocación de certificados guardadas en memoria "caché", aun no estando caducadas, no garantizan que dispongan de información de revocación actualizada.

4.9.7 FRECUENCIA DE EMISIÓN DEL LCR

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

La LCR mantiene publicado obligatoriamente:

- el certificado revocado hasta que expire, y
- el certificado suspendido, mientras permanezca tal condición.

En caso que sean utilizadas frecuencias de emisión específicas de LCR para las DPC implementadas, deben ser descriptos en estas DPC, en el ítem correspondiente.

4.9.8 LATENCIA MÁXIMA PARA LCR

El tiempo máximo entre la generación de una LCR y su publicación en el repositorio será como máximo de 1 (hora) hora posterior a su generación.

4.9.9 DISPONIBILIDAD PARA REVOCACIÓN/VERIFICACIÓN DE ESTADO EN LÍNEA

El PCSC DOCUMENTA S.A. proporciona un servidor web donde publica las LCR para la verificación del estado de los certificados que emite. Asimismo, la AV vinculada al PCSC DOCUMENTA S.A. permite, mediante el protocolo OCSP, verificar el estado de los certificados.

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

La autenticidad del LCR/OCSP además debe confirmarse mediante la verificación de la firma del PCSC DOCUMENTA S.A. y del período de validez del LCR/OCSP.

4.9.10 REQUISITOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA

La verificación de un estado de un certificado por la parte usuaria deberá ser por medio del protocolo OCSP directamente con el PCSC DOCUMENTA S.A. o una AV vinculada. En el caso de recurrir a la AV vinculada al PCSC DOCUMENTA S.A., la parte usuaria debe disponer de un software que sea capaz de operar con el protocolo OCSP para obtener la información sobre el certificado.

Si se requieren procedimientos específicos para las PC implementadas, se deben describir en dichas PC, en el ítem correspondiente.

4.9.11 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES

No aplica.

4.9.12 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA

En caso que la clave privada del certificado emitido por el PCSC DOCUMENTA S.A. a un suscriptor se vea comprometida, el titular del certificado deberá comunicar el hecho inmediatamente al PCSC DOCUMENTA S.A. o a la AR vinculada que realizó el procedimiento de registro, si corresponde se revocará de inmediato de acuerdo a lo establecido en el ítem 4.9. En el caso que haya requisitos específicos para las PC implementadas, los mismos deben ser descriptos en esas PC, en el ítem correspondiente.

En el caso de compromiso de la clave privada del PCSC DOCUMENTA S.A. será notificado, en la medida posible, todos los participantes de la ICP Paraguay, especialmente a:

- Todos los suscriptores de certificados emitidos.
- Terceros que confían, los que se tenga conocimiento.

Además, el PCSC DOCUMENTA S.A. publicará el compromiso de su clave en su sitio principal de internet.

4.9.13 CIRCUNSTANCIAS PARA SUSPENSIÓN

Siempre que se prevea la posibilidad de suspender los certificados, el PCSC DOCUMENTA S.A. procederá conforme a los siguientes supuestos:

a) formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado, el creador del sello.
b) sospecha o duda de violación o puesta en peligro del secreto de los datos de creación de firma o de sello, o del PCSC, o utilización indebida de dichos datos por un tercero.
c) resolución judicial o administrativa competente que lo ordene.
d) sospecha o duda de la falsedad o inexactitud de los datos aportados para la expedición del certificado y que consten en él, o alteración posterior de las circunstancias verificadas para la expedición del certificado.

De manera previa o simultánea a la indicación de la suspensión de un certificado electrónico cualificado en el servicio de consulta sobre el estado de validez de los certificados por él expedidos, el

PCSC DOCUMENTA S.A. informará al titular de certificado o al responsable del mismo acerca de esta circunstancia, especificando los motivos, la fecha y la hora en que el certificado quedará sin efecto. La vigencia del certificado se extinguirá si transcurrido el plazo de duración de la suspensión, el prestador no la hubiera levantado.

4.9.14 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

La suspensión de un certificado sólo podrá realizarse:

a) por solicitud formulada a través del firmante, la persona física o jurídica representada por éste, un tercero autorizado o el creador del sello;
b) resolución judicial o administrativa competente que lo ordene.
c) por solicitud de la empresa u organización, cuando en el certificado se detalla el cargo o función que ocupa en la organización y es proporcionado por la misma al titular, por ser éste, su empleado o funcionario;
d) por el PCSC emitente;
e) por una AR vinculada al PCSC emitente;

4.9.15 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

El PCSC DOCUMENTA S.A. deberá garantizar que quienes están autorizados a solicitar la suspensión conforme al ítem 4.9.14, puedan, fácilmente y en cualquier momento, solicitar la suspensión de sus respectivos certificados.

Como directrices generales, se establece que:

a) el solicitante de suspensión de un certificado será identificado;
b) las solicitudes de suspensión, así como las acciones resultantes de ellas serán registradas y almacenadas;
c) se documentarán las razones de la suspensión de un certificado; y
d) la suspensión de un certificado terminará con la generación y publicación de una LCR que contenga los datos del certificado suspendido y, en el caso de la utilización de consulta OCSP, con la actualización del estado del certificado en la base de datos del PCSC.

El PCSC DOCUMENTA S.A., debe registrar la suspensión, en el caso de certificado electrónico cualificado, en su base de datos de certificados y publicar el estado del certificado oportunamente y, en todo caso, en un plazo de veinticuatro (24) horas después de la recepción de la solicitud. La suspensión será efectiva inmediatamente después de su publicación.

Se garantiza que el PCSC DOCUMENTA S.A. responde plenamente por todos los daños causados por el uso de un certificado en el período comprendido entre la solicitud de su suspensión y la emisión de la LCR correspondiente.

En caso de que sean requeridos procedimientos de suspensión específicos para las PCs implementadas, los mismos serán descriptos en esas PCs, en el ítem correspondiente.

4.9.16 LÍMITES DEL PERÍODO DE SUSPENSIÓN

El límite del periodo de suspensión será establecido por el titular del certificado. La vigencia del certificado se extinguirá si transcurrido el plazo de duración de la suspensión, el PCSC no la hubiera levantado.

4.10 SERVICIOS DE ESTADO DEL CERTIFICADO

4.10.1 CARACTERÍSTICAS OPERACIONALES

El PCSC DOCUMENTA S.A. proporciona un servicio de estado de certificado en forma de un punto de distribución de LCR en los certificados y OCSP, conforme al ítem 4.9.9

4.10.2 DISPONIBILIDAD DEL SERVICIO

El servicio de publicación de la LCR y el servicio de consulta en línea por medio del protocolo OCSP están disponibles en el repositorio público durante las veinticuatro horas, los siete días de la semana. En caso de interrupción por causa de fuerza mayor, el servicio se deberá restablecer en un plazo no mayor a veinticuatro horas, garantizando la disponibilidad del servicio con un mínimo de 99,5% anual, un tiempo programado de inactividad máximo de 0.5% anual.

4.10.3 CARACTERÍSTICAS OPCIONALES

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

Para hacer uso del servicio de validación en línea es responsabilidad de la parte usuaria disponer de un cliente OCSP que cumpla el RFC 6960.

4.11 FIN DE ACTIVIDADES

La extinción de la validez de un certificado se produce en los siguientes casos:

- Revocación del certificado por cualquiera de las causas recogidas en el apartado 4.9.1.
- Expiración de la vigencia del certificado.

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

El PCSC DOCUMENTA S.A. almacena ni copia, por sí o a través de un tercero, los datos de creación de firma o sello de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del firmante o del creador del sello. En este caso, se utilizarán sistemas y productos fiables, incluidos canales de comunicación electrónica seguros, se aplicarán procedimientos y mecanismos técnicos y organizativos adecuados, para garantizar que el entorno sea fiable y se utilice bajo el control

exclusivo del titular del certificado. Además, se custodiarán y protegerán los datos de creación de firma o de sello, frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

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

Este ítem no aplica.

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

Para ejecutar de modo seguro sus funciones de generación de claves, identificación, auditoría y archivo de registro, el PCSC DOCUMENTA S.A. y sus AR vinculadas han dispuesto e implantado controles de seguridad física y lógica en todas sus instalaciones, al igual que procedimientos de auditoría, tanto interna como externa.

5.1 CONTROLES FÍSICOS

5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

La localización de las instalaciones del PCSC DOCUMENTA S.A. donde se albergan los sistemas de certificación, no deberá ser públicamente identificada. No deberá haber identificación pública externa de las instalaciones e internamente, no deberá ser admitido ambientes compartidos que permitan la visibilidad de las operaciones de emisión, suspensión y revocación de los certificados. Esas operaciones deberán ser segregadas en compartimientos cerrados y físicamente protegidos.

Los centros de datos donde se aloja la infraestructura disponen de al menos, los siguientes elementos de seguridad física:

a) instalaciones para equipamientos de apoyo, tales como: máquinas de aire acondicionado, grupos de generadores, UPS, baterías, tableros de distribución de energía y de telefonía, subestaciones, rectificadores, estabilizadores y similares;
b) instalaciones para sistemas de telecomunicaciones;
c) los sistemas de puesta a tierra y protección contra rayos; e
d) iluminación de emergencia;

5.1.2 ACCESO FÍSICO

El PCSC DOCUMENTA S.A. implementa un sistema de control de acceso físico que garantice la seguridad de sus instalaciones, conforme a al ítem 9 “control de accesos” de la norma ISO 27002:2013 y los siguientes puntos:

5.1.2.1 NIVELES DE ACCESO FÍSICO

Se definen por los menos 4 (cuatro) niveles de acceso físico a los diversos ambientes del centro de datos del PCSC DOCUMENTA S.A., más 2 (dos) niveles relativos a la protección de la clave privada del PCSC.

En el primer nivel deberá situarse la primera barrera de acceso a las instalaciones del PCSC. Para acceder al área del nivel 1, cada persona deberá ser identificada y registrada por el personal de seguridad, a partir de ese nivel personas extrañas a la operativa del PCSC deberán transitar debidamente identificadas y acompañadas. Ningún tipo de proceso operacional o administrativo del PCSC deberá ser ejecutado en ese nivel.

Excepto en los casos previstos por la ley, la posesión de armas no será admitida en las instalaciones del PCSC, desde el nivel 1. A partir de ese nivel, equipos de grabación, fotografía, vídeo, sonido o similares, así como los ordenadores portátiles, será controlado su ingreso y sólo pueden ser utilizados mediante la autorización formal y supervisada.

