CONTROL DOCUMENTAL

DOCUMENTO	
Título: Declaración de Practicas de Certificación de la CA de Documenta S.A.	**Soporte lógico:** https://www.documenta.com.py/firmadigital/descargas
Fecha: 02/01/2017	**Ubicación física:** Documenta S.A.
Código: PKIpy-DocSA-CPSv2.0.0	
Versión: 2.0.0	

REGISTRO DE CAMBIOS		
Versión	**Fecha**	**Motivo del cambio**
2.0.0	02/01/2017	Modificación de la Normativa Vigente

DISTRIBUCION DEL DOCUMENTO	
Nombre	Área
CA de Documenta S. A	Todas las Áreas
RA de Documenta S. A	Todas las Áreas
Sede Administrativa Documenta S.A.	Todas las Áreas
DOCUMENTO PÚBLICO Y GRATUITO	

Preparado	**Revisado**	**Aprobado**	**Aceptado**
Javier Dávalos	Beltrán Ortiz	José Oricchio	José Minardi
Supervisor Firma Digital	Coordinador de Seguridad	Director Ejecutivo Documenta S. A	Presidente Documenta S.A.

Contenido

1. INTRODUCCION 10
1.1. Descripción General 10
1.2. Nombre e identificación del documento 11
1.3. Participantes de la PKI 11
1.3.1. Autoridades Certificadoras (CA) 12
1.3.2. Autoridades de Registro (RA) 12
1.3.3. Prestadores de Servicios de Soporte (PSS) 13
1.3.4 Suscriptores 13
1.3.5 Parte que confía 14
1.3.6 Otros Participantes 14
1.4. Uso del certificado 14
1.4.1 Usos apropiados del Certificado 14
1.4.2 Usos prohibidos del certificado 15
1.5. Administración de la Política 15
1.5.1 Organización que administra el documento 15
1.5.2 Persona de Contacto 15
1.5.3 Persona que determina la adecuación de la CPS a la Política 15
1.5.4 Procedimientos de aprobación de la CPS 15
1.6 Definiciones y acrónimos 15
1.6.1 Definiciones 15
1.6.2 Acrónimos 22
2. RESPONSABILIDADES DE PUBLICACION 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 25
3. IDENTIFICACION Y AUTENTICACION 26
3.1. Nombres 26
3.1.1. Tipos de Nombres 27
3.1.2. Necesidad de Nombres significativos 27
3.1.3. Anonimato o seudónimos de los suscriptores 27
3.1.4. Reglas para interpretación de varias formas de Nombres 27
3.1.5. Unicidad de nombres 28
3.1.6. Reconocimiento, autenticación y rol de las marcas registradas 28
3.2. Validación inicial de la 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 30
3.2.4. Autenticación de identidad de una máquina o aplicación 32
3.2.5. Información del suscriptor no verificada 33
3.2.6. Validación de la Autoridad (capacidad de hecho) 33
3.2.7. Criterios para interoperabilidad 33
3.3. Identificación y autenticación para solicitudes de re emisión de claves 34
3.3.1. Identificación y autenticación para re emisión de claves 34
3.3.2. Identificación y autenticación para la re emisión de claves después de una revocación 34
3.4. Identificación y autenticación para solicitudes de revocación 34
4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO 34
4.1. Solicitud de certificado 34
4.1.1 Quién puede presentar una solicitud de certificado 35
4.1.2. Proceso de inscripción y responsabilidades 35
4.2. Procesamiento de la Solicitud del Certificado 36
4.2.1. Ejecución de las funciones de identificación y autenticación 36
4.2.2. Aprobación o rechazo de Solicitudes de Certificados 36
4.2.3. Tiempo para procesar solicitudes de certificados 36
4.3. Emisión del certificado 36
4.3.1. Acciones del PSC durante la emisión de los certificados 36
4.3.2. Notificación al suscriptor sobre la emisión del certificado digital 37
4.4. Aceptación del certificado 37
4.4.1. Conducta constitutiva de aceptación del certificado 37
4.4.2. Publicación del certificado por el PSC 37
4.4.3. Notificación de la emisión del certificado por el PSC a otras entidades 37
4.5. Uso del par de claves y del certificado 37
4.5.1. Uso de la clave privada y del certificado por el suscriptor 37
4.5.2. Uso de la clave pública y del certificado por la parte que confía 38
4.6. Renovación del certificado 38
4.6.1. Circunstancias para renovación de certificados 38
4.6.2. Quién puede solicitar renovación 38
4.6.3. Procesamiento de solicitudes de renovación de certificado 38
4.6.4. Notificación al suscriptor sobre la emisión de un nuevo certificado 38
4.6.5. Conducta constitutiva de aceptación de un certificado renovado 38
4.6.6. Publicación por el PSC del certificado renovado 39
4.6.7. Notificación por el PSC de la emisión de un certificado a otras entidades 39
4.7. Re-emisión de claves de certificado 39
4.7.1. Circunstancias para re-emisión de claves de certificado 39
4.7.2. Quién puede solicitar la re-emisión claves 39
4.7.3. Procesamiento de solicitudes de re-emision de claves de certificado 39

4.7.4. Notificación al suscriptor sobre la re-emisión de un nuevo certificado 39
4.7.5. Conducta constitutiva de aceptación de un certificado re-emitido..... 39
4.7.6. Publicación por el PSC de los certificados re-emitidos 39
4.7.7. Notificación por el PSC de la re-emisión de un certificado a otras entidades 39
4.8. Modificación de certificados..... 39
4.8.1. Circunstancias para modificación del certificado..... 39
4.8.2. Quién puede solicitar modificación del certificado..... 39
4.8.3. Procesamiento de solicitudes de modificación del certificado 40
4.8.4. Notificación al suscriptor de la emisión de un nuevo certificado 40
4.8.5. Conducta constitutiva de aceptación del certificado modificado 40
4.8.6. Publicación por el PSC de los certificados modificados 40
4.8.7. Notificación por la CA de emisión de certificado a otras entidades..... 40
4.9. Revocación y suspensión..... 40
4.9.1. Circunstancias para la revocación 40
4.9.2. Quién puede solicitar revocación..... 41
4.9.3. Procedimiento para la solicitud de revocación 41
4.9.4. Periodo de gracia para solicitud de revocación 42
4.9.5. Tiempo dentro del cual el PSC debe procesar la solicitud de revocación 42
4.9.6. Requerimientos de verificación de revocación para las partes que confían 42
4.9.7. Frecuencia de emisión del CRL 43
4.9.8. Latencia máxima para CRL..... 43
4.9.9 Requisitos de verificación del CRL..... 43
4.9.10 Disponibilidad de verificación de revocación/estado en línea..... 43
4.9.11 Requerimientos para verificar la revocación en línea..... 44
4.9.12 Otras formas de advertencia de revocación disponibles 44
4.9.13 Requerimientos especiales por compromiso de clave privada 44
4.9.14 Cincunstancias para suspensión..... 44
4.9.15 Quién puede solicitar la suspensión 44
4.9.16 Procedimiento para la solicitud de suspensión 44
4.9.17 Límites del periodo de suspensión 44
4.10. Servicios de comprobación de estado de certificados..... 44
4.10.1. Características operacionales..... 44
4.10.2. Disponibilidad del servicio 45
4.10.3. Características opcionales 45
4.11. Fin de la suscripción 45
4.12. Custodia y recuperación de claves 45
4.12.1. Políticas y prácticas de custodia y recuperación de claves 45
4.12.2. Políticas y practicas de recuperación y encapsulación de claves de sesión..... 45
5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES 45

5.1. Controles físicos 46
5.1.1. Localización y construcción del sitio 46
5.1.2. Acceso físico 46
5.1.3. Energía y aire acondicionado 50
5.1.4. Exposición al agua 51
5.1.5. Prevención y protección contra fuego 52
5.1.6. Almacenamiento de medios 52
5.1.7. Eliminación de residuos 52
5.1.8. Respaldo fuera de sitio 52
5.1.9. Instalaciones técnicas de la RA 52
5.2. Controles procedimentales 53
5.2.1. Roles de confianza 53
5.2.2. Número de personas requeridas por tarea 55
5.2.3. Identificación y autenticación para cada rol 55
5.2.4. Roles que requieren separación de funciones 56
5.3. Controles de personal 56
5.3.1 Requerimientos de experiencia, capacidades y autorización 56
5.3.2 Procedimientos de verificación de antecedentes 57
5.3.3 Requerimientos de capacitación 57
5.3.4 Requerimientos y frecuencia de capacitación 57
5.3.5 Frecuencia y secuencia en la rotación de las funciones 57
5.3.6 Sanciones para acciones no autorizadas 58
5.3.7 Requisitos de contratación a terceros 58
5.3.8 Documentación suministrada al personal 58
5.4. Procedimiento de registro de auditoría 59
5.4.1 Tipos de eventos registrados 59
5.4.2 Frecuencia de procesamiento del registro (logs) 60
5.4.3 Periodo de conservación del registro (logs) de auditoría 61
5.4.4 Protección del registro (logs) de auditoría 61
5.4.5 Procedimientos de respaldo (backup) de registro (logs) de auditoría 61
5.4.6 Sistema de recolección de información de auditoría (interno vs externo) 61
5.4.7 Notificación al sujeto que causa el evento 61
5.4.8 Evaluación de vulnerabilidades 61
5.5. Archivos de registros 61
5.5.1. Tipos de registros archivados 61
5.5.2. Periodos de retención para archivos 62
5.5.3. Protección de archivos 62
5.5.4. Procedimientos de respaldo (backup) de archivo 62
5.5.5. Requerimientos para sellado de tiempo de registros 63

5.5.6. Sistema de recolección de archivo (interno o externo) 63
5.5.7. Procedimientos para obtener y verificar la información archivada 63
5.6. Cambio de clave 63
5.7. Recuperación de desastres y compromiso 65
5.7.1 Procedimiento para el manejo de incidente y compromiso 65
5.7.2 Corrupción de datos, software y/o recursos computacionales 65
5.7.3 Procedimientos de compromiso de clave privada de la Entidad 65
5.7.4 Capacidad de continuidad del negocio después de un desastre 66
5.7.5 Actividades de las Autoridades de Registro 66
5.8. Extinción de un PSC 67
6. CONTROLES TÉCNICOS DE SEGURIDAD 68
6.1. Generación e instalación del par de claves 68
6.1.1. Generación del par de claves 68
6.1.2. Entrega de la clave privada al suscriptor 68
6.1.3. Entrega de la clave pública al emisor del certificado 68
6.1.4. Entrega de la clave pública de la CA a las Partes que confían 69
6.1.5. Tamaño de la clave 69
6.1.6. Generación de parámetros de clave asimétricas y verificación de calidad 69
6.1.7. Propósitos de usos de clave (campo Key Usage X.509 v3) 69
6.1.8. Generación de clave por hardware o software 70
6.2. Controles de ingeniería del módulo criptográfico y protección de la clave privada 70
6.2.1 Estándares y controles del módulo criptográfico 70
6.2.2. Control multi-persona de clave privada 70
6.2.3. Custodia/recuperación de la clave privada 70
6.2.4. Respaldo/copia de la clave privada 71
6.2.5. Archivado de la clave privada 71
6.2.6. Transferencia de clave privada hacia o desde un módulo criptográfico 71
6.2.7. Almacenamiento de la clave privada en el módulo criptográfico 71
6.2.8. Método de activación de clave privada 72
6.2.9. Métodos de desactivación de la clave privada 72
6.2.10. Destrucción de clave privada 72
6.2.11. Clasificación del módulo criptográfico 72
6.3. Otros aspectos de gestión del par de claves 73
6.3.1. Archivo de la clave pública 73
6.3.2. Periodo operacional del certificado y periodo de uso del par de claves 73
6.4. Datos de activación 73
6.4.1 Generación e instalación de los datos de activación 73
6.4.2 Protección de los datos de activación 73
6.4.3 Otros aspectos de los datos de activación 73

6.5. Controles de seguridad del computador 73
6.5.1. Requerimientos técnicos de seguridad de computador específicos 74
6.5.2. Clasificación de la seguridad del computador 74
6.5.3. Controles de seguridad para las Autoridades de Registro 75
6.6. Controles técnicos del ciclo de vida 75
6.6.1. Controles para el desarrollo del sistema 75
6.6.2. Controles de gestión de seguridad 75
6.6.3. Controles de seguridad del ciclo de vida 75
6.6.4. Controles en la generación de CRL 76
6.7. Controles de seguridad de red 76
6.7.1 Directrices generales 76
6.7.2 Firewall 76
6.7.3 Sistema de Detección de Intruso (IDS) 77
6.7.4 Registro de acceso no autorizado a la red 77
6.8. Controles de ingeniería del modulo criptográfico. 77
7. PERFILES DE CERTIFICADOS, CRL Y OCSP 77
7.1. Perfil de certificado 77
7.1.1. Número de versión 79
7.1.2. Extensiones del certificado 79
7.1.3. Identificadores de objeto de algoritmos 79
7.1.4. Formas del nombre 79
7.1.5 Restricciones del nombre 80
7.1.6 Identificador de objeto de política de certificado 80
7.1.7 Uso de la extensión Restricciones de Política (Policy Constraints) 80
7.1.8 Semántica y sintaxis de los Calificadores de Política (Policy Qualifier) 80
7.1.9 Semántica de procesamiento para la extensión de Políticas de Certificado (Certificate Policies) 80
7.2. Perfil de la CRL 80
7.2.1. Número (s) de versión 81
7.2.2. CRL y extensiones de entradas de CRL 81
7.2.2.1 Número CRL (CRL number) 81
7.2.2.2 Identificador de clave de Autoridad 81
7.3. Perfil de OCSP 81
7.3.1. Número(s) de versión 81
7.3.2. Extensiones de OCSP 81
8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES 82
8.1. Frecuencia o circunstancias de evaluación 82
8.2. Identidad/calidades del evaluador 82
8.3. Relación del evaluador con la Entidad evaluada 82
8.4. Aspectos cubiertos por la evaluación 83

8.5. Acciones tomadas como resultado de una deficiencia 83
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 84
9.1.3. Tarifas de acceso a información del estado o revocación 84
9.1.4. Tarifas por otros servicios 84
9.1.5. Políticas de reembolso 84
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
9.4. 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 86
9.4.4. Responsabilidad para proteger información privada 86
9.4.5. Notificación y consentimiento para usar información privada 86
9.4.6. Divulgación de acuerdo con un proceso judicial o administrativo 87
9.4.7 Otras circunstancias de divulgación de información 87
9.5. Derecho de propiedad intelectual 87
9.6. Representaciones y garantías 87
9.6.1. Representaciones y garantías del PSC 87
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 90
9.6.5. Representaciones y garantías del Repositorio 91
9.6.6. Representaciones y garantías de otros participantes 91
9.7. Exención de garantía 91
9.8. Limitaciones de responsabilidad legal 92
9.9. Indemnizaciones 92
9.9.1. Indemnizaciones por daños ocasionados por la CA de DOCUMENTA S.A. 93
9.9.2. Indemnizaciones por los daños ocasionados por los Suscriptores 93
9.9.3. Indemnizaciones por los daños ocasionados por los Terceros que confían 93
9.10. Plazo y finalización 93

9.10.1. Plazo 93
9.10.2. Finalización 93
9.10.3. Efectos de la finalización y supervivencia 94
9.11. Notificación individual y comunicaciones con participantes 94
9.12. Enmiendas 94
9.12.1. Procedimientos para enmiendas 94
9.12.2. Procedimiento para publicación y notificación 94
9.12.3. Circunstancias en que los OID deben ser cambiados 94
9.13. Disposiciones para resolución de disputas 94
9.14. Normativa aplicable 95
9.15. Adecuación a la ley aplicable 95
9.16. Disposiciones varias 95
9.16.1. Acuerdo completo 95
9.16.2. Asignación 95
9.16.3. Divisibilidad 95
9.16.4. Aplicación (Honorarios de abogados y renuncia de derechos) 95
9.16.5. Fuerza mayor 95
9.16.6. Resolución por la vía judicial 95
9.17. Otras disposiciones 95
10. DOCUMENTOS DE REFERENCIA 95

1. INTRODUCCION

1.1. Descripción General

La expedición de certificados electrónicos a entidades que deseen actuar como Autoridades de Certificación subordinadas o Prestadoras de Servicios de Certificación emitiendo certificados digitales bajo la jerarquía del Certificado de la Autoridad Certificadora Raíz del Paraguay (CA del Paraguay), requerirá de una habilitación del Ministerio de Industria y Comercio (MIC), como autoridad de aplicación (AA) de Ley N° 4017/2010 su Decreto Reglamentario Nº 7.369/2011 y la Ley N° 4610/2012.

Dichas normativas establecen la validez jurídica de la Firma Electrónica, la Firma Digital, los mensajes de datos y el expediente electrónico y regula la utilización de estas herramientas, así como el funcionamiento de las Prestadoras de Servicios de Certificación, sus requisitos y obligaciones.

El Ministerio de Industria y Comercio como ente regulador debe:

- Administrar la Autoridad Certificación Raíz del Paraguay.
- Dictar las normas que regulen el Servicio de Certificación Digital en el País.
- Habilitar a los Prestadores de Servicios de Certificación.
- Auditar a los Prestadores de Servicios de Certificación.
- Revocar la habilitación de los Prestadores de Servicios de Certificación.
- Imponer sanciones a los Prestadores de Servicio de Certificación.

El Ministerio de Industria y Comercio tiene entre sus cometidos la administración de la Autoridad Certificadora Raíz del Paraguay. Dicha Autoridad Certificadora es la raíz de toda la Jerarquía de PKI, cuenta con un certificado autoafirmado y aceptado por los terceros que establezcan confianza en la PKI del Paraguay.