El segundo nivel será interno al primero y deberá requerir, de la misma forma que el primero, una identificación individual de las personas que en él accedan. Ese será el nivel mínimo de seguridad requerido para la ejecución de cualquier proceso operacional o administrativo del PCSC. El paso del primer al segundo nivel deberá exigir por lo menos 1 (uno) factor de autenticación electrónica y tarjeta de identificación visible.

En el tercer nivel deberá situarse dentro del segundo nivel y será el primer nivel en albergar material y actividades sensibles de la operativa del PCSC. Cualquier actividad relativa al ciclo de vida de los certificados electrónicos deberá estar localizada a partir de este nivel. Personas que no están involucradas con esas actividades no deberán tener permiso para acceder a este nivel. Las personas que no poseen permiso de acceso no podrán permanecer en ese nivel si no estuviesen acompañadas por alguien que tenga permiso de acceso.

En este nivel deberán ser controladas tanto las entradas como las salidas de cada persona autorizada. Los mecanismos de control que deberán ser requeridos para acceder a ese nivel son dos: algún tipo de identificación individual, como una tarjeta electrónica, y la identificación biométrica. Teléfonos móviles y otros equipos de comunicación portátil, con excepción de los necesarios para el funcionamiento del PCSC, no serán aceptadas desde el nivel 3.

En el cuarto nivel, interno al tercero, donde han de desplegarse, actividades especialmente sensibles a la operación del PCSC, tales como la emisión y revocación de los certificados y la emisión de la LCR. Todos los sistemas y equipamientos necesarios a estas actividades deberán estar localizados a partir de este nivel. El nivel 4 deberá poseer 2 (dos) factores de autenticación como mínimo (uno de ellos biométrico) y tarjeta de identificación visible y, adicionalmente, deberá exigir, en cada acceso a su ambiente, la identificación de, como mínimo, 2 (dos) personas autorizadas. En este nivel, la permanencia de esas personas deberá ser exigida mientras el ambiente estuviera ocupado.

En el cuarto nivel, todas las barreras físicas (paredes y barrotes) deben ser sólidas, extendiéndose desde el piso real al techo real. Las paredes, piso y techo deberán ser realizadas de modo a prevenir las amenazas de acceso no autorizado, agua, vapor, gas y fuego. Las tuberías de refrigeración, de energía o de

comunicación no deberán permitir la penetración física en las áreas de cuarto nivel. Adicionalmente, debe tener una protección contra las interferencias electromagnéticas externas.

Este ambiente deberá ser construido según las normas internacionales aplicables.

Podrá existir, en el centro de datos, varios ambientes del cuarto nivel para albergar y segregar, cuando fuera el caso:

a) equipamientos de producción on-line y cofre de almacenamiento;
b) equipamientos de producción off-line y cofre de almacenamiento; y
c) equipamientos de redes e infraestructura (firewall, ruteadores, switches y servidores).

En el quinto nivel, interno al ambiente del nivel 4, deberá disponerse de un cofre o un gabinete reforzado, donde estarán almacenados: materiales criptográficos, tales como, claves, datos de activación, sus copias y equipamientos criptográficos.

Para garantizar la seguridad del material almacenado, el cofre o el gabinete deberán obedecer las siguientes especificaciones mínimas:

a) estar hecho de acero o con material de resistencia equivalente; y
b) poseer cerraduras antirrobo.

En el sexto nivel, interno al ambiente del nivel 4, deberá comprender un cofre o un gabinete reforzado. Los datos de activación de la clave privada del PCSC deberán ser almacenados en ese ambiente.

Para garantizar la seguridad del material almacenado, el cofre o el gabinete deberán obedecer las siguientes especificaciones mínimas:

a) estar hecho de acero o con material de resistencia equivalente; y
b) poseer cerraduras antirrobo.

5.1.2.2 SISTEMAS FÍSICOS DE DETECCIÓN

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

Las cintas de vídeo resultantes de grabación 24x7 deberán ser almacenadas, como mínimo, 4 (cuatro) años. Ellas deberán ser testeadas (verificación de estrechos aleatorios en el inicio, medio y final de la cinta) por lo menos cada 3 (tres) meses, con la elección, como mínimo, de 1 (una) cinta referente a cada semana. Esas cintas deberán ser almacenadas en el ambiente del nivel 3.

Todas las puertas de transición entre los ambientes de niveles 3 y 4 deberán ser monitoreadas por un sistema de notificación de alarmas. Donde hubiere, a partir del nivel 2, vidrios separando niveles de acceso, deberá ser implementado un mecanismo de alarma de quiebra de vidrios, que deberá estar funcionando ininterrumpidamente.

En todos los ambientes del cuarto nivel, una alarma de detección de movimientos deberá permanecer activa hasta que se satisfaga el criterio de acceso al ambiente. Así que si, debido a la salida de uno o más empleados, trae como consecuencia que el criterio mínimo de ocupación deje de ser satisfecha, deberán activarse automáticamente los sensores de presencia.

Los sistemas de notificación de alarmas deberán utilizar por lo menos 2 (dos) medios de notificación: sonoro y visual.

El sistema de monitoreo de las cámaras de video, así como el sistema de notificación de alarma, deberán ser permanentemente monitoreados por el personal autorizado y estar localizados en el nivel 3. Las instalaciones del sistema de monitoreo, a su vez, deben ser monitoreados por cámaras de vídeo cuyo posicionamiento debería permitir el seguimiento de las acciones del personal autorizado.

5.1.2.3 SISTEMAS DE CONTROL DE ACCESO

El sistema de control de acceso deberá estar en el ambiente de nivel 4.

5.1.2.4 MECANISMOS DE EMERGENCIA

Mecanismos específicos son implementados por el PCSC DOCUMENTA S.A. para garantizar la seguridad de su personal y de sus equipamientos en situaciones de emergencia. Esos mecanismos deberán permitir el desbloqueo de las puertas por medio de accionamiento mecánico, para la salida de emergencia de todos los ambientes con control de acceso. La salida efectuada por medio de estos mecanismos debe accionar inmediatamente las alarmas de apertura de puertas.

Se podrá especificar e implementar otros mecanismos de emergencia, específicos necesarios para cada tipo de instalación. Todos los procedimientos referentes a esos mecanismos de emergencia deberán ser documentados. Los mecanismos y procedimientos de emergencia deberán ser verificados semestralmente, por medio de simulación de situaciones de emergencia.

5.1.3 ENERGÍA Y AIRE ACONDICIONADO

La infraestructura del ambiente de certificación del PCSC DOCUMENTA S.A. deberá ser dimensionada con sistemas y dispositivos que garanticen el funcionamiento ininterrumpido de energía eléctrica en las instalaciones. Las condiciones de funcionamiento ininterrumpido de energía deben ser mantenidas de forma de atender los requisitos disponibilidad de los sistemas del PCSC y de sus respectivos servicios. Un sistema puesto a tierra deberá ser implantado.

Todos los cables eléctricos deben estar protegidos por tuberías y conductos apropiados.

Deberán ser utilizados tuberías, conductos, canaletas, paneles y cajas (de paso, distribución y terminación) diseñadas y construidas de forma a facilitar la inspección y detección de intentos de manipulación. Deberán ser utilizados conductos separados para los cables de energía, de telefonía y de datos.

Todos los cables deben ser catalogados, identificados e inspeccionados periódicamente, al menos cada seis (6) meses, en busca de evidencia de violación u otras anomalías.

Deberán ser mantenidos actualizados los registros sobre la topología de la red de cables, de acuerdo a los requisitos de confidencialidad establecidos en el ítem 13 “seguridad en las telecomunicaciones” de la norma ISO 27002/2013. Cualquier modificación en esa red deberá ser previamente documentada.

No deberán ser admitidas instalaciones provisorias, cableados expuestas o directamente conectadas a tomas sin la utilización de conectores adecuados.

El sistema climatización deberá cumplir con los requisitos de temperatura y humedad exigidos por

los equipamientos utilizados en el ambiente y disponer de filtros de polvo. En los ambientes de nivel 4, el sistema de climatización deberá ser independiente y tolerable a fallas.

La temperatura de los ambientes atendidos por el sistema de climatización deberá ser permanentemente monitoreada por el sistema de notificación de alarmas.

Los sistemas de aire acondicionados de los ambientes de nivel 4 deberán ser internos, con cambio de aire realizado apenas por la abertura de la puerta.

La capacidad de redundancia de toda la estructura de energía y aire acondicionado deberá ser garantizada, por medio de:

a) generadores de un tamaño compatible;
b) generadores de reserva;
c) sistemas de UPS redundantes; y
d) sistemas redundantes de aire acondicionado.

5.1.4 EXPOSICIÓN AL AGUA

La estructura interna al ambiente de nivel 4, deberá proveer protección física contra exposición a agua, filtraciones e inundaciones provenientes de cualquier fuente externa.

5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

El sistema de prevención contra incendios, internos a los ambientes deberán posibilitar alarmas preventivas antes que el humo sea visible, activados solamente con la presencia de partículas que caracterizan el sobrecalentamiento de materiales eléctricos y otros materiales combustibles presentes en las instalaciones.

En las instalaciones del PCSC DOCUMENTA S.A. no está permitido fumar o portar objetos que produzcan fuego o chispa.

El nivel 4 deberá poseer un sistema para detección precoz de humo y un sistema de extinción de incendio por gas.

En caso de incendio de las instalaciones del PCSC DOCUMENTA S.A., o el aumento de la temperatura interna del ambiente del nivel 4, no deberá exceder 50 grados Celsius, y el ambiente deberá soportar esta condición, como mínimo, 1 (una) hora.

5.1.6 ALMACENAMIENTO DE MEDIOS

El PCSC DOCUMENTA S.A. asegura el adecuado manejo y protección de los medios de almacenamiento de información, que contengan datos críticos o sensibles del sistema, contra daños accidentales (agua, fuego, electromagnetismo) y deberá impedir, detectar y prevenir su uso no autorizado, acceso o su divulgación.

La información relacionada a la infraestructura del PCSC debe almacenarse de forma segura en armarios ignífugos y cofres de seguridad, según la clasificación de la información en ellos contenida.

5.1.7 ELIMINACIÓN DE RESIDUOS

Todos los documentos en papel que contengan información clasificada como sensible deberán ser triturados antes de ir como residuo.