El Ministerio de Industria y Comercio como AA de la normativa vigente habilita la operación de los Prestadores de Servicios de Certificación (PSC) en la República del Paraguay, de esta manera los PSC habilitados pasan a ser parte de la cadena de confianza de la Infraestructura de Clave Pública del Paraguay.

Este documento recoge la **Declaración de Prácticas de Certificación (CPS por sus siglas en ingles) de DOCUMENTA S.A.**, que estipula el funcionamiento y operaciones como Prestador de Servicios de Certificación (PSC) dentro de la PKI del Paraguay.

La presente CPS se ha estructurado teniendo en cuenta las recomendaciones de la (Request for comments) RFC 3647 "Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework", de IETF. Con el propósito de facilitar la lectura y análisis del documento se incluyen todas las secciones establecidas en dicha RFC apareciendo la frase "No estipulado" en las secciones para las que no se haya previsto nada.

Todos los certificados que se emite dentro de la PKI del Paraguay son conformes con la versión 3 del estándar X.509, permitiendo la inclusión de extensiones para certificación de atributos.

Esta CPS es específicamente aplicable a:

- Prestador de Servicios de Certificación (PSC).
- Usuario Final.
- Parte que confía.

1.2. Nombre e identificación del documento

Nombre del documento	**Declaración de Prácticas de Certificación de DOCUMENTA S.A.**
Versión del documento	**2.0.0**
Estado del documento	**Versión inicial**
Fecha de emisión	**02/01/2017**
Fecha de expiración	**No aplicable**
OID (Object Identifier)	**1.3.6.1.4.1.48315.1.1.2.2**
Ubicación de la CPS	https://www.documenta.com.py/firmadigital/descargas/cpsv2.pdf

1.3. Participantes de la PKI

Las entidades y personas intervinientes en la PKI son las que se enumeran a continuación:

1. Autoridades de Certificación (CA).
2. Autoridades de Registro (RA).
3. Prestadores de Servicio de Soporte (PSS).
4. Suscriptores.
5. Terceros que confían en los certificados de la PKI del Paraguay.

6. Otros Participantes.

1.3.1. Autoridades Certificadoras (CA)

Son las personas, políticas, procedimientos y sistemas informáticos encargados de la emisión de certificados digitales 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 PKI Paraguay se denominan:

- **Autoridad Certificadora Raíz del Paraguay (CA Raíz):** emite certificados a los PSC 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 PSC.

  En el Paraguay, la cadena de certificación tiene como máximo dos niveles, en el primer nivel se encuentra la CA Raíz, en el segundo nivel, uno o varios PSC, éstos solo podrán emitir certificados digitales a usuarios finales. Se constituye como CA Raíz del Paraguay el MIC.
- **Prestador de Servicios de Certificación (PSC):** es la persona jurídica que emite certificados digitales a los usuarios finales.

  El PSC DOCUMENTA S.A, una vez habilitado, pasó a ser parte de la cadena de confianza de la PKI Paraguay, y cuenta con un certificado digital firmado y emitido por la CA Raíz, generando de esta manera una estructura jerárquica.

1.3.2. Autoridades de Registro (RA)

Son las personas, políticas, procedimientos y sistemas informáticos encargados de la verificación de la identidad de los solicitantes de certificados digitales y si procede, de los atributos asociados a los mismos.

Las Autoridades de Registro (RA) llevarán a cabo la identificación de los solicitantes de certificados conforme a las normas de esta CP y el acuerdo suscrito con la CA.

DOCUMENTA S.A. cumple funciones de RA. Además, podrá mediante un contrato de prestación de servicio establecer Autoridades de Registros Delegadas siempre y cuando las mismas estén autorizadas por la CA Raíz, en todo el territorio de la república, cumpliendo las normas y procedimientos establecidos

en el documento "Características Mínimas de Seguridad para las Autoridades de Registro de la Infraestructura de Claves Publicas del Paraguay" y la normativa vigente, previa comunicación y autorización de la AA. Siempre bajo el control y supervisión de DOCUMENTA S.A.

Los datos referentes a las RA habilitadas por DOCUMENTA S.A. se encuentran en la dirección de página web (URL) https://www.documenta.com.py/firmadigital/ra

La CA de DOCUMENTA S.A. mantiene publicada en el sitio las siguientes informaciones actualizadas:

- Identificación y vinculación de todas las RA habilitadas, con informaciones sobre las CP que implementan,
- Para cada RA habilitada, las direcciones de sus instalaciones técnicas, cuyo funcionamiento haya sido autorizado por la CA Raíz.
- Para cada RA habilitada, el tipo de vínculo con eventuales locales provisorios autorizados por la CA Raíz, con fecha de creación y cierre de actividades;
- Identificación y vínculo de las RA deshabilitadas dentro de la cadena PKI Paraguay, con su respectiva fecha de cese de actividades;
- Instalaciones técnicas de la RA habilitada que ha dejado de operar, con su respectiva fecha de cierre de actividades;
- Acuerdos operacionales celebrados entre las RA vinculadas con otra RA dentro de la PKI Paraguay, si fuera el caso.

1.3.3. Prestadores de Servicios de Soporte (PSS)

PSS son entidades externas a las que recurre DOCUMENTA S.A. para desempeñar actividades descritas en esta CP o en la CPS y se clasifican en dos categorías, conforme al tipo de servicio prestado.

- Disponibilización de infraestructura física y lógica;
- Disponibilización de recursos humanos especializados;

Las informaciones actualizadas de las PSS habilitadas por DOCUMENTA S.A. se encuentran en la dirección de página web (URL) https://www.documenta.com.py/firmadigital/pss

1.3.4 Suscriptores

Se definen como aquellas personas físicas o jurídicas sujetos de

derechos, con capacidad suficiente para obtener un certificado digital de la CA de DOCUMENTA S.A. a título propio o en su condición de representante de una persona jurídica.

A los efectos anteriores tendrán la consideración de suscriptores toda persona física o jurídica a quien se emite un certificado digital, dentro de la jerarquía PKI Paraguay.

1.3.5 Parte que confía

En el ámbito de esta CP, las partes que confían son las personas o entidades diferentes del titular que deciden aceptar y confiar en los certificados emitidos por DOCUMENTA S.A. dentro de la jerarquía PKI Paraguay.

Una parte que confía puede o no ser un suscriptor.

1.3.6 Otros Participantes

No estipulado

1.4. Uso del certificado

1.4.1 Usos apropiados del Certificado

Las Políticas de Certificación de 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 se describen los usos apropiados del Certificado de la CA raíz y del PSC DOCUMENTA S.A:

TIPO	DESCRIPCIÓN DE USO APROPIADO
Certificado de CA Raíz	Firma de Certificado a PSC. Firma de CRL de PSC. • Firma de Certificado (Certificate Signing). • Firma CRL sin conexión (Off line CRL Signing).
Certificado de la CA de Documenta S.A.	Firma de Certificado a sus suscriptores. Firma de CRL de sus suscriptores. • Firma de Certificado (Certificate Signing). • Firma de CRL (CRL Signing).

1.4.2 Usos prohibidos del certificado

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

1.5. Administración de la Política

1.5.1 Organización que administra el documento

Nombre	DOCUMENTA S.A.
Dirección	Avda. General Máximo Santos N°698 Asunción – Paraguay
Código Postal	1535
Correo electrónico	firmadigital@documenta.com.py
Página Web	www.documenta.com.py

1.5.2 Persona de Contacto

Nombre	GERENTE GENERAL DE DOCUMENTA S.A.
Dirección	Avda. General Máximo Santos N°698 Asunción – Paraguay
Código Postal	1535
Teléfono	+59521492503/3
Correo electrónico	firmadigital@documenta.com.py

1.5.3 Persona que determina la adecuación de la CPS a la Política

El Director General de Firma Digital y Comercio Electrónico del MIC, será el encargado de determinar la adecuación de la CPS de DOCUMENTA S.A.

1.5.4 Procedimientos de aprobación de la CPS

El MIC aprobará el contenido de la Declaración de Practicas de Certificación de DOCUMENTA S.A. y sus posteriores enmiendas o modificaciones.

1.6 Definiciones y acrónimos

1.6.1 Definiciones

Acuerdo de Suscriptores: Es un acuerdo entre la CA Raíz y el PSC, y entre el PSC y el usuario final, que establece los derechos y responsabilidades de las partes con respecto a la emisión y gestión de los certificados. Éste acuerdo, requiere la aceptación explícita tanto del PSC, como del suscriptor, respectivamente.

Agente de Registro: Persona responsable de la ejecución de actividades relacionadas con la RA, que realiza la validación y verificación de la solicitud de certificado.

Armario ignífugo: Armario equipado con sistemas de protección contra el fuego para aislar los productos almacenados en su interior.

Autenticación: Proceso técnico que permite determinar la identidad de la persona que firma electrónicamente, en función del mensaje firmado por éste, y al cual se le vincula. Éste proceso no otorga certificación notarial ni fe pública.

Autoridad de Aplicación (AA): Ministerio de Industria y Comercio a través de la Dirección General de Firma Digital y Comercio Electrónico, dependiente del Viceministerio de Comercio. Órgano Regulador competente designado por Ley, establecido por el artículo 38 de la Ley 4610/2012 que modifica y amplía la Ley N° 4017/2010 “De validez jurídica de la Firma Electrónica, Firma Digital, los Mensajes de Datos y el Expediente Electrónico”.

Autoridad Certificadora (CA): Entidad que presta servicios de emisión, gestión, revocación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de una RA y VA. En el marco de la PKI Paraguay, son Autoridades Certificadoras, la CA Raíz del Paraguay y el PSC.

Autoridad Certificadora Raíz (CA Raíz): Es la Autoridad de Certificación Raíz de la PKI Paraguay, cuya función principal es habilitar al PSC y emitirle certificados digitales. Posee un certificado auto firmado y es a partir de allí, donde comienza la cadena de confianza.

Autoridad de Certificación Intermedia (CAI): Entidad cuyo certificado de clave pública ha sido firmado digitalmente por la autoridad de certificación raíz; es responsable de la emisión de certificados a usuarios finales.

Autoridad de Registro (RA): Entidad responsable de la identificación y autenticación de titulares de certificados digitales, la misma no emite ni firma certificados. Una RA puede ayudar en el proceso de solicitud del certificado, en el proceso de revocación o en ambos. La RA, no necesita ser un organismo separado, sino

que puede ser parte de la CA.

Autoridad de Validación (VA): Entidad responsable de suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una autoridad de registro y certificados por la autoridad de certificación. La VA, no necesita ser un organismo separado, sino que puede ser parte de la CA.

Cadena de certificación: Lista ordenada de certificados que contiene un certificado de usuario final y certificados de CA, que termina en un certificado raíz. El emisor del certificado del usuario final es el titular del certificado de CA y a su vez, el emisor del certificado de CA es el titular del certificado de CA Raíz. El usuario final o la parte que confía, debe verificar la validez de los certificados en la cadena.

Ceremonia de claves: Procedimiento mediante el cual es generado un par de claves de CA, su clave privada es generada y almacenada en un módulo criptográfico, y debe ser respaldada con el mismo nivel de seguridad que la clave original. Este procedimiento debe ser documentado.

Certificado Digital (CD): Es un documento electrónico, generado y firmado por una CA legalmente habilitada para el efecto, el cual vincula un par de claves con una persona física o jurídica confirmando su identidad.

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

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

Claves criptográficas: Valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.

Clave pública y privada: La criptografía en la que se basa la PKI Paraguay, es la criptografía asimétrica. En ella se emplea un par de claves: lo que se cifra con una de ellas, sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y está incorporada en el certificado digital, mientras que a la otra se le denomina privada y está bajo la custodia del titular del certificado.

Cofre de seguridad: Compartimiento para almacenar materiales o documentos sensibles de la CA, debe ser resistente al fuego y

ofrecer protección a aperturas forzadas.

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

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

Datos de activación: Valores de los datos, distintos a las claves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos.

Declaración de Prácticas de Certificación (CPS): Declaración de las prácticas que emplea una CA al emitir certificados y que define la infraestructura, políticas y procedimientos que utiliza la CA para satisfacer los requisitos especificados en la CP vigente.

Delta CRL: Partición del CRL, dentro de una unidad de tiempo, que contiene los cambios realizados al CRL base desde su última actualización.

Emisión: Comprende la generación de los Certificados, cuyo proceso, es una función de la CA.

Emisor del certificado: Organización cuyo nombre aparece en el campo emisor de un certificado.

Encriptación: Proceso para convertir la información a un formato más seguro. Se convierte mediante un proceso matemático a un formato codificado, es decir ininteligible.

Estándares Técnicos Internacionales: Requisitos de orden técnico y de uso internacional que deben observarse en la emisión de firmas electrónicas y en las prácticas de certificación.

Firma Digital: Es una firma electrónica certificada por un prestador habilitado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincula únicamente al mismo y a los datos a lo que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.

Grupo Electrógeno: 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.

Habilitación: Autorización que otorga el MIC al PSC para emitir certificados digitales a usuarios finales, una vez cumplidos los requisitos y condiciones establecidos en la norma.

Huella digital (Código de verificación o resumen): Secuencia de bits de longitud fija obtenida como resultado de procesar un mensaje de datos con un algoritmo, de tal manera que: (1) el mensaje de datos produzca siempre el mismo código de verificación cada vez que se le aplique dicho algoritmo (2) sea improbable, a través de medios técnicos, que el mensaje de datos pueda ser derivado o reconstruido a partir del código de verificación producido por el algoritmo (3) sea improbable, por medios técnicos, se pueda encontrar dos mensajes de datos que produzcan el mismo código de verificación al usar el mismo algoritmo.

Identificación: Procedimiento de reconocimiento de la identidad de un solicitante o titular de certificado dentro de la jerarquía PKI Paraguay.

Identificador de Objeto (OID): Serie única de números enteros, que identifica inequívocamente un objeto de información.

Infraestructura de Clave Pública (PKI): Es un conjunto de personas, políticas, procedimientos y sistemas informáticos necesarios para proporcionar servicios de autenticación, integridad y no repudio, mediante el uso de criptografía de claves públicas y privadas y de certificados digitales, así como la publicación de información, consultas de vigencia y validez de los mismos.

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.

Jerarquía PKI: Jerarquía de confianza que se conforma por un conjunto de autoridades de certificación que mantienen relaciones de confianza por las cuales una CA de nivel superior

(CA Raíz) garantiza la confiabilidad de una o varias de nivel inferior (PSC) y a su vez, de los certificados emitidos por éstos a los suscriptores.

Lista de certificados revocados (CRL): Lista emitida por una CA, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.

Módulo criptográfico: Software o Hardware criptográfico que genera y almacenas claves criptográficas.

Módulo de Seguridad de Hardware (HSM, Hardware Security Module): Dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas.

No Repudio: Refiere que la posesión de un documento electrónico y la firma digital asociada al mismo, será prueba efectiva del contenido y del autor del documento.

Par de claves: Son las claves privada y pública de un cripto sistema asimétrico. La clave privada y la clave pública están relacionadas matemáticamente y poseen ciertas propiedades, entre ellas que es imposible deducir la clave privada de la clave pública conocida.

PKCS#1: Estándar de criptografía de clave pública #1, desarrollado por RSA Security Inc., que proporciona las definiciones básicas y recomendaciones para la implementación de algoritmo RSA para criptografía de clave pública.

PKCS#10 (Certification Request Syntax Standard): Estándar desarrollado por RSA que define la sintaxis de una petición de certificado.

Parte que confía: Es toda persona física o jurídica diferente del titular, que decide aceptar y confiar en un certificado emitido bajo la jerarquía de la PKI Paraguay.

Perfil del certificado: Especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).

Periodo de operación: Periodo de vigencia de un certificado, que comienza en la fecha y la hora en que es emitido por una CA, y termina en la fecha y la hora en que expira o se revoca el mismo.

Periodo de uso: Refiere al tiempo establecido para los certificados emitidos dentro la jerarquía de la PKI para determinados usos.

Política: Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

Política de Certificación (CP): Documento en el cual la CA, define

el conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad particular y/o una clase de aplicaciones con requisitos comunes de seguridad.

Práctica: Modo o método que particularmente observa alguien en sus operaciones.

Prestador de Servicios de Certificación (PSC): Entidad habilitada ante la AA, encargada de operar una CA en el marco de la PKI Paraguay. El PSC debe contar con un certificado digital emitido por la CA Raíz del Paraguay y solo podrá emitir certificados a usuarios finales.

Registro de Auditoría: Registro cronológico de las actividades del sistema, el cual es suficiente para permitir la reconstrucción, revisión e inspección de la secuencia de los ambientes y de las actividades que rodean o que conducen a cada acontecimiento en la ruta de una transacción desde su inicio hasta la salida de los resultados finales.

Repositorio: Sitio principal de internet confiable y accesible, mantenido por la CA con el fin de difundir su información pública.

Rol de confianza: Función crítica que desempeña personal de la CA, que si se realiza insatisfactoriamente puede tener un impacto adverso sobre el grado de confianza proporcionado por la CA.

Ruta del certificado: Secuencia ordenada de certificados de entidades que, junto a la clave pública de la entidad inicial en la ruta, puede ser procesada para obtener la clave pública de la entidad final en la ruta.

Servicio OCSP: Permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la CA sobre el estado de un certificado.

Solicitante de Certificado: Persona física o jurídica que solicita la emisión de un certificado a una CA.

Solicitud de Firma de Certificado (CSR): Es una petición de certificado digital que se envía a la CA. Mediante la información contendida en el CSR, la CA, puede emitir el certificado digital una vez realizadas las comprobaciones que correspondan.

Suscriptor: Persona física o jurídica titular de un certificado digital emitido por una CA.