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

5.1.8 RESPALDO FUERA DE SITIO

Las instalaciones de respaldo deberán cumplir con los requisitos mínimos establecidos por este documento. Su localización deberá ser tal que, en caso de siniestro que torne inoperante la instalación principal del PCSC, las instalaciones de respaldo no se vean afectadas y tomen totalmente las operaciones del PCSC en condiciones idénticas en, un máximo, de 48 (cuarenta y ocho) horas.

5.2 CONTROLES PROCEDIMENTALES

El PCSC DOCUMENTA S.A. procura que toda la gestión, tanto la relativa a los procedimientos operacionales como a la de administración, se lleve a cabo de forma segura, conforme a lo establecido en este documento, realizando auditorías periódicas.

Asimismo, se ha diseñado una segregación de funciones, para evitar que una sola persona pueda conseguir el control total de la infraestructura.

5.2.1 ROLES DE CONFIANZA

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

Los Roles contemplan, al menos las siguientes responsabilidades que a continuación serán descriptos:

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

las instalaciones del PCSC;

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

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

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

e) responsables del ciclo de vida de claves criptográficas: son los responsables de la gestión del ciclo de vida de las claves criptográficas (ejemplo: oficial criptográfico, oficial de activación, etc.);

f) responsables de desarrollo de sistemas del PCSC: serán los encargados del diseño de las arquitecturas de programación, de control y supervisión de los desarrollos encomendados y de la correcta documentación de las aplicaciones; y

g) agentes de registros: son los responsables de la realización de las actividades inherentes a una RA, realizan la identificación de los solicitantes en la solicitud de emisión/suspensión/revocación de un certificado y autoriza en el sistema la emisión o revocación del mismo.

Todos los operadores del sistema de certificación del PCSC DOCUMENTA S.A. reciben

entrenamiento específico antes de obtener cualquier tipo de acceso. El tipo o nivel de acceso serán determinados, en un documento formal, con base en las necesidades de cada perfil.

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

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Se establece el requisito de control multi-usuarios para la generación y la utilización de la clave privada del PCSC DOCUMENTA S.A., de la forma definida en el ítem 6.2.2.

Todas las tareas ejecutadas en el ambiente donde está localizado el equipamiento de certificación del PCSC deberá requerir, como mínimo, de 2 (dos) de sus empleados o funcionarios con rol de confianza. Las demás tareas del PCSC podrán ser ejecutadas por un único empleado o funcionario.

5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Se garantiza que todo empleado o funcionario que asume un rol de confianza en el PCSC DOCUMENTA S.A. será identificado y su perfil será verificado antes de que:

a) sean incluido en una lista de acceso a las instalaciones del PCSC;
b) sean incluido en una lista para acceso físico al sistema de certificación del PCSC;
c) reciban un certificado electrónico para ejecutar sus actividades operacionales en el PCSC; y
d) reciban una cuenta de usuario del sistema de certificación del PCSC.

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

a) ser directamente asignados a un único empleado o funcionario;
b) no ser compartidos; y
c) restringirse a las acciones asociadas con el perfil para el que fueron creados.

5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES

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

a) los responsables del ciclo de vida de claves criptográficas no podrán cumplir funciones de los responsables de auditoría;
b) los responsables de sistemas no podrán cumplir funciones de los responsables de seguridad ni de los responsables de auditoría;
c) los responsables de seguridad no podrán cumplir funciones de los responsables de sistemas, de los responsables del ciclo de vida de claves criptográficas, de los agentes de

registros ni de los responsables de auditoría; y

d) los responsables de auditoría no podrán cumplir otra función o rol.

Además, otras tareas que deben ser segregadas son:

a) la puesta en operación del PCSC en producción;
b) la emisión o destrucción de los certificados del PCSC; y
c) la validación de información en los sistemas de certificación del PCSC y de solicitudes de emisión/revocación o información del suscriptor.

5.3 CONTROLES DE PERSONAL

Todos los empleados o funcionarios del PCSC DOCUMENTA S.A., de las AR y de los PSS vinculados, a cargo de las tareas operativas, registraron en un contrato o término de responsabilidad:

a) los términos y condiciones del perfil que ocuparán;
b) el compromiso de observar las reglas, políticas y normas aplicables a la ICP-Paraguay; y
c) el compromiso de no divulgar información confidencial a la que tenga acceso.

5.3.1 REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

Todo el personal del PCSC DOCUMENTA S.A. y de las AR vinculadas e involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, suspensión, revocación y gerenciamiento de certificados deberá ser seleccionado y admitido, conforme a lo establecido en el ítem 7 “seguridad ligada a los recursos humanos” de la norma ISO 27002/2013 y además deberán:

a) haber demostrado capacidad para ejecutar sus deberes;
b) haber suscripto un acuerdo de confidencialidad y disponibilidad;
c) no poseer otros antecedentes que puedan interferir o causar conflicto con los del PCSC;
d) no tener antecedentes de negligencia o incumplimiento de labores; y
e) no tener antecedentes judiciales ni policiales.

5.3.2 PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Con propósito de resguardar la seguridad y credibilidad de las entidades, todo personal del PCSC DOCUMENTA S.A. y de las AR vinculadas involucradas en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados deberá ser sometido a:

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

5.3.3 REQUERIMIENTOS DE CAPACITACIÓN

Todo el personal del PCSC DOCUMENTA S.A. y de las AR vinculadas, involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados deberá recibir entrenamiento documentado suficiente para el dominio de los siguientes temas:

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

5.3.4 REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

Todo el personal del PCSC DOCUMENTA S.A. y de las AR vinculadas, involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados deberá ser mantenido y actualizado sobre eventuales cambios o modificaciones tecnológicas de los sistemas del PCSC o de las RA.

5.3.5 FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

DOCUMENTA S.A. efectuará rotaciones de trabajo entre los distintos roles del PCSC y las AR vinculadas al menos una vez cada 5 años, con el objetivo de incrementar la seguridad y garantizar la continuidad, en caso de ausencia de alguno de los trabadores.

Antes de asumir las nuevas funciones, el personal debe recibir una capacitación y/o actualización de acuerdo al rol específico, que le permita cumplir con las tareas satisfactoriamente.

5.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS

En la eventualidad de una acción no autorizada, real o sospechada, realizada por una persona encargada del proceso operacional del PCSC DOCUMENTA S.A. o de una AR vinculada, el PCSC deberá de inmediato, suspender el acceso de esa persona a su sistema de certificación, iniciar un procedimiento administrativo para determinar los hechos y, si es necesario, tomar las medidas legales pertinentes.

El proceso administrativo referido en el párrafo anterior deberá contener, como mínimo, los siguientes puntos:

a) relato de lo ocurrido con el modo de operación;
b) identificación de los involucrados;
c) eventuales perjuicios causados;
d) las sanciones aplicadas, si fuere el caso; y
e) conclusiones.

Concluido el proceso administrativo, el PCSC deberá comunicar sus conclusiones a la AC Raíz-Py.

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

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

5.3.7 REQUISITOS DE CONTRATACIÓN A TERCEROS

Todo el personal del PCSC DOCUMENTA S.A. y de las AR vinculadas, involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados, deberá ser contratado conforme a lo establecido en los ítems 7 “seguridad ligada a los recursos humanos” y 15 “relaciones con suministradores” norma ISO 27002/2013 y bajo las siguientes condiciones mínimas:

a) que exista un contrato con cláusulas propias de los roles de confianza y estipula sanciones para las acciones no autorizadas;
b) que el PCSC responsable o AR vinculada no posea personal disponible para llenar los roles de confianza;
c) que el personal a contratar cumpla con los mismos requisitos del ítem 5.3.1; y
d) que una vez finalizado el servicio contratado se revoquen los derechos de acceso.

5.3.8 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

El PCSC DOCUMENTA S.A. pone a disposición de todo el personal del PCSC y para todo el personal de las AR vinculados al menos:

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

Toda documentación entregada o disponibilizada al personal deberá estar clasificada y deberá ser mantenida actualizada.

5.4 PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

5.4.1 TIPOS DE EVENTOS REGISTRADOS

El PCSC DOCUMENTA S.A., registra en archivos de auditoría, todos los eventos relacionados a la seguridad de su sistema de certificación. Entre otros, los siguientes eventos deberán obligatoriamente estar incluidos en los archivos de auditoría:

a) iniciación y terminación del sistema de certificación;
b) los intentos de crear, eliminar, establecer contraseñas o cambiar los privilegios del

sistema de los operadores del PCSC;

c) los cambios en la configuración del PCSC o en sus claves;
d) los cambios en las políticas de creación de certificados;
e) los intentos de acceso (*login*) y de salida del sistema (*logoff*);
f) los intentos no autorizados de acceso a los archivos del sistema;
g) la generación de claves propias del PCSC o de claves de sus usuarios finales;
h) la emisión y revocación de certificados;
i) la generación de la LCR;
j) los intentos de iniciar, remover, habilitar y deshabilitar a los usuarios de sistemas y actualizar y recuperar sus claves;
k) las operaciones fallidas de escritura o lectura en el repositorio de los certificadosy de la LCR, en su caso; y
l) las operaciones de escritura en ese repositorio, en su caso.

El PCSC responsable de la DPC deberá también registrar, electrónicamente o manualmente, informaciones de seguridad no generadas directamente por el sistema de certificación, tales como:

a) registros de accesos físicos;
b) el mantenimiento y los cambios en la configuración de sus sistemas;
c) los cambios de personal y los cambios de su rol de confianza;
d) los informes de discrepancia y de compromiso; y
e) el registro de destrucción de los medios de almacenamiento que contienen las claves criptográficas, de datos de activación de certificados o de la información personal de los usuarios.

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

Para facilitar los procesos de auditoría, toda documentación relacionada a los servicios del PCSC deberá ser almacenada, electrónicamente o manualmente, en un local único, conforme a lo establecido en el ítem 12 “seguridad en la operativa” de la norma ISO 27002/2013.

El PCSC responsable de la DPC, deberá registrar electrónicamente archivos de auditorías de todos los eventos relacionados a la validación y aprobación de la solicitud, así como la revocación de los certificados. Los siguientes eventos deberán obligatoriamente estar incluidos en los archivos de auditoría:

a) los AGR que realizan las operaciones;
b) fecha y hora de las operaciones;
c) la asociación entre los agentes que realizan la validación, aprobación y el certificado generado; y
d) la firma digital del ejecutante.

El PCSC a la que está vinculada la RA, debe establecer, en un documento que esté disponible en las auditorías de cumplimiento, el local de archivo de las copias de los documentos utilizados para la identificación del suscriptor, presentados en el momento de la solicitud y revocación de certificados. El formulario de solicitud y el Contrato de Prestación de Servicios de Confianza.

5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)

Los registros se analizarán, al menos, una vez al mes, en las auditorías periódicas de la ICP, y de manera anual cuando sean necesarios.

Todos los eventos significativos deberán ser explicados en un informe de auditoría de registros. Tal análisis deberá involucrar una inspección breve de todos los registros, con la verificación de que no fueron alterados, seguida de una investigación más detallada de cualquier alerta o irregularidades en esos registros. Todas las medidas adoptadas como resultado de este análisis deberán ser documentadas.

5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

La información generada en los registros de eventos se conserva localmente sus por los menos 2 (dos) meses y, consecuentemente, deberá almacenarlos de la manera descrita en el ítem 5.5.2.

Además de las revisiones oficiales, los registros de auditoría deben ser revisados en respuesta a una alerta, por irregularidades o incidentes dentro de los sistemas del PCSC.

5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

El PCSC DOCUMENTA S.A. posee un sistema de registro de eventos para proteger sus registros de auditoría contra lectura no autorizada, modificación y eliminación, utilizando mecanismos de protección conforme a lo dispuesto al Ítem 12 “seguridad en la operativa” de la norma ISO 27002/2013

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

El PCSC DOCUMENTA S.A. genera copia de los registros de auditoría, como mínimo, una vez al mes.

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

Los archivos de registro son almacenados en los sistemas internos, mediante una combinación de procesos automáticos y manuales ejecutados por las aplicaciones de el PCSC DOCUMENTA S.A.

5.4.7 NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

Cuando un evento es almacenado por el registro, no se requiere notificar al causante de dicho evento, a excepción de que el evento sea de índole accidental y resulta probable que pueda volver a ocurrir.

5.4.8 EVALUACIÓN DE VULNERABILIDADES

Los eventos que indiquen posibles vulnerabilidades, detectados en el análisis periódico de los registros de auditoria, serán analizadas detalladamente y, dependiendo de su gravedad, registradas por separado. Acciones correctivas que surjan deberán ser implementadas y registradas con fines de auditoria.

5.5 ARCHIVOS DE REGISTROS

5.5.1 TIPOS DE REGISTROS ARCHIVADOS

El PCSC DOCUMENTA S.A. y sus AR vinculadas conservan toda la información relevante sobre las operaciones realizadas con los certificados durante los periodos de tiempo establecidos, se deben archivar los siguientes datos:

m) solicitudes de certificados;
n) solicitudes de revocación de certificados;
o) notificaciones de compromiso de claves privadas;
p) emisiones y revocaciones de certificados;
q) emisiones de LCR;
r) cambio de claves criptográficas del PCSC responsable;
s) Información de auditoría prevista en el ítem 5.4.1.

5.5.2 PERÍODOS DE RETENCIÓN PARA ARCHIVOS

- Las LCRs y los certificados emitidos de firma digital deberán ser conservados permanentemente para fines de consulta histórica;
- Los dossiers de los titulares de certificado como mínimo, por 10 (diez) años, a contar desde la fecha de expiración o revocación del certificado; y
- Las demás informaciones, inclusive los archivos de auditoría deberán ser almacenadas, como mínimo, 10 (diez) años.

5.5.3 PROTECCIÓN DE ARCHIVOS

Todos los registros archivados deberán ser clasificados y almacenados con los requisitos de seguridad compatibles con esta clasificación, conforme a lo establecido en el ítem 12 “seguridad en la operativa” de la norma ISO 27002/2013.

5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO

Una segunda copia de todo el material archivado deberá ser almacenada en un local externo al PCSC DOCUMENTA S.A., recibiendo el mínimo tipo de protección utilizada para el archivo principal.

Las copias de seguridad deberán seguir los periodos de retención definidos para los registros de las cuales son copias.

El PCSC responsable de la DPC deberá verificar la integridad de esas copias de seguridad, como mínimo, cada 6 (seis) meses.

5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

Este ítem no aplica.

5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO)

Todo el archivado de información se realiza de manera interna a la ICP de DOCUMENTA S.A.

5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA

Los eventos registrados están protegidos mediante técnicas criptográficas, de forma que nadie salvo las propias aplicaciones de visualización y gestión de eventos pueda acceder a ellos. Sólo el personal autorizado tiene acceso a los archivos físicos de soportes y archivos informáticos, para llevar a cabo verificaciones de integridad u otras.

Esta verificación debe ser llevada a cabo por el Auditor, que debe tener acceso a las herramientas de verificación y control de integridad del registro de eventos de la ICP de DOCUMENTA S.A.

También se llevan a cabo pruebas de restauración de la información archivada al menos una vez al año.

5.6 CAMBIO DE CLAVE

El PCSC DOCUMENTA S.A. debe cambiar su clave de acuerdo con el *tiempo de uso* y *tiempo operacional* delos certificados emitidos dentro de la ICPP, este cambio técnicamente implica la emisiónde un nuevo certificado. *El tiempo operacional* de un certificado coincide con el descripto en loscampos de ‘’Válido desde’’ y ‘’Válido hasta’’ del mismo. El *tiempo de uso* refiere al establecido para los certificados emitidos en el marco de la ICPP para determinados usos, como seaprecia a continuación:

Tipo de Certificado	Tiempo de uso en años	Tiempo operacional en años	Descripción
Certificado de Suscriptores (F2, F3, C2 y C3)	2	2	El certificado emitido al usuario final es otorgado por un tiempo máximo de dos años, al finalizar ese periodo pierde su validez.
Certificado de Suscriptores (F1 y C1)	1	1	El certificado emitido al usuario final es otorgado por un tiempo máximo de un año, al finalizar ese periodo pierde su validez
Certificado de PCSC	8	10	El Certificado emitido al PCSC tendrá un tiempo operacional de 10 años, que resulta de la suma del tiempo de uso de su certificado (8 años) más el tiempo de validez máximo del certificado de su suscriptor (2 años). Solamente durante el tiempo de uso de su certificado, el PCSC podrá emitir certificados a usuarios o suscriptores. En los años restantes del tiempo operacional sólo podráfirmar el LCR de usuarios o suscriptores.

Certificado AC Raíz-Py	10	20	El Certificado emitido a la AC Raíz-Py tendrá un tiempo operacional de 20 años, que resulta de la suma del tiempo de uso de su certificado (10 años) más el tiempo de validez máximo del certificado de su suscriptor (10 años). Solamente durante el tiempo de uso de su certificado, la AC Raíz-Py podrá emitir certificados a un PCSC. En los años restantes del tiempo operacional sólo podrá firmar el LCR de PCSC.

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

Por lo tanto, el certificado anterior podrá ser utilizado únicamente para firmar la LCR correspondiente y validar la cadena de confianza de la ICPP; el nuevo certificado emitido, será utilizado para emitir nuevos certificados y firmar la nueva lista de LCR.

El PCSC DOCUMENTA S.A. tiene la obligación de garantizar que el tiempo máximo de uso en años de los certificados de niveles inferiores se ajusta con el tiempo operacional de todos los niveles superiores.

5.7 RECUPERACIÓN DE DESASTRES Y COMPROMISO

Los procedimientos de recuperación utilizados por el PCSC DOCUMENTA S.A. está conforme a lo establecido en el ítem 17 “aspectos de seguridad de la información en la gestión de la continuidad del negocio” de la norma ISO 27002:2013, previsto en la PCN del PCSC.

5.7.1 PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO

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

Los procedimientos previstos en el PCN de las AR vinculadas al PCSC DOCUMENTA S.A. para la recuperación total o parcial de las actividades de las RA, contienen al menos la siguiente información:

a) identificación de eventos que pueden causar interrupciones en los procesos delnegocio, por ejemplo, fallas de equipos, inundaciones e incendios, si fuera el caso;
b) identificación y concordancia de todas las responsabilidades y procedimientos de emergencia;
c) implementación de procedimientos de emergencia que permitan la recuperación y restauración dentro de los plazos necesarios;
d) documentación de procesos y procedimientos conforme a lo establecido;
e) capacitación adecuada del personal en procedimientos y procesos de emergencia definidos, incluida la gestión de crisis; y

f) prueba y actualización de planes.

5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES

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

En el caso de verse afectados certificados emitidos, se notificará del hecho a los usuarios de los mismos y se procederá a una nueva certificación.

Los procedimientos de recuperación utilizados en caso de que la revocación del certificado del PCSC DOCUMENTA S.A. se describen en el Ítem 5.7.3

5.7.3 PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD

5.7.3.1 CERTIFICADO DE ENTIDAD ES REVOCADO

Se notificará a todos los suscriptores afectados de la revocación del certificado del PCSC DOCUMENTA S.A. y se procederá a la revocación de todos los certificados emitidos.

5.7.3.2 CLAVE DE ENTIDAD ESTÁ COMPROMETIDA

En el caso de compromiso de la clave privada del PCSC DOCUMENTA S.A., se procederá a solicitar al MIC su revocación inmediata. Cesando el servicio de emisión de Certificados a usuarios finales o suscriptores.

5.7.4 CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

En este ítem de la DPC, deben ser descriptos los procedimientos de recuperación utilizados por el PCSC después de la ocurrencia de un desastre natural o de otra naturaleza, antes del restablecimiento de un ambiente seguro.

El sistema de Autoridad de Certificación de DOCUMENTA S.A. puede ser reconstruido en caso de desastre. Para llevar a cabo esta reconstrucción es necesario contar con:

- Un sistema con hardware, software y dispositivo Hardware Criptográfico de Seguridad similar al existente con anterioridad al desastre.
- Las claves de administrador de la Autoridad de Certificación de DOCUMENTA S.A.
- Una copia de respaldo de los discos del sistema anterior al desastre.

Con estos elementos es posible reconstruir el sistema tal y como estaba en el momento de la copia de respaldo realizada y, por lo tanto, recuperar la CA, incluidas sus claves privadas.