Usuario final: Persona física o jurídica que adquiere un certificado digital de un PSC.

Validez de la firma: Aplicabilidad (apto para el uso previsto) y estado (activo, revocado o expirado) de un certificado.

Verificación de la firma: Determinación y validación de: a) que la firma digital fue creada durante el periodo operacional de un certificado válido por la clave privada correspondiente a la clave pública que se encuentra en el certificado; b) que el mensaje no ha sido alterado desde que su firma digital fue creada.

X. 500: Estándar desarrollado por la ITU que define las recomendaciones del directorio. Da lugar a la serie de recomendaciones siguientes: X.501, X.509, X.511. X.518, X.519, X.520, X.521, X.525.

X. 509: Estándar desarrollado por la ITU, que define el formato electrónico básico para certificados electrónicos.

1.6.2 Acrónimos

C: País (del inglés, Country).

CA: Autoridad Certificadora (CA por sus siglas en inglés Certificate Authority)

CAI: Autoridad de Certificación Intermedia.

CA Raíz: Autoridad Certificadora Raíz del Paraguay

CI: Cédula de identidad

CN: Nombre común (del inglés, Common Name).

CP: Políticas de Certificación (CP por sus siglas en inglés Certificate Policy).

CPS: Declaración de Prácticas de Certificación (CPS por sus siglas en inglés Certification Practice Statement).

CRL: Lista de certificados revocados (CRL por sus siglas en inglés certificate revocation list).

CSR: Solicitud de firma de certificado (CSR por sus siglas en inglés Certificate Signing Request). Conjunto de datos, que contienen una clave pública y su firma electrónica utilizando la clave privada asociada, enviado a la Autoridad de Certificación para la emisión de un certificado electrónico que contenga dicha clave pública.

DGFD&CE: Dirección General de Firma Digital y Comercio Electrónico dependiente del Vice Ministerio de Comercio.

DN: Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de un directorio X.500.

DNS: Servicio de nombre de dominio (DNS por sus siglas en inglés Domaine Name server).

ETSI: Instituto Europeo de Normas de Telecomunicaciones (ETSI por sus siglas en inglés European Telecomunications Standards Institute)

FIPS Estándares Federales de Procesamiento de la Información

(FIPS por sus siglas en inglés Federal Information Processing Standards).

HSM: Modulo de seguridad 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).

ITU-T: Unión Internacional de Telecomunicaciones – Sector de Normalización de las telecomunicaciones (ITU-T por sus siglas en inglés International Telecomunication Union – Telecomunication Standardization Sector).

MIC: Ministerio de Industria y Comercio.

O: Organización (del inglés Organization).

OCSP: Servicio de validación de certificados en línea (OCSP por sus siglas en inglés Online Certificate Status Protocol).

OID: Identificador de Objeto (OID por sus siglas en inglés Object Identifier).

OU: Unidad Organizacional (OU, por sus siglas en inglés Organization Unit).

PIN: Número de Identificación Personal (por sus siglas en inglés, Personal Identification Number).

PKCS: Norma de criptografía de clave pública (PKCS por sus siglas en inglés, Public Key Cryptography Standards).

PKI: Infraestructura de Clave Pública (PKI por sus siglas en inglés Public Key Infrastructure).

PSC: Prestador de Servicios de Certificación

PY: Paraguay

RA: Autoridad de Registro (RA por sus siglas en inglés Registration Authority).

RFC: Petición de Comentarios (RFC por sus siglas en inglés Request for Comments).

RSA: Sistema criptográfico de clave pública desarrollado por Rivers, Shamir y Adleman.

RUC: Registro Único del Contribuyente.

SN: Número de Serie (del inglés, Serial Number).

SSL: Capa de Conexión Segura (SSL por sus siglas en inglés Secure Sockets Layer).

TLS: Conexión de capa segura (TLS por sus siglas en inglés, Transport Layer Security)

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).
VA: Autoridad de Validación (VA por sus siglas en inglés Validation Autority).

2. RESPONSABILIDADES DE PUBLICACION Y DEL REPOSITORIO

2.1. Repositorios

El repositorio de la CA de DOCUMENTA S.A. está disponible en un 99,5% anual, 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.

Las informaciones del repositorio son publicadas en la página web htpps://www.documenta.com.py

El acceso se realiza vía HTTPS

2.2. Publicación de Información de Certificación

El repositorio de la CA de 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% anual, un tiempo programado de inactividad máximo de 0,5% anual.

La CA de 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.

La CA de DOCUMENTA S.A. mantiene publicada, entre otros aspectos la versión actualizada de:

Lista de certificados revocados CRL	https://www.documenta.com.py/firmadigital/descargas/crldoc.crl
Servicio de OCSP	http://www.documenta.com.py/firmadigital/oscp
CA Raíz del Paraguay	https://www.documenta.com.py/firmadigital/descargas/caraizpy.crt

Certificado de CA Documenta S.A.	https://www.documenta.com.py/firmadigital/descargas/cadoc.crt
CPS	https://www.documenta.com.py/firmadigital/descargas/cpsv2.pdf
Política de Certificación F1	https://www.documenta.com.py/firmadigital/descargas/cpf1.pdf
Política de Certificación F2	https://www.documenta.com.py/firmadigital/descargas/cpf2.pdf
Consulta de certificados emitidos	https://www.documenta.com.py/certificados_emitidos.php
Acuerdo de Suscriptores	https://www.documenta.com.py/firmadigital/descargas/acuerdo_suscriptor_documenta.pdf
Información de RA delegadas	https://www.documenta.com.py/firmadigital/ra
Información de los PSS vinculados	https://www.documenta.com.py/firmadigital/pss

Además, se publican Leyes, decretos, reglamentos y resoluciones que rigen la actividad de la PKI Paraguay; las resoluciones que habilitan, suspenden o revocan al PSC; y la información relevante del resultado de la última auditoría que hubiere sido objeto.

2.3. Tiempo o frecuencia de Publicación

Las enmiendas o modificaciones de la CPS se publicarán de acuerdo con lo establecido en el punto 9.12 de este documento.

Las actualizaciones del Acuerdo de Suscriptores 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

El acceso para la consulta de las informaciones establecidas en el Item 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. IDENTIFICACION Y AUTENTICACION

3.1. Nombres

Los requisitos y procedimientos de identificación y autenticación utilizadas por las RA vinculadas a la CA de DOCUMENTA S.A. son:

a) Validación de solicitud de certificado: realizada mediante presencia física del interesado presentando los documentos de identificación indicados en los Ítems 3.2.2, 3.2.3 y 3.2.4 comprendiendo las siguientes etapas:

I. Confirmación de Identidad de la persona física: comprobar que la persona que se presenta como titular interesado en un certificado de persona física sea realmente aquella cuyos datos constan en la documentación presentada. Está prohibido cualquier especie de representación para este fin. En caso de persona jurídica, comprobar que la persona física que se presenta como su representante es realmente aquella cuyos datos constan en la documentación presentada. El responsable de uso del certificado digital para persona jurídica debe comparecer presencialmente. Está prohibido cualquier especie de representación para este fin;

II. Confirmación de la identidad de una persona jurídica: comprobar que los documentos presentados refieren efectivamente a la persona jurídica, titular del certificado y de que la persona que se presenta como representante legal de la persona jurídica realmente posea tal atribución. Esta etapa sólo se realiza en caso de tratarse de un certificado de persona jurídica; y

III. Autorización de emisión del certificado: confirmar los datos de solicitud de certificado con el conjunto de los documentos presentados y autorizar la expedición del certificado en el sistema del PSC;

b) Verificación de la solicitud de certificado: confirmar la validación realizada, señalando que debe ser ejecutado, obligatoriamente:

I. por el agente de registro distinto al que ejecutó la tarea en la etapa de validación;

II. en una de las instalaciones técnicas de la RA debidamente autorizada a funcionar por el PSC al cual está vinculada;

III. únicamente después de la recepción, en la instalación técnica de la RA, de las copias de las documentaciones presentadas en la etapa de validación; y

IV. 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.

El proceso de validación de la identidad podrá ser realizado por el agente de registro fuera del ambiente físico de la RA, siempre que haya utilizado un ambiente computacional auditable y

debidamente registrado en el inventario de hardware y software de la RA.

Todas las etapas de los procesos de validación y verificación de la solicitud de certificados deben ser registradas y firmadas por los ejecutantes. Estos registros se realizan a los efectos de permitir la reconstrucción completa de procesos ejecutados, con fines de auditoría.

Deben ser mantenidos los archivos con las copias de todos los documentos utilizados para la confirmación de la identidad de la persona jurídica. Las copias podrán ser mantenidas en papel o en forma digitalizada, sujeto a las condiciones expuestas en este documento.

3.1.1. Tipos de Nombres

El tipo de nombre admitido para los titulares de los certificados emitidos conforme a la presente CPS son el Nombre Distintivo (Distinguished Name) según lo establecido en el estándar ITU X.500, direcciones de correo electrónico, dirección de página web (URL), u otra información que permita la identificación única del titular.

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

No se admite el anonimato de los certificados emitidos por la CA de DOCUMENTA S.A. Asimismo, el seudónimo no se considera un nombre significativo del solicitante y no se utilizará como parte del Certificado.

3.1.4. Reglas para interpretación de varias formas de Nombres

Certificado de CA de DOCUMENTA S.A

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

Tipo de Documento	Prefijo	Formato
Cédula Tributaria – RUC	RUC	RUC 99999999-9

Certificado de Persona Jurídica

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

Tipo de Documento	Prefijo	Formato
Cédula Tributaria – RUC	RUC	RUC99999999-9

Certificado de Persona Física

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

Tipo de Documento	Prefijo	Formato
Cédula de Identidad	CI	CI9999999

Certificado de máquina o aplicación

Tipo de Documento	Prefijo	Formato
Cédula de Identidad	MCI	CI9999999
Cédula Tributaria – RUC	MRUC	RUC99999999-9

3.1.5. Unicidad de nombres

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

3.1.6. Reconocimiento, autenticación y rol de las marcas registradas

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. También, durante el proceso de verificación de identidad, corresponderá al solicitante del certificado demostrar su derecho a usar un nombre específico.

DOCUMENTA S.A. tiene el derecho de rechazar una solicitud de certificado a causa de conflicto de nombre.

3.2. Validación inicial de la identidad

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

El titular del certificado de persona jurídica, será la persona física, designada por la organización como responsable del certificado, que será el titular de la clave privada.

La confirmación de la identidad de la persona jurídica y de la persona física responsable del certificado deberá realizarse en los siguientes términos:

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

I. Si la entidad es pública:

- Copia simple de la Ley o Carta Orgánica que crea o autoriza su creación.
- Documento que acredite la representación legal de la máxima autoridad.
- Número de registro único del contribuyente (RUC), en caso de que la entidad pública sea sujeto tributario.

II. si la entidad es privada:

- Copia autenticada del documento de constitución de la Sociedad.
- Copia autenticada de acta de la última asamblea ordinaria y extraordinaria.
- Copia autenticada del Acta de la última sesión;
- Prueba de la inscripción en el registro nacional de personas jurídicas.
- Certificado de cumplimiento tributario.
- Número de registro único del contribuyente (RUC); y

La confirmación de la identidad de el/los representante/s legal/es de la persona jurídica y del responsable del uso del certificado, se hará mediante la presentación de los documentos exigidos en el Ítem 3.2.3, con la presencia física de estos y la firma del documento de solicitud de certificado que trata el ítem 4.1.

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, sin abreviaturas, en el campo *Subject*, como parte del *Common Name*, que compone parte del *Distinguished Name*;

b) Número de registro único del contribuyente (RUC) según la cédula tributaria en el campo *Subject,* como parte del *SerialNumber*, que compone parte del Distinguished Name;

c) Nombre completo de la persona física responsable del certificado según documento de identidad, sin abreviaturas, en el campo *Subject Alternative Name* OID=2.5.4.3

d) Número de cédula de Identidad Policial de la persona física responsable del certificado según documento de identidad, en el campo *Subject Alternative Name* OID=2.5.4.5.

La RA vinculada a la CA de DOCUMENTA S.A. debe comprobar la información suministrada por el solicitante contra los datos oficiales correspondientes. Si hay diferencias en relación con los datos del documento de identidad de la persona física, la expedición del certificado digital debe ser suspendida y el solicitante debe regularizar su situación ante el organismo competente.

Cada CP puede definir como obligatoria llenar otros campos.

Además, el titular del certificado, a su criterio y mediante una declaración explícita en el documento de solicitud de certificado, puede solicitar llenar los campos con las siguientes informaciones:

a) el correo del titular del certificado; y

b) El cargo que ocupa en la organización el responsable del certificado.

Para ello, el titular deberá presentar la documentación que respalde la información que la RA considere necesaria, caso por caso, en su versión original, y una copia autenticada por notario público para dejar agregado al legajo. DOCUMENTA S.A. mantiene un archivo con copias de todos los documentos utilizados.

3.2.3. Autenticación de identidad de persona física

El solicitante de certificados de persona física deberá proporcionar la siguiente información:

Datos personales:

- Primer nombre.
- Segundo nombre.
- Primer apellido.
- Segundo apellido
- Cédula de identidad

- Dirección de correo electrónico
- Fecha de nacimiento

Para poder autenticar la identidad de la persona física, el solicitante deberá comparecer en el puesto de inscripción de la RA de DOCUMENTA S.A. con su Cédula de Identidad Policial Paraguaya, y otro documento oficial, por ejemplo, su licencia de conducir. Además, de los datos proporcionados en la solicitud, en el puesto de inscripción se podrán capturar los datos biométricos del solicitante.

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

- Nombre completo de la persona física titular del certificado, según el documento de identidad, en el campo Subject, como parte del Common Name, que compone parte del Distinguished Name; y
- Número de cédula de Identidad Policial de la persona física, según documento de identidad, en el campo Subject, como parte del SerialNumber, que compone parte del Distinguished Name.

La RA de DOCUMENTA S.A. debe comprobar la información suministrada por el solicitante contra los datos oficiales correspondientes. Si hay diferencias en relación con los datos del documento de identidad, la expedición del certificado digital debe ser suspendida y el solicitante debe regularizar su situación ante el organismo competente.

Cada CP puede definir como obligatoria llenar otros campos.

Además, el titular del certificado, a su criterio y mediante una declaración explícita en el documento de solicitud de certificado, puede llenar los campos con las siguientes informaciones:

- Nombre de la organización en el que presta servicio el titular del certificado
- Nombre de la unidad de la organización en el que presta servicio el titular del certificado.
- Número de cédula tributaria correspondiente a la organización en el que presta servicio el titular del certificado.

- Cargo o título del titular del certificado.

Para ello, el titular deberá presentar la documentación que respalde la información que la RA considere necesaria, caso por caso, en su versión original, y una copia autenticada por notario público para dejar agregado al legajo. Debe tenerse un archivo con copias de todos los documentos utilizados.

3.2.4. Autenticación de identidad de una máquina o aplicación

En el caso de los certificados expedidos para una maquina o aplicación, el titular es la persona física o jurídica que solicita el certificado. En el caso de que el solicitante sea una persona jurídica, se deberá indicar al responsable del certificado, que será el titular de la clave privada.

Si el titular del certificado es una persona física, se deberá confirmar su identidad según lo estipulado en el Ítem 3.2.3 y la firma del documento de *solicitud de certificado* qué trata el Ítem 4.1.

Si el titular del certificado es una persona jurídica, se deberá confirmar su identidad según lo estipulado en el Ítem 3.2.2 y la firma del documento de *solicitud de certificado* qué trata el Ítem 4.1.

Procedimientos para la identificación de una maquina o aplicación:

a) Para emisión de certificados de máquinas que se utilizan como servidores, la solicitud debe contener el nombre del servidor y el número de serie del equipamiento.

b) Para certificados de maquina o aplicación que utilizan URL en el campo *Common Name*, se debe comprobar si el solicitante del certificado tiene el registro del nombre de dominio por el órgano competente, o tenga el permiso del propietario del dominio para utilizar ese nombre. En este caso, se debe presentar la documentación correspondiente (autorización o similar) firmado por el titular del dominio.

La información obligatoria contenida en los campos del certificado expedido a un dispositivo o aplicación, debe coincidir exactamente con la información contenida en los siguientes documentos:

a) URL o nombre de la aplicación, en el campo *Subject*, como parte del *Common Name*, que compone el *Distinguished Name*;

b) En el caso que el titular sea una persona jurídica:

b1 Número de registro único del contribuyente (RUC) de la persona jurídica según la cédula tributaria en el campo *Subject,* como parte del *SerialNumber*, que compone parte del Distinguished Name;

b.2 Nombre de la razón social de la persona jurídica según documento constitutivo, en el campo *Subject Alternative Name OID=2.5.4.10;*

b.3 Nombre completo de la persona física responsable del certificado según documento de identidad, sin abreviaturas, en el campo *Subject Alternative Name OID=2.5.4.3*

b.4 Número de cédula de identidad policial de la persona física responsable del certificado según documento de identidad, en el campo *Subject Alternative OID=2.5.4.5.*

c) En el caso que el titular sea una persona física

c.1 Número de cédula de identidad policial de la persona física, según documento de identidad, en el campo *Subject*, como parte del *SerialNumber*, que compone parte del *Distinguished Name*;

c.2 Nombre completo de la persona física responsable del certificado según documento de identidad, sin abreviaturas, en el campo *Subject Alternative Name* OID=2.5.4.3

Además, el titular del certificado, a su criterio y mediante una declaración explícita en el documento de *solicitud de certificado*, puede solicitar llenar los campos con las siguientes informaciones:

a) el correo del responsable del certificado;

b) El cargo o título del responsable del certificado en caso de ser persona jurídica.