El almacenado, tanto de las tarjetas de acceso de los administradores de las AC como de las copias de los discos de sistema de cada CA, se lleva a cabo en un lugar diferente, lo suficientemente alejado y

protegido como para dificultar al máximo la concurrencia de catástrofes simultáneas en los sistemas en producción y en los elementos de recuperación.

5.8 EXTINCIÓN DE UN PCSC O ENTIDADES VINCULADAS

En caso que el PCSC DOCUMENTA S.A., deje de operar deberá cumplir, como mínimo, con lo siguiente:

a) solicitar a AA, con al menos un mes de anticipación la cancelación de su suscripción en el registro público de PCSCs, comunicándole el destino que dará a los datos de los certificados, especificando, en su caso, los que va a transferiry a quién, cuando proceda;
b) notificar a sus suscriptores con al menos un mes de anticipación antes de la suspensión efectiva o cese de sus operaciones;
c) publicar en su sitio principal de Internet la fecha de suspensión de los servicios con al menos un mes de anticipación;
d) publicar la fecha de suspensión de sus servicios por el plazo de 3 días consecutivos en un diario de gran circulación, 10 días hábiles antes de la suspensión efectiva o cese de las operaciones;
e) preservar toda la información en concordancia con esta DPC y la normativa aplicable; y
f) proceder a la eliminación y destrucción de la clave privada mediante un mecanismo que impida su reconstrucción.

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

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

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

En el caso de que una RA, VA o PSS vinculada al PCSC DOCUMENTA S.A. cese en el ejercicio de las funciones, transferirá los registros que mantenga al PCSC, mientras exista la obligación de mantener archivada la información, y de no ser así, ésta será destruida.

6. CONTROLES TÉCNICOS DE SEGURIDAD

6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1 GENERACIÓN DEL PAR DE CLAVES

El par de claves criptográficas del PCSC responsable deberá ser generado por la AA, posterior a la habilitación otorgada por el MIC vía resolución ministerial.

El proceso de generación del par de claves del PCSC DOCUMENTA S.A. se realiza mediante hardware.

El par de claves deberá ser generado solamente por el titular del certificado correspondiente.

Cada PC implementada por el PCSC responsable debe definir el proceso utilizado para la generación de claves criptográficas de los titulares de los certificados, en base a los requerimientos establecidos en el documento DOC-ICPP-04 [1].

6.1.2 ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR

Ítem no aplicable. La generación y guarda de una clave privada será responsabilidad exclusiva del titular del certificado correspondiente.

6.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

Para la generación del CSR por el PCSC DOCUMENTA S.A., se adoptará el formato definido en el documento DOC-ICPP-06 [3].

Los procedimientos específicos aplicables deben ser detallados en cada PC implementada.

La clave pública del PCSC DOCUMENTA S.A. es entregada a la AC Raíz mediante la entrega de una solicitud de firma de certificado (CSR) en el formato definido en el documento DOC-ICPP-06 [3]

6.1.4 ENTREGA DE LA CLAVE PÚBLICA DE LA AC A LAS PARTES QUE CONFÍAN

Las formas para la disponibilización del certificado del PCSC DOCUMENTA S.A., y de todos los certificados de la cadena de certificación, para los usuarios y las partes que confían de la ICPP, comprenden, entre otras:

a) en el momento de disponibilización de un certificado para su titular, usando elformato definido en el documento, DOC-ICPP-06 [3];
b) un directorio;
c) una página WEB del PCSC; y
d) otros medios seguros aprobados por la AA.

6.1.5 TAMAÑO DE LA CLAVE

El tamaño de las claves para cada tipo de certificado emitido por el PCSC DOCUMENTA S.A. son definidos en base a los requerimientos aplicables establecidos en el documento DOC-ICPP-04 [1].

El tamaño de las claves del PCSC DOCUMENTA S.A. se definen en base a los requerimientos aplicables establecidos en el documento DOC-ICPP-06 [3].

6.1.6 GENERACIÓN DE PARÁMETROS DE CLAVE ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD

Los parámetros de verificación de calidad, deberán ser verificados de acuerdo con las normas

establecidas por el patrón definido en el documento DOC-ICPP-06 [3].

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

La clave privada del PCSC DOCUMENTA S.A. deberá ser utilizada solamente para la firma de los certificados por ella emitidos y de sus LCR.

Los usos admitidos de la clave para cada tipo de certificado emitido por el PCSC DOCUMENTA S.A. vienen definidos por la Política de Certificación que le sea de aplicación.

Ha de tenerse en cuenta que la eficacia de las limitaciones basadas en extensiones de los certificados depende, en ocasiones, de la operatividad de aplicaciones informáticas que no han sido fabricadas ni controladas por DOCUMENTA S.A.

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

6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO

El módulo criptográfico de generación de claves asimétricas del PCSC DOCUMENTA S.A. adoptará los patrones definidos en el documento DOC-ICPP-06 [3].

Los patrones requeridos para los módulos de generación de claves criptográficas de los titulares de certificados generados por el PCSC DOCUMENTA S.A. son aquellas definidas en el documento DOC-ICPP-06 [3]. Cada PC implementada debe especificar los requisitos adicionales aplicables.

6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA

La clave privada del PCSC DOCUMENTA S.A. se encuentra bajo control multi-persona para su utilización. Como mínimo serán requeridos 2 (dos) operadores designados por el PCSC.

6.2.3 CUSTODIA (ESCROW) DE LA CLAVE PRIVADA

El PCSC DOCUMENTA S.A. no almacena ni copia las claves privadas de los titulares de certificados de firma digital (tipo F).

La clave privada del PCSC DOCUMENTA S.A. está respaldada bajo la protección de dispositivos seguros y a los que sólo las personas con rol de confianza autorizada por DOCUMENTA S.A. tiene acceso.

6.2.4 RESPALDO/COPIA DE LA CLAVE PRIVADA

Cualquier persona física o jurídica, titular de certificado, podrá, a su criterio, mantener una copia de su propia clave privada.

El PCSC DOCUMENTA S.A. mantiene una copia de seguridad de su propia clave privada.

El PCSC DOCUMENTA S.A. no mantiene copia de seguridad de la clave privada del titular de certificado de firma digital por ella emitida. Por solicitud del respectivo titular, o empresa u organización, cuando el titular del certificado es su empleado/funcionario o cliente, el PCSC podrá mantener una copia

de seguridad de la clave privada correspondiente al certificado de cifrado por ella emitida. Cada PC debe definir los requisitos específicos aplicables.

En cualquier caso, la copia de seguridad deberá ser almacenada cifrada por un algoritmo simétrico definido en el documento DOC-ICPP-06 [3] y protegida con un nivel de seguridad no inferior a aquel definido para la clave original.

6.2.5 ARCHIVADO DE LA CLAVE PRIVADA

Las claves deberán ser archivadas en un nivel de seguridad no inferior a aquella definida para la clave original. No deben ser archivadas las claves privadas de uso permitido para firma digital.

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

6.2.6 TRANSFERENCIA DE CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRIPTOGRÁFICO

La transferencia de la clave privada del PCSC DOCUMENTA S.A. sólo se puede hacer entre módulos criptográficos (HSM) y requiere de la intervención de personal con rol de confianza autorizado por el PCSC.

Cada PC implementada debe definir, cuando sea aplicable, los requisitos de transferencia de la clave privada de los titulares del certificado de un módulo criptográfico a otro.

6.2.7 ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

Los requisitos aplicables al módulo criptográfico para almacenar la clave privada del PCSC DOCUMENTA S.A. adoptarán los patrones definidos en el documento DOC-ICPP-06 [3].

Cada PC definirá el medio utilizado para el almacenamiento de la clave privada del usuario final, en base a los requerimientos establecidos en el documento DOC-ICPP-04 [1].

6.2.8 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

La clave privada del PCSC DOCUMENTA S.A. se activa mediante la inicialización del software por medio de la combinación mínima de operadores asignados. Éste es el único método de activación de dicha clave privada.

Concretamente, son necesarios 3 de un total de 5 operadores de DOCUMENTA S.A. para activar la clave privada de cualquiera del PCSC.

Los métodos de activación de clave están protegidos, y para accederlos se deben contar con al menos dos factores de autenticación.

6.2.9 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

El procedimiento de desactivación de la clave privada lo realiza personal con rol de confianza con control multipersona mediante la parada de la aplicación informática del PCSC.

Cada PC implementada debe describir los requisitos y procedimientos necesarios para la

desactivación de la clave privada de la entidad titular de certificado.

6.2.10MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA

El procedimiento para la destrucción de las claves privadas del PCSC DOCUMENTA S.A. requiere de una autorización para destruirlas.

La destrucción se realizará utilizando los comandos establecidos para borrar físicamente de la memoria del Módulo criptográfico de hardware la parte en la que estaban grabadas las claves, para ello, éste debe ser limpiado por medio de inicialización de ceros (zeroize command).

El procedimiento de destrucción de clave privada, debe estar documentado y realizado por personal con rol de confianza con control multipersona con al menos dos factores de autenticación.

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

Cada PC implementada debe describir los requisitos y procedimientos necesarios para destrucción de la clave privada de la entidad titular de certificado.

6.3 OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

6.3.1 ARCHIVO DE LA CLAVE PÚBLICA

DOCUMENTA S.A. mantiene un archivo de la clave pública del PCSC DOCUMENTA S.A., todos los certificados de firma digital emitidas y las LCR emitidas, permanentemente, para la verificación de firmas generadas durante su periodo de validez.

El archivo dispone de medios de protección frente a las manipulaciones que pretendan efectuarse sobre la información contenida.

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

La clave privada del PCSC DOCUMENTA S.A. y de los titulares de certificados electrónicos, tendrán un periodo operacional y periodo de uso en el marco de la ICPP conforme a lo descripto en el ítem 5.6 de este documento. 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.

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

6.4 DATOS DE ACTIVACIÓN

6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

El PCSC DOCUMENTA S.A. mantiene estrictos controles de sus datos de activación para operar los módulos criptográficos conforme a lo establecido en el ítem 6.2.2. Además, debe garantizar que los datos de activación de la clave privada del PCSC responsable serán únicos.

Cada PC implementada garantiza que los datos de activación de la clave privada del titular del certificado serán únicos.

6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Se garantiza que los datos de activación de la clave privada del PCSC DOCUMENTA S.A. son protegidos contra el uso no autorizado, por medio de mecanismos de criptografía y de control de acceso físico.

Cada PC implementada debe garantizar que los datos de activación de la clave privada de la persona física o jurídica titular del certificado, si se utiliza, serán protegidos contra el uso no autorizado.

6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Sin estipulaciones

6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos, como en el caso de auditorías externas o internas e inspecciones.

6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

La generación del par de claves del PCSC DOCUMENTA S.A. será realizada offline para impedir el acceso remoto no autorizado.

Cada computador del PCSC DOCUMENTA S.A., relacionado directamente con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados, implementa, entre otras, las siguientes características:

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

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

Cualquier equipo o parte del mismo, para ser sometidos a mantenimiento deberán haber borrado la información confidencial que contenga y controlar su número de serie y las fechas de envío y recepción. Al regresar a las instalaciones del PCSC, el equipo que fue sometido a mantenimiento debe ser inspeccionado. Cualquier equipo que ya no se utilice de forma permanente, deberán ser destruidas de él, de

manera definitiva, todas las informaciones sensibles almacenadas, relativas a la actividad del PCSC. Todos estos eventos deberán ser registrados con fines de auditoría.

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

6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

DOCUMENTA S.A. evalúa de forma permanente su nivel de seguridad de cara a identificar posibles debilidades y establecer las correspondientes acciones correctoras mediante auditorías externas e internas, así con la realización continua de controles de seguridad.

6.5.3 CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO

Los requisitos de seguridad computacional de las estaciones de trabajo y de los computadores utilizados por la AR vinculadas al PCSC DOCUMENTA S.A. para los procesos de validación y aprobación de certificados cumplen con lo establecido en el documento DOC-ICPP-05 [2].

6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos.

6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA

Los requisitos de seguridad son exigibles, desde su inicio, tanto en la adquisición de sistemas informáticos como en el desarrollo de los mismos ya que puedan tener algún impacto sobre la seguridad de ICP de DOCUMENTA S.A.

El PCSC mantiene controles que proporcionen una seguridad razonable de las actividades de desarrollo y mantenimiento de los sistemas de la certificación.

Los nuevos sistemas o para la expansión de los sistemas existentes, deben especificar los requisitos de control, seguir procedimientos de prueba de software y control de cambios para la implementación de software. Toda la documentación del ciclo de vida del sistema, debe estar disponible para su verificación.

El PCSC mantener controles sobre el acceso a las bibliotecas fuente de programas.

Los procesos de proyecto y desarrollo conducidos por el PCSC, proveen documentación suficiente para soportar evaluaciones de seguridad externas de los componentes del PCSC.

6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

El PCSC DOCUMENTA S.A mantiene un inventario de todos los activos informáticos y realizan una clasificación de los mismos de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración del sistema de certificación utilizado por el PCSC DOCUMENTA S.A. y por las AR vinculadas se audita de forma periódica y se realiza un seguimiento de las necesidades de capacidad.

6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Existen controles de seguridad a lo largo de todo el ciclo de vida de los sistemas con algún impacto en la seguridad de la ICP.

DOCUMENTA S.A. realiza controles para proporcionar seguridad al dispositivo que realiza la generación de las claves. Para evitar posibles incidencias en los sistemas se establecen los siguientes controles:

- El hardware de generación de claves es probado antes de su puesta en producción.
- La generación de claves se produce dentro de los módulos criptográficos que cumplan los requisitos de la técnica y del negocio.
- Los procedimientos para el almacenamiento seguro del hardware criptográfico y los materiales de activación después de la ceremonia de generación de claves.

6.6.4 CONTROLES EN LA GENERACIÓN DE LCR

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

6.7 CONTROLES DE SEGURIDAD DE RED

6.7.1 DIRECTRICES GENERALES

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

Todos los servidores y elementos de la infraestructura y protección de redes, tales como ruteadores, hubs, switches, firewalls y sistemas de detección de intrusos (IDS), localizados en el segmento de red en que se hospeda el sistema de certificación del PCSC, deberán estar localizados y operar en un ambiente de nivel, como mínimo, 4 (cuatro).

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

El acceso lógico a los elementos de la infraestructura y protección de la red deberán restringirse por medio de un sistema de autenticación y autorización de acceso. Los ruteadores (routers) conectados a redes externas deberán implementar filtros de paquetes de datos, que sólo permitan conexiones a los servicios y servidores previamente definidos como objeto de acceso externo.

6.7.2 FIREWALL

Mecanismos de firewall se deberán implementar en equipos de uso específico, configurados exclusivamente para esa función. Un firewall deberá promover el aislamiento, en subredes específicas, de los equipos servidores con acceso externo - la denominada "zona desmilitarizada" (DMZ) - en relación a

los equipos con acceso exclusivamente interno al PCSC.

El software de firewall, entre otras características, deberá implementar registros de auditoría.

6.7.3 SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

El sistema de detección de intrusos deberá tener la capacidad de ser configurado para reconocer ataques en tiempo real y responder automáticamente, con medidas tales como: enviar traps SNMP, ejecutar programas definidos por la administración de la red, enviar e-mail a los administradores, enviar mensajes de alerta al firewall o al terminal de gerenciamiento, promover la desconexión automática de conexiones sospechosas, o incluso la reconfiguración del firewall.

El IDS deberá ser capaz de reconocer diferentes patrones de ataques, incluso contra el propio sistema, con la posibilidad de actualizar su base de reconocimiento.

El IDS deberá proveer un registro de los eventos en logs, recuperables en archivos de tipo texto, e implementar una gestión de la configuración.

6.7.4 REGISTRO DE ACCESO NO AUTORIZADO A LA RED

Las tentativas de acceso no autorizado en ruteadores, Firewall o IDS, deberán ser registradas en archivos para posterior análisis, que podrá ser automatizada. La frecuencia de examen de los archivos de registro deberá ser, como mínimo, diario y todas las acciones tomadas como resultado de este examen deben ser documentadas.

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, LCR Y OCSP

7.1 PERFIL DEL CERTIFICADO

Todos los certificados emitidos por el PCSC DOCUMENTA S.A. cumplen con la norma ITU X.509 o ISO/IEC 9594-8, según el perfil establecido en RFC 5280.

A continuación, se detalla el contenido de los elementos más importantes del Certificado del PCSC DOCUMENTA S. A.:

CAMPO	COMPONENTE
1. Versión	V3
2. Número de Serie	576388f13ef79820623e207697bed999

3. Signature Algorithm	sha256RSA
4. Hash Signature Algorithm	Sha256
5. Issuer	CN = AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY O = MINISTERIO DE INDUSTRIA Y COMERCIO C = PY
6. Válido desde	lunes, 28 de marzo de 2022 17:04:26
7. Válido hasta	domingo, 28 de marzo de 2032 17:04:26
8. Subject	CN = CA-DOCUMENTA S.A. O = DOCUMENTA S.A. C = PY SERIALNUMBER = RUC80050172-1
9. Subject Public Key Info	Algoritmo: RSA Encryption Longitud:4096 bits
10. Subject Key Identifier	SHA-1 hash de la clave pública del titular
11. Authority Key Identifier	SHA-1 hash de la clave pública del emisor
12. Auth. Information Access **.CAIssuers** **.OCSP**	Se utilizará http://www.acraiz.gov.py/crt/ac_raiz_py_sha256.crt https://www.digito.com.py/ocsp
13. Certificate Policies **.Policy Identifier** **.URL DPC** **.Notice Referente**	Se utilizará Directivas del certificado http://www.acraiz.gov.py/DPC/politicas.pdf Certificados emitidos dentro del marco de la ICP Paraguay bajo la jerarquía de su ACRaíz
14. CRLDistributionPoints	http://www.acraiz.gov.py/arl/ac_raiz_py.crl
15. BasicConstraints	Tipo de asunto=Entidad de certificación (CA) Restricción de longitud de ruta=0
16. KeyUsage	Firma de certificados, Firma CRL sin conexión, Firma de lista de revocación de certificados (CRL) (06)

7.1.1 NÚMERO DE VERSIÓN

Todos los certificados emitidos por el PCSC DOCUMENTA S.A. implementa la versión 3 (tres) del estándar ITU X.509.

7.1.2 EXTENSIONES DEL CERTIFICADO

Las extensiones utilizadas en el certificado del PCSC DOCUMENTA S.A. son:

e) **Identificador de la clave de la Autoridad Certificadora** "***Authority Key Identifier*", no crítica:** el campo key Identifier debe contener el hash SHA-1 de laclave pública de la AC Raíz que emite el certificado;

f) **Identificador de la clave del suscriptor** "***Subject Key Identifier*", no crítica:** debe contener el hash SHA-1 de la clave pública del PCSC titular del certificado;

g) **Uso de Claves** "***Key Usage*", crítica:** solamente los bits *keyCertSign* y *CRLSign* deben estar activados;

h) **Políticas de Certificación "*Certificate Policies*", no crítica:**

d.1.1) el campo ***policyIdentifier*** debe contener el OID de la PC aplicable.

d.1.2) el campo **policyQualifiers** debe contener la dirección Web de la PC aplicable.

i) **Restricciones Básicas** "***Basic Constraints*", crítica:** debe contener el campo SubjectType CA=True y el campo PathLenConstraint debe tener valor cero;

j) **Puntos de distribución de las CRL** "**CRL Distribution Points", no crítica:** debe contener la dirección Web donde se obtiene la LCR correspondiente al certificado;y

k) **Acceso a la Información de la Autoridad Certificadora "Authority Information Access", no crítica:** debe contener el método de *acceso id-ad-calssuer* alcertificado de la AC Raíz, para recuperar la cadena de certificación.

7.1.3 IDENTIFICADORES DE OBJETO DE ALGORÍTMOS

Los certificados del PCSC DOCUMENTA S.A. deberán ser firmados utilizando el algoritmo definido en el documento DOC-ICPP-06 [3].

7.1.4 FORMAS DEL NOMBRE

El nombre del PCSC DOCUMENTA S.A., que consta el campo "Subject", deberá adoptar el "Distinguished Name" (DN) del estándar ITU X.500/ISO 9594 de la siguiente forma:

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

b) **OID=2.5.4.10 O= [***denominación o razón social de la persona jurídica habilitada como PCSC en mayúsculas y sin tildes, según documento de identificación***]**;

c) **OID: 2.5.4.3** **CN= [***siglas* **CA-** *seguido de la denominación o razón social de la persona jurídica habilitada como PCSC en mayúsculas y sin tildes, según documento de identificación***]**; y

d) **OID: 2.5.4.5** **Serial Number [** *conforme al formato descripto en el ítem 3.1.4.1 de este documento***]**.