Para ello, el titular deberá presentar la documentación que respalde la información que la RA considere necesaria, caso por caso, en su versión original y una copia autenticada por notario público para dejar agregado al legajo. Debe tenerse un archivo con copias de todos los documentos utilizados.

3.2.5. Información del suscriptor no verificada

No se contempla la inclusión de información no verificada en los certificados emitidos por la CA de DOCUMENTA S.A.

3.2.6. Validación de la Autoridad (capacidad de hecho)

DOCUMENTA S.A. Determinará si el solicitante se encuentra apto para solicitar un tipo de certificado específico. Además, debe validar que el solicitante no posea impedimentos legales.

En el caso de Certificados de Personas Físicas, validará:

- Nombre y documento de identidad
- Mayoría de edad.

En el caso que el solicitante sea Persona Jurídica debe verificar:

- Nombre o razón social y Cédula Tributaria
- Nombre del representante legal y documento de identidad.

DOCUMENTA S.A. verificará la información suministrada por el solicitante contra los datos oficiales correspondientes.

3.2.7. Criterios para interoperabilidad

Podrán ser reconocidos los Certificados Digitales Extranjeros de conformidad a la normativa vigente. Para el efecto, el estado

paraguayo deberá suscribir Acuerdos Internacionales con sus pares extranjeros, salvo que, por protocolo adicional a un tratado vigente, los países suscriptores del mismo hayan acordado el reconocimiento recíproco de los certificados digitales emitidos en los respectivos países.

3.3. Identificación y autenticación para solicitudes de re emisión de claves

3.3.1. Identificación y autenticación para re emisión de claves

No se permite la re emisión de claves.

3.3.2. Identificación y autenticación para la re emisión de claves después de una revocación

No se permite bajo estas circunstancias, la re emisión de claves. Luego del procedimiento de Revocación, se debe solicitar la emisión de un nuevo certificado.

3.4. Identificación y autenticación para solicitudes de revocación

Los procedimientos aceptados para la autenticación del solicitante de la revocación 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 a través de los procesos de autenticación, de identidad (sección 3.2.3)
- Cualquier otro medio establecido por DOCUMENTA S.A. y aprobado por el MIC que permita una identificación veraz y segura.

Los sujetos habilitados para solicitar la revocación se encuentran establecidos en la sección 4.9.2 y los procedimientos de revocación en la sección 4.9.3.

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1. Solicitud de certificado

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

- La comprobación de los atributos de identificación que constan en el certificado conforme al ítem 3.

- Una Solicitud de Certificado firmada por el titular del certificado o por el responsable del uso del certificado, en caso de la persona jurídica.

4.1.1 Quién puede presentar una solicitud de certificado

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

- Para el caso de certificado de persona física, toda persona, mayor de edad, sin distinción, con un documento de identidad válido, que será el sujeto a cuyo nombre se emita el certificado.
- Para el caso de certificado de persona jurídica, el representante legal o el responsable del uso del certificado con poder suficiente.
- Para el caso de certificado de equipo o aplicación, el representante legal o el responsable del uso del certificado con poder suficiente si el solicitante es una persona jurídica, o toda persona, mayor de edad, sin distinción, con un documento de identidad válido si el solicitante es una persona física.

4.1.2. Proceso de inscripción y responsabilidades

Es atribución de cada RA de DOCUMENTA S.A. dentro de la PKI Paraguay determinar la adecuación del tipo de certificado a las características de las funciones del solicitante, de acuerdo con lo previsto en la Política de Certificación aplicable en cada caso. La RA podrá autorizar o denegar la solicitud de certificación.

Las solicitudes de los certificados, una vez completadas, serán enviadas a CA de DOCUMENTA S.A. por la RA correspondiente.

DOCUMENTA S.A. Tiene la responsabilidad de:

- Ejecutar el proceso de registro y verificación de identidad del solicitante.
- Validar la información suministrada en la solicitud de certificado (CSR).
- Informar al suscriptor de sus deberes y responsabilidades con respecto al uso de certificados.
- Emitir y entregar el Certificado de acuerdo con la información suministrada en la solicitud

Todo solicitante que desee un certificado deberá:

- Cumplimentar el formulario de solicitud del certificado con toda la información que DOCUMENTA S.A. requiera para la emisión del mismo. Cabe destacar que no toda la información solicitada aparecerá en el certificado y que ésta será conservada, de manera confidencial.
- Entregar la solicitud del certificado, que incluye la clave pública, en el caso de que el par de claves lo haya

generado el solicitante, a la RA correspondiente y el certificado se genere directamente a partir de la solicitud. En la correspondiente CP se establecerá el procedimiento de entrega.

La existencia del formulario de solicitud y en general el procedimiento de solicitud de certificados queda definido en la Política de Certificación correspondiente a cada uno de los certificados.

4.2. Procesamiento de la Solicitud del Certificado

4.2.1. Ejecución de las funciones de identificación y autenticación

La RA vinculada a la CA de DOCUMENTA S.A. debe velar por la identificación y autenticación de acuerdo con las disposiciones establecidas en el punto 3.2

4.2.2. Aprobación o rechazo de Solicitudes de Certificados

La emisión del certificado tendrá lugar una vez que la RA de DOCUMENTA S. A haya llevado a cabo las verificaciones necesarias para validar la solicitud de certificación.

La RA vinculada a la CA de DOCUMENTA S.A. debe rechazar la solicitud de certificado en los casos que no se dé cumplimiento a la normativa vigente y a lo establecido en esta CPS.

4.2.3. Tiempo para procesar solicitudes de certificados

Se establece el plazo máximo de cinco días hábiles para la tramitación de la solicitud del certificado, contados a partir de haberse verificado la identidad del solicitante y admitida la solicitud.

En caso que la CA de DOCUMENTA S.A. supere el plazo máximo establecido para la tramitación de la solicitud, deberá informar al solicitante de las causas que motivaron la demora y el nuevo plazo en el que se tramitará la solicitud.

4.3. Emisión del certificado

4.3.1. Acciones del PSC durante la emisión de los certificados

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

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

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

4.3.2. Notificación al suscriptor sobre la emisión del certificado digital

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 CP 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 del certificado

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

Los certificados que exijan la presentación de una identificación, requerirán la aceptación explícita del titular del certificado y el reconocimiento de que está de acuerdo con los términos y condiciones contenidos en el Acuerdo de Suscriptores., que rige los derechos y obligaciones entre la CA de DOCUMENTA S.A. y el titular, y de que éste conoce la existencia de la presente CPS y la CP vinculada al certificado emitido, que recogen técnica y operativamente los servicios de certificación digital prestados en el marco de la PKI Paraguay.

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

4.4.2. Publicación del certificado por el PSC

Documenta S.A. publicará información de los certificados que emite a través de un mecanismo de consulta que estará disponible en el sitio principal de Internet.

Además, DOCUMENTA S.A. publica en su repositorio público su certificado digital y el de la CA raíz.

4.4.3. Notificación de la emisión del certificado por el PSC a otras entidades

No se definen entidades externas que necesiten o requieran ser notificados a cerca de los certificados emitidos por la CA.

4.5. Uso del par de claves y del certificado

4.5.1. Uso de la clave privada y del certificado por el suscriptor

Las responsabilidades y limitaciones de uso del par de claves y del certificado se establecerán en la correspondiente CP. En cualquier caso, el titular sólo podrá utilizar la clave privada y el certificado para los usos autorizados en la CP y de acuerdo con lo establecido en los campos **'Key Usage'** y **'Extended Key Usage'** del certificado. Del mismo modo, el titular solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso, establecidas en la CPS y CP, y sólo para lo que éstas establezcan.
Tras la expiración o revocación del certificado, el titular dejará de usar la clave privada.

4.5.2. Uso de la clave pública y del certificado por la parte que confía

Los Terceros que Confían sólo pueden depositar su confianza en los certificados para aquello que establezca la correspondiente CP y de acuerdo con lo establecido en el campo 'Key Usage' y 'Extended Key Usage' del certificado. Los Terceros que Confían han de realizar las operaciones de clave pública de manera adecuada para confiar en el certificado, así como asumir la responsabilidad de verificar el estado del certificado utilizando los mecanismos establecidos en esta CPS y en la correspondiente CP. Asimismo, se adhieren a las condiciones de uso establecidas en dichos documentos.

4.6. Renovación del certificado

La renovación del certificado no está permitida por esta CPS, cuando un certificado requiera ser renovado debe solicitarse uno nuevo, de acuerdo con la sección 4.1 de esta CPS.

4.6.1. Circunstancias para renovación de certificados

No estipulado.

4.6.2. Quién puede solicitar renovación

No estipulado.

4.6.3. Procesamiento de solicitudes de renovación de certificado

No estipulado.

4.6.4. Notificación al suscriptor sobre la emisión de un nuevo certificado

No estipulado.

4.6.5. Conducta constitutiva de aceptación de un certificado renovado

No estipulado.

4.6.6. Publicación por el PSC del certificado renovado

No estipulado.

4.6.7. Notificación por el PSC de la emisión de un certificado a otras entidades

No estipulado.

4.7. Re-emisión de claves de certificado

La renovación con cambio de claves no está permitida por esta CPS, cuando un certificado requiera ser re-emitido debe solicitarse un nuevo certificado, de acuerdo con la sección 4.1 de esta CPS.

4.7.1. Circunstancias para re-emisión de claves de certificado

No estipulado.

4.7.2. Quién puede solicitar la re-emisión claves

No estipulado.

4.7.3. Procesamiento de solicitudes de re-emision de claves de certificado

No estipulado.

4.7.4. Notificación al suscriptor sobre la re-emisión de un nuevo certificado

No estipulado.

4.7.5. Conducta constitutiva de aceptación de un certificado re-emitido

No estipulado.

4.7.6. Publicación por el PSC de los certificados re-emitidos

No estipulado.

4.7.7. Notificación por el PSC de la re-emisión de un certificado a otras entidades

No estipulado.

4.8. Modificación de certificados

Cuando se requiera la modificación de la información contenida en un certificado debe revocarse y realizar una solicitud para un nuevo certificado, de acuerdo con la sección 4.1 de esta CPS.

4.8.1. Circunstancias para modificación del certificado

No estipulado

4.8.2. Quién puede solicitar modificación del certificado

No estipulado.

4.8.3. Procesamiento de solicitudes de modificación del certificado

No estipulado.

4.8.4. Notificación al suscriptor de la emisión de un nuevo certificado

No estipulado.

4.8.5. Conducta constitutiva de aceptación del certificado modificado

No estipulado.

4.8.6. Publicación por el PSC de los certificados modificados

No estipulado.

4.8.7. Notificación por la CA de emisión de certificado a otras entidades

No estipulado.

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:

- Modificación de alguno de los datos contenidos en el certificado;
- Descubrimiento que algunos de los datos aportados en la solicitud de certificado es incorrecto, así como la alteración o modificación de las circunstancias verificadas para la expedición del certificado;
- Descubrimiento que algunos de los datos contenidos en el certificado es incorrecto.

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

- Compromiso de la clave privada o de la infraestructura o sistemas de la CA que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de este incidente;
- Infracción, por la CA de DOCUMENTA S.A. de los requisitos previstos en los procedimientos de gestión de los certificados, establecidos en su propia CP y CPS;
- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del titular del certificado;
- Acceso o utilización no autorizada, por un tercero, de la clave privada del titular;

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

c) Circunstancias que afectan la seguridad del dispositivo criptográfico

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico;
- Pérdida o inutilización por daños del dispositivo criptográfico;
- Acceso no autorizado, por un tercero, a los datos de activación de la clave privada del titular del certificado;

d) Circunstancias que afectan al suscriptor

- Infracción del titular del certificado en sus obligaciones, responsabilidad y garantías, establecidas en la CP y CPS del PSC que emitió el certificado;
- La incapacidad de hecho sobrevenida o la muerte del titular del certificado;
- La extinción de la persona jurídica titular del certificado;
- Solicitud de revocación del certificado por su titular de acuerdo con lo establecido en la CP y en la CPS.

e) Otras causales especificadas en la normativa y reglamentación vigente.

4.9.2. Quién puede solicitar revocación

La revocación de un certificado sólo podrá realizarse:

- por petición del titular del certificado;
- por solicitud del responsable del certificado en el caso de un certificado de persona jurídica o un certificado de maquina o aplicación;
- 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, funcionario o servidor;
- por DOCUMENTA S.A. en su condición de PSC emitente;
- por una RA vinculada a la CA de DOCUMENTA S.A;
- por determinación de la CA Raíz del Paraguay;
- 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 tiempo, solicitarla revocación de sus respectivos certificados. En el caso que sean

requeridos procedimientos específicos para las CP implementadas, los mismos deben ser descriptos en esas CP, en el ítem correspondiente.

Como directrices generales se establece que:

a) el Solicitante de revocación de un certificado debe ser identificado;

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

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

d) la revocación de un certificado terminará con la generación y publicación de una CRL 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 de la CA de DOCUMENTA S.A.

El plazo máximo admitido para la conclusión del proceso de revocación del certificado después de la recepción de la respectiva solicitud, para todos los certificados descriptos en esta CPS, será de 12 (doce) horas.

4.9.4. Periodo de gracia para solicitud de revocación

La revocación se llevará a cabo de forma inmediata a la tramitación de cada solicitud verificada como válida. Por tanto, no existe ningún periodo de gracia asociado a este proceso durante el que se pueda anular la solicitud de revocación.

4.9.5. Tiempo dentro del cual el PSC debe procesar la solicitud de revocación

Las solicitudes de revocación deben resolverse tan rápido como sea posible en un tiempo no superior a 12 horas siempre y cuando estén configuradas las circunstancias definidas en el Ítem 4.9.1

En caso que sean requeridos plazos específicos para las CP implementadas, los mismos deben ser descriptos en esas CP, en el ítem correspondiente, que no podrán superar las 12 horas.

4.9.6. Requerimientos de verificación de revocación para las partes que confían

La evaluación del estado del certificado, y de todos los certificados de la CA en la cadena a la que pertenece el mismo, es obligatoria para cada uso de los certificados por las Partes que Confían, antes de confiar en él.

Para ello, los Terceros que Confían pueden verificar el estado del certificado mediante el servicio de: OCSP o la CRL más reciente, proveída por la CA de DOCUMENTA S.A.

Los Terceros que Confían deberán comprobar la validez de la CRL previamente a cada uno de sus usos y descargar la nueva CRL del

repositorio de la CA de 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.

Cuando la CP de aplicación admita otras formas de divulgación de información de revocación, los requisitos para la comprobación de dicha información se especificarán en la propia CP.

4.9.7. Frecuencia de emisión del CRL

DOCUMENTA S.A. Publicará una nueva CRL en su repositorio en el momento en que se produzca cualquier revocación. En cualquier caso, DOCUMENTA S.A. Publicará una nueva CRL en su repositorio a intervalos no superiores a 12 horas, aunque no se hayan producido modificaciones en la CRL, es decir, aunque no se haya revocado ningún certificado desde la última publicación.

La CA Raíz publicará una nueva CRL en su repositorio inmediatamente cuando surja una revocación o con una frecuencia de emisión máxima de 45 días para la CRL referente a los PSC

En caso que sean utilizadas frecuencias de emisión específicos de CRL para las CP implementadas, deben ser descriptos en estas CP, en el ítem correspondiente, que no podrán supercar las 12 horas.

4.9.8. Latencia máxima para CRL

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

En caso que sean requeridas la latencia máxima para la CRL, específicas para las CP implementadas, deben ser descriptos en estas CP, en el ítem correspondiente.

4.9.9 Requisitos de verificación del CRL

En el caso de recurrir a la validación a través de la CRL, el certificado deberá tener su validez verificada, en la respectiva CRL, antes de utilizarlo. La autenticidad de la CRL deberá también ser confirmada, por medio de la verificación de la firma de la CA de DOCUMENTA S.A. en el periodo de validez de la CRL.

4.9.10 Disponibilidad de verificación de revocación/estado en línea

DOCUMENTA S.A. proporciona un servidor web donde publica las CRL para la verificación del estado de los certificados que emite. Asimismo, existe una Autoridad de Validación de DOCUMENTA S.A. que, mediante el protocolo OCSP, permite verificar el estado de los certificados.

4.9.11 Requerimientos para verificar la revocación en línea

En el caso de recurrir a la Autoridad de Validación de DOCUMENTA S.A. el Tercero que Confía debe disponer de un software que sea capaz de operar con el protocolo OCSP para obtener la información sobre el certificado.

4.9.12 Otras formas de advertencia de revocación disponibles

DOCUMENTA S.A. dispone de un Sistema de Consulta de Certificados emitidos en su repositorio público.

4.9.13 Requerimientos especiales por compromiso de clave privada

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

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

Además la CA de DOCUMENTA S.A. publicará el compromiso de su clave en su sitio principal de internet y procederá a la inmediata gestión de la revocación de su certificado y el de sus suscriptores. DOCUMENTA S.A. publicará el certificado revocado en el repositorio.

4.9.14 Cincunstancias para suspensión

No estipulado.

4.9.15 Quién puede solicitar la suspensión

No estipulado.

4.9.16 Procedimiento para la solicitud de suspensión

No estipulado.

4.9.17 Límites del periodo de suspensión

No estipulado.

4.10. Servicios de comprobación de estado de certificados

4.10.1. Características operacionales

DOCUMENTA S.A. dispone como mínimo de dos servicios que proporcionan información sobre el estado de los certificados emitidos por su CA:

- Publicación de las listas de revocación de certificados (CRL). El acceso a las CRL se realiza vía HTTPS.
- Servicio de validación en línea (Autoridad de Validación, VA) que implementa el Online Certificate Status Protocol siguiendo la RFC 2560.

- Sistema de consulta de certificados emitidos.