7.1.5 RESTRICCIONES DEL NOMBRE

Conforme con cada PC implementada, adoptando las restricciones establecidas por la ICPP en el documento DOC-ICPP-04 [1].

7.1.6 IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO

Conforme a lo estipulado en los ítems 1.2 y 1.4.1.

Todo certificado emitido bajo esta DPC 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.

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

Dirección Web (URL) de la PC y de la DPC aplicables: https://www.digito.com.py/descargas

Los certificados emitidos 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)

Las extensiones críticas deben interpretarse de acuerdo con RFC 5280.

7.2 PERFIL DE LA LCR

Los Listas de Certificados Revocados LCR deberán ser firmados utilizando el algoritmo definido en el documento DOC-ICPP-06 [3] y cumplen con el RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" y contienen los elementos básicos especificados en el siguiente cuadro:

Campo	Valor o restricciones
Versión (Version)	X.509 versión 2 (v2).

Algoritmo de firma (Signature Algorithm)	Algoritmo usado para la firma del LCR. Como mínimo es SHA256With RSAEncryption
Emisor (Issuer)	Entidad que emite y firma la LCR.
Fecha efectiva (Effective Date)	Fecha de emisión de la LCR.
Siguiente actualización (NextUpdate)	Fecha para la cual es emitida la siguiente LCR. La frecuencia de emisión del LCR está acorde con lo requerido en la sección 4.9.7
Certificados revocados (Certificate Revoked)	Lista de certificados revocados, incluyendo el número de serie del certificado revocado y la fecha de revocación.
Extensiones	
Número CRL (CRL Number)	Orden secuencial de emisión de LCR
Identificador de clave de Autoridad (Authority Key Identifier)	Identificador de la clave pública de AC que emite.
Punto de distribución del CRL (Distribuition Points)	Este Campo es usado para indicar las direcciones donde puede ser encontrado el LCR correspondientes a la AC que emitió el certificado

7.2.1 NÚMERO (S) DE VERSIÓN

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

7.2.2 LCR Y EXTENSIONES DE ENTRADAS DE LCR

De acuerdo a lo establecido en el ítem 7.2.

7.3 PERFIL DE OCSP

Las Respuestas OCSP deberán ser firmados utilizando el algoritmo definido en el documento DOC-ICPP-06 [3].

7.3.1 NÚMERO (S) DE VERSIÓN

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

7.3.2 EXTENSIONES DE OCSP

Si se implementa, debe cumplir con RFC 6960.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

El Art. 42 de la Ley Nro. 4017/2010 establece que los PCSC, deben ser auditados periódicamente, de acuerdo con el sistema de auditoría que diseñe y apruebe el MIC.

Por Resolución Ministerial se establece el sistema de auditoría al cual será sometido el PCSC.

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

El proceso de auditoría incluye entre otras: Revisión de seguridad y de prácticas, las cuales incluyen instalaciones, documentos de seguridad, declaración de prácticas de certificación, acuerdos entre las partes, política de privacidad y validación de los planes para asegurar el cumplimiento de estándares.

El MIC o terceros designados por él, serán responsables de ejecutar las auditorías, de acuerdo a lo estipulado en la normativa vigente.

Cada PCSC, debe implementar un programa de auditorías internas conforme a lo estipulado en el sistema de auditoría que diseñe el MIC y lo establecido en el ítem 18 “cumplimiento” de la norma ISO 27002/2013 para la verificación de su sistema de gestión.

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

8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

La auditoría externa al PCSC DOCUMENTA S.A. se deberá ejecutar al menos una vez al año y los costos deben ser asumidos por el PCSC.

Además, DOCUMENTA S.A. realizará auditoría interna, como mínimo, una vez al año.

8.2 IDENTIDAD/CALIDAD DEL EVALUADOR

Todo equipo o persona designada para realizar una auditoría de seguridad sobre la ICP de DOCUMENTA S.A. deberá contar con adecuada capacitación y experiencia en:

- Tecnología de ICP y criptografía
- Tecnología de la información y seguridad.

8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA

Para el caso de las auditorías externas, los auditores deberán ser independientes e imparciales y que deberán ejecutar las evaluaciones acordes a los procedimientos establecidos.

Para el caso de las auditorías internas, los auditores deberán ser independientes funcionalmente del área objeto de evaluación.

8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN

Los aspectos cubiertos por la evaluación incluirán, como mínimo:

a) controles de seguridad física y estándares técnicos de seguridad;
b) confidencialidad y calidad de los sistemas de control;
c) integridad y disponibilidad de los datos;
d) cumplimiento de los estándares tecnológicos;
e) seguridad del personal;
f) cumplimiento de la política y declaración de prácticas de certificación;
g) procesos de certificación de clave pública;
h) política de seguridad y privacidad;
i) controles administrativos del PCSC;
j) administración de los servicios del PCSC; y
k) revisión de contratos.

8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA

En caso de detectarse una irregularidad en la Auditoría externa realizada al PCSC, podrán tomarse entre otras las siguientes acciones dependiendo de la gravedad de la misma:

l) indicar las irregularidades, pero permitir al PCSC responsable o a las VA y AR vinculadas que continúen sus operaciones hasta la próxima auditoría programada;
m) permitir al PCSC responsable o a las VA y AR vinculadas que continúen sus operaciones con un máximo de treinta días corridos, tiempo durante el cual deberá subsanar la irregularidad detectada;
n) recomendar suspender la operación del PCSC responsable o a las VA y AR vinculadas.

En caso de que se resuelva la suspensión de actividades del PCSC, este sólo podrá realizar servicios de soporte técnico y atención a los titulares de certificados ya existentes, en ningún caso podrá seguir brindando servicios de certificación.

8.6 COMUNICACIÓN DE RESULTADOS

El PCSC DOCUMENTA S.A. publica en su sitio principal de Internet los informes relevantes de las auditorías realizadas.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 TARIFAS

9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

Las políticas tarifarias y reembolso aplicables a la materia se especifican en la Política de Certificación que le sea de aplicación.

9.1.2 TARIFAS DE ACCESO A CERTIFICADOS

Este ítem no aplica.

9.1.3 TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN

No hay tarifa de revocación ni de acceso a la información del estado del certificado.

9.1.4 TARIFAS POR OTROS SERVICIOS

Este ítem no aplica.

9.1.5 POLÍTICAS DE REEMBOLSO

En el caso de que alguna Política de Certificación especifique alguna tarifa aplicable a la prestación de servicios de certificación por parte del PCSC DOCUMENTA S.A. para el tipo de certificados que emita, será obligado determinar la política de reembolso correspondiente.

9.2 RESPONSABILIDAD FINANCIERA

9.2.1 COBERTURA DE SEGURO

DOCUMENTA S.A. cuenta con un medio de garantía suficiente para cubrir las actividades inherentes a su gestión de conformidad con lo establecido en la normativa vigente.

9.2.2 OTROS ACTIVOS

Este ítem no aplica.

9.2.3 COBERTURA DE SEGURO O GARANTÍA PARA USUARIOS FINALES

En el caso que sean aplicadas cobertura de seguro o garantía para usuarios finales, serán especificadas en cada PC implementada correspondiente.

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

Se declara expresamente como información confidencial y no podrá ser divulgada a terceros, excepto en los casos en que la normativa exija lo contrario:

- Las claves privadas PCSC DOUMENTA S.A.
- La información referida a los parámetros de seguridad, control y procedimientos de auditoría.
- Documentaciones que guardan relación los dossiers de titulares de certificados generados por el PCSC.
- Planes de contingencia y recuperación de desastres.

- Información o documentos que la AC Raíz haya determinado como confidencial.
- Registros de Auditoría.
- Los planes de negocio y estados financieros de los suscriptores.

Se debe asegurar la reserva de toda información que mantiene la CA, que pudiera perjudicar la normal realización de las operaciones.

9.3.2 INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL

Los tipos de informaciones consideradas NO confidenciales por el PCSC DOCUMENTA S.A. de la DPC y por las AR y VA a ellas vinculadas, comprenden, entre otros:

a) los certificados y las LCR emitidas por la CA;
b) las PC implementadas por el PCSC;
c) la DPC del PCSC; y
d) la conclusión de los informes de auditoría.

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

9.3.3 RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

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

La clave privada de firma digital del PCSC DOCUMENTA S.A. fue generada y mantenida por la propia CA, que será responsable de mantener su confidencialidad.

Los titulares de certificados emitidos para personas físicas o sus responsables para el uso de los certificados emitidos para personas jurídicas, equipos o aplicaciones, tendrán las atribuciones de generación, y confidencialidad de sus respectivas claves privadas.

En el caso de certificados de cifrado emitidos por el PCSC, el PCSC podrá custodiar las claves privadas y será responsable de mantener y garantizar la confidencialidad de las mismas.

Si existen responsabilidades específicas para las DPC implementadas, las mismas deben ser descriptas en esas DPC, en el ítem correspondiente.

9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL

9.4.1 PLAN DE PRIVACIDAD

El PCSC DOCUMENTA S.A. y las AR vinculadas implementan Políticas de Privacidad para garantizar la protección de los datos personales. Dicha política contemplar aspectos y procedimientos de seguridad organizativos con el fin de garantizar que los datos personales a los que tenga acceso son protegidos ante su pérdida, destrucción, daño y procesamiento no autorizado.

9.4.2 INFORMACIÓN TRATADA COMO PRIVADA

Cualquier información acerca de los suscriptores que no esté públicamente disponible a través del contenido del certificado emitido y servicios de LCR/OCSP son tratadas como información privada.

9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

En este ítem de la DPC se debe de indicar que el tratamiento de la información que no es considerada como privada, estará sujeto a lo que dispone la normativa al efecto. Únicamente se considera pública la información contenida en el certificado y LCRs/OCSP.

9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

El PCSC DOCUMENTA S.A. y las AR vinculadas son responsables de la divulgación indebida de información privada, por lo que deben de asegurar que no pueda ser comprometida o divulgada a terceros.

9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

La información privada obtenida por el PCSC DOCUMENTA S.A. podrá ser utilizada o divulgada a terceros, previa notificación al titular y con su autorización expresa.

El titular del certificado o su representante en el caso de un certificado de persona jurídica tendrán amplio acceso a cualquiera de sus propios datos e identificaciones, y podrán autorizar la divulgación de sus registros a otras personas.