4.10.2. Disponibilidad del servicio

El servicio, en sus tres variantes establecidas en el apartado anterior, están disponibles de forma ininterrumpida todos los días del año, tanto para los Terceros que Confían como para los Titulares de los certificados u otras partes que los requieran.

DOCUMENTA S.A. garantiza la disponibilidad del servicio de publicación en el repositorio público de la CRL, del Sistema de Consulta de Certificados Emitidos, y el servicio de consulta en línea por medio del protocolo OCSP con un mínimo de 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

4.10.3. Características opcionales

DOCUMENTA S.A. en ningún caso proporcionará un cliente OCSP para hacer uso del Servicio de validación en línea. Es responsabilidad de quien desee utilizar dicho servicio disponer de un Cliente OCSP que cumpla la RFC 2560.

4.11. Fin de la suscripción

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. Políticas y prácticas de custodia y recuperación de claves

DOCUMENTA S.A. no custodia los datos de creación de firma de sus suscriptores.

Para los efectos del Plan de Continuidad de Negocio, la clave privada de la CA de DOCUMENTA S.A. está custodiada y respaldada bajo estrictas normas de seguridad, y almacenada en dispositivos criptográficos FIPS 140-2 nivel 3, que garantizan la no divulgación de las claves.

4.12.2. Políticas y practicas de recuperación y encapsulación de claves de sesión

No estipulado.

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

A fin de asegurar la confiabilidad y seguridad de sus operaciones como prestador de servicios de certificación, la CA de

DOCUMENTA S.A. y sus RA 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, para el seguimiento y verificación del cumplimiento de las políticas, directivas y procedimientos en materia de seguridad.

5.1. Controles físicos

5.1.1. Localización y construcción del sitio

La localización de las instalaciones donde se albergan los sistemas de certificación de DOCUMENTA S.A. 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 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:

- Muros perimetrales Reforzados.
- Generación de energía redundante.
- Sistema ininterrumpible de energía.
- Sistema de UPS redundante.
- Doble acometida eléctrica.
- Sistema de enfriamiento de precisión redundante.
- Sistema de detección, extinción y supresión automática de fuego.
- Sistema de monitoreo de infraestructura.
- Sistema de tierras físicas y pararrayos.
- Suministro de energía eléctrica regulada y con protección.
- Sistema de aire acondicionado HVAC.
- Seguridad física 24/7 (subsistema de seguridad mediante guardias de seguridad).
- Sistema CCTV con grabación con movimiento.
- Sistema de iluminación de emergencia.

Las instalaciones donde se emiten los certificados de la CA de DOCUMENTA S.A. se protege con su propio y único perímetro físico.

5.1.2. Acceso físico

DOCUMENTA S.A. implementa un sistema de control de acceso físico que garantiza la seguridad de sus instalaciones, conforme al item 9 “control de accesos” de la norma ISO 27002:2013 y los

siguientes puntos:

Niveles de acceso

Los centros de datos donde se aloja la infraestructura tecnológica de DOCUMENTA S.A. cuentan con seis niveles de seguridad física:

- Primer nivel: Primera barra de acceso a las instalaciones de DOCUMENTA S.A. Para acceder en el 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 de la CA deberán transitar debidamente identificadas y acompañadas. Ningún tipo de proceso operacional o administrativo de la CA 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 PSC, 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.

- Segundo nivel: Área interna al perímetro anterior, de acceso más estricto y restringido que el primero. Requiere, una identificación individual de las personas que en él accedan. Ese será el nivel mínimo de seguridad requerido para la ejecución de cualquier proceso operacional o administrativo de DOCUMENTA S.A. El paso del primer al segundo perimetro deberá exigir por lo menos 1 (uno) factor de autenticación electrónica y tarjeta de identificación visible.
- Tercer nivel: Área interna al perímetro anterior, de acceso más estricto y restringido que el segundo. Cualquier actividad relativa al ciclo de vida de los certificados digitales deberá estar localizada a partir de este perímetro. Personas que no están involucradas con esas actividades no deberán tener permiso para acceder a este perímetro. Personas que no poseen permiso de acceso no podrán permanecer en ese perímetro si no estuviesen acompañadas por alguien que tenga permiso de acceso.

En este perímetro 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 como mínimo requerirán de 2 (dos) factores de autenticación electrónica y tarjeta de identificación visible.

Teléfonos móviles y otros equipos de comunicación portátil, con excepción de los necesarios para el funcionamiento del PSC, no serán aceptadas desde el nivel 3.

- Cuarto nivel: acceso al área de operaciones críticas de la CA. Área interna al nivel anterior, de acceso más estricto y restringido que el tercero. Todos los sistemas y equipamientos necesarios a estas actividades deberán estar localizados a partir de este perímetro. En el cuarto perimetro deberán 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 perimetro, la permanencia de esas personas deberá ser exigida mientras el ambiente estuviera ocupado.

En el cuarto nivel, todas las paredes, piso y techo deberán ser revestidos con material resistente. 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, 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 of-line y cofre de almacenamiento; y

c) Equipamientos de redes e infraestructura (firewall, ruteadores, switches y servidores)

a) Estar hecho de acero o con material de resistencia equivalente

- Quinto nivel: disponer 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

b) Poseer cerraduras antirrobo.

Área interna al cuarto nivel.

- Sexto nivel: Área interna al cuarto nivel, deberá comprender un cofre o un gabinete reforzado. Los datos de activación de la clave privada del PSC 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.

Sistemas físicos de detección: la transición entre los diferentes perímetros 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, 1(un) año. 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 activo 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 los menos 2(dos) medios de notificación: sonoro y visual.
El sistema de monitoreo de las cámaras de video, así como el sistema de notificación de alarma, deberán ser permanentemente monitoreados por el personal autorizado en el ambiente de nivel 3 deben 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.

Sistema de control de acceso: el sistema de control de acceso deberá estar en el ambiente de nivel 4.
Mecanismos de emergencia: mecanismos específicos deberán ser implementados por el PSC 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.

EL PSC 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 se documentados. Los mecanismos y procedimientos de emergencia deberán ser verificados semestralmente, por medio de simulación de situaciones de emergencia.

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

- Muros perimetrales Reforzados.
- Generación de energía redundante.
- Sistema ininterrumpible de energía.
- Sistema de UPS redundante.
- Doble acometida eléctrica.
- Sistema de enfriamiento de precisión redundante.
- Sistema de detección, extinción y supresión automática de fuego.
- Sistema de monitoreo de infraestructura.
- Sistema de tierras físicas y pararrayos.
- Suministro de energía eléctrica regulada y con protección.
- Sistema de aire acondicionado HVAC.
- Seguridad física 24/7 (subsistema de seguridad mediante guardias de seguridad).
- Sistema CCTV con grabación con movimiento.

5.1.3. Energía y aire acondicionado

La infraestructura de DOCUMENTA S.A cuenta con:

Suministro eléctrico:

- PDU redundadas.
- Dispone de grupos electrógenos, redundados para aquellas circunstancias en las que se presente un déficit en la generación eléctrica o sean frecuentes y/o prolongados los cortes en el suministro eléctrico.
- UPS: permite mantener la alimentación ininterrumpida mediante baterías cuando falla el suministro o se produce una anomalía. Alta disponibilidad y redundancia de los equipos.
- Doble acometida eléctrica para los equipos.
- Sistema de puesta a tierra implantado.
- Dispone de tuberías, conductos, canaletas, paneles y

cajas (de paso, distribución y terminación) diseñadas y construídas de forma a facilitar la inspección y detección de intentos de manipulación.

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.

Aire acondicionado:

- Sistema de enfriamiento de precisión redundante.
- Sistema de aire acondicionado HVAC.

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.

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

5.1.4. Exposición al agua

La infraestructura de DOCUMENTA S.A. cuenta con:

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

5.1.5. Prevención y protección contra fuego

Las salas donde se ubican los activos de la infraestructura Tecnológica de DOCUMENTA S.A. disponen de los medios adecuados (varios niveles de sistemas automáticos de detección y extinción de incendios) para la protección de su contenido contra incendios.

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

En las instalaciones del PSC 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 PSC, o el aumento 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

La información se dispone en medios de forma segura, según la clasificación de la información en ellas contenidas y deberá impedir, detectar y prevenir su uso no autorizado, acceso o su divulgación.

La información relacionada a la infraestructura de la CA de DOCUMENTA S.A. 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

Se ha adoptado una política de gestión de residuos que garantiza el almacenamiento seguro de cualquier material que pudiera contener información, así como una política de gestión de los soportes removibles.

5.1.8. Respaldo fuera de sitio

En caso de siniestro que torne inoperante la instalación principal del DOCUMENTA S.A. las instalaciones de respaldo no se verán afectadas y tomarán totalmente las operaciones del DOCUMENTA S.A. en condiciones idénticas en, un máximo, de 48 (cuarenta y ocho) horas.

5.1.9. Instalaciones técnicas de la RA

Las instalaciones técnicas de las RA vinculadas a la CA de DOCUMENTA S.A. deberán cumplir con los requisitos establecidos en el documento CARACTERÍSTICAS MÍNIMAS DE SEGURIDAD PARA AUTORIDADES DE REGISTRO DEL PARAGUAY.

5.2. Controles procedimentales

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

Estos roles contemplan, al menos las siguientes responsabilidades:

- ***Coordinador de Seguridad:*** Debe llevar a cabo la actualización e implementación de las políticas y procedimientos de seguridad que han sido aprobadas por la CA, controlar la formalización de los convenios entre el personal y la CA, comunicar las medidas disciplinarias acordadas, supervisando su cumplimiento. Asimismo, debe cumplir y hacer cumplir las políticas de seguridad de la CA y debe encargarse de cualquier aspecto relativo a la seguridad de la PKI, desde la seguridad física hasta la seguridad de las aplicaciones, pasando por la seguridad de la red. Es el encargado de gestionar los sistemas de gestión perimetral y en concreto de verificar la correcta gestión de las reglas de los firewalls. Debe comprobar la correcta instalación, configuración y gestión de los sistemas de detección de intrusos y de las herramientas asociadas a estos, asimismo debe 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 de la CA.
- ***Jefe de Área*****:** es el responsable de autorizar la emisión de un certificado o la revocación del mismo. Bajo su control y supervision, se encuentra el personal adscripto a la misma. Es su responsabilidad:
  - Recibir y dar curso a las denuncias que podrían afectar a su personal, proponiendo las medidas disciplinarias correspondientes.
  - Efectuar un control permanente de la adecuación de los recursos materiales y humanos que cuenta el área a su cargo, con el fin de atender a las necesidades de servicio que tiene encomendadas.
- ***Administrador de Sistemas:*** Los responsables de este rol

no deberán estar implicados en tareas de auditoría interna. Son encargados de la instalación y configuración de sistemas operativos y del mantenimiento y actualización de los programas instalados. Tiene 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. Son responsables de mantener el inventario de servidores y resto de componentes de los sistemas de certificación de la CA y asumen la gestión de los servicios de ruteamiento y gestión de reglas de firewall, gestión y mantenimiento de los sistemas de detección de intrusos, etc. Son encargados de la instalación de hardware criptográfico de CA y de la eliminación del hardware criptográfico de CA de producción. Son responsables del mantenimiento o reparación de equipos criptográficos de la CA (incluida la instalación de nuevos hardware, firmware, o software), y la eliminación de desmontaje y permanente por el uso.

- ***Receptor de Registro:*** el mismo tendrá a su cargo realizar la validación de identidad inicial del Solicitante.
- ***Responsable de la operación diaria de la CA:*** se encarga de 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. Son responsables de mantener la información suficiente como para poder restaurar cualquiera de los sistemas en el menor tiempo posible. Encargados de la gestión y mantenimiento de los sistemas de energía, aire acondicionado y prevención de incendios.
- ***Auditor Interno de la CA:*** son los responsables de las tareas de ejecución y revisión de auditoría interna del sistema. Esta auditoría interna debe realizarse de acuerdo con las normas y criterios de auditoría establecidos en la presente CPS. Además cuenta con la capacidad de acceder a los registros del sistema.
- ***Funciones de gestión del ciclo de vida de claves criptográficas:*** Se distinguen los siguientes responsables para la gestión del ciclo de vida de las claves criptográficas:
  - ***Oficial Criptográfico:*** Responsable de la Administración del token/HSM, establecimiento de la política de seguridad del token, inicialización del token y creación de usuarios.

- ***Oficial de Activación:*** Responsible de activar las claves del HSM para que no se pueda hacer uso de las mismas.
- ***Oficial de Backup:*** es el responsable del Token de Backup, establecimiento de la política de clonado y de la creación/transferencia de dominios de clonado.
- ***Oficial de acceso remoto:*** es el responsable de establecer una conexión PED remota.
- ***Usuario de Partición:*** es el encargado de la generación de claves, firma y cifrado/descifrado.
- **Oficial de Registro:** el mismo tendrá a su cargo realización del proceso de emisión y revocación del certificado del suscriptor.
- **Oficial de Generación del CRL:** Encargado de generar y exportar en ficheros la CRL emitidas por la CA. Además son responsables de activar los servicios OCSP y asegurar la disponibilidad del CRL.

- ***Desarrollo de sistemas de la CA***: Son encargados del diseño de las arquitecturas de programación, de control y supervisión de los desarrollos encomendados y de la correcta documentación de las aplicaciones.

5.2.2. Número de personas requeridas por tarea

Los requisitos de control multi-usuarios para la generación y la utilización de la clave privada de la CA de DOCUMENTA S.A. se establecen en el ítem 6.2.2.

Se requiere un mínimo de dos empleados con rol de confianza para realizar operaciones sobre la PKI de la CA de DOCUMENTA S.A. Las demás tareas del PSC podrán ser ejecutadas por un único empleado.

DOCUMENTA S.A. mantiene y ejecuta procedimientos de control rigurosos para asegurar la segregación de funciones.

5.2.3. Identificación y autenticación para cada rol

Todo empleado que asume un rol de confianza en la CA de DOCUMENTA S.A. será identificado y su perfil será verificado antes de que:

- Sean incluido en una lista de acceso a las instalaciones de la CA
- Sean incluido en una lista para acceso físico al sistema de certificación de la CA
- Reciban un certificado electrónico para ejecutar sus actividades operacionales en la CA
- Reciban una cuenta de usuario del sistema de certificación de la CA.

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

- Ser directamente asignados a un único empleado
- No ser compartidos
- Restringirse a las acciones asociadas con el perfil para el que fueron creados.

5.2.4. Roles que requieren separación de funciones

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

- Incompatibilidad entre el rol auditor interno de la CA y cualquier otro rol.
- Incompatibilidad entre el rol de Coordinador de Seguridad y Administrador de Sistemas.
- Incompatibilidad entre el rol de Coordinador de Seguridad y Oficial de Registro.
- Incompatibilidad entre el rol de Coordinador de Seguridad y Usuario de Partición.

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

- La validación de información en aplicaciones de certificado y de solicitudes o información del suscriptor.
- La aceptación, rechazo, otros procesamientos de la aplicación de certificado, solicitud de revocación.
- La emisión o revocación de los certificados, incluyendo personal con acceso a porciones restringidas del repositorio.
- La emisión o destrucción de los certificados de la CA.
- La puesta en operación de la CA en producción.

5.3. Controles de personal

5.3.1 Requerimientos de experiencia, capacidades y autorización

El personal que ejecuta tareas de confianza en la PKI de DOCUMENTA S.A, y de las RA vinculadas, debe poseer cualificación y experiencia en entornos de servicios de certificación e infraestructura de clave pública, conforme a lo establecido en el Ítem 7 "Seguridad ligada a los recursos humanos" de la norma ISO 27002/2013 y además deben:

- Haber demostrado capacidad para ejecutar sus deberes.
- Haber suscripto un acuerdo de confidencialidad y disponibilidad.
- No poseer otros deberes que puedan interferir o causar conflicto con los de la CA.

- No tener antecedentes de negligencia o incumplimiento de labores.
- No tener antecedentes penales.

5.3.2 Procedimientos de verificación de antecedentes

DOCUMENTA S.A. cuenta con procedimientos para verificar la cualificación y experiencia del personal que ejecuta tareas de confianza en la CA y las RA vinculadas de DOCUMENTA S.A. El procedimiento incluye:

- Confirmación de empleos anteriores.
- Título académico y cursos obtenidos.
- Verificación de conocimientos específicos.
- Verificación de antecedentes judiciales y policiales.

5.3.3 Requerimientos de capacitación

El personal que ejecuta tareas de confianza en la CA y las RA vinculadas de DOCUMENTA S.A. debe estar sujeto a una formación específica, incluida en el Plan Anual de Capacitación. La información debe incluir:

- Conceptos básicos de PKI.
- Principios y mecanismos de seguridad del PSC y de las RA vinculadas.
- Sistema de certificación en uso de DOCUMENTA S.A.
- Servicios prestados por la Autoridad de Certificación.
- Aspectos legales relativos a la prestación de servicios de certificación.
- Normativa que rige la materia (Políticas de Certificación, Declaración de Prácticas de Certificación, entre otros).
- Procedimientos de operación, administración y mantenimiento para cada rol específico.
- Gestión de incidencias.
- Procedimientos para la recuperación de la operación en caso de desastres, para cada rol específico.
- Reconocimiento de firmas y validación de documentos presentados en los Ítem 3.2.2, 3.2.3 y 3.2.4

5.3.4 Requerimientos y frecuencia de capacitación

Se proveerá formación al personal de la CA de DOCUMENTA S.A. y sus RA vinculadas ante cambios tecnológicos o en los sistemas de seguridad, introducción de nuevas herramientas, modificación de procedimientos operativos, cambios en la CPS, CP u otros documentos relacionados al funcionamiento, administración y/o gestión de la infraestructura de clave pública.

5.3.5 Frecuencia y secuencia en la rotación de las funciones

DOCUMENTA S.A. efectuará rotaciones de trabajo entre los

distintos roles de la CA y las RA vinculadas al menos una vez cada 3 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

Las prácticas que deben cumplir el personal DOCUMENTA S.A. y el procedimiento sancionador que incumplan las mismas, son recogidas en el Reglamento Interno de DOCUMENTA S.A. y de acuerdo a lo estipulado en el documento suscripto para los roles de confianza.

5.3.7 Requisitos de contratación a terceros

DOCUMENTA S.A. puede contratar personal externo, consultores o terceros, conforme a lo establecido en los Ítems 7 “seguridad ligada a los recursos humanos” y 15 “relaciones con suministradores” norma ISO 27002/2013 bajo las siguientes condiciones:

- Existe un contrato con cláusulas propias de los roles de gestión y estipula sanciones para las actuaciones no autorizadas.
- DOCUMENTA S.A. o las RA vinculadas no poseen personal disponible para los roles de gestión contratados.
- Los contratistas cumplen con los mismos requisitos expuestos en el punto 5.3.1.
- Finalizados los servicios, se dará de baja al usuario y se le revocarán los accesos.

5.3.8 Documentación suministrada al personal

DOCUMENTA S.A. proporciona al personal de la CA y las RA vinculadas toda la documentación y buenas prácticas de seguridad de la información necesarias para el correcto desempeño de sus tareas. Entre la documentación se encuentran:

- Su CPS.
- La CP que implementa.
- Procedimienos y documentación operacional relativa a las actividades de DOCUMENTA S.A.
- Política de Seguridad que implementa DOCUMENTA S.A.
- Contratos, normas y politicas relevantes para sus actividades.
- Otros que se consideren necesario.

5.4. Procedimiento de registro de auditoría

5.4.1 Tipos de eventos registrados

DOCUMENTA S.A, deberá registrar en archivos de auditoria, 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 auditoria:

- Iniciación y terminación del sistema de certificación;
- Los intentos de crear, eliminar, establecer contraseñas o cambiar los privilegios del sistema de los operadores de la CA o la RA vinculada;
- Los cambios en la configuración de la CA o en sus llaves;
- Los cambios en las políticas de creación de certificados;
- Los intentos de acceso (*login*) y de salida del sistema (*logoff*);
- Los intentos no autorizados de acceso a los archivos del sistema;
- La generación de claves propias de la CA o de claves de sus usuarios finales;
- La emisión y revocación de certificados;
- La generación de la CRL;
- Los intentos de iniciar, remover, habilitar y deshabilitar a los usuarios de sistemas y actualizar y recuperar sus claves;
- Las operaciones fallidas de escritura o lectura en el repositorio de los certificados y de la CRL, en su caso; y
- Las operaciones de escritura en ese repositorio, en su caso.

DOCUMENTA S.A. registrará, electrónicamente o manualmente, informaciones de seguridad no generadas directamente por el sistema de certificación, tales como:

- Registros de accesos físicos;
- El mantenimiento y los cambios en la configuración de sus sistemas
- Los cambios de personal y los cambios de su rol de confianza
- Los informes de discrepancia y de compromiso.
- 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 auditoria, 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 la CA de DOCUMENTA S.A. deberá se almacenada, electrónicamente y/o manualmente, en un local único, conforme a lo establecido en el ítem 12 “seguridad en la operativa” de la norma ISO 27002/2013.

La RA vinculada a la CA de DOCUMENTA S.A, deberá registrar electrónicamente y/o manualmente archivos de auditorías de todos los eventos relacionados a la validación y aprobación de la solicitud, así como la revocación de los certificados. Los siguientes eventos deberán obligatoriamente estar incluidos en los archivos de auditoria:

- Los agentes de registros que realizan las operaciones;
- fecha y hora de las operaciones;
- La asociación entre los agentes que realizan la validación, aprobación y y el certificado generado;
- La firma digital del ejecutante.

DOCUMENTA S.A. establecerá, en un documento que esté disponible en las auditorias 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 acuerdo de suscriptores.

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 PKI, y de manera anual cuando sea necesario.

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 de la CA.

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.

Los registros de auditorías deben ser recuperados solamente por personal autorizado, ya sea por razones válidas del negocio o por seguridad.

5.4.3 Periodo de conservación del registro (logs) de auditoría

La información generada en los registros de eventos se conserva localmente por dos meses y, consecuentemente, deberá almacenarlos de la manera descripta en el ítem 5.5.2

5.4.4 Protección del registro (logs) de auditoría

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

La CA de 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 la CA de 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

DOCUMENTA S.A. conserva toda la información relevante sobre las operaciones realizadas con los certificados durante los periodos de tiempo establecidos, se deben archivar los siguientes datos:

- Durante el inicio de operaciones de DOCUMENTA S.A. como PSC:
  - La resolución de Habilitación emitida por la Autoridad de Aplicación

- el CP y el CPS de DOCUMENTA S. A;
- Cualquier acuerdo contractual para establecer los límites del PSC o la RA vinculada;
- La configuración del sistema que requiere la CA de DOCUMENTA S.A.

- Durante la operativa del PSC:
  - Modificaciones o actualizaciones de cualquiera de los ítems anteriores.
  - solicitudes de certificados o de revocación;
  - documentación para autenticar la identidad del suscriptor;
  - documentación de recepción y aceptación del certificado;
  - todos los certificados y CRL (información de revocación) tanto emitidos o publicados;
  - notificaciones de compromiso de clave privada;
  - registros de auditoría previstas en el punto 5.4.1;
  - otros datos o aplicaciones para verificar el contenido de los archivos;

5.5.2. Periodos de retención para archivos

La CRL y los certificados emitidos de firma digital deberán ser conservados permanentemente para fines de consulta histórica. Las copias de los documentos para identificación del suscriptor, presentados en el momento de la solicitud y de la revocación de certificados, el formulario de solicitud y el Acuerdo de Suscriptores deberán ser conservados, como mínimo, por 10 años, a contar desde la fecha de expiración o revocación del certificado.

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

5.5.3. Protección de archivos

Los eventos de aplicativos están protegidos de forma que nadie, salvo las propias aplicaciones de visualización, con su debido control de accesos, pueda acceder a ellos. Así mismo, la documentación en papel que se genere con motivo de los procedimientos de la PKI, será almacenada de forma segura en las instalaciones DOCUMENTA S.A.

Todos los registros archivados son clasificados y almacenados de acuerdo a los requisitos de seguridad, 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

DOCUMENTA S.A. mantiene procedimientos adecuados de respaldo de archivos (físicos y electrónicos), tanto en el sitio

principal como en el alterno, que aseguran la disponibilidad de los mismos, de acuerdo a un análisis de riesgos determinado por los factores de operación del PSC.

DOCUMENTA S.A. verifica la integridad de esas copias de seguridad, como mínimo, cada 6 (seis) meses.

5.5.5. Requerimientos para sellado de tiempo de registros

Sin estipulaciones

5.5.6. Sistema de recolección de archivo (interno o externo)

Todo el archivado de información se realiza de forma interna a la PKI 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 PKI 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

DOCUMENTA S.A. debe cambiar sus claves de acuerdo con el tiempo de uso y tiempo operacional de los certificados emitidos dentro de la PKI Paraguay, este cambio técnicamente implica la emisión de un nuevo certificado.

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

Nivel de Jerarquía	Tiempo de uso en años	Tiempo operacional en años	Descripción
Certificado de Suscriptores (modulo hardware)	2	2	El certificado emitido al usuario final es otorgado por un tiempo máximo de dos años, al finalizar ese período pierde su validez
Certificado de Suscriptores (modulo software)	1	1	El certificado emitido al usuario final es otorgado por un tiempo máximo de un año, al finalizar ese período pierde su validez
Certificado de PSC DOCUMENTA S.A.	8	10	El Certificado emitido al PSC 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 PSC podrá emitir certificados a usuarios o suscriptores. En los años restantes del tiempo operacional solo podrá firmar la CRL de usuarios o suscriptores.
Certificado CA Raíz	10	20	El Certificado emitido a la CA Raíz 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 CA Raiz podrá emitir certificados a un PSC. En los años restantes del tiempo operacional solo podrá firmar la CRL de PSC.

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

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

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

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

5.7. Recuperación de desastres y compromiso

5.7.1 Procedimiento para el manejo de incidente y compromiso

Los requisitos relacionados a los procedimientos de notificación y de recuperación de desastres, previstos en el Plan de Continuidad del Negocio de la CA de DOCUMENTA S.A. se establecen conforme a lo establecido en el ítem 16 “gestión de incidentes en la seguridad de la información” de la norma ISO 27002/2013, para garantizar la continuidad de sus servicios críticos.

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 PKI 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 de la CA de DOCUMENTA S.A. se describen en el Ítem 5.7.3

5.7.3 Procedimientos de compromiso de clave privada de la Entidad

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

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

5.7.4 Capacidad de continuidad del negocio después de un desastre

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 CA 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.

Los procedimientos de recuperación utilizados por la CA de 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

5.7.5 Actividades de las Autoridades de Registro

Los procedimientos previstos en el Plan de Continuidad del Negocio de las RA vinculadas a la CA de DOCUMENTA S.A. para la recuperación, total o parcial de sus actividades, contiene las siguientes informaciones:

a) Identificación de eventos que pueden causar interrupciones en los procesos del negocio, por ejemplo, falla de equipamientos, inundación e incendios;

b) Identificación y concordancias de todas las responsabilidades y procedimientos de emergencia;

c) Implementación de procedimientos de emergencia que permitan la recuperación y restauración en los plazos necesarios. Se debe prestar especial atención a la evaluación de la recuperación de la documentación almacenada en instalaciones técnicas afectados por el desastre;

d) Documentación de los procesos y procedimientos acordados;

e) Entrenamiento adecuado del personal en los procedimientos y procesos de emergencia definidos, incluido el gerenciamiento de crisis;

f) Prueba y actualización de los planes.

5.8. Extinción de un PSC

La terminación de la CA de DOCUMENTA S.A. o una RA o PSS vinculada a ella puede producirse en los siguientes casos:

- Cuando se extinga el plazo de vigencia del certificado y no se haya solicitado un nuevo certificado.
- En el caso que el PSC finalice sus servicios y por lo tanto, deje de operar.
- Si se hallare comprometida la clave privada de la CA de DOCUMENTA S.A. o se produjera un desastre que ocasionare daños a las instalaciones del mismo que causare la destrucción de la clave privada y su copia de respaldo, el mismo debe solicitar que se revoque su certificado.

En caso que un PSC, deje de operar deberá cumplir con lo siguiente:

- Publicar en su sitio principal de internet la fecha de suspensión de los servicios con al menos 60 días de anticipación.
- 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.
- Notificar a sus suscriptores por lo menos 30 días antes de la suspensión efectiva o cese de sus operaciones.
- Proceder a la eliminación y destrucción de la clave privada mediante un mecanismo que impida su reconstrucción.

En caso que el PSC, 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 CRL. Recién una vez vencidos o revocados todos los certificados emitidos, y cuya revocación esté publicada, cesa automáticamente la responsabilidad del PSC.

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

El MIC a través de la DGFDyCE custodiará toda la información referida al cese de operación del PSC, además publicará el cese de

actividades o finalización del servicio del PSC en su sitio principal de internet.

Asimismo, los certificados que continúen vigentes, podrán ser transferidos a otro prestador de servicios de certificación, previo consentimiento del firmante y por cuenta del prestador de servicios de certificación.

En el caso de que la Autoridad de Registro o un PSS cese en el ejercicio de las funciones, transferirá los registros que mantenga a la CA DOCUMENTA S.A., mientras exista la obligación de mantener archivada la información, y de no ser así, ésta será destruida.

6. CONTROLES TÉCNICOS DE SEGURIDAD

En el ámbito de la presente CPS se especificarán los detalles concernientes a las claves de la autoridad de certificación de DOCUMENTA S.A. Los detalles relativos a las claves de los titulares de los certificados se podrán consultar en la Política de Certificación que corresponda en función del tipo de certificado.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

Los pares de claves para los componentes internos de PKI de DOCUMENTA S.A. se generan en módulos de hardware criptográficos con certificación FIPS 140-2 Nivel 3 que tiene instalados en sus sistemas. Los pares de claves para el resto de titulares se generan en función de lo estipulado en la Política de Certificación aplicable a cada certificado.

Los dispositivos hardware o software a utilizar en la generación de claves para cada tipo de certificado emitido por DOCUMENTA S.A. vienen definidos por la Política de Certificación que le sea de aplicación.

6.1.2. Entrega de la clave privada al suscriptor

No estipulada. La generación y guarda de una clave privada será responsabilidad exclusiva del titular del certificado correspondiente.

6.1.3. Entrega de la clave pública al emisor del certificado

La clave pública de la CA de DOCUMENTA S.A. es entregada a la CA Raíz mediante la entrega de una solicitud de firma de certificado (CSR) en el formato definido en el documento NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.

Todo el proceso de generación de CSR se realiza conforme a los

procedimientos para ello establecidos.

Las claves públicas transferidas deben ser entregadas a través de mecanismos que aseguren su autenticidad e integridad, impidiendo que sean alteradas en el tránsito.

6.1.4. Entrega de la clave pública de la CA a las Partes que confían

La clave pública de la CA de DOCUMENTA S.A. y de la CA Raíz del Paraguay está a disposición de las partes que confían en el Repositorio de DOCUMENTA S.A. (ver apartado 2.1) en el formato establecido en el documento NORMAS DE ALGORITMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY, sin perjuicio de que una CP pueda establecer mecanismos adicionales de entrega de dichas claves.

6.1.5. Tamaño de la clave

El tamaño de las claves de la CA de DOCUMENTA S.A. es de 4096 bits.

El tamaño de las claves para cada tipo de certificado emitido por DOCUMENTA S.A. viene definido por la Política de Certificación que le sea de aplicación.

6.1.6. Generación de parámetros de clave asimétricas y verificación de calidad

Los parámetros de generación de claves asimétricas de la CA de DOCUMENTA S.A. adopta el padrón definido en el documento NORMAS Y ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.

Los parámetros de verificación de calidad, son verificados de acuerdo con las normas establecidas por el patrón definido en el documento NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.

Los parámetros de generación de claves para cada tipo de certificado emitido por la CA de DOCUMENTA S.A. vienen definidos en la Política de Certificación que le sea de aplicación.

Los procedimientos y medios de comprobación de la calidad de los parámetros de generación de claves para cada tipo de certificado emitido por DOCUMENTA S.A. vienen definidos por la Política de Certificación que le sea de aplicación.

6.1.7. Propósitos de usos de clave (campo Key Usage X.509 v3)

La Clave privada de la CA de DOCUMENTA S.A. podrá ser utilizado con el único propósito de:

- firmar los certificados de sus Suscriptores.
- Firmar la CRL correspondiente.
- Firmar peticiones de OCSP.

Los usos admitidos de la clave para cada tipo de certificado emitido por la CA de 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.

6.1.8. Generación de clave por hardware o software

El proceso de generación del par de claves de la CA de DOCUMENTA S.A., es realizado en un módulo criptográfico de hardware que cumple, con el estándar FIPS 140-2 nivel 3.

Cada CP implementada debe caracterizar el proceso utilizado para la generación de claves criptográficas de los titulares de certificados.

6.2. Controles de ingeniería del módulo criptográfico y protección de la clave privada

6.2.1 Estándares y controles del módulo criptográfico

Los módulos utilizados para la creación de claves utilizadas por la CA de DOCUMENTA S.A. cumplen con la certificación FIPS 140-2 de nivel 3.

La puesta en marcha de una Autoridad de Certificación, teniendo en cuenta que se utiliza un módulo Criptográfico de seguridad (HSM), conlleva las siguientes tareas:

- Inicialización del estado del módulo HSM.
- Creación de las claves de los intervinientes.
- Generación de las claves de la CA.

DOCUMENTA S.A. utiliza módulos criptográficos hardware y software disponibles comercialmente desarrollados por terceros.

Cada CP implementada debe especificar los requisitos adicionales aplicables para los módulos de generación de claves criptográficas de los titulares de certificado.

6.2.2. Control multi-persona de clave privada

La clave privada de la CA de DOCUMENTA S.A. se encuentra bajo control multipersona. Ésta se activa mediante la inicialización del software de CA por medio de la combinación mínima de operadores de la CA correspondiente. Éste es el único método de activación de dicha clave privada.

Son necesarios 3 operadores de DOCUMENTA S.A. de un total de 5, para activar y usar la clave privada de dicha CA.

6.2.3. Custodia/recuperación de la clave privada

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

6.2.4. Respaldo/copia de la clave privada

La clave privada de la CA de 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.

Los respaldos de clave privada de la CA de DOCUMENTA S.A. son únicamente para propósitos de recuperación en caso de una contingencia o desastre.

La clave privada de certificado para firma digital del suscriptor no es respaldada por ningún motivo en la CA de DOCUMENTA S.A.

Cualquier entidad titular de certificado, podrá, a su criterio, mantener una copia de su propia clave privada.

Por solicitud del respectivo titular, o empresa u organización, cuando el titular del certificado es su empleado o cliente, el PSC podrá mantener una copia de seguridad de la clave privada correspondiente al certificado de cifrado por ella emitida. Cada CP debe definir los requisitos específicos aplicables.

6.2.5. Archivado de la clave privada

Las claves privadas de los certificados de firma digital nunca serán archivadas para garantizar el no repudio.

En el caso de los certificados de cifrado, las claves podrán ser archivadas, en un nivel de seguridad no inferior a aquella definida para la clave original.