La autorización formal se podrá formalizar:

a) por medios electrónicos, conteniendo una firma válida garantizada por un certificado reconocido por la ICPP; o
b) mediante solicitud por escrito firmada.

9.4.6 DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO

La información privada solamente podrá divulgarse en el marco de un procedimiento judicial o administrativo cuya solicitud emane de una orden judicial o autoridad administrativa competente.

9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

Este ítem no aplica.

9.4.8 INFORMACIÓN A TERCEROS

Aplicase lo dispuesto en el ítem 9.4.5 de la DPC.

9.5 DERECHO DE PROPIEDAD INTELECTUAL

Según legislación vigente.

9.6 REPRESENTACIONES Y GARANTÍAS

9.6.1 REPRESENTACIONES Y GARANTÍAS DEL PCSC

El PCSC DOCUMENTA S.A., en el marco de prestación de servicios de certificación, responderá por el incumplimiento de lo establecido en las Políticas, Declaración de Prácticas de certificación y en la normativa vigente. De igual manera asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de certificación.

9.6.1.1 AUTORIZACIÓN PARA CERTIFICADO

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

9.6.1.2 PRECISIÓN DE LA INFORMACIÓN

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

9.6.1.3 IDENTIFICACIÓN DEL SOLICITANTE

El PCSC DOCUMENTA S.A. implementa procedimientos para verificar la identificación de los solicitantes de certificados, contenidos en los ítems 3 y 4 de esta DPC. El PCSC, en el ámbito de la identificación del solicitante contenido en los certificados que emite, analiza, audita e inspecciona los procesos de la AR conforme sus DPC, DPC y normas complementarias.

9.6.1.4 CONSENTIMIENTO DE LOS TITULARES

El PCSC DOCUMENTA S.A. implementa el formulario de Solicitud y Contrato de Prestación de Servicios de Confianza para la expresión del consentimiento del titular de conformidad a los formatos de Solicitud y Contrato de Prestación de Servicios de Confianza establecidos por la AC Raíz, contenidos en los puntos 3 y 4 de esta DPC.

9.6.1.5 SERVICIO

El PCSC DOCUMENTA S.A. mantiene acceso 24x7 a su repositorio con información sobre sus propios certificados, consulta de certificados emitidos y LCR/OCSP.

9.6.1.6 REVOCACIÓN

El PCSC DOCUMENTA S.A. revocará los certificados de la ICP- Paraguay por cualquier motivo especificado en este documento.

9.6.1.7 EXISTENCIA LEGAL

La presente DPC se ajusta a las disposiciones de la Ley Nro. 4017/2010 sus modificaciones y reglamentaciones.

9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA RA

Aplicase conforme al ítem 4 de esta DPC.

9.6.3 REPRESENTACIONES Y GARANTÍAS DEL SUSCRIPTOR

Toda la información necesaria para la identificación del titular del certificado debe proporcionarse de manera completa y precisa. Al aceptar un certificado emitido por el PCSC, el titular es responsable de toda la información proporcionada por él, contenida en ese certificado.

El PCSC debe informar a la AC Raíz-Py de cualquier compromiso de su clave privada y solicitar la revocación inmediata de su certificado.

9.6.4 REPRESENTACIONES Y GARANTÍAS DE LAS PARTES QUE CONFÍAN

La parte usuaria; es aquel que confía en el contenido, validez y aplicabilidad del certificado electrónico.

Constituyen derechos de la parte usuaria:

a) negarse a utilizar el certificado para fines distintos de los previstos en esta DPC;y
b) verificar, en cualquier momento, la vigencia del certificado.
c) El certificado del PCSC se considera válido cuando:
    - ha sido emitido por la AC Raíz-Py;
    - no aparece como revocado por la AC Raíz-Py;
    - no ha expirado; y
    - puede ser verificado utilizando el certificado válido de la AC Raíz-Py.

El uso o aceptación de certificados sin observar las medidas descriptas es por cuenta y riesgo de la parte usuaria, que usa o acepta la utilización del certificado respectivo.

9.6.5 REPRESENTACIONES Y GARANTÍAS DEL REPOSITORIO

El repositorio del PCSC DOCUMENTA:

a) disponibiliza, inmediatamente después de su emisión, los certificados emitidospor el PCSC y su LCR;
b) Se encuentra disponible para consulta durante 24 (veinticuatro) horas al día, siete (7) días a la semana; y
c) aplica los recursos necesarios para la seguridad de los datos almacenados enél.

9.6.6 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES

Este ítem no aplica.

9.7 EXENCIÓN DE GARANTÍA

Este ítem no aplica.

9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL

A excepción de lo establecido por las disposiciones de la presente DPC, en la Ley Nº 4017/2010, Ley Nº 4610/2014, su decreto reglamentario Nº 7369/2011, el PCSC DOCUMENTA S.A. no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros que confían.

9.9 INDEMNIZACIONES

El PCSC DOCUMENTA S.A. responderá ante el tribunal contencioso administrativo correspondiente por los daños y perjuicios que se cause al firmante, terceros o a cualquier persona, en el ejercicio de su actividad como prestador de servicios de certificación en los términos establecidos en la Ley Nº 4017/2010, Ley Nº 4610/2014, su decreto reglamentario N° 7369/2011 y la presente DPC. A tal efecto para el cálculo del monto de la indemnización se aplicarán las normas generales del procedimiento administrativo y responsabilidad contractual o extracontractual correspondientes.

9.10 PLAZO Y FINALIZACIÓN

9.10.1 PLAZO

La DPC 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 DPC permanecerá en vigencia indefinidamente, siendo válida y efectiva hasta que sea revocada o sustituida.

9.10.3 EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

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

9.11 NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las prácticas descritas en esta DPC se realizará mediante mensaje electrónico o por escrito mediante correo certificado dirigido a cualquiera de las direcciones contenidas en el punto 1.5 Administración de las Políticas. Las comunicaciones electrónicas producirán sus efectos una vez que las reciba el destinatario al que van

dirigidas.

9.12 ENMIENDAS

9.12.1 PROCEDIMIENTOS PARA ENMIENDAS

El procedimiento para enmiendas y que propuestas de modificación de la DPC son revisadas y aprobadas por la AA antes de ser implementadas. Las modificaciones se documentan y mantienen actualizados a través de versiones.

9.12.2 PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

Toda enmienda o modificación de la DPC, deberá ser publicada en el repositorio del PCSC DOCUMENTA S.A.

9.12.3 CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

Los cambios en los OIDs corresponden a nuevas políticas que contengan otros objetos con OID adicionales. Si la estructura del certificado se mantiene entonces no es necesario cambiar los OIDs.

9.13 DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

La DPC del PCSC DOCUMENTA S.A. no prevalecerá sobre las normas, criterios, prácticas y procedimientos establecidos por el MIC.

Todas reclamaciones entre usuarios y el PCSC DOCUMENTA S.A. deberán ser comunicadas por la parte en disputa a el PCSC DOCUMENTA S.A., con el fin de intentar resolverlo entre las mismas partes.

En el caso de que no se llegue a un acuerdo entre las partes, la resolución de cualquier conflicto que pudiera surgir se someterá a los juzgados y tribunales de la ciudad capital del República del Paraguay.

9.14 NORMATIVA APLICABLE

Esta DPC se rige por la legislación de la República del Paraguay, en particular la Ley Nro. 4017/2010, su modificación y reglamentaciones, y la legislación que la sustituya o modifique, así como las demás leyes y normas vigentes en el Paraguay.

9.15 ADECUACIÓN A LA LEY APLICABLE

La DPC se adecua a la legislación aplicable y el PCSC DOCUMENTAS.A. se compromete a cumplir y observar las disposiciones previstas en ella.

9.16 DISPOSICIONES VARIAS

9.16.1 ACUERDO COMPLETO

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

Esta DPC representa las obligaciones y deberes aplicables al PCSC y autoridades vinculadas.

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

9.16.2 ASIGNACIÓN

Los derechos y obligaciones previstos en esta DPC, no pueden ser cedidos ni transferidos a terceros.

9.16.3 DIVISIBILIDAD

La invalidez, nulidad o ineficacia de cualquiera de las disposiciones de esta DPC no perjudicará las demás disposiciones, que seguirán siendo plenamente válidas y efectivas.

9.16.4 APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DEDERECHOS)

Este ítem no aplica

9.16.5 FUERZA MAYOR

Los Acuerdos de Suscriptores incluyen cláusulas de fuerza mayor para proteger al PCSC DOCUMENTA S.A.

9.17 OTRAS DISPOSICIONES

Éste ítem no aplica.

10. DOCUMENTOS DE REFERENCIA

10.1 REFERENCIAS

- 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 Nº 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 Nº 4017/2010 "de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico".
- RFC 3647: "Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework".
- RFC 4210: "Internet X.509 Public Key Infrastructure. Certificate Management Protocol (CMP)".
- RFC 5280: "Internet X.509 Public Key Infrastructure. Certificate and CertificateRevocation List

(CRL) Profile".

- RFC 6712: "Internet X.509 Public Key Infrastructure. HTTP Transfer for the Certificate Management Protocol (CMP)".
- RFC 6960: "X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP".
- ISO/IEC27002:" -Information technology - Security techniques - Code of practice for information security management".
- ITU 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".
- WebTrust Principles and Criteria for Certification Authorities.
- WebTrustSM/TM Principles and Criteria for Registration Authorities.

10.2 REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	Directivas obligatorias para la formulación y elaboración de la política de certificación de los Prestadores Cualificados de Servicios de Confianza de la ICPP	DOC-ICPP-04
[2]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación del PCSC que genera o gestiona datos de creación de firma electrónica y/o de sello electrónico.	DOC-ICPP-07
[3]	Procedimiento de identificación del solicitante de certificados por videoconferencia en la ICPP	DOC-ICPP-17
[4]	Características mínimas de seguridad para las autoridades de registro de la ICPP.	DOC-ICPP-05
[5]	Normas de algoritmos criptográficos de la ICPP.	DOC-ICPP-06
[6]	Guía para la acreditación de los organismos de evaluación de la conformidad	DOC-ICPP-11
[7]	Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP	DOC-ICPP-12
[8]	Criterios y procedimientos para la inspección de los miembros de las entidades de la ICPP	DOC-ICPP-14
[9]	Directrices de la Política tarifaria de la AC Raíz-Py	DOC-ICPP-13