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 de la CA de sólo se puede hacer entre módulos criptográficos (HSM) y requiere de la intervención de personal con rol de confianza autorizado por DOCUMENTA S.A. Cada CP 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

La CA de DOCUMENTA S.A. mantiene almacenada su clave privada original y su copia de seguridad en módulos criptográficos de hardware que cumplen, como mínimo, con el estándar FIPS 140-2 nivel 3.

La CA de DOCUMENTA S.A. no podrá mantener almacenada 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 o cliente, la CA

podrá mantener almacenada una copia de la clave privada correspondiente al certificado de cifrado por ella emitida. Cada CP debe definir los requisitos específicos aplicables.

En cualquier caso, la clave privada deberá ser almacenada cifrada por un algoritmo simétrico definido en el documento NORMAS Y ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.

6.2.8. Método de activación de clave privada

La clave privada de la CA de DOCUMENTA S.A. se activa mediante la inicialización del software de CA por medio de la combinación mínima de operadores de la CA correspondiente. 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 de la CA.

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

6.2.9. Métodos 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 de la CA.

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

6.2.10. Destrucción de clave privada

El procedimiento para la destrucción de las claves privadas de 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 CP implementada debe describir los requisitos y procedimientos necesarios para destrucción de la clave privada de la entidad titular de certificado.

6.2.11. Clasificación del módulo criptográfico

El módulo criptográfico de la CA de DOCUMENTA S.A. cumple minimamente el estándar FIPS 140-2 nivel 3.

Cuando sea el caso, la CP implementada debe describir la

clasificación del módulo criptográfico utilizado por las entidades titulares de los certificados.

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 de la CA de DOCUMENTA S.A., todos los certificados de firma digital emitidas y las CRL 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. Periodo operacional del certificado y periodo de uso del par de claves

Los periodos de uso de la clave son descriptos en la sección 5.6 de la presente CPS.

6.4. Datos de activación

6.4.1 Generación e instalación de los datos de activación

La CA de DOCUMENTA S.A. mantiene estrictos controles en los datos de activación para operar los módulos criptográficos.

Para ello cuenta con datos de activación de múltiples factores para protección de los accesos al uso de claves privadas.

Su activación requiere de un control de múltiples partes (es decir, “m” de “n”) con un valor mínimo de tres para “m”.

Cada CP implementada debe describir la clasificación del módulo criptográfico utilizado por las entidades titulares de los certificados.

6.4.2 Protección de los datos de activación

Sólo el personal autorizado de la CA de DOCUMENTA S.A., posee los dispositivos criptográficas de hardware con capacidad de activación de la CA y conoce los PIN y contraseñas para acceder a los datos de activación.

El método desarrollado por DOCUMENTA S.A. permite a su suscriptor generar por sí solo, y sin intervención de terceros los datos de activación. El suscriptor es responsable de custodiar debidamente los datos de activación.

6.4.3 Otros aspectos de los datos de activación

Los datos de activación de los módulos criptográficos de la CA de DOCUMENTA S.A. son cambiados al menos una vez cada seis meses.

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

Cada computador de la CA de DOCUMENTA S.A. y las RA vinculadas, relacionado directamente con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificado, debe implementar, entre otras, las siguientes características:

a) Control de acceso a los servicios y perfiles de la CA de DOCUMENTA S.A. o RA vinculada;

b) Clara segregación de tareas y atribuciones relacionadas con cada rol de confianza de la CA de DOCUMENTA S.A. o RA vinculada;

c) Uso de criptografía para seguridad de base de datos, cuando sea requerido por la clasificación de su información;

d) Generación y almacenamiento de registros de auditoria de la CA de DOCUMENTA S.A. o RA vinculada;

e) Mecanismos internos de seguridad para garantizar la integridad de datos y procesos críticos; y

f) Mecanismos para copias de seguridad (*backup*).

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

Cualquier equipo o parte del mismo, para ser sometidos a mantenimiento 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 de la CA de DOCUMENTA S.A. o la RA vinculada, el equipo que fue sometido a mantenimiento debe ser inspeccionado. Cualquier equipo que ya no se utilice de forma permanente, deberá ser destruidas de él, de manera definitiva, todas las informaciones sensibles almacenadas, relativas a la actividad del PSC. Todos estos eventos deberán ser registrados con fines de auditoría.

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

Los requisitos específicos aplicables deben ser descriptos en cada CP implementada.

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 portátiles utilizados por la RA vinculadas a la CA de DOCUMENTA S.A. para los procesos de validación y aprobación de certificados cumplen con lo establecido en el documento CARACTERÍSTICAS MINÍMAS DE SEGURIDAD PARA LAS RA DE LA PKI PARAGUAY.

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 PKI de DOCUMENTA S.A.

La CA debe mantener controles que proporcionen una seguridad razonable de las actividades de desarrollo y mantenimiento de los sistemas de la CA.

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.

La CA debe mantener controles sobre el acceso a las bibliotecas fuente de programas.

6.6.2. Controles de gestión de seguridad

La CA de DOCUMENTA S.A y sus RA vinculadas mantienen 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 de los sistemas 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 PKI.

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 producen 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 CRL

Antes de su publicación, todas las CRL generadas por la CA de DOCUMENTA S.A. son comprobadas la consistencia de su contenido, comparándolos con el contenido esperado en relación al número de CRL, la fecha / hora de emisión y otra informaciones relevantes.

6.7. Controles de seguridad de red

6.7.1 Directrices generales

A continuación se decriben los controles relativos a la seguridad de red de la CA de DOCUMENTA S.A., incluidos firewalls y recursos similares.

En los servidores del sistema de certificación de la CA de DOCUMENTA S.A; sólo los servicios estrictamente necesarios para el funcionamiento de la aplicación son 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 la certificación de la CA de DOCUMENTA S.A., son localizados y operan 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 (parches), disponibilizadas por los respectivos fabricantes son implementadas inmediatamente después del testeo en el ambiente de homologación.

El acceso lógico a los elementos de la infraestructura y protección de la red se restringe por medio de un sistema de autenticación y autorización de acceso. Los Routeadores conectados a redes externas implementan 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 implementan en equipos de uso específico, configurados exclusivamente para esa función. Un firewall promueve el aislamiento, en subredes específicas, de los equipos servidores con acceso externo - la denominada "zona

desmilitarizada" (DMZ) - en relación a los equipos con acceso exclusivamente interno al PSC.
El software de firewall, implementa registros de auditoría.

6.7.3 Sistema de Detección de Intruso (IDS)

El sistema de detección de intruso tiene 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 redes, 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 la reconfiguración del firewall.
El sistema de detección de intrusiones deberá ser capaz de reconocer diferentes patrones de ataques, incluso contra el propio sistema, con la posibilidad de actualizar su base de reconocimiento.
El sistema de detección de intruso 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 routeadores, Firewall u IDs- son 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 son documentadas.

6.8. Controles de ingeniería del modulo criptográfico.

El módulo criptográfico de la CA adopta el estándar definido en el documento NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.

7. PERFILES DE CERTIFICADOS, CRL Y OCSP

7.1. Perfil de certificado

El certificado digital de la CA de DOCUMENTA S.A. cumple con:

- ITU-T X.509 V.3 Information technology Open systems interconnection TheDirectory: Public-key and attribute certificate frameworks

A continuación se detalla el contenido de las extensiones más importantes del **Certificado de la CA de DOCUMENTA S. A**:

CAMPO	COMPONENTE PROPUESTO	CRITICA
1. Versión	V3	
2. Signature Algorithm	sha256WithRSAEncryption	
3. Issuer	CN = AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY O = MINISTERIO DE INDUSTRIA Y COMERCIO C = PY	
4. Validez	[10 AÑOS]	
5. Subject	CN = CA-DOCUMENTA S.A. O = DOCUMENTA S.A. C = PY SERIALNUMBER = RUC 80050172-1	
6. Subject Public Key Info	Algoritmo: RSA Encryption Longitud:4096 bits	
7. Certificate Policies **.Policy Identifier** **.URL CPS** **.Notice Referente**	**Se utilizará** Directivas del certificado http://www.acraiz.gov.py/cps/politicas.pdf Certificados emitidos dentro del marco de la PKI Paraguay bajo la jerarquía de su ACRaíz	
8. CRLDistributionPoints	http://www.acraiz.gov.py/arl/ac_raiz_py.crl	NO
9. Auth. Information Access **.CAIssuers** **.OCSP**	**Se utilizará** http://www.acraiz.gov.py/crt/ac_raiz_py_sha256.crt http://www.documenta.py/firmadigital/oscp	NO
10. BasicConstraints	Tipo de asunto=Entidad de certificación (CA) Restricción de longitud de ruta=0	**SI**
11. KeyUsage	Firma de Certificado (Certificate Signing) Firma de CRL (CRL Signing).	**SI**

12. Subject Key Identifier	SHA-1 hash de la clave pública	NO
14. Authority Key Identifier **.KeyIdentifier** **.AuthorityCertIssuer** **.AuthorityCertSerialNumber**	**Se utilizará** SHA-1 hash de la clave pública del emisor **No utilizado** **No utilizado**	NO

7.1.1. Número de versión

La PKI de DOCUMENTA S.A. soporta y utiliza certificados X.509 versión 3 (X.509 v3)

7.1.2. Extensiones del certificado

Las extensiones utilizadas de forma genérica en el certificado de la CA de DOCUMENTA S.A. son:

- KeyUsage. **Calificada como crítica.**
- CertificatePolicies. **Calificada como no crítica.**
- BasicConstraints. **Calificada como crítica.**
- CRLDistributionPoint. **Calificada como no crítica.**
- Authority Key Identifier. **Calificada como no crítica**.
- Subject Key Identifier. **Calificada como no crítica.**

7.1.3. Identificadores de objeto de algoritmos

Identificador de objeto (OID) de algoritmo criptográfico

- sha256WithRSAEncryption (1.2.840.113549.1.1.11).

Identificador de objeto (OID) de clave pública

- RSAEncryption (1.2.840.113549.1.1.1).

7.1.4. Formas del nombre

Los nombres de la CA de DOCUMENTA S.A., referente a la extensión **subject** del certificado, adopta el “Distinguished Name” (DN) del estandar ITU X509 y es la que se describe como ejemplo en la siguiente tabla:

CAMPO	VALOR DE EJEMPLO
CN	CA-DOCUMENTA S.A.
O	DOCUMENTA S.A.
C	PY
SERIALNUMBER	RUC 80050172-1

7.1.5 Restricciones del nombre

Conforme a lo estipulado en cada CP implementada.

7.1.6 Identificador de objeto de política de certificado

Conforme a lo estupado en el Ítem 1.2.

7.1.7 Uso de la extensión Restricciones de Política (Policy Constraints)

No estipulado

7.1.8 Semántica y sintaxis de los Calificadores de Política (Policy Qualifier)

La extensión Certificate Policies contiene los siguientes Policy Qualifiers:

- URL CPS: contiene la URL, la CPS y la CP que rigen el certificado.
- Notice Reference: Nota de texto que se despliega en la pantalla, a instancia de una aplicación o persona, cuando un tercero verifica el certificado.

En el campo NoticeReference se incluirá un texto con información básica sobre el certificado y las políticas a que está sujeto.

7.1.9 Semántica de procesamiento para la extensión de Políticas de Certificado (Certificate Policies)

No estipulado.

7.2. Perfil de la CRL

Las listas de revocación de certificados 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 CRL. Como mínimo es SHA256With RSAEncryption
Emisor (Issuer)	Entidad que emite y firma la CRL.
Fecha efectiva (Effective Date)	Fecha de emisión de la CRL.
Siguiente actualización (NextUpdate)	Fecha para la cual es emitida la siguiente CRL. La frecuencia de emisión del CRL 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 CRL
Identificador de clave de Autoridad (Authority Key Identifier)	Identificador de la clave pública de CA que emite.
Punto de distribución del CRL (Distribuition Points)	Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado

7.2.1. Número (s) de versión

La PKI de DOCUMENTA S.A. soporta y utiliza CRL X.509 versión 2 (v2).

7.2.2. CRL y extensiones de entradas de CRL

7.2.2.1 Número CRL (CRL number)

Orden secuencial de emisión de CRL. Calificada como crítica

7.2.2.2 Identificador de clave de Autoridad

El método para la generación del identificador está basado en la clave pública de la CA de DOCUMENTA S.A. de acuerdo a lo descrito por el RFC 5280. Calificada no como crítica.

7.3. Perfil de OCSP

El servicio de validación de certificados en línea OCSP (Online Certificate Status Protocol) es una forma para obtener información reciente sobre el estado de un certificado. El servicio OCSP que implementa la CA de DOCUMENTA S.A. cumple con lo estipulado en el RFC-2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”.

7.3.1. Número(s) de versión

La PKI de DOCUMENTA S.A. soporta y utiliza mínimamente la versión 1 del RFC 2560.

7.3.2. Extensiones de OCSP

No estipulado.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

El Art. 42 de la Ley Nro. 4017/2010 establece que los PSC, 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 PSC.

Todo PSC está obligado al cumplimiento de las auditorías, éstas permiten establecer una confianza razonable en el marco de la PKI Paraguay. 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, será responsable de ejecutar las auditorias, de acuerdo a lo estipulado en la normativa vigente.

Cada PSC, debe implementar un programa de auditorías internas conforme a lo estipulado en el sistema de auditoria 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

Se llevará a cabo una auditoría externa sobre la PKI de DOCUMENTA S.A. de forma regular al menos una vez al año y los costos serán asumidos por DOCUMENTA S.A. Con ello se garantiza la adecuación de su funcionamiento y operativa con las estipulaciones incluidas en esta CPS y las CP.

DOCUMENTA S.A. realizará una auditoría interna al menos una vez al año.

8.2. Identidad/calidades del evaluador

Todo equipo o persona designada para realizar una auditoría de seguridad sobre la PKI de DOCUMENTA S.A. deberá cumplir los siguientes requisitos:

- Adecuada capacitación y experiencia en tecnología de PKI y criptografía, tecnología de la información y seguridad.
- Independencia a nivel organizativo de la CA de DOCUMENTA S.A.

8.3. Relación del evaluador con la Entidad evaluada

Al margen de la función de auditoría, el auditor externo y la parte

auditada (DOCUMENTA S.A.) no deberán tener relación alguna que pueda derivar en un conflicto de intereses.

Para el caso de las Auditorías internas, el Auditor debe ser independiente funcionalmente del área objeto de evaluación.

8.4. Aspectos cubiertos por la evaluación

La auditoría determinará la adecuación de los servicios de la CA de DOCUMENTA S.A. con esta CPS y las CP aplicables. También determinará los riesgos del incumplimiento de la adecuación con la operativa definida por esos documentos.

El ámbito de actividad de una auditoría incluirá, al menos a:

- Política de seguridad.
- Controles de seguridad física y estándares técnicos de seguridad.
- Evaluación tecnológica:
  - Confidencialidad y calidad de los sistemas de control.
  - Integridad y disponibilidad de los datos.
  - Cumplimiento de los estándares tecnológicos.
  - Administración de los servicios de la CA.
- Seguridad del personal
- Cumplimiento de la Política y Declaración de Prácticas de Certificación.
- Revisión de Contratos.
- Controles administrativos del PSC
- Procesos de certificación de clave pública
- Cumplimiento de la legislación vigente, entre otros.

8.5. Acciones tomadas como resultado de una deficiencia

La identificación de deficiencias detectadas como resultado de la auditoría (interna o externa) dará lugar a la adopción de medidas correctivas. El auditor, será el responsable de la determinación de las mismas.

En caso de detectarse una irregularidad en la Auditoría externa realizada a la CA de DOCUMENTA S.A., podrán tomarse entre otras las siguientes acciones dependiendo de la gravedad de la misma:

- Indicar las irregularidades, pero permitir al PSC que continúe sus operaciones hasta la próxima Auditoría programada
- Permitir al PSC que continúe sus operaciones con un máximo de treinta días corridos, tiempo durante el cual

deberá subsanar la irregularidad detectada, caso contrario se procederá a la Suspensión.

- Suspender la operación de la CA de DOCUMENTA S.A. o sus RA vinculadas.

En caso que se ordene la suspensión de actividades del PSC, solo podrá realizar servicios de soporte técnico y atención a los suscriptores ya existentes, en ningún caso podrá seguir brindando servicios de certificación.

8.6. Comunicación de resultados

El equipo auditor comunicará los resultados de la auditoría a la Autoridad de Aplicación, al Coordinador de Seguridad de DOCUMENTA S.A., así como a gerencia de DOCUMENTA S.A. y de la Autoridad en la que se detecten incidencias.

DOCUMENTA S.A. publicará 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 tarifas de emisión y revocación de cada certificado se especifican en la Política de Certificación que le sea de aplicación.

9.1.2. Tarifas de acceso a certificados

Las tarifas de acceso a los certificados se especifican en la Política de Certificación que les sea de aplicación.

9.1.3. Tarifas de acceso a información del estado o revocación

Las tarifas de acceso a la información de estado o revocación de cada certificado se especifican en la Política de Certificación que le sea de aplicación.

9.1.4. Tarifas por otros servicios

No se aplicará ninguna tarifa por el servicio de información sobre esta CPS, ni las políticas de certificación administradas por la DOCUMENTA S.A., ni por ningún otro servicio adicional del que se tenga conocimiento en el momento de la elaboración del presente documento.

9.1.5. Políticas de reembolso

En el caso de que alguna Política de Certificación especifique alguna tarifa aplicable a la prestación de servicios de certificación o revocación por parte de la CA de DOCUMENTA S.A. para el tipo de certificados que defina, 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

DOCUMENTA S.A. posee suficientes recursos financieros para mantener sus operaciones y ejecutar sus deberes, y es capaz de administrar el riesgo de responsabilidad para los suscriptores y partes que confían.

9.2.3 Cobertura de seguro o garantía para usuarios finales

No estipulado

9.3. Confidencialidad de la información comercial

La clave privada de firma digital de la CA de DOCUMENTA S.A. fue generada y mantenida por la propia CA, que será responsable de mantener su confidencialidad. La divulgación o utilización indebida de la clave privada de firma digital por la CA, será de su entera responsabilidad.

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.

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 de la Autoridad Certificadora de Documenta S.A.
- La información referida a los parámetros de seguridad, control y procedimientos de auditoría.
- Documentaciones que guardan relación con la Solicitud de suscriptores.
- Planes de contingencia y recuperación de desastres.
- Información o documentos que la CA 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

Se considera información pública y por lo tanto accesible por terceros:

- La contenida en la presente Declaración de Prácticas de Certificación.
- La incluida en las Políticas de certificación que le sean de aplicación.
- Los certificados emitidos por la CA de DOCUMENTA S.A.
- La lista de los certificados revocados.
- Las versiones públicas de la PSS
- La conclusion de los informes de auditoría.

9.4. Privacidad de información personal

DOCUMENTA S.A. está obligada a garantizar la protección, la confidencialidad y el debido uso de la información suministrada por los usuarios de los servicios de certificación de conformidad con normativa vigente.

9.4.1. Plan de Privacidad

La CA de DOCUMENTA S.A. y las RA vinculadas a ella, implementan políticas de privacidad de información, de acuerdo con la normativa vigente.

No se puede divulgar o vender información de los suscriptores o información de identificación de éstos.

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 CRL, debe ser tratada como información privada.

9.4.3. Información que no es considerada como privada

El tratamiento de la información que no es considerada como privada, estará sujeto a lo que dispone la normativa vigente al efecto. Únicamente se considera pública la información contenida en el certificado.

9.4.4. Responsabilidad para proteger información privada

La CA de DOCUMENTA S.A. debe asegurar que la información privada no pueda ser comprometida o divulgada a terceras partes.

9.4.5. Notificación y consentimiento para usar información privada

La información privada no puede ser usada sin el consentimiento de las partes. Consentida, la CA de DOCUMENTA S.A. no requiere

notificar a los suscriptores para usar información privada.

9.4.6. Divulgación de acuerdo con un proceso judicial o administrativo

Para divulgar información privada se requiere de una orden judicial que así lo determine y se divulgará estrictamente la información solicitada.

9.4.7 Otras circunstancias de divulgación de información

La información privada podrá ser divulgada en otras circunstancias, siempre que ésta resulte expresamente prevista por la legislación aplicable.

9.5. Derecho de propiedad intelectual

DOCUMENTA S.A. es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta CPS. Se prohíbe por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva de DOCUMENTA S.A. sin la autorización expresa por su parte.

9.6. Representaciones y garantías

9.6.1. Representaciones y garantías del PSC

La CA de DOCUMENTA S.A. es responsable del cumplimiento de sus obligaciones, según se establecen en esta CPS, incluso aunque parte de su actividad sea realizada mediante contratación externa. Asimismo, La CA de DOCUMENTA S.A. proporcionará sus servicios de forma consistente con esta CPS.
La CA de DOCUMENTA S.A. tiene las siguientes obligaciones:

a) operar de acuerdo a su CPS y CP que implementa;
b) generar y gestionar sus pares de claves criptográficas;
c) asegurar la protección de sus claves privadas;
d) notificar a la CA raíz, emisor de su certificado, cuando se presenta el compromiso de su clave privada y solicitar la revocación inmediata del correspondiente certificado;
e) notificar a sus usuarios cuando hay una sospecha de compromiso de su clave privada o una nueva emisión de su par de claves o la terminación de prestación de su servicio;
f) distribuir su propio certificado;
g) emitir, expedir y distribuir los certificados de las RA a ellas vinculadas, y de los usuarios finales;

h) informar la emisión del certificado al respectivo solicitante;

i) revocar los certificados por el emitidos;

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

k) publicar, en su sitio principal internet, su CPS, y las CP aprobadas que implementa;

l) publicar, en su sitio principal de Internet, las informaciones definidas en el ítem 2.2. de este documento;

m) publicar, en su sitio principal internet, las informaciones sobre la desvinculación de una RA, así como la extinción de la instalación técnica.

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

o) identificar y registrar todas las acciones ejecutadas, conformes a las normas, prácticas y reglas establecidas por la Autoridad de Aplicación.

p) adoptar las medidas de seguridad y de control previstas en la CPS, CP y políticas de seguridad (PS) que se implementa, con sujeción a las normas, criterios, prácticas y procedimientos establecidos por la Autoridad de Aplicación.

q) mantener el cumplimiento de sus procesos, procedimientos y actividades con las normas, prácticas y reglas establecidos por la Autoridad de Aplicación y la normativa vigente;

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

s) mantener y anualmente realizar prueba de su Plan de Continuidad de Negocios (PCN);

t) mantener el contrato de seguro de responsabilidad civil resultante de las actividades de certificación digital y de registro, con una cobertura suficiente y compatible con el riesgo de estas actividades.

u) informar a terceras partes 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 t) de este ítem;

v) informar a la CA raíz, mensualmente, la cantidad de certificados digitales emitidos y revocados;

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

9.6.2. Representaciones y garantías de la RA

Las RA vinculadas a la CA de DOCUMENTA S.A. deben cumplir las siguientes obligaciones:

a) recibir las solicitudes de emisión y revocación de los certificados;
b) confirmar la identidad del solicitante y validar la solicitud;
c) comunicar la solicitud de emisión o revocación del certificado a la CA de DOCUMENTA S.A. utilizando un protocolo de comunicación segura, conforme al patrón definido en el documento CARACTERÍSTICAS MÍNIMAS DE SEGURIDAD PARA LAS RA DE LA PKI PARAGUAY.
d) informar a los respectivos titulares la emisión o revocación de sus certificados;
e) proporcionar los certificados emitidos por la CA de DOCUMENTA S.A. a sus respectivos solicitantes;
f) identificar y registrar todas las acciones ejecutadas, conforme a las normas, prácticas y reglas establecidas por le MIC y la normativa vigente;
g) mantener el cumplimiento de sus procesos, procedimientos y actividades con las normas, criterios, prácticas y reglas establecidas por la CA de DOCUMENTA S.A., el MIC y en especial con lo contenido en el documento CARACTERÍSTICAS MÍNIMAS DE SEGURIDAD PARA LAS RA DE LA PKI PARAGUAY;
h) mantener y garantizar la seguridad de la información por ella tratada, de acuerdo a lo establecido en las normas, criterio, prácticas y procedimientos establecidos por el MIC;
i) mantener y anualmente realizar prueba de su Plan de Continuidad de Negocios (PCN);
j) proceder al reconocimiento de las firmas y de la validez de los documentos presentados en la forma de los ítems 3.2.2, 3.2.3 y 3.2.4.
k) garantizar que todas las aprobaciones de la solicitud de certificados sean realizadas en las instalaciones técnicas autorizadas para funcionar como RA.

9.6.3. Representaciones y garantías del suscriptor

Es obligación de los titulares de los certificados emitidos bajo la presente CPS:

- Suministrar información exacta, completa y veraz con relación a los datos que los encargados de su verificación les soliciten para realizar el proceso de registro.
- Informar a los responsables de la CA de DOCUMENTA S.A. de cualquier modificación de esta información.
- Conocer y aceptar las condiciones de utilización de los certificados, en particular las contenidas en esta CPS y en

las CP que sean de aplicación, así como las modificaciones de las mismas.

- Limitar y adecuar el uso del certificado al ámbito estipulado por la Política de Certificación pertinente y la presente CPS.
- Poner el cuidado y medios necesarios para garantizar la custodia de su dispositivo criptográfico, evitando su pérdida, divulgación, modificación o uso no autorizado.
- Es responsabilidad del titular mantener bajo su exclusivo conocimiento el valor de sus datos de activación (PIN, PUK).
- Solicitar inmediatamente la revocación de un certificado en el caso de detección de inexactitudes en la información contenida en el mismo o tener conocimiento o sospecha del compromiso de la clave privada correspondiente a la clave pública contenida en el certificado, entre otras causas por: pérdida, robo, compromiso potencial, conocimiento por terceros del PIN y/o PUK.
- No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica (hardware y software) de los servicios de certificación.
- No transferir ni delegar a un tercero sus responsabilidades sobre un certificado que le haya sido asignado.
- Cualquier otra que se derive de la ley, su reglamentación, de esta CPS o de las Políticas de Certificación.

En el caso de certificado emitido a las personas jurídicas, equipo o aplicación, estas obligaciones se aplican al responsable del uso certificado.

9.6.4. Representaciones y garantías de las partes que confían

Es obligación de las partes que confían en los certificados emitidos por la CA de DOCUEMENTA S.A.:

- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y la Política de Certificación pertinente.
- Verificar la validez de los certificados en el momento de la recepción de los documentos firmados digitalmente mediante la comprobación de que el certificado es válido y no ha caducado o ha sido revocado.
- Asumir su responsabilidad en la verificación de las firmas digitales.
- Asumir su responsabilidad en la comprobación de la

validez y revocación de los certificados que acepta y en que confía.

- Tener conocimiento de las garantías y responsabilidades derivadas de la aceptación de los certificados en los que confía y aceptar sujetarse a las mismas.
- Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.

9.6.5. Representaciones y garantías del Repositorio

El repositorio público de la CA de DOCUMENTA S.A. debe:

- disponibilizar, inmediatamente después de su emisión, los certificados emitidos por la CA y su CRL.
- estar disponible para consulta durante 24 (veinticuatro) horas al día, siete (7) días a la semana; y
- aplicar los recursos necesarios para la seguridad de los datos almacenados en él.

9.6.6. Representaciones y garantías de otros participantes

No estipulado.

9.7. Exención de garantía

La CA de DOCUMENTA S.A. solo responderá en el caso de incumplimiento de las obligaciones contenidas en Ley Nº 4017/2010, Ley Nº 4610/2014, decreto N° 7369/2011, en la presente CPS y en las Políticas de Certificación específicas.

La CA de DOCUMENTA S.A. sólo responderá de los daños y perjuicios causados por el uso indebido del certificado, cuando se haya consignado en él o en su Política de Certificación asociada, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.

La CA de DOCUMENTA S.A. no representa en forma alguna a los usuarios ni a terceras partes aceptantes de los certificados que emite.

La CA de DOCUMENTA S.A. no asume ninguna responsabilidad en caso de cualquier tipo de pérdida o perjuicio:

- De los servicios que presta, en caso de guerra, catástrofes naturales o cualquier otro supuesto de caso fortuito o de fuerza mayor: alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico y/o telefónico, virus informáticos, deficiencias en los servicios de telecomunicaciones o el compromiso de las claves asimétricas derivado de un riesgo tecnológico

imprevisible.

- Ocasionados durante el periodo comprendido entre la solicitud de un certificado y su entrega al usuario.
- Ocasionados durante el periodo comprendido entre la revocación de un certificado y el momento de publicación de la siguiente CRL.
- Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos, la Política de Certificación pertinente y esta CPS.
- Ocasionados por el mal uso de la información contenida en el certificado.
- Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por la CA de DOCUMENTA S.A.
- DOCUMENTA S.A. no asumirá responsabilidad alguna en relación al uso de los Certificados emitidos por su CA y el par de claves privada/pública asociado a sus titulares para cualquier actividad no especificada en la CPS o en las Políticas de Certificación correspondientes.
- DOCUMENTA S.A., como Prestador de Servicios de Certificación, no será responsable del contenido de los documentos electrónicos, ni mensajes de datos firmados con sus certificados ni de cualquier otro uso de sus certificados, como pueden ser procesos de cifrado o comunicaciones.

9.8. Limitaciones de responsabilidad legal

A excepción de lo establecido por las disposiciones de la presente CPS, en la Ley Nº 4017/2010, Ley Nº 4610/2014, su decreto reglamentario Nº 7369/2011, La CA de 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

La CA de 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 CPS. 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.

9.9.1. Indemnizaciones por daños ocasionados por la CA de DOCUMENTA S.A.

Las indemnizaciones que tenga que asumir la CA de DOCUMENTA S.A. por daños efectuados a terceros se hará en base a los términos establecidos en la establecidos en la Ley Nº 4017/2010, Ley Nº 4610/2014, su decreto reglamentario N° 7369/2011 y la presente CPS. La CA de DOCUMENTA S.A. no asume ninguna otra responsabilidad ante titulares de certificados o terceros que confían o acepten los certificados.

9.9.2. Indemnizaciones por los daños ocasionados por los Suscriptores

Tanto suscriptores como terceros son responsables por apoderarse, destruir, modificar, adulterar, indebidamente los datos de una firma o certificado digital durante o después de la fecha de creación del certificado y son sujetos a indemnizaciones por responsabilidad civil y penal según lo determinen los tribunales correspondientes de conformidad con Ley Nº 4017/2010, Ley Nº 4610/2014, su decreto reglamentario N° 7369/2011.

9.9.3. Indemnizaciones por los daños ocasionados por los Terceros que confían

Tanto suscriptores como terceros son responsables por apoderarse, destruir, modificar, adulterar, indebidamente los datos de una firma o certificado digital durante o después de la fecha de creación del certificado y son sujetos a indemnizaciones por responsabilidad civil y penal según lo determinen Ley Nº 4017/2010, Ley Nº 4610/2014, su decreto reglamentario N° 7369/2011.

9.10. Plazo y finalización

9.10.1. Plazo

Esta CPS entra en vigor desde el momento de su publicación en el repositorio de CA de DOCUMENTA S.A. previa aprobación por el MIC.

Esta CPS estará en vigor mientras no se derogue expresamente por la emisión de una nueva versión.

9.10.2. Finalización

Esta CPS será sustituida por una nueva versión con independencia de la trascendencia de los cambios efectuados en la misma, de

forma que siempre será de aplicación en su totalidad.
Cuando la CPS quede derogada se retirará del repositorio público de la CA de DOCUMENTA S.A.

9.10.3. Efectos de la finalización y supervivencia

Las obligaciones y restricciones que establece esta CPS, en referencia a auditorías, información confidencial, obligaciones y responsabilidades de la CA de DOCUMENTA S.A., nacidas bajo su vigencia, subsistirán tras su sustitución o derogación por una nueva versión en todo en lo que no se oponga a ésta.

9.11. Notificación individual y comunicaciones con participantes

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las prácticas descritas en esta CPS 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

La Autoridad con atribuciones para revisar y aprobar cambios sobre la CPS y las PCs de la CA de DOCUMENTA S.A. es la Dirección General de Firma Digital y Comercio Electrónico del MIC.

9.12.2. Procedimiento para publicación y notificación

Toda enmienda o modificación de la presente CPS y las CP implementadas, se publicará en el sitio principal de Internet de la CA.

9.12.3. Circunstancias en que los OID deben ser cambiados

Sin estipulaciones.

9.13. Disposiciones para resolución de disputas

Todas reclamaciones entre usuarios y la CA de DOCUMENTA S.A. deberán ser comunicadas por la parte en disputa a la CA de 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

La presente CPS se adecua a legislación vigente aplicable a la materia.

9.15. Adecuación a la ley aplicable

La responsabilidad del MIC en su calidad de Autoridad de Aplicación es la de velar por el cumplimiento de la legislación aplicable indicada en el apartado anterior.

9.16. Disposiciones varias

9.16.1. Acuerdo completo

Sin estipulaciones.

9.16.2. Asignación

Sin estipulaciones.

9.16.3. Divisibilidad

En el caso de que una o más cláusulas de esta CPS sean o llegasen a ser declaradas inconstitucional por la Corte Suprema de Justicia, el resto de las cláusulas de estas políticas se mantendrán vigentes.

9.16.4. Aplicación (Honorarios de abogados y renuncia de derechos)

Sin estipulaciones.

9.16.5. Fuerza mayor

Los Acuerdos de Suscriptores incluyen cláusulas de fuerza mayor para proteger a la CA de DOCUMENTA S.A.

9.16.6. Resolución por la vía judicial

Los conflictos entre la CA de DOCUMENTA S.A., suscriptores y terceros que surjan como Prestador de Servicios de Certificación se resolverán, una vez agotada la vía gubernativa, ante el tribunal Contencioso- Administrativo correspondiente.

9.17. Otras disposiciones

El PSC habilitado de conformidad a los términos de una CP derogada de la CA Raiz, se adecuará a las disposiciones de la nueva CP en el plazo establecido por la Resolución que la ponga en vigencia.

La CPS Y CPs de la CA de DOCUMENTA S.A. guarda concordancia con las disposiciones establecidas por Autoridad de Aplicación

10. DOCUMENTOS DE REFERENCIA

Los siguientes documentos referenciados son aplicados para la

confección de las políticas de certificación.

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- RFC 3739 “Internet X.509 Public Key Infrastructure Qualified Certificates Profile.
- RFC2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol OCSP”.
- RFC 3647: “Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework”.
- ISO 3166 “Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países.
- Ley Nro. 4017/2010 ‘’De validez jurídica de la firma electrónica, la firma digital, mensaje de datos y el expediente electrónico’’.
- Ley Nro. 4610/2012 que modifica y amplía la Ley Nro. 4017/2010.
- Decreto Reglamentario Nro. 7369/2011.
- CP y CPS de la CA raíz del Paraguay.
- Directivas Obligatorias Para La Formulación Y Elaboración De La Práctica De Certificación De Los Prestadores De Servicios De Certificación (PSC) V1.0
- Directivas Obligatorias Para La Formulación Y Elaboración De La Política De Certificación De Los Prestadores De Servicios De Certificación (PSC) V1.0
- Características Mínimas De Seguridad Para La Autoridades De Registro De La Infraestructura De Claves Públicas Del Paraguay V 1.0
- Normas De Algoritmos Criptográficos PKI-Paraguay V1.